

Hitachi Content Platform (HCP)

COMPLIANCE ASSESSMENT

SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d)
and the MiFID II Delegated Regulation(72)(1)

Abstract

Hitachi Content Platform (HCP), by Hitachi Vantara, is a scalable object storage solution that provides a secure and efficient way to store, manage, share, and protect unstructured data. HCP offers S3 Object Lock and HCP Retention features, both of which are designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format, when properly configured and applied to each required record.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of HCP (see Section 1.3, *HCP 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);
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d); and
- The European Parliament and the Council of the European Union in Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation), Article 72(1).

It is Cohasset's opinion that HCP, when S3 Object Lock or HCP Retention features are properly configured and applied to each required record, meets the requirements for electronic records set forth in the above Rules.

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.

Table of Contents

Abstract 1

Table of Contents 2

1 • Introduction 3

 1.1 Overview of the Regulatory Requirements 3

 1.2 Purpose and Approach 4

 1.3 HCP Overview and Assessment Scope..... 5

2 • Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)..... 7

 2.1 Record and Audit-Trail 7

 2.2 Non-Rewriteable, Non-Erasable Record Format 8

 2.3 Record Storage Verification 27

 2.4 Capacity to Download and Transfer Records and Location Information 28

 2.5 Record Redundancy 31

 2.6 Audit System 33

3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) 35

4 • Summary Assessment of Compliance with MiFID II Delegated Regulation(72)(1)..... 38

5 • Conclusions 41

Appendix A • Overview of Relevant Electronic Records Requirements 42

 A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) *Electronic Recordkeeping System* Requirements..... 42

 A.2 Overview of FINRA Rule 4511(c) *Electronic Recordkeeping System* Requirements..... 44

 A.3 Overview of CFTC Rule 1.31(c)-(d) *Electronic Regulatory Records* Requirements 45

 A.4 Overview of the *Medium and Retention of Records* Requirements of MiFID II 46

About Cohasset Associates, Inc. 48

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 Hitachi Content Platform (HCP) 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 entities¹, the SEC stipulates recordkeeping requirements, including retention periods.

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

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

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

1.1.2 FINRA Rule 4511(c) Requirements

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

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

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

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

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

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

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

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

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

1.1.4 MiFID II Delegated Regulation(72)(1) Requirements

On January 3, 2018, *Directive 2014/65/EU*⁴, Markets in Financial Instruments Directive II (MiFID II), became effective and established a definition of durable medium for recordkeeping to enable the client to store and access its information. As a supplement to MiFID II, the *Commission Delegated Regulation (EU) 2017/565*⁵ (the *MiFID II Delegated Regulation*), Article 72(1), requires records to be “*retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority*” and specifies the recordkeeping conditions that must be met.

For additional information, refer to Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1)*, and Appendix A.4, *Overview of the Medium and Retention of Records Requirements of MiFID II*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of Hitachi Content Platform (HCP) for preserving required electronic records, Hitachi Vantara 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.

Hitachi Vantara engaged Cohasset to:

- Assess the functionality of HCP, 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 HCP; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*;

⁴ *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.*

⁵ *Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.*

- Associate the requirements of Article 72(1) of the MiFID II Delegated Regulation with the assessed functionality of HCP; see Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1)*; 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 HCP and its functionality or other Hitachi Vantara products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) product demonstrations, including system setup and configuration, (c) system documentation, (d) user and system Administrator guides, and (e) related materials provided by Hitachi Vantara 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 HCP Overview and Assessment Scope

1.3.1 HCP Overview

Hitachi Content Platform (HCP), by Hitachi Vantara, is a scalable object storage solution that provides a secure and efficient way to store, manage, share, and protect unstructured data. HCP offers S3 Object Lock and HCP Retention features, both of which are designed to meet securities industry requirements for preserving objects⁶ in a non-rewriteable, non-erasable format, when properly configured and applied to each required record.

The logical architecture for applying each retention type is depicted in Figure 1:

- **Buckets:** HCP is divided into one or more Buckets (a.k.a. Namespaces), which are unique, logical repositories that contain objects or object versions.
 - Specific configurations, as described in Section 2.2., *Non-Rewriteable, Non-Erasable Record Format*, define the two retention types supported within HCP:

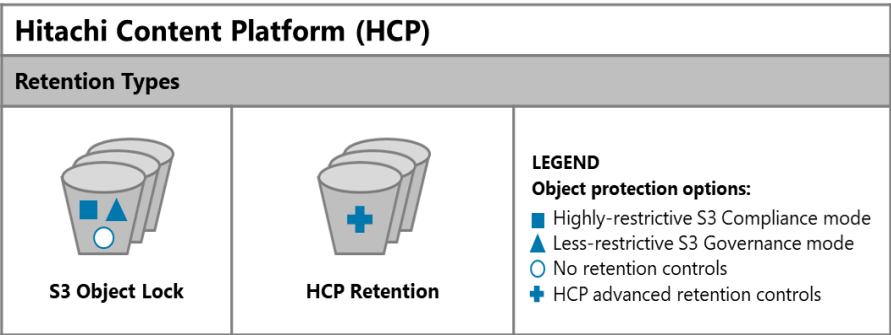


Figure 1: Logical architecture of HCP retention type alternatives

⁶ 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 file, version, or object to recognize that the content may be required for regulatory compliance.

1. **S3 Object Lock** is designed for compatibility with Amazon Simple Storage Service (Amazon S3) APIs⁷ and leverages the **S3 Object Lock** feature for time-based retention controls, legal holds and deletion operations. Accordingly, a single Bucket can retain record versions with *Compliance* mode, *Governance* mode or no retention controls set on the record version.
2. **HCP Retention** supports the use of multiple access protocols, including the Hitachi APIs for Amazon S3⁸, Network File System (NFS), Common Internet File System (CIFS) and HCP object protocols. The HCP Retention feature provides a superset of integrated retention controls for time-based and event-based retention, as well as legal hold and deletion operations. The Retention Mode of *Compliance* or *Governance* is set for the Bucket and automatically applies to all record versions.

To meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format, a Retention Type must be configured for the Bucket and retention controls must be applied to each required record or record version.

1.3.2 Assessment Scope

This assessment is focused specifically on the compliance-related capabilities of HCP, when (a) a Retention Type (i.e., S3 Object Lock or HCP Retention) is properly configured for the Bucket and (b) retention controls are applied to each required record or record version.

For this report, Cohasset assessed HCP when deployed as follows:

1. Fully integrated HCP software, version 9.7, running on a Hitachi-qualified, enterprise-grade turnkey object storage appliance which provides fully integrated logical and physical storage management, administrative and user controls. The Hitachi qualified appliance may use internal disks, flash storage, SAN-attached storage (minimum RAID6⁹ required), or S series storage node appliances which provide erasure code protected storage pools.
2. The HCP Virtual Machine (HCP VM) deployed as a virtualized HCP system in a VMware vSphere® environment or in a Kernel-based Virtual Machine (KVM) environment; both solutions must utilize storage that meets the requirements stipulated in the guides and best practices of VMWare and the storage vendor.

Note: Deploying Hitachi Content Platform in cloud mode or on cloud-tiered storage are outside the scope of this assessment report.

⁷ The S3-compatible APIs (application program interfaces) are designed for compatibility with Amazon Simple Storage Service (Amazon S3) REST APIs, including APIs associated with retention, holds and deletion operations and other features.

⁸ When the HCP Retention type is configured for a Bucket, the Hitachi's S3-compatible APIs are congruent with the feature set of the HCP REST APIs and leverage unique extensions for retention, holds and deletion operations, and other features.

⁹ Redundant Array of Independent Disks (RAID): A method for recording data to magnetic disk devices that provides for various levels of error correction and read or write performance improvements. RAID6 employs striped disks with dual parity and combines four or more disks in a way that provides for correction of detected errors for up to as many as two full disk units of data during read back.

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

This section presents Cohasset's assessment of the functionality of Hitachi Content Platform (HCP), by Hitachi Vantara, for compliance with the electronic recordkeeping system requirements promulgated in SEC Rules 17a-4(f)(2) and 18a-6(e)(2), as well as describes how the solution supports the regulated entity in meeting the audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

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

- **Compliance Requirement** – Excerpt of relevant regulatory requirement in SEC Rules 17a-4(f) and 18a-6(e) and Cohasset's interpretation of the specific requirement
 - ◆ Both SEC Rules 17a-4(f) and 18a-6(e) are addressed in this section, since the electronic recordkeeping system requirements (principles, controls and testable outcomes) are the same, though the Rules specify their respective regulations and regulators and include semantic differences.
- **Compliance Assessment** – Summary statement assessing compliance of HCP
- **HCP 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 HCP, as described in Section 1.3, *HCP 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.*¹⁰ [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.*¹¹ [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed HCP 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 HCP, with the features and controls described in Sections 2.2 through 2.6 of this report.

Reminder: This requirement pertains to the regulated entity's business purpose data processing system (i.e., a trading system), when configured to retain the record and its complete time-stamped audit trail. This requirement is an alternative to the more stringent non-rewriteable, non-erasable record format requirement (i.e., write-once, read-many or WORM requirement), which is assessed in Section 2.2.

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

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

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

¹⁰ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

¹¹ 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.¹² [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.¹³ [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of HCP meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based¹⁴ and event-based¹⁵ retention periods and legal holds, when (a) the retention features are properly configured, (b) retention controls are applied to each required record, as described in Section 2.2.3, and (c) 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 HCP Capabilities

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

2.2.3.1 Overview

► For compliance with this SEC requirement:

- The Bucket in HCP must be configured with one of the mutually exclusive retention types: (1) S3 Object Lock or (2) HCP Retention.

¹² 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

¹³ Electronic Storage of Broker-Dealer Records, Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25283, (May 12, 2003) (2003 Interpretative Release).

¹⁴ Time-based retention periods require records to be retained for a fixed contiguous period of time from the creation or storage timestamp. Time-based retention is supported by both HCP Retention and S3 Object Lock.

¹⁵ 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. Event-based retention is supported by only HCP Retention.

- Retention controls must be applied to each record or record version and set to either:
 - ◆ Highly-restrictive *Compliance* mode, or
 - ◆ Less-restrictive *Governance* mode, which is referred to as *Enterprise* mode when using HCP Retention.
- The following table separately summarizes the highly-restrictive and less-restrictive integrated retention protections when the retention features are properly configured and applied to each required record (or record version). The superset of capabilities supported by HCP Retention are identified. See the subsections following this table, for information on how to configure the retention features and details about the resulting integrated controls.

