Cohasset Associates

SEC 17a-4(f), FINRA 4511(c) and MiFID II Compliance Assessment

Hitachi Content Platform (HCP)

Abstract

The Hitachi Content Platform (HCP) is a highly efficient, object storage solution designed to support large scale repositories of unstructured content. The *compliance mode* feature is designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format. HCP in *compliance mode* applies integrated control codes to prevent stored objects from being modified, overwritten or deleted until the specified retention period has expired and any associated legal holds have been released.

In this Assessment Report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of HCP (see Section 1.3, *HCP Overview and Assessment Scope*) relative to the following regulations:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).
- Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (i.e., MiFID II).

It is Cohasset's opinion that HCP, when properly configured, meets the five requirements related to recording and non-rewriteable / non-erasable storage of electronic records and either meets or supports the three requirements for an audit system, as specified in SEC Rule 17a-4(f) and FINRA Rule 4511(c). Additionally, the assessed capabilities of HCP meet the requirements defined in the MiFID II Directive and the supplementing Delegated Regulation.

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to Cohasset's practice is its delivery of records management and information governance professional consulting services, education and training. Cohasset's expert consulting services are tailored to support a multitude of regulated organizations, including those in the financial services industry. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls with their organizations' business priorities and facilitating regulatory compliance and risk mitigation, all the while generating measurable business efficiencies.

Cohasset has assessed the spectrum of storage technologies and systems designed to meet the requirements of the Securities and Exchange Commission Rule 17a-4(f), as defined by 1) the No Action Letter in 1993 (allowing broker dealers to use non-rewriteable, non-erasable digital storage media); 2) the issuance of the Rule in 1997; and 3) the Interpretive Release in 2003, which authorizes the use of erasable storage, conditioned on integrated control codes, to prevent premature deletion of records.

Table of Contents

1 | Introduction

Regulators, world-wide, establish explicit requirements for regulated entities that elect to retain books and records[1] on electronic storage media. Given the prevalence of electronic retention of books and records, these requirements apply to most broker-dealers and other organizations with similarly regulated operations.

This Introduction *briefly summarizes the regulatory environment pertaining to this assessment, explains the purpose and approach for Cohasset's assessment, and provides an overview of HCP and the scope of this assessment.*

1.1 Overview of the Regulatory Requirements for Electronic Recordkeeping

1.1.1 SEC Rule 17a-4(f) Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4, the SEC stipulates recordkeeping requirements, including retention periods, for the securities broker-dealer industry. On February 12, 1997, the SEC adopted amendments to 17 CFR § 240.17a-4 (the Rule or Rule 17a-4). These amendments to paragraph (f) expressly allow books and records to be retained on electronic storage media, subject to explicit standards.

> *The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4.*[2] [emphasis added]

Further, the SEC issued two Interpretive Releases (No. 34-44238 on May 1, 2001, and No. 34-47806 on May 7, 2003), which pertain specifically to the electronic storage media requirements of paragraph (f).

For additional information, refer to Section 4.1, Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to the format and media requirements of SEC Rule 17a-4, for the 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.*

---

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

[2] Exchange Act Release No. 38245 (Feb. 5, 1997), 62 FR 6470 (Feb. 12, 1997) (Adopting Release).

1.1.3 MiFID II Durable Medium Requirements

On May 20, 1997, the concept of *durable medium* was first introduced in the European Union in the *Distance Selling Directive 97/7/EC*[3] as an alternative to paper as the support or medium for information.

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. As a supplement to MiFID II, the *Commission Delegated Regulation (EU) 2017/565*[5] *(Delegated Regulation),* 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.

Refer to Section 3, *Summary Assessment of Compliance with MiFID II Durable Medium Requirements*, which correlates these MiFID II requirements to the capabilities of HCP. Additionally, refer to Section 6.4, *Overview of MiFID II Durable Medium Requirements for Recordkeeping*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of HCP, Hitachi Vantara engaged Cohasset Associates, Inc. (Cohasset). As a highly-respected consulting firm, Cohasset has recognized expertise and more than 40 years of experience with the legal, technical and operational issues associated with the records management practices of companies regulated by the SEC. Additional information about Cohasset is provided in the last section of this report.

Hitachi Vantara engaged Cohasset to:

- Assess the capabilities of HCP, in *compliance mode*, in comparison to the five requirements of SEC Rule 17a-4(f) for recording and the non-rewriteable / non-erasable storage of electronic record objects and associated metadata and the three requirements for an audit system; see Section 2, *Assessment of Compliance with SEC Rule 17a-4(f);*
- Associate the *durable medium* requirements of MiFID II and the retention of records requirements in Article 72(1) of the *Delegated Regulation*, which supplements MiFID II, to the assessed capabilities of HCP in *compliance mode*; see Section 3, *Summary Assessment of Compliance with MiFID II Durable Medium Requirements*; and
- Prepare this Assessment Report, enumerating the results of its assessment.

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

---

[3] *Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts;* the validity period of this Directive expired June 13, 2014.

[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*

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection, by Cohasset, of Hitachi Content Platform and its capabilities or other Hitachi Vantara products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) user and system administrator guides, and (d) other directly-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

Hitachi Content Platform (HCP) provides organizations and service providers a solution for consolidating information produced by users, applications and devices. Information is stored on a central, highly scalable platform to enable better understanding, governance, access and mobility control, as well as to identify insights and extract value for agile data driven decisions. Further, HCP is a highly efficient, object storage solution able to support large scale repositories of unstructured content for long-term archiving under automated policy controls.

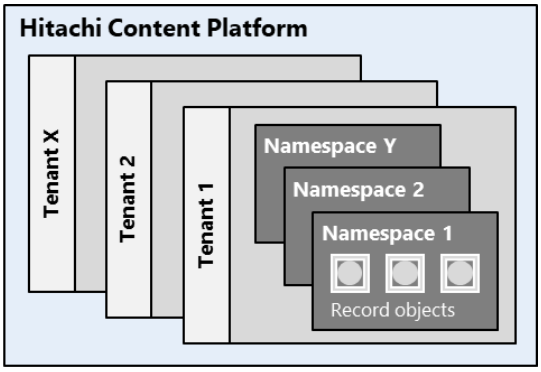

Figure 1: Storage Architecture

The HCP storage architecture, as depicted in Figure 1, is based on the division of physical storage into multiple tenants (e.g., an entity or division of an entity), with each tenant being further divided into one or more namespaces (e.g., unique, logical repositories that may contain record objects for an organizational function or a specific business application). Specific settings can be defined for a namespace that provide for retention, replication and access controls. Directories, filenames, and custom metadata from the source application are supported and remain intact within the HCP namespace. HCP offers two retention modes for managing namespaces: *enterprise* and *compliance*.

The scope of this assessment is focused specifically on the compliance-related capabilities of HCP, operating under the following conditions and configurations:

- *Compliance mode* is enabled for the namespace.
- One (or a combination) of the following two software/hardware environments is configured:
    1. *HCP appliance*: Fully integrated HCP software and hardware storage solution provided by Hitachi Vantara as an enterprise-grade turnkey object storage appliance which provides fully integrated logical and physical storage management, administrative and user controls. Object storage on the appliance is either: 1) internal disks, 2) SAN-attached storage (minimum RAID6[6] required), or 3) S series storage node appliances which provide erasure code (EC) protected storage pools.

[6] 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. *Hitachi Content Platform virtual machine (HCP VM)*: HCP VM installed as a virtualized HCP system in a VMware vSphere