	Highly-restrictive <i>Compliance</i> mode	Less-restrictive <i>Governance</i> (a.k.a. <i>Enterprise</i>) mode
Protecting record content and immutable metadata	● Overwriting records or modifying the record content and associated system metadata is prohibited. ○ For S3 Object Lock, Versioning must be enabled, which protects the record content and associated system metadata for its lifespan. Attempts to modify or overwrite create a new version, with separate retention controls. ○ For HCP Retention, records and associated system metadata are protected by disabling the write permissions until the record's retention period expires and any Hold is removed (cleared). ▪ Additionally, HCP <u>prohibits</u> the creation of new versions of a record that is under retention (i.e., the applied retention period is <u>not</u> expired) or has a Hold applied. ● Renaming objects and Version IDs is prohibited. ● Renaming a non-empty Bucket or directory (i.e., a folder) is prohibited, when S3-compatible APIs are enabled on the Bucket.	
Restricting changes to retention protections	● <i>Compliance</i> mode <u>cannot</u> be downgraded to <i>Governance</i> mode (for S3 Object Lock) or <i>Enterprise</i> mode (for HCP Retention). ● <i>Compliance</i> mode <u>cannot</u> be removed (cleared) for a record or record version. ● Retention periods applied to a record or a record version <u>cannot</u> be reduced or removed (cleared). ● See Section 2.2.3.3.3, <i>Record Operations and Controls</i>.	● The Retention Mode <u>can</u> be upgraded to <i>Compliance</i> mode. Additionally, the Retention Mode can be removed by administrators with special permissions (e.g., <i>BypassGovernanceRetention</i> or a compliance role). ● Retention periods applied in less-restrictive <i>Governance</i> mode (for S3 Object Lock) or <i>Enterprise</i> mode (for HCP Retention) can be reduced or removed by administrators with special permissions (e.g., <i>BypassGovernanceRetention</i> or a compliance role). ● <u>Note</u>: Procedural controls and monitoring are required to scrutinize administrator actions and ensure compliant retention protections are <u>not</u> circumvented. ● See Section 2.2.3.3.3, <i>Record Operations and Controls</i>.
Applying and removing Holds	● For S3 Object Lock, a Legal Hold may be separately applied to each record version with or without retention controls. When applied to a record version, the Hold prohibits deletion until the Hold is removed (cleared). ● For HCP Retention, the term Hold refers to both Legal Holds and Labeled Holds, which are two separate features. A Hold may be applied to records with or without retention controls. When applied to a record, the Hold prohibits deletion of the record and its versions until the Hold is removed (cleared). ● See Section 2.2.3.4, <i>Holds</i>.	
Restricting deletion of Buckets and records	● Records and record versions with <i>Compliance</i> mode retention controls can only be deleted when eligible. Administrators with special permissions <u>cannot</u> circumvent retention controls.	● Administrators with special permissions <u>can</u> circumvent retention controls and prematurely delete records and record versions. ● <u>Note</u>: Procedural controls and monitoring are required to scrutinize administrator actions and ensure compliant retention protections are <u>not</u> circumvented.

	Highly-restrictive <i>Compliance</i> mode	Less-restrictive <i>Governance</i> (a.k.a. Enterprise) mode
	• Additionally, a Delete Marker may be inserted to hide a record and its versions, when Versioning is enabled for a Bucket. Removing the Delete Marker reinstates the record and its versions. • Only empty Buckets can be deleted. • See Section 2.2.3.5, <i>Deletion Controls</i>.	

2.2.3.2 Bucket Configurations

- ▶ For compliance with this SEC requirement, the Bucket in HCP must be configured with one of the mutually exclusive retention types: (1) S3 Object Lock or (2) HCP Retention.
 - S3 Object Lock is designed for compatibility with Amazon S3 Object Lock.
 - HCP Retention supports a superset of capabilities.
- ▶ The specific Bucket (a.k.a. Namespace) configurations for each Retention Type are separately described in the following table. Since HCP Retention supports a superset of capabilities, its additional configurations are explained. This side-by-side arrangement facilitates comparison of these mutually exclusive features. Also, see Section 2.2.3.3, *Record Definition and Controls*, for details on retention controls, holds and deletion associated with these Bucket configurations.

	S3 Object Lock Bucket Configurations	HCP Retention Bucket Configurations
Bucket name	• Objects or object versions (i.e., records or record versions) are stored in a Bucket. • The Bucket name must be unique within the Tenant.	
Bucket Retention Type	• S3 Object Lock must be enabled as the Retention Type, which allows S3 Object Lock retention controls to be applied to record versions, for compliance with the Rules. • Once enabled, S3 Object Lock <u>cannot</u> be disabled.	• HCP Retention must be enabled as the Retention Type, which allows HCP Retention controls to be applied to records and record versions, for compliance with the Rules. • Once enabled, HCP Retention <u>cannot</u> be disabled. • Also see the row entitled <u>Default Retention Mode</u>, which must be configured.
Protocols	• The S3-compatible protocol <u>must</u> be enabled. • <u>Note</u>: NFS, CIFS, and HCP Object protocols are <u>disallowed</u>. • Access Control Lists (ACLs) may be enabled.	• The S3-compatible protocol <u>may</u> be enabled. • NFS, CIFS, and HCP Object protocols may be enabled. • ACLs may be enabled.
Versioning	• Versioning is <u>mandatory</u>: it must be enabled and <u>cannot</u> be disabled or suspended. • Each version has separately applied retention and Hold protections. ○ A new version can be stored at any time, with its separate retention and Hold protections. ○ An existing version can be deleted, if eligible. (See Section 2.2.3.5, <i>Deletion Controls</i>.)	• Versioning is <u>optional</u>. However, Versioning is <u>disallowed</u> for Buckets with NFS, CIFS, WebDAV, or SMTP protocols. • Acceptable Versioning statuses are: ○ No explicit Versioning status (if Versioning on the Bucket has never been enabled or disabled) ○ Enabled ○ Disabled ○ Suspended (if Versioning was disabled after having been enabled) • When the record is either under retention (i.e., the applied retention period is <u>not</u> expired) or subject to a Hold, the creation of a new version is prohibited.

COMPLIANCE ASSESSMENT REPORT

Hitachi Content Platform (HCP): SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation(72)(1)

	S3 Object Lock Bucket Configurations	HCP Retention Bucket Configurations
Overwrite	• N/A. This is an extended feature for HCP Retention. • S3 Object Lock requires Versioning to be enabled, and the setting for the Overwrite feature is <u>disregarded</u>.	• If Versioning is disabled, the Overwrite feature <u>can</u> be enabled. • If the Overwrite feature is enabled, only records that are <u>not</u> under retention and are <u>not</u> subject to a Hold can be overwritten by a new version.
Version Pruning	• When Versioning is enabled, <u>optionally</u>, set Version Pruning to automatically prune (delete) eligible versions that are older than a specified duration of time. • <u>Important Note</u>: To be eligible for pruning, the version must be <u>both</u> (a) eligible for deletion (considering retention settings and Holds) and (b) older than the duration of time specified for Version Pruning. ◦ With S3 Object Lock, retention settings and Legal Holds are applied to each version, separately. ◦ With HCP Retention, retention settings apply separately to each version and Holds are applied only to the current (top) version, which automatically protects all versions of the record.	
Delete Markers	• The Delete Markers feature is <u>mandatory</u>; it must be enabled and <u>cannot</u> be disabled. • See Section 2.2.3.5, <i>Deletion Controls</i>, for a description of Delete Marker behavior.	• The Delete Markers feature is <u>optional</u>. Versioning is a prerequisite to enabling Delete Markers. • Once enabled, the Delete Markers feature <u>cannot</u> be disabled. • See Section 2.2.3.5, <i>Deletion Controls</i>, for a description of Delete Marker behavior.
Default Retention Mode	• During Bucket creation the Default Retention toggle is disabled and can be enabled. • When enabled, a <u>Default Retention Mode</u> must be configured as either: ◦ <i>Compliance</i> mode, which is highly-restrictive or ◦ <i>Governance</i> mode, which is less-restrictive and requires procedural controls and monitoring to scrutinize <i>BypassGovernanceRetention</i> actions taken to override retention protections or prematurely delete record versions. • Default Retention Mode and Default Retention Period (see next row) are a <u>pair</u> of configurations; requiring both or neither to be set. These <u>defaults</u> apply during storage/write operations to <u>new</u> record versions, when retention controls are <u>not</u> transmitted with the record version. See Section 2.2.3.3.1, <i>Applying S3 Object Lock Retention</i>. • Authorized administrators may change or remove (clear) these default configurations at any time, since the defaults only apply to record versions stored in the future and do <u>not</u> affect previously stored record versions.	• Configuring a <u>Default Retention Mode</u> is <u>mandatory</u> and must be set to either: ◦ <i>Compliance</i> mode, which is highly-restrictive or ◦ <i>Enterprise</i> mode, which is less-restrictive and requires procedural controls and monitoring to scrutinize Privileged Delete actions taken to prematurely delete records. • The Default Retention Mode automatically applies to all records in the Bucket. • After setting the Default Retention Mode: ◦ <i>Compliance</i> mode <u>cannot</u> be downgraded to <i>Enterprise</i> mode and <u>cannot</u> be removed (cleared). ◦ <i>Enterprise</i> mode <u>can</u> be upgraded to <i>Compliance</i> mode, and thereafter, highly-restrictive <i>Compliance</i> mode retention controls apply to records in the Bucket that are under retention.

	S3 Object Lock Bucket Configurations	HCP Retention Bucket Configurations
Default Retention Period	- The Default Retention toggle can be enabled or disabled. When enabled, a <u>Default Retention Period</u> must be configured and is specified in days or years, with a maximum of 100 years. - Default Retention Mode (see row above) and Default Retention Period are a pair of configurations, requiring both or neither to be set. Authorized administrators may change or remove (clear) these default configurations at any time, since the defaults only apply to record versions stored in the future and do <u>not</u> affect previously stored record versions. - These <u>defaults</u> apply during storage/write operations to <u>new</u> record versions, when retention controls are <u>not</u> transmitted with the record version. See Section 2.2.3.3.1, <i>Applying S3 Object Lock Retention</i>. - The Default Retention Period is added to the record version's creation/storage timestamp to calculate a <i>Retain Until Date</i> (a datetime value) which is stored as an attribute of the record version. - Therefore, setting appropriate default configurations when the Bucket is empty and maintaining appropriate configurations assures retention controls are applied to all records stored in the Bucket.	- Initially, the Default Retention Period is <i>Deletion Allowed</i> (zero). - Authorized administrators may change this default at any time, since the default only applies to records stored in the future and does <u>not</u> affect previously stored records. Valid Default Retention Periods include: Offset (i.e., duration of time) in years, months, and/or days that is added to the object creation timestamp to calculate the object's retention period. Retention Class, which applies the <i>Retention Class</i> to an object (for additional details, see next Row entitled <i>Retention Classes</i>). Deletion Allowed (zero), which indicates that no Default Retention Period is applied to the object. Deletion Prohibited (minus 1), which specifies that the object <u>cannot</u> be deleted, except by a Privileged Delete, if the Bucket is in <i>Enterprise</i> mode. Initial Unspecified (minus 2), is designed for use with event-based retention and specifies that the object <u>cannot</u> be deleted, except by a Privileged Delete and Privileged Purge. Fixed Future Date, which assigns the same explicit retention timestamp to each object. <u>Caution:</u> If the fixed date is in the past, the Bucket's Default Retention Period reverts to <i>Deletion Allowed</i>, which is <u>not</u> compliant with the Rules, since it allows objects to be deleted at any time. - The Default Retention Period applies during storage/write operations to <u>new</u> records when the retention period is <u>not</u> transmitted with the record. See Section 2.2.3.3.2, <i>Applying HCP Retention</i>. - Therefore, setting an appropriate Default Retention Period when the Bucket is empty and maintaining appropriate configurations assures retention controls are applied to all records stored in the Bucket.

COMPLIANCE ASSESSMENT REPORT

Hitachi Content Platform (HCP): SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation(72)(1)

	S3 Object Lock Bucket Configurations	HCP Retention Bucket Configurations					
Retention Classes	N/A. This is an extended feature for HCP Retention. S3-compatible Object Lock does <u>not</u> utilize <i>Retention Classes</i> or the other special retention settings.	<i>Retention Classes</i> are optional and may be configured and applied to a Bucket for use as the retention setting for an object. - The <i>Retention Class</i> retention periods are the same as the Default Retention Periods:<table><tr><td> Offset </td></tr><tr><td> Deletion Allowed (zero) </td></tr><tr><td> Deletion Prohibited (minus 1) </td></tr><tr><td> Initial Unspecified (minus 2) </td></tr><tr><td> Fixed Future Date </td></tr></table> - Only certain modifications can be made to <i>Retention Classes</i>: - When the Bucket is set to <i>Compliance</i> mode, the offset can be extended (but not reduced). Further the <i>Retention Class</i> <u>cannot</u> be deleted. - When the Bucket is set to <i>Enterprise</i> mode, the offset can be changed (extended or reduced). Further the Retention Class can be deleted.	Offset	Deletion Allowed (zero)	Deletion Prohibited (minus 1)	Initial Unspecified (minus 2)	Fixed Future Date
Offset							
Deletion Allowed (zero)							
Deletion Prohibited (minus 1)							
Initial Unspecified (minus 2)							
Fixed Future Date							
Minimum Retention After Initial Unspecified	N/A. This is an extended feature for HCP Retention. S3-compatible Object Lock does <u>not</u> support <i>Initial Unspecified</i> or the other special retention settings.	- The <i>Minimum Retention After Initial Unspecified</i> is optional and sets a guardrail to validate the Offset period that the source system sets when removing the object's <i>Initial Unspecified</i> (minus 2) value. <u>Note</u>: <i>Initial Unspecified</i> (minus 2) value is designed for <u>event-based</u> retention periods. When the event occurs, the <i>Initial Unspecified</i> (minus 2) value is changed to the final (post-event) retention period, which should represent the fixed portion of an event-based retention period. Setting a <i>Minimum Retention After Initial Unspecified</i> ensures the final (post-event) retention period meets this guardrail.					
Retention atime (last access time) Synchronization	N/A. This is an extended feature for HCP Retention. S3-compatible Object Lock does <u>not</u> support atime synching to set or maintain a record's <i>Retain Until Date</i>.	- The atime synchronization feature is optional and can be enabled or disabled, at any time. - When enabled, atime values are automatically synchronized with retention settings for subsequently added records, except that: - The atime value of a record is set to the time the record is stored when: - The record is added through NFS with an initial retention setting of <i>Deletion Allowed</i>. - The record is added through any protocol with an initial retention setting that is either <i>Initial Unspecified</i> or a <i>Retention Class</i>. - The atime value is <u>not</u> updated if the new value would reduce the retention period, i.e., the atime cannot be used to reduce a retention period once assigned to a record.					

	S3 Object Lock Bucket Configurations	HCP Retention Bucket Configurations
Annotations and Custom Metadata	N/A. Configurations are <u>not</u> required for custom metadata (property/value pairs), which HCP stores as annotations named .metapairs.	- Bucket configurations for annotations include: - Allow annotations to be added, replaced, and deleted for records under retention. - Allow annotations to be added for records under retention (and disallow replacing and deleting annotations). This is the default. - Disallow all annotations operations (adding, replacing and deleting annotations) for records under retention.
Disposition	- Disposition may be enabled on a Bucket at any time. - Disposition automatically deletes the current (top) version of a versioned object, when eligible because it is no longer under retention and is not subject to a Hold. <u>Note</u>: Disposition does not delete old versions.	
Multipart Uploads	- For cloud-optimized Buckets, the multipart uploads feature can be enabled. - Multipart upload is the process of creating a record by dividing the record data into parts and individually uploading the parts. The result is a single record that behaves the same as records stored using a single PUT record request.	

2.2.3.3 Record Definition and Controls

- Each version of a record is separately managed and is comprised of four elements:
 1. The complete **content** of the record (e.g., document, image, video, or database image).
 2. **System metadata** including:
 - ◆ *Immutable metadata*, e.g., unique Record Object Name and Version ID, record creation/storage timestamp, object size and cryptographic hash value.
 - ◆ *Mutable metadata*, e.g., policies (e.g., retention, number of replicas or duplicates for data protection policies and Holds) that influence how transactions and internal processes affect the record.
 3. Optional **custom metadata** (a.k.a. *annotations*), which can be defined by the regulated entity.
 4. Simple object **Access Control Lists (ACLs)**, which define user permissions for various operations.
- The following two subsections separately describe the methods of initially applying and later modifying retention protections applied to records and record versions:
 - Section 2.2.3.3.1, *Applying S3 Object Lock Retention*
 - Section 2.2.3.3.2, *Applying HCP Retention*
- Additionally, Section 2.2.3.3.3, *Record Operations and Controls*, compares the retention protections derived from S3 Object Lock and HCP Retention.

2.2.3.3.1 Applying S3 Object Lock Retention

- When using S3 Object Lock for compliance with the non-rewriteable, non-erasable requirement of the Rules, a record requiring time-based retention must (1) be stored in a Bucket that is properly configured with S3

Object Lock and (2) have appropriate retention controls applied to required record versions. This subsection addresses methods of initially applying and subsequently modifying a record version's retention settings.

- ▶ The Bucket's Versioning configuration must be enabled, and separate retention controls and optional Legal Hold attributes must be explicitly applied to each record version. As a result, a single Bucket may store separate records with (a) retention controls in *Compliance* mode, (b) retention controls in *Governance* mode, and (c) no retention controls.
 - Additionally, the Legal Hold attribute may be applied to records, independent of retention controls. See 2.2.3.4, *Holds*, for additional information.
- ▶ The following table summarizes the retention controls (Retention Mode and the *Retain Until Date*) applied during the storage process, based on (a) the retention attributes transmitted with the record version (columns with orange highlighted headings) and (b) the *Object Lock* default retention settings configured for the Bucket (columns with blue highlighted headings).

Transmitted Retention Mode	Transmitted Retain Until Date	Record Version's Retention Controls if Bucket has <u>no</u> default retention settings	Record Version's Retention Controls if Bucket <u>has</u> default retention settings
Null	MM/DD/YYYY	• Error returned, write operation fails because <u>both</u> retention attributes were not transmitted	
Null	Null	• Record version is stored <u>without</u> retention controls	• Record version is set to the Bucket's <u>Default Retention Mode</u> (<i>Compliance</i> or <i>Governance</i>) and <i>Retain Until Date</i> is record version's creation/storage date + Bucket's <u>Default Retention Period</u>
<i>Governance</i>	MM/DD/YYYY	• Record version is set to <i>Governance</i> mode and <i>Retain Until Date</i> is MM/DD/YYYY	
<i>Governance</i>	Null	• Error returned, write operation fails because <u>both</u> retention attributes were not transmitted	
<i>Compliance</i>	MM/DD/YYYY	• Record version is set to <i>Compliance</i> mode and <i>Retain Until Date</i> is MM/DD/YYYY	
<i>Compliance</i>	Null	• Error returned, write operation fails because <u>both</u> retention attributes were not transmitted	

- ▶ In addition to applying retention controls during record creation/storage, explicit retention controls may be applied to existing record versions, as described in the following table.
 - If the Version ID is explicitly identified, the updated retention attributes apply to the explicit record version, and if the Version ID is not explicitly identified, the updated retention attributes apply to the current (top) version.
 - Retention attributes cannot be applied to a Delete Marker. Attempts to set retention attributes on a Delete Marker will fail.
 - Changes to the retention attributes do not generate a new version and do not affect the record version's creation/storage (last modified) timestamp.
 - The Retention Mode and *Retain Until Date* must be submitted as a pair. If only one attribute is transmitted, the operation fails. For this reason, only pairs are depicted in the following table.

COMPLIANCE ASSESSMENT REPORT

Hitachi Content Platform (HCP): SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation(72)(1)

Current Retention Mode	Transmitted Retention Mode	Transmitted Retain Until Date	Modifications to the object version retention attributes
Null	Governance	MM/DD/YYYY	Object version is set to <i>Governance</i> mode and <i>Retain Until Date</i> is MM/DD/YYYY.
Null	Compliance	MM/DD/YYYY	Object version is set to <i>Compliance</i> mode and <i>Retain Until Date</i> is MM/DD/YYYY.
Governance	Null	Null	Retention controls are removed (cleared) when <i>BypassGovernanceRetention</i> is used.
Governance	Governance	MM/DD/YYYY	- If the <i>Retain Until Date</i> is being extended, the operation succeeds. - If the <i>Retain Until Date</i> is being reduced, the operation succeeds when <i>BypassGovernanceRetention</i> is used.
Governance	Compliance	MM/DD/YYYY	- If the <i>Retain Until Date</i> is being extended, the operation succeeds, and the record version's mode is set to <i>Compliance</i>. - If the <i>Retain Until Date</i> is being reduced, the operation succeeds when <i>BypassGovernanceRetention</i> is used.
Compliance	Null	Null	The operation fails; <i>Compliance</i> mode retention controls <u>cannot</u> be removed (cleared).
Compliance	Governance	MM/DD/YYYY	The operation fails; <i>Compliance</i> mode retention controls cannot be changed to less-restrictive <i>Governance</i> mode.
Compliance	Compliance	MM/DD/YYYY	- If the <i>Retain Until Date</i> is being extended, the operation succeeds. - If the <i>Retain Until Date</i> is being reduced, the operation fails because <i>Compliance</i> mode retention controls cannot be made less restrictive (cannot be reduced).

2.2.3.3.2 Applying HCP Retention

- ▶ When using HCP Retention for compliance with the non-rewriteable, non-erasable requirement of the Rules, a record requiring time-based or event-based retention must (1) be stored in a Bucket that is properly configured with HCP Retention and (2) have appropriate retention controls applied to required records. This subsection addresses methods of initially applying and subsequently modifying a record's retention period.
- ▶ A Retention Mode of highly-restrictive *Compliance* or less-restrictive *Enterprise* mode must be configured for the Bucket and automatically applies to all record versions stored in the Bucket.
- ▶ Holds may be applied to records, independent of retention controls. If the record has versions, when a Hold is applied to the current (top) version of the record, the Hold automatically protects all of its versions, and the creation of a new version is prohibited. See 2.2.3.4, *Holds*, for additional information.
- ▶ A retention period is applied to a record using one of the following four methods. If the record has versions, (a) the retention period applies to the record and its versions and (b) the creation of new versions is prohibited.
 1. A **Default Retention Period** is configured for a Bucket and is automatically applied to each record that is transmitted without a specific retention period.
 2. A **Retention Class** is applied to a record either when it is (a) inherited from the Bucket's default retention settings or (b) is explicitly transmitted by the source system, as metadata for the record. When a *Retention Class* transmitted by the source system does not match one of the defined *Retention Classes* for the specified Bucket, the record is rejected and handled as an error condition.
 3. The **atime (last access time) is synchronized** as the retention period (Retain Until Date). When a Bucket is configured to synchronize retention with a file system, any updates to the atime on one storage

solution are synchronized on the other storage solution, as long as the update is allowed. For example, a retention period cannot be reduced.

4. Explicit retention period may be transmitted (a) when storing the record or (b) to update the retention period for an existing record.

- ◆ When storing a new record or setting retention for an existing record that is not under retention, any retention period (past or present) can be specified. If the retention period is in the past (is expired), the record is immediately eligible for deletion, if no Holds are applied.
- ◆ The *Retention Class* applied to a record can be replaced with a different *Retention Class* that has a longer retention period. However, the existing *Retention Class* cannot be replaced with an explicit retention setting, such as *Deletion Prohibited* or a *Fixed Future Date*.
- ◆ An explicit *Fixed Future Date* applied to a record may be replaced with a date that is further in the future but cannot be set to an earlier date.
- ◆ The constraints for special retention periods are enumerated in the following table. Changing the retention period to *Deletion Allowed* (zero) essentially removes the record's retention period.

<i>Deletion Allowed</i> (zero or minus zero)	● Allows the record to be deleted at any time. ● This value can be assigned to a record when (a) it is being added to the Bucket or (b) when the record's existing retention period is <i>Initial Unspecified</i> (minus 2). ● The value of minus zero is equivalent to zero.
<i>Deletion Prohibited</i> (minus 1)	● Prevents the record from being deleted, except by a Privileged Delete, when the Bucket is in <i>Enterprise</i> mode. ● Prevents the record's retention setting from being changed or removed (cleared). ● This value can be assigned, at any time, to a record that is <u>not</u> in a <i>Retention Class</i>. ● Note: If a record is assigned to a <i>Retention Class</i> that is subsequently deleted, the retention setting for affected records is automatically changed to <i>Deletion Prohibited</i> (minus 1).
<i>Initial Unspecified</i> (minus 2)	● Specifies that the record does <u>not</u> yet have a retention setting. ○ Note: Setting the <i>Minimum Retention After Initial Unspecified</i> to an appropriate duration ensures the record is kept at least as long as the specified minimum time. ▪ When the Bucket is in <i>Compliance</i> mode, the value of <i>Minimum Retention After Initial Unspecified</i> can be increased but cannot be reduced and cannot be removed (cleared). ▪ When the Bucket is in <i>Enterprise</i> mode, <i>Minimum Retention After Initial Unspecified</i> value can be changed to any value. ● Prevents creation of a new version. ● Prevents the record from being deleted, except by a Privileged Delete, when the Bucket is in <i>Enterprise</i> mode. ● This value can be assigned to a record when (a) it is being added to the Bucket or (b) when a record's retention period is being changed from <i>Deletion Allowed</i> (zero or minus zero) to <i>Initial Unspecified</i> (minus 2). ● Note: If a record is assigned to a retention setting of <i>Initial Unspecified</i> (minus 2): ○ If the <i>Minimum Retention After Initial Unspecified</i> is <u>not</u> set, the record's retention can be changed to any retention setting. ○ If the <i>Minimum Retention After Initial Unspecified</i> <u>is</u> set, changes to the record's retention setting must adhere to this <i>Minimum Retention After Initial Unspecified</i> value.

<i>Datetime</i>	- Prevents the record from being deleted until the specified <i>Datetime</i> (<i>Retain Until Date</i>), except by a Privileged Delete, when the Bucket is in <i>Enterprise</i> mode. - This value can be assigned to a record that is <u>not</u> assigned to a <i>Retention Class</i>, if the specified <i>Datetime</i> (<i>Retain Until Date</i>) is later than the current retention setting for the record. <u>Note</u>: If a record is assigned to a retention setting of <i>Deletion Prohibited</i> (minus 1), it <u>cannot</u> be changed to a specified <i>Datetime</i> (<i>Retain Until Date</i>).
<i>Offset</i>	- Specifies to retain the record for a duration of time (a retention <i>Offset</i>) from one of the following values: - The time the record was added to the Bucket - The current retention setting for the record - The current time - Prevents the record from being deleted until the <u>calculated</u> retain until date, except by a Privileged Delete, when the Bucket is in <i>Enterprise</i> mode. - This value can be assigned to a record when (a) it is being added to the Bucket or (b) when a record's retention period is being changed from <i>Deletion Allowed</i> (zero or minus zero) to a retention <i>Offset</i>, as long as the record is <u>not</u> assigned to a <i>Retention Class</i>. <u>Note</u>: If a record is assigned to a retention setting of <i>Deletion Prohibited</i> (minus 1), it <u>cannot</u> be changed to a retention <i>Offset</i>.

- For records requiring event-based retention, a retention period of *Initial Unspecified* (minus 2) should be applied when the record is first stored. This *Initial Unspecified* retention period protects a record for an indefinite period of time, until a triggering event occurs.
- When the triggering event occurs, the source system replaces the *Initial Unspecified* (minus 2) retention setting with an *Offset* that is specified in years, months, and/or days, which is validated against the *Minimum Retention After Initial Unspecified* guardrail defined for the Bucket. The record will be retained for the greater of (a) the *Offset* retention period transmitted by the source system or (b) the value of the *Minimum Retention After Initial Unspecified* guardrail.

2.2.3.3.3 [Record Operations and Controls](#)

The following table separately describes the integrated controls applied to records by (a) S3 Object Lock and (b) HCP Retention. This side-by-side arrangement facilitates comparison of these mutually exclusive features. Distinctions are made when the integrated controls are different for highly-restrictive *Compliance* mode and less-restrictive *Governance* (a.k.a. *Enterprise*) mode.

	S3 Object Lock Controls	HCP Retention Controls
Managing versions, protecting record content and immutable metadata	- Versioning is <u>mandatory</u>, which prohibits overwriting or modifying the record content and associated system metadata for its lifespan. - Updates to the contents of the record or its immutable metadata results in storing a new record version with a unique Version ID. - Retention controls and Holds are applied <u>separately</u> to each record version. <u>Note</u>: The Overwrite feature is <u>not</u> relevant to Buckets with S3 Object Lock enabled. Since	- For records that are under retention (i.e., the applied retention period is <u>not</u> expired) or subject to one or more Holds (i.e., Legal Hold and/or Labeled Hold), all write permissions are disabled for the content of the record, its versions, and associated system metadata. Therefore: - The content <u>cannot</u> be modified or overwritten. - A new version <u>cannot</u> be stored. <u>Note</u>: When multiple versions exist, the same retention period and Holds apply to all versions.

COMPLIANCE ASSESSMENT REPORT

Hitachi Content Platform (HCP): SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation(72)(1)

	S3 Object Lock Controls	HCP Retention Controls
	Versioning must be enabled for S3 Object Lock, the Overwrite feature <u>cannot</u> be enabled.	- For records that are <u>not</u> under retention and are <u>not</u> subject to a Legal Hold or Labeled Hold: - If Versioning is <u>Enabled</u>, modifications to the record or its system metadata are stored as a new version, with a unique Version ID. - If Versioning is <u>Disabled</u> or <u>Suspended</u>: - If the Overwrite feature is <u>enabled</u>, modifications to the record or its system metadata overwrite the current (top) version. - If the Overwrite feature is <u>disabled</u>, the attempt to overwrite the record is <u>rejected</u>.
Protecting immutable metadata	- Immutable system metadata (e.g., unique Record Object Name and Version ID, object create/storage timestamp, object size and cryptographic hash value) is protected inherently for each record version. - Renaming a non-empty Bucket or directory (i.e., a folder) is prohibited, when S3-compatible APIs are enabled on the Bucket.	
Restricting changes to retention settings	- S3 Object Lock <u>cannot</u> be disabled for a Bucket, after having been enabled. - After applying highly-restrictive Compliance mode retention on a record version, the mode <u>cannot</u> be downgraded to <i>Governance</i> or removed (cleared). Also, each record version's <i>Retain Until Date</i> <u>cannot</u> be reduced, but can be extended, at any time. - After applying less-restrictive Governance mode retention on a record version, the mode <u>can</u> be upgraded to <i>Compliance</i> and the <i>Retain Until Date</i> applied to a record <u>can</u> be extended, at any time. - Users with <i>BypassGovernanceRetention</i> privileges can (a) reduce a record version's <i>Retain Until Date</i>, (b) remove a record version's retention controls, or (c) delete a record before expiration of its <i>Retain Until Date</i>. See Section 2.2.3.5, <i>Deletion Controls</i>.	- The retention period for a record <u>cannot</u> be modified if a Legal Hold or Labeled Hold applies to the record. Therefore, the following information on modifying retention controls only applies to records that do <u>not</u> have an applied Hold. - After setting a Bucket to highly-restrictive Compliance mode, it <u>cannot</u> be downgraded to <i>Enterprise</i> mode and the Retention Mode <u>cannot</u> be removed (cleared). Modifications to Retention Classes associated with a Bucket in <i>Compliance</i> mode can result <u>only</u> in <u>extending</u> the retention period. <i>Retention Classes</i> <u>cannot</u> be deleted. - The retention period applied to a record <u>cannot</u> be reduced. - After setting a Bucket to less-restrictive Enterprise mode, it <u>can</u> be upgraded to <i>Compliance</i> mode. Modifications to Retention Classes associated with a Bucket in <i>Enterprise</i> mode can result in <u>either extending or reducing</u> the retention period. <i>Retention Classes</i> <u>can</u> be deleted. This automatically changes the retention setting for affected records to <i>Deletion Prohibited</i> (minus 1). - The retention period applied to a record can be reduced by administrators with special permissions (e.g., a compliance role). - Users with Privileged Delete permissions can delete a record before its retention period expires. See Section 2.2.3.5, <i>Deletion Controls</i>.
Managing event-based retention settings	N/A. This is an extended feature for HCP Retention. S3-compatible Object Lock does <u>not</u> support event-based retention.	HCP Retention supports event-based retention periods; see Section 2.2.3.3.2, <i>Applying HCP Retention</i>, for an explanation of how to manage event-based retention settings.

COMPLIANCE ASSESSMENT REPORT

Hitachi Content Platform (HCP): SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation(72)(1)

	S3 Object Lock Controls	HCP Retention Controls
Applying and removing legal holds	While a Hold is applied to a record version, it <u>cannot</u> be deleted, by any means, even if the retention period is expired.	- When a Hold is applied to a record: - Creation of a new record version is <u>prohibited</u>. - Changes to the content and retention settings of the record and any versions are <u>prohibited</u>. - Deletion of the record and its versions is <u>prohibited</u>, even if its retention period has expired.
	- After all Holds are removed (cleared) from the record, deletion eligibility is based on the retention controls; see Section 2.2.3.4, <i>Deletion Controls</i>. - Holds may be applied to records with or without retention settings. - See Section 2.2.3.4, <i>Holds</i>, for additional information.	
Restricting deletion of records	- After applying highly-restrictive Compliance mode, deletion of a specific record version is <u>prohibited</u> until its <i>Retain Until Date</i> is expired and any Hold is removed (cleared). - Accordingly, highly-restrictive Compliance mode assures retention protections <u>cannot</u> be circumvented by any user or process. - After applying less-restrictive Governance mode: - Standard users are <u>prohibited</u> from deleting a specific record version until its <i>Retain Until Date</i> expires and any Hold is removed (cleared) from the version. - Users with <i>BypassGovernanceRetention</i> permissions may delete a specific record version before its <i>Retain Until Date</i> is expired. However, when a Hold applies, the record version <u>cannot</u> be deleted using <i>BypassGovernanceRetention</i>. - Accordingly, less-restrictive Governance mode requires procedural controls and monitoring to scrutinize <i>BypassGovernanceRetention</i> actions. - Deletion of the record (without identifying the Version ID) appends a Delete Marker, as the current (top) version, and all existing record versions remain unmodifiable and are stored as the version history. - Removing the Delete Marker reinstates the original versions.	- For Buckets in highly-restrictive Compliance mode, deletion is <u>prohibited</u> until the record version's retention period is expired and any Holds are removed (cleared) from the record. - Accordingly, highly-restrictive Compliance mode assures retention protections <u>cannot</u> be circumvented by any user or process. - For Buckets in less-restrictive Enterprise mode: - Standard users are <u>prohibited</u> from deleting a specific record version until the applied retention expires and any Holds are removed (cleared) from the record. - Users with <i>Privileged Delete</i> or <i>Privileged Purge</i> permissions may delete or purge record versions that are under retention (i.e., the applied retention period is <u>not</u> expired). However, when a Hold applies, delete and purge actions are <u>prohibited</u>. - Accordingly, less-restrictive Enterprise mode requires procedural controls and monitoring to scrutinize these <i>Privileged</i> actions. - When Versioning is <u>enabled</u>: - A Delete Marker or Delete Record is created as the current (top) version and the deleted records are retained in version history. - Removing the Delete Marker or restoring a specific Version ID reinstates an original version.
	See Section 2.2.3.5, <i>Deletion Controls</i>, for information on HCP's deletion operations including (a) delete, (b) purge, (c) Privileged Delete and Privileged Purge, (d) disposition, and (e) version pruning.	
Restricting Bucket deletion	A Bucket <u>cannot</u> be deleted unless it is empty. Accordingly, retention settings cannot be circumvented by deleting a non-empty Bucket.	
Copying records	- A record may be copied to a different Bucket. - The creation/storage timestamp of the copy reflects the timestamp when the copy is stored in the destination Bucket (<u>not</u> the timestamp when the record was originally stored in the source Bucket). - Retention settings and Holds attribute must be separately applied to the new copy, in accordance with the configurations of the Bucket where the new copy is stored. - Buckets <u>cannot</u> be copied.	

	S3 Object Lock Controls	HCP Retention Controls
Moving records	- Records <u>cannot</u> be moved to another Bucket. - Buckets <u>cannot</u> be moved to a different Tenant.	
Multipart Uploads	- For cloud-optimized Buckets, multipart uploads can be performed, if the feature is enabled. Multipart upload is the process of creating a record by dividing the record data into parts and individually uploading the parts. The result is a single record that behaves the same as records stored using a single PUT record request. - The retention controls and Holds (as described above) may be applied to the record after the upload is marked as complete.	
Changing Permissions	Access control lists (ACLs) may be modified and modifications do <u>not</u> create a new version, however, ACLs may not be deleted.	

2.2.3.4 Holds

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

The following table separately describes the integrated controls associated with (a) Hold¹⁶ features for Buckets configured with S3 Object Lock and (b) Hold¹⁷ features for Buckets configured with HCP Retention. This side-by-side arrangement facilitates comparison of these mutually exclusive features.

	Hold features for S3 Object Lock	Hold features for HCP Retention
Legal Holds	- A Legal Hold can be applied to any record version in a Bucket with S3 Object Lock enabled, whether or not the record version has retention settings. - Legal Holds must be applied separately to each record version relevant to the Legal Hold. - If no version is specified, the Legal Hold is applied to the current (top) version; and, if the current (top) version is a Delete Marker, the Legal Hold attribute is <u>not</u> updated. - See the last row of this table for a description of the restrictions resulting from the Legal Hold. - A Legal Hold can be removed (cleared) from the record version when it is no longer relevant, thereafter the retention settings are honored.	- A Legal Hold (a.k.a., a single Hold) can be applied to any record in a Bucket with HCP Retention configured, whether or not the record has retention settings. - Once set, it applies to the record and its versions. - See the last row of this table for a description of the restrictions resulting from the Legal Hold. - The Legal Hold can be removed (cleared) from the record, after which the record's Labeled Holds and retention settings are honored. - Clearing the Legal Hold automatically removes (clears) it from the record and its versions.
Labeled Holds	N/A. This is an extended feature for HCP Retention. S3-compatible Object Lock does <u>not</u> support Labeled Holds.	- A Labeled Hold is a named Hold that has a unique identifier. - A Labeled Hold can be applied to multiple records in a Bucket with HCP Retention configured, whether or not the record has retention settings.

¹⁶ For S3 Object Lock, the term Hold refers to the Legal Hold attribute, which may be set (Yes) or cleared (No) for a record version.

¹⁷ For HCP Retention, the term Hold refers to both Legal Holds (a.k.a., single holds) and Labeled Holds which may be applied to records.

	Hold features for S3 Object Lock	Hold features for HCP Retention
		- Once set, it applies to the record and its versions. - See the last row of this table for a description of the restrictions resulting from the Labeled Hold. - A Labeled Hold can be removed (cleared) from the record when it is no longer relevant, after which the Legal Holds and retention settings are honored. - Clearing the Labeled Hold automatically removes (clears) it from the record and its versions.
Combination of Legal Holds and Labeled Holds	N/A. This is an extended feature for HCP Retention. S3-compatible Object Lock does <u>not</u> support Labeled Holds.	A record can have a Legal Hold and up to 100 Labeled Holds at the same time. These Hold settings are independent of one another and apply to the record and its versions.
Restrictions effectuated by a Hold	- When a Legal Hold is applied to a record version, Deletion of the record version is <u>prohibited</u>. - Deletion of the record version by users with <u>BypassGovernanceRetention</u> permissions are also <u>prohibited</u>. <u>Note</u>: Custom metadata may be updated, if the Bucket is configured to allow changes to custom metadata for records under retention.	- When a Legal Hold and/or a Labeled Hold is applied to a record, the Hold applies automatically to the record's versions: - New versions <u>cannot</u> be created. - Retention settings <u>cannot</u> be changed. - Deletion, including <u>Privileged Delete</u> and <u>Privileged Purge</u> actions, are <u>prohibited</u> for the record and its versions. <u>Note</u>: Custom metadata may be updated, if the Bucket is configured to allow changes to custom metadata for records under retention.

2.2.3.5 Deletion Controls

The following table separately describes the delete actions for (a) S3 Object Lock and (b) HCP Retention. This side-by-side arrangement facilitates comparison of these mutually exclusive features. Distinctions are made when the integrated controls are different for highly-restrictive *Compliance* mode and less-restrictive *Governance* (a.k.a. *Enterprise*) mode.

	S3 Object Lock Controls	HCP Retention Controls
Deletion eligibility	- The <i>Retain Until Date</i> and Legal Hold attribute are separately stored for each record version. - The record version is eligible for deletion by a standard user requires both: - The version's <i>Retain Until Date</i> has expired and - The version's Legal Hold attribute is removed (cleared). - Additionally, see the row entitled <i>Special delete features</i> for the <i>BypassGovernanceRetention</i> feature.	- A record's retention period and Hold(s) apply to the record and its versions. The scope of the deletion action – whether it deletes just the object, the object together with its version history, or only specific versions – depends on the specific deletion operation being performed. - Eligibility for deletion by a standard user requires: - Expiration of the applied retention period (i.e., the record is no longer under retention), and - Legal Holds and Labeled Holds are removed (cleared) from the record, thereby clearing the Hold for all versions. - Additionally, see the row entitled <i>Special delete features</i> for Privileged features.

COMPLIANCE ASSESSMENT REPORT

Hitachi Content Platform (HCP): SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation(72)(1)

	S3 Object Lock Controls	HCP Retention Controls
Deleting a record	- When the Version ID <u>is</u> specified, a delete action taken by a standard user is successful when it is eligible for deletion, which requires both: - The version's explicitly stored <i>Retain Until Date</i> is in the past and - The version's explicitly stored Legal Hold attribute is removed (cleared). Otherwise, the delete action is rejected. - When the Version ID is <u>not</u> specified, an action to delete a <u>record</u> (regardless of the status of the retention and Holds), appends a Delete Marker as the current (top) version. - Delete Markers can be removed (cleared) by specifying the Version ID of the Delete Marker, which results in reinstating or recovering the deleted record versions.	- When Versioning is <u>disabled</u>, a delete action taken by a standard user is successful when it is eligible for deletion, which requires both: - The record is no longer under retention (i.e., the applied retention period is expired), and - Holds are removed (cleared) from the record. Otherwise, the delete action is rejected. - When Versioning is <u>enabled</u>: - The deleted record is retained in version history. - A Delete Marker or Delete Record is created as the current (top) version. - A version in the version history can be reinstated as the current (top) version by removing the Delete Marker or restoring a specific Version ID. - The scope of the delete actions – whether it deletes (a) the record only, (b) the record together with its version history, or (c) specific versions – depends on the specific delete operation being performed, as described in the next table.
Disposition (Automated deletion)	- The Disposition feature can be set to automatically delete the current (top) version of a record, when the following conditions are met: - It is <u>not</u> under retention (retention has expired), - Holds are removed (cleared), and - The current (top) version is <u>not</u> a Delete Marker.	- The Disposition feature can be set to automatically delete the current (top) version of a record, when it is <u>not</u> under retention (retention has expired) and Holds are removed (cleared). - If the record is in an HCP <i>Retention Class</i>, the class must have Automatic Deletion (Disposition) enabled. Note: Records with <i>Deletion Prohibited</i> (minus 1) or <i>Initial Unspecified</i> (minus 2) retention settings are <u>not</u> automatically deleted.
Privileged delete	If the record version has Governance mode, users with <i>BypassGovernanceRetention</i> permissions can delete a record version <u>before</u> the applied retention period has expired, if <u>no</u> Holds are applied to the record.	If the Bucket has Enterprise mode, users with Privileged permissions can delete a record (Privileged Delete) <u>before</u> the record's retention period has expired, if <u>no</u> Holds are applied to the record.
Purging of records	N/A. This is an extended feature for HCP Retention. The Purging records feature does <u>not</u> apply to S3-compatible Object Lock.	Users with Delete and Purge permissions may run the Purge (HTTP Delete) operation to permanently purge all versions of the record, if the current (top) version is no longer under retention and is <u>not</u> subject to a Hold.
Privileged Purging of records	N/A. This is an extended feature for HCP Retention. Privileged Purge features do <u>not</u> apply to S3-compatible Object Lock.	Users with Delete, Purge and Privileged permissions may run the Privileged Purge (Delete) operation to permanently purge all versions of the record, whether the current (top) version is under retention or not, provided that no Holds are applied to the record and the retention is applied in Enterprise mode.
Version Pruning	- Version Pruning may be enabled to automatically delete version history that is older than a specified duration of time. Important Note: Version Pruning does <u>not</u> delete versions if either (a) the record is under retention or (b) a Hold is applied. Version Pruning also does <u>not</u> delete the current (top) version of a record.	

	S3 Object Lock Controls	HCP Retention Controls
Secure Deletion (Shredding)	- Secure Deletion (Shredding) overwrites storage during deletion operations to prevent reconstruction of the record data or metadata, including custom metadata. - When configured, Secure Deletion (Shredding) applies to all deletion operations including (a) delete, (b) purge, (c) Privileged Delete and Privileged Purge, (d) disposition, and (e) version pruning. - A default Secure Deletion (Shredding) can be set for the Bucket, and when configured, it automatically applies to objects stored after the default is enabled. - Additionally, Secure Deletion may be explicitly specified for a record. Important Note: Once Secure Deletion (Shredding) is set for a record, it <u>cannot</u> be removed (cleared).	
Deleting Tenants and Bucket	- A Tenant <u>cannot</u> be deleted through any mechanism, if it contains one or more Buckets with (a) S3 Object Lock enabled or (b) HCP Retention in <i>Compliance</i> mode. - A Bucket <u>cannot</u> be deleted unless it is empty.	

2.2.3.6 Security

In addition to the stringent retention protection and management controls described above, which include Object Access Control Lists to manage simple per object access permissions, HCP provides the following security capabilities, which support the authenticity and reliability of the records.

- ▶ HCP interfaces with customized operating systems. To enhance security:
 - All unused modules and extensions should be removed, and
 - Security hardening should be updated regularly.
- ▶ Role-Based Access Control (RBAC), set at both system and tenant levels, provide the means to constrain access to functionality for administrators and users.
- ▶ HCP relies on embedded firewall technology to lock down access ports not specifically needed for core software functionality (i.e., access to root/shell requires use of SSH keys). Each Node runs its own firewall to block all ports not associated with an active HCP service.
 - Additionally, HCP may be configured to restrict administrative tasks to an isolated Virtual Local Area Network (VLAN) or to a specific network port physically isolated on a management network.
- ▶ Encryption of records is available as follows:
 - Hypertext transport-layer encryption (HTTPS) and Transport Layer Security (TLS) are available to protect data in transit.
 - HCP offers fully-managed AES encryption of objects and metadata while at rest. The encryption key is generated during system installation and stored internally, distributed across several storage nodes. No external key management is required.
 - HCP supports Key Management Interoperability Protocol (KMIP) for encryption of stored data.
- ▶ HCP can be configured either (a) to require secure HTTPS in the URL request or (b) to accept both HTTP and HTTPS in the URL request.

2.2.3.7 Clock Management

- ▶ To protect against the possibility of premature deletion of records that could result from accelerating the system time clock, [time synchronization settings](#) must be configured:
 - The HCP system must be configured in Time Compliance Mode to disallow changes to time settings.
 - Every HCP system clock that is controlling a Bucket with S3 Object Lock or HCP Retention enabled, including all systems within a replication topology, must be configured with Chrony, which is a versatile implementation of the Network Time Protocol (NTP).
 - ◆ A minimum of three external time servers is recommended by Hitachi Vantara.
 - ◆ Once configured and synchronized with NTP clocks, the system clock is automatically checked against the external time source and resynchronized as required. This constant synchronization prevents, or immediately corrects, any inadvertent or intentional administrative modifications to a system time clock that could result in the premature deletion of 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 Buckets that will be utilized to store SEC-regulated books and records with S3 Object Lock or HCP Retention features.
- ▶ Applying appropriate retention controls to each required record version. Cohasset recommends these controls be applied within 24 hours of storing the record.
 - Cohasset recommends configuring appropriate Default Retention settings for Buckets that will store records required for compliance with SEC Rules. These defaults assure that record versions are stored with retention controls.
 - Note: The *Deletion Allowed* retention period does not comply with the Rules, since it allows the object to be deleted at any time.
- ▶ Using HCP Retention for records requiring event-based¹⁸ retention periods since S3 Object Lock does not support event-based (conditional) retention periods; and setting a *Minimum Retention After Initial Unspecified* governing value for event-based retention to ensure any future retention period exceeds the minimum value and appropriately managing event-based retention attributes.
- ▶ Limiting the creation and management of Delete Markers. Specifically, Cohasset recommends always specifying the Version ID with delete actions.
- ▶ Applying Holds to records that require preservation for legal matters, government investigations, external audits and other similar circumstances, and removing the Holds when the applicable action is completed.

¹⁸ 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.

- ▶ Setting appropriate security controls, such as: (1) restricting network ports and protocol access, (2) establishing roles-based access, (3) encrypting data in transit and at rest, and (4) requiring secure HTTPS in the URL request.
- ▶ Synchronizing HCP system clocks with an external time source and disallowing changes to the time settings through the HCP Console to prevent tampering that could result in the premature deletion of records.
- ▶ Disallowing cloud-only and cloud-tiered storage (e.g., Amazon S3, Google Cloud Storage, Microsoft Azure) for the official or replica of the records, since retention controls are not currently extended to the cloud storage environment. Note: Tiering to the cloud is allowed to facilitate access, but the cloud copy cannot be utilized for compliance purposes.

Additionally, the regulated entity is responsible for (a) authorizing user privileges and (b) maintaining appropriate technology, encryption keys, and other information and services needed to retain the records.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

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 affirms that the functionality of HCP meets this SEC requirement for complete and accurate recording of records and post-recording verification processes, when properly configured as described in Section 2.3.3 and the considerations identified in Section 2.3.4 are satisfied.

2.3.3 HCP Capabilities

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

2.3.3.1 Recording Process

- ▶ A combination of checks and balances in the advanced magnetic recording technology (such as inter-component and inter-step cyclical redundancy checks (CRCs), as well as write-error detection and correction) are relied upon to assure that the records are written in a high-quality and accurate manner.
- ▶ Fibre Channel arrays are included as part of the Hitachi Virtual Storage Platform and incorporate RAID6 (dual path, dual controllers) or [Dynamic Drive Protection](#) for advanced data protection.
- ▶ A combination of replication and other redundancy features, such as erasure coding, are configuration options to protect records and record metadata; see Section 2.5, *Record Redundancy*.

- ▶ HCP S3-compatible API requests are protected with hash-based message authentication code (HMAC), known as signature version 4. The code protects both the record (object data) and its metadata from manipulation. HCP software rejects object writes with an invalid signature.
- ▶ Object uploads, using HCP S3-compatible APIs, support an entity tag (ETag) which protects the record (object data or data part) with a cryptographic hash. HCP software rejects object writes if the ETag does not match the content.
- ▶ HCP allows the source system to transmit a cryptographic hash to validate transmission. Upon receipt, HCP recalculates the hash value and either (a) writes the record only if the hash values match or (b) returns the hash value to the source system for validation that HCP received and stored the record correctly.
 - The cryptographic hash value is stored as metadata for each record and subsequently uses the hash value for post-recording, periodic quality and integrity checks and for automated record repair.
- ▶ Bucket storage quotas are verified prior to storing records. Should insufficient space exist, the write operation is rejected, and an error notification is issued.

2.3.3.2 Post-Recording Verification Process

- ▶ During retrieval of a record, HCP recalculates the hash value for the record and compares it to the hash value calculated at the time of recording. If the hash values are not equal, HCP attempts to recover the record from a local copy or replica. If the recovery methods are unsuccessful, HCP sends an error message to the source system and logs the event for a system Administrator to analyze and correct.
- ▶ To validate continued data integrity, HCP content verification service regularly and frequently scans data at rest to verify that recalculated hash values match stored values. In the event the hash values do not match, HCP automatically initiates the repair, or restoration of the object from a replica.

2.3.4 Additional Considerations

- ▶ The source system is responsible for transmitting the complete contents of the required records and HCP validates the accuracy of the recording process.
- ▶ Cohasset recommends that the integrity of each record transmitted from the source system to HCP be validated, whereby the source system will calculate a hash value of the record and metadata and compare that computed value to the one returned to the source by HCP at the conclusion of the write process. This process allows the source system to determine if HCP correctly received and stored the record.

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

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]

- Reasonably usable electronic format that is compatible with commonly used systems for accessing and reading electronic records.

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

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

2.4.2 Compliance Assessment

It is Cohasset's opinion that the functionality of HCP meets this SEC requirement to maintain capacity to readily download and transfer the records and information used to locate the records, when (a) properly configured, as described in Section 2.4.3, and (b) the considerations described in Section 2.4.4 are satisfied.

2.4.3 HCP Capabilities

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

► [HCP S3-compatible APIs](#) include:

- List records and record metadata:
 - ◆ GET Bucket (List Objects) Version 2 (ListObjectsV2) returns a list of some or all (groups of 1,000) objects in a Bucket. Request parameters can be used as selection criteria, such as matching a partial key prefix, to return a subset of the objects in a Bucket. If the most recent version is a Delete Marker the record object is not returned in the list.
 - ◆ GET Bucket Object Versions returns a list of the record versions in a Bucket. This can return the metadata of all versions of all objects in a Bucket, including Delete Markers. This is particularly useful for versioned Buckets to manage, retrieve, or restore previous versions of an object.
 - ◆ HCP maintains a directory structure and lists the full path of the object.
 - Retrieve records in a Bucket, using the *GET Object* command:
 - ◆ When the request includes the Version ID, the specific record version is returned.
 - ◆ When the request excludes the Version ID, the most recent version is returned, unless the most recent version is a Delete Marker, in which case an error code (i.e., 404 Not Found) is returned.
 - Download selected record objects and the associated metadata (index) attributes to a designated storage location. When multiple versions of a record are stored, the top-level version is returned, by default. The specific Version ID must be specified in the search and download requests.
- The [HCP Search Console](#) is a web application, which utilizes a *metadata query engine* to query Bucket contents. (Note: The query engine is also available for use separately by the metadata query API.)
- Searching must be enabled for the System, Tenant and Bucket, which causes the query engine to create and maintain an index of objects contained within a Bucket. Standard indexing includes system metadata, custom metadata, and ACLs.

- ◆ **Note:** Only indexed objects are returned as part of the search results. Objects that are not indexed may still be retrieved through other means.
- Content *classes* may be defined for a Bucket, as well as specific content *properties* (named constructs within custom metadata), to provide enhanced search capabilities.
- Authorized users may perform three types of searches from the HCP search console:
 - ◆ **Simple search:** Provides Boolean search of object names, document titles, and email subject lines.
 - ◆ **Structured search:** Allows for more advanced searches against metadata, content classes and properties.
 - ◆ **Advanced search:** Enables combining search criteria and operators to further refine search results.
- A list of objects matching the search criteria is returned; the object itself is not returned. Users may further filter the search results, open any of the listed objects to see content, or export the list as a comma-separated-values (CSV) or XML file. The exported file will include either the object URL alone or the URL and record metadata, depending on the search performed.
- ▶ The HCP metadata query API supports two types of queries to search for objects that meet specified criteria:
 1. Object-based queries search only for objects currently in the repository. Only the current version can be returned for objects with multiple versions.
 - ◆ Search for objects using the object (a) system metadata, (b) custom metadata, (c) ACLs and (d) location (i.e., the Bucket and/or directory that contains the object). The robust query language allows search criteria to be combined.
 2. Operation-based queries search for both (a) objects currently in the repository and (b) information about objects that have been deleted. For Buckets that support Versioning, both the current (top) version and prior versions records can be returned.
 - ◆ Criteria for operation-based queries can include object status (for example, created or deleted), change time, index setting, and location.
- ▶ The HCP Namespace Browser may be used to (1) list directories within the Bucket, (2) view a list of all objects contained within a directory including metadata, such as record name, storage date, and retention attributes, and (3) view and/or retrieve objects.
 - HCP can download objects and subsequently open it in the default application (if available) or provides a prompt to select a compatible software application or save the object. Additionally, the HCP search console can be launched from the HCP browser to facilitate more advanced searches.
- ▶ Industry Standard Protocols, such as (a) HCP S3-compatible APIs, (b) NFS, (c) CIFS, and (d) HCP Object protocols may be used, in lieu of the HCP Search Console or HCP Namespace Browser, to programmatically search for and export selected records.
- ▶ Once the records have been retrieved, local tools may be used to view, reproduce or transfer the records to a medium acceptable under the Rules.
- ▶ In addition, Hitachi Content Intelligence (HCI) is a separate data discovery and transformation product that may be used to execute HCP content searches.

- Hitachi Content Intelligence (HCI) Extracts is capable of extracting a variety of disparate structured, semi-structured and unstructured content from both Hitachi and third-party repositories, whether located on-premises or in the cloud.
- Leveraging advanced workflow capabilities, HCI allows the regulated entity to specify data sources and create conditional search filters that when applied, streamline the content that is returned to a central user interface.
 - ◆ Content displayed on the user interface can be customized for individual users or groups and via configurable Access Control Lists (ACLs), access to sensitive content may be restricted.
 - ◆ Previews of certain content, such as images or videos, can be embedded along with content metadata.
 - ◆ Data can be extracted from search results to create new indexes to facilitate future searches.
 - ◆ New tags or custom metadata can be added or appended to content.
- From the search results user interface, selected content may be viewed, exported to another system, or downloaded to a medium acceptable under the Rules.
- Additionally, HCI is an extensible solution, built on an open-core architecture, allowing developers to integrate search and workflow capabilities with other services or systems via RESTful APIs.
- Download selected record objects and the associated metadata (index) attributes to a designated storage location. When multiple versions of a record are stored, the top-level version is returned, by default. The specific Version ID must be specified in the search and download requests.

2.4.4 Additional Considerations

The regulated entity is responsible for: (a) authorizing user privileges, (b) maintaining appropriate technology and resource capacity, Hitachi Vantara licenses, encryption keys, and other information and services needed to use HCP to readily access, download, and transfer the records and the information needed to locate the records, and (c) 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.¹⁹ [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.²⁰ [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 affirms that the functionality of HCP 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 (a) properly configured as described in Section 2.5.3 and (b) the considerations described in Section 2.5.4 are satisfied.

2.5.3 HCP Capabilities

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

2.5.3.1 Redundant Set of Records

- ▶ To meet this requirement to separately store a persistent redundant copy of the records, HCP can be set up in a replication topology, typically in separate geographic locations. Each system in the replication topology must be set up with an equivalently configured Bucket (see Section 2.2.3.2, *Bucket Configurations*), where a duplicate of each record and associated metadata can be asynchronously recorded.
 - User and group accounts, *Retention Classes*, content classes, compliance log messages, and most other tenant log messages are replicated. However, changes to the retention settings and record deletion may not automatically propagate to the replica.
 - The Data Protection Level (DPL) of a Bucket can be set to at least two (2) duplicates (up to four duplicates are allowed). Each duplicate is recorded on a separate local storage node, thereby improving the accessibility, preservation and recovery of at least one of the duplicates should one of the storage nodes not be available. Should one record be in error or not be available, the record can be accessed from the duplicate. The record in error can then be restored from the duplicate. HCP automatically generates duplicates, as defined for the Bucket, to ensure that the required number of duplicates is maintained.

¹⁹ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

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

- Should one Bucket become inaccessible, the record can then be retrieved from a duplicate stored on another system. A record found in error on one HCP Compliance Mode system can be restored from a replica.
- ▶ Additionally, two (2) copies of metadata are stored using RAID6 to provide reliable metadata recovery.

2.5.3.2 Other Redundancy Capabilities

- ▶ For cloud-optimized Buckets, erasure coding protection options can be configured:
 - Hitachi S-series node using 20+6 erasure coding, which requires purpose-built hardware with dual path and dual controller configurations.
 - Geographically Erasure Coded (Geo-EC) volumes configured to distribute data across multiple geographically dispersed clusters using erasure coding schemes, such as 1+1, 2+1, 3+1, 4+1, and 5+1, which specifies the number of data blocks and parity blocks used.
- ▶ The erasure coded data segments are retained for the full retention period and any applied Legal Holds, which assures that a replica can be accurately regenerated from the erasure coded data should an error occur in one segment of the data.

2.5.4 Additional Considerations

The regulated entity is responsible for maintaining the technology, storage capacity, encryption keys, and other information and services needed to use HCP and permit access to the redundant records, as well as:

- ▶ Properly configuring replication and other redundancy features.
- ▶ Managing replication collisions.
- ▶ Ensuring that record deletion and changes to the retention settings are made to the redundant records.

2.6 Audit System

2.6.1 Compliance Requirement

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

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

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

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

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

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

2.6.2 Compliance Assessment

Cohasset asserts that HCP supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.6.3 HCP Capabilities

The regulated entity is responsible for an audit system, and compliance is supported by HCP.

- ▶ Record versions cannot be overwritten, and therefore, changes to a record version cannot be input, when the record is under retention (the retention period has not expired) or has a Hold applied.
- ▶ HCP immutably retains the record object name and version ID, which must be unique.
- ▶ In addition, HCP stores a system-generated creation/storage timestamp as immutable metadata of each record version.
- ▶ Applying retention controls ensures that contents of a record cannot be modified or overwritten. Therefore, both the record and its immutable metadata are immutably stored over its lifespan.
- ▶ The HCP **internal access log** tracks the following record compliance events and captures the requesting IP address, username, date/time/time zone, full record name, status code, size, Bucket name, and tenant name:
 - Initial capture of records,
 - Assignment and extension of retention attributes,
 - Assignment or removal of Legal Holds,
 - Deletion of eligible records (i.e., records with a *retention expiration date* in the past and no assigned Legal Hold attribute). Privileged Delete actions, which are allowed only in Buckets in *Enterprise* mode, are also captured in the *access log*.
 - The *internal access log* events can be generated for download in a single zip file and subsequently ingested into a security information event management tool.
- ▶ Additionally, the HCP **tenant log** tracks *Retention Class* activities (e.g., add and modify *Retention Class*) for a Bucket and captures the requesting user or service ID, date/time and description of the event. The *tenant log* events are not deleted and are available via the tenant management console.
- ▶ The HCP system can be configured to stream both *tenant logs* and *internal access logs* to a syslog server. Then, tools in the syslog environment can be used to sort and query the log activity and produce the requested audit trail data in the format and medium required.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and changes made to the records. In addition to relying on the immutable metadata, the regulated entity may utilize HCP audit features. When relying on the HCP internal access log, Cohasset recommends copying the audit events to a security information event management tool.

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

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

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

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

The proposed amendments to Rules 17a-4 and 18a-6 and the [CFTC] principles-based approach recommended by the commenters share an objective: ensuring the authenticity and reliability of regulatory records. However, the audit-trail requirement is more likely to achieve this objective because, like the existing WORM requirement, it sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.²¹ [emphasis added]

In Section 2 of this report, Cohasset separately assesses HCP with S3 Object Lock and HCP Retention configured in:

- Highly-restrictive *Compliance* mode, which provides both overwrite protection and strict deletion and retention protections, or
- Less-restrictive *Enterprise* or *Governance* modes, which provide overwrite protections but requires administrative procedures and monitoring to ensure compliant retention, since administrators are allowed to (a) delete a record before its retention period expires and (b) reduce or remove retention protections.

See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for separate information on (s) S3 Object Lock and (b) HCP Retention.

In the following table, Cohasset correlates specific *principles-based* CFTC requirements for electronic records with the functionality of HCP when configured to meet SEC requirements. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of HCP, relative to these requirements.

²¹ 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)
<i>(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:</i> <i>(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the <u>authenticity and reliability</u> of such regulatory records in accordance with the Act and Commission regulations in this chapter.</i> <i>(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the <u>authenticity and reliability</u> of electronic regulatory records, including, without limitation:</i> <i>(i) Systems that maintain the security, signature, and data as necessary to ensure the <u>authenticity</u> of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;</i>	It is Cohasset's opinion that HCP meets the CFTC requirements in (c)(1) and (c)(2)(i); specifically: • Both S3 Object Lock and HCP Retention meet requirements for records²² with <u>time-based</u> retention, and HCP Retention meets requirements for records with <u>event-based</u> retention. • Both S3 Object Lock and HCP Retention meet <u>time-based</u> retention requirements. • Additionally, HCP Retention meets <u>event-based</u> retention requirements. The functionality that supports retention, authenticity and reliability of electronic records is described in the following sections of this report: • Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i> • Section 2.3, <i>Record Storage Verification</i> • Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i> • Section 2.6, <i>Audit System</i> Additionally, for <u>records stored electronically</u>, the CFTC definition of <u>regulatory records</u> in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification: <u>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:</u> <u>(i) Any data necessary to access, search, or display any such books and records; and</u> <u>(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.</u> [emphasis added] HCP retains immutable metadata 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 include the following: • Unique Object Name and Version ID, within a Tenant, • Object creation/storage timestamp, and • Object size. Additionally, mutable metadata that is stored for records includes retention settings and Holds. The most recent values of mutable metadata are retained for the same time period as the associated records.

²² 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.

COMPLIANCE ASSESSMENT REPORT

Hitachi Content Platform (HCP): SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation(72)(1)

CFTC 1.31(c)-(d) Regulation [emphasis added]	Compliance Assessment Relative to CFTC 1.31(c)-(d)
(ii) <i>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</i>	It is Cohasset's opinion that HCP capabilities described in Section 2.5, <i>Record Redundancy</i>, 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 <u>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</u>.
(iii) <i>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.</i>	The regulated entity is required to create and retain an <i>up-to-date inventory</i>, as required for compliance with 17 CFR § 1.31(c)(iii).
(d) <i>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:</i> (1) <i>Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.</i> (2) <i>Production of paper regulatory records. ***</i> (3) <i>Production of electronic regulatory records.</i> (i) <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.</i> (ii) <i>A records entity must produce such regulatory records in the form and medium requested promptly, upon request, unless otherwise directed by the Commission representative.</i> (4) <i>Production of original regulatory records. ***</i>	It is Cohasset's opinion that HCP 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, <i>Non-Rewriteable, Non-Erasable Record Format</i> • Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i> • Section 2.6, <i>Audit System</i>

4 • Summary Assessment of Compliance with MiFID II Delegated Regulation(72)(1)

The objective of this section is to document Cohasset's assessment of the functionality of HCP, as described in Section 1.3, *HCP Overview and Assessment Scope*, in comparison to the following requirements of the *Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation)*. Specifically, Article 72(1) defines medium and retention of records requirements:

1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:

(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;

(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;

(c) it is not possible for the records otherwise to be manipulated or altered;

(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and

(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used. [emphasis added]

Paragraph (e), above, recognizes the technology evolution and defines requirements or conditions for regulated entities that retain records electronically. The approach is consistent with the SEC, which also sets forth standards that the electronic storage media must satisfy to be acceptable.

Additionally, the Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MiFID II) defines durable medium as follows:

(62) 'durable medium' means any instrument which:

(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information; and

(b) allows the unchanged reproduction of the information stored. [emphasis added]

While the above pertains to enabling the client to store and access its information, regulated entities often apply the MiFID II durable medium requirements to internally retained information, assuring it is immutable, retained for the appropriate time period and stored in a manner that assures unchanged reproduction. For this reason, Cohasset included this citation in its analysis for this section of the report.

In Section 2 of this report, Cohasset separately assesses HCP with S3 Object Lock and HCP Retention configured in:

- Highly-restrictive *Compliance* mode, which provides both overwrite protection and strict deletion and retention protections, or

- Less-restrictive *Enterprise* or *Governance* modes, which provide overwrite protections but require administrative procedures and monitoring to ensure compliant retention, since administrators are allowed to (a) delete a record before its retention period expires and (b) reduce or remove retention protections.

See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for separate information on (a) S3 Object Lock and (b) HCP Retention.

In the following table, Cohasset correlates specific MiFID II requirements for electronic records with the functionality of HCP when configured to meet SEC requirements. The first column enumerates specific electronic records requirements for (a) *durable medium* in MiFID II and (b) the *medium* and retention of records in the *Delegated Regulation*, which supplements MiFID II. The second column provides Cohasset's analysis and opinion regarding the ability of HCP, relative to these requirements.

Regulatory excerpts of MiFID II media requirements [emphasis added]	Compliance assessment and analysis of HCP relative to these MiFID II media requirements
Directive 2014/65/EU (MiFID II) Article 4(1)(62) <u>(62) 'durable medium' means any instrument which:</u> <u>(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information</u> ***** Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1) <u>(1) The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:</u> *****	While these requirements pertain to the regulated entity's client and regulator, the regulated entity itself would have a similar need to store the record for the required retention period. It is Cohasset's opinion that the following HCP features apply retention controls to records and associated system and custom metadata: • Both S3 Object Lock and HCP Retention meet <u>time-based</u> retention requirements. • Additionally, HCP Retention meets <u>event-based</u> retention requirements. See Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i>, for additional information. Further, HCP assures the accurate recording (storage) of the record content and associated metadata, as explained in Section 2.3, <i>Record Storage Verification</i>. The quality and accuracy of the recording process is verified: (a) during the initial recording of the record, (b) using post-recording verification during read-back, and (c) by conducting periodic consistency and integrity checking.
Directive 2014/65/EU (MiFID II) Article 4(1)(62) <u>(62) 'durable medium' means any instrument which:</u> ***** <u>(b) allows the unchanged reproduction of the information stored:</u> Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1) <u>1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:</u> ***** <u>(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;</u> <u>(c) it is not possible for the records otherwise to be manipulated or altered;</u> *****	It is Cohasset's opinion that the features of HCP with S3 Object Lock and HCP Retention, achieve the non-rewriteable, non-erasable storage requirements necessary to assure that record content is unchangeable. See Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i>, for additional information. If the regulated entity corrects or amends a record in the source system, it must store each rendition as a new record (or record version). The features for non-rewriteable, non-erasable format assure that the original record is <u>not</u> modified. Further, HCP stores a cryptographic hash value as metadata for each record and subsequently uses the hash value for post-recording, periodic quality and integrity checks and for automated record repair, as described in Section 2.3, <i>Record Storage Verification</i>.

Regulatory excerpts of MiFID II media requirements [emphasis added]	Compliance assessment and analysis of HCP relative to these MiFID II media requirements
Directive 2014/65/EU (MiFID II) Article 4(1)(62) <i>(62) ‘durable medium’ means any instrument which:</i> <i>(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information</i> <i>(b) allows the unchanged reproduction of the information stored;</i> Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1) <i>1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:</i> ***** <i>(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;</i> ***** <i>(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and</i> *****	Cohasset asserts that HCP provides the following tools for retrieving records: 1. HCP S3-compatible APIs to list and retrieve records and record metadata 2. Search Console for HCP 3. HCP Metadata query API 4. Industry Standard Protocols, such as (a) NFS, (b) CIFS, and (e) HCP Object protocols 5. Hitachi Content Intelligence (HCI) The selected records may be downloaded, and local capabilities may be used to view, filter, print or produce the records in an acceptable format and medium. See Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i>, for additional information. Further, when Data Protection Level (DPL) or replication are properly configured, HCP ensures that records are readily available by writing multiple copies of the records and metadata. Additionally, when cloud-optimization is set, erasure coding may be configured to accurately regenerate a record from erasure coded data should an error occur in any segment of the data, or an availability problem be encountered in any one facility. See Section 2.5, <i>Record Redundancy</i>, for additional information.
Directive 2014/65/EU (MiFID II) Article 4(1)(62) N/A Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1) <i>1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:</i> ***** <i>(e) the firm’s arrangements comply with the record keeping requirements irrespective of the technology used.</i> *****	Cohasset asserts that HCP provides the following tools for retrieving records: 1. HCP S3-compatible APIs to list and retrieve records and record metadata 2. Search Console for HCP 3. HCP Metadata query API 4. Industry Standard Protocols, such as (a) NFS, (b) CIFS, and (c) HCP Object protocols 5. Hitachi Content Intelligence (HCI) The selected records and associated metadata may be downloaded, and local capabilities may be used to view, filter, print or produce the records in an acceptable format and medium. See Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i>, for additional information. As may be required, the regulated entity may transfer records to other media or migrate records to new file formats, in advance of technological obsolescence.

5 • Conclusions

Cohasset assessed the functionality of Hitachi Content Platform (HCP)²³ 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 HCP, when properly configured, has the following capabilities, which meet the regulatory requirements:

- ▶ Maintains records and immutable record metadata in a non-rewriteable, non-erasable format for (a) time-based retention periods, using either S3 Object Lock or HCP Retention, and (b) event-based retention periods using HCP Retention.
- ▶ Applies Holds to immutably preserve records for a subpoena, legal hold or similar circumstances, and permits clearing the Holds when the matter is released.
- ▶ Prohibits deletion of a record and its immutable metadata until the retention period for the record is expired and any Hold is removed (cleared). Note: When the less-restrictive *Governance* (a.k.a. *Enterprise*) mode is applied, procedural controls and monitoring are required to scrutinize Privileged actions to reduce or remove retention controls or prematurely delete required records.
- ▶ Verifies the accuracy of the process for storing and retaining the records using cryptographic hash values and content verification processes.
- ▶ Provides the capacity and tools to (a) search for records, (b) list the object names, and (c) download the records and associated metadata for a browser or other local tool to render as a human-readable view and produce in the requested electronic format.
- ▶ Maintains redundancy to either retrieve or regenerate an accurate replica of the record should an error occur or an availability problem be encountered.
- ▶ Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that HCP, with S3 Object Lock or HCP Retention, when properly configured and utilized to store and retain time-based records in non-rewriteable, non-erasable record format, 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). In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d) and the medium and *retention of records* requirements of the *MiFID II Delegated Regulation*(72)(1).

²³ See Section 1.3, *HCP Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

Appendix A • Overview of Relevant Electronic Records Requirements

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

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

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

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments²⁴ 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.*²⁵ [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.*²⁶ [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.

²⁴ The compliance dates are May 3, 2023, for 17 CFR § 240.17a-4, and November 3, 2023, for 17 CFR § 240.18a-6.

²⁵ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

²⁶ 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.²⁷ [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.²⁸ [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."*²⁹ [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^{***30} [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 SBS/MSBSP Recordkeeping Adopting Release).*

²⁷ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

²⁸ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

²⁹ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

³⁰ 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.³¹ [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.³² [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.³³ [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 HCP 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).³⁴

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.

³¹ 2003 Interpretive Release, 68 FR 25282.

³² 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).

³³ 2003 Interpretive Release, 68 FR 25283.

³⁴ 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.³⁵ [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 HCP in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

³⁵ Recordkeeping, 82 FR 24482 (May 30, 2017) (2017 CFTC Adopting Release).

A.4 Overview of the *Medium and Retention of Records* Requirements of MiFID II

Markets in Financial Instruments Directive II (MiFID II), approved by the European Parliament as *Directive 2014/65/EU*, became effective January 3, 2018. Specifically, Article 4(1)(62) of MiFID II defines durable medium as:

(62) 'durable medium' means any instrument which:

(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information; and

(b) allows the unchanged reproduction of the information stored; [emphasis added]

While the above pertains to enabling the client to store and access its information, regulated entities often apply the MiFID II durable medium requirements to internally retained information, assuring it is immutable, retained for the appropriate time period and stored in a manner that assures the unchanged reproduction.

Further, with implementation of the revised MiFID II, investment firms must arrange for records to be kept for all services, activities and transactions. The key recordkeeping provisions are in Article 16, *Organisational requirements*, paragraphs 6 and 7:

6. *An investment firm shall arrange for records to be kept of all services, activities and transactions undertaken by it which shall be sufficient to enable the competent authority to fulfil its supervisory tasks and to perform the enforcement actions under this Directive, Regulation (EU) No 600/2014, Directive 2014/57/EU and Regulation (EU) No 596/2014, and in particular to ascertain that the investment firm has complied with all obligations including those with respect to clients or potential clients and to the integrity of the market.*

7. *Records shall include the recording of telephone conversations or electronic communications relating to, at least, transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission and execution of client orders.*

Such telephone conversations and electronic communications shall also include those that are intended to result in transactions concluded when dealing on own account or in the provision of client order services that relate to the reception, transmission and execution of client orders, even if those conversations or communications do not result in the conclusion of such transactions or in the provision of client order services.

For those purposes, an investment firm shall take all reasonable steps to record relevant telephone conversations and electronic communications, made with, sent from or received by equipment provided by the investment firm to an employee or contractor or the use of which by an employee or contractor has been accepted or permitted by the investment firm.

Orders may be placed by clients through other channels, however such communications must be made in a durable medium such as mails, faxes, emails or documentation of client orders made at meetings. In particular, the content of relevant face-to-face conversations with a client may be recorded by using written minutes or notes. Such orders shall be considered equivalent to orders received by telephone.

The records kept in accordance with this paragraph shall be provided to the client involved upon request and shall be kept for a period of five years and, where requested by the competent authority, for a period of up to seven years.
[emphasis added]

Article 16(6) allowed the Commission to make delegated legislation, resulting in the issuance of *Commission Delegated Regulation (EU) 2017/565 (the MiFID II Delegated Regulation)*.

The *MiFID II Delegated Regulation* in Section 8, *Record-keeping*, Article 72, *Retention of records*, paragraph 1, specifies:

1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:

(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;

(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;

(c) it is not possible for the records otherwise to be manipulated or altered;

(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and

(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used. [emphasis added]

See Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1)*, for a summary assessment of the capabilities of HCP in relation to requirements for (a) *durable medium* in MiFID II and (b) medium and retention of records in the *MiFID II Delegated Regulation*.

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.

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.

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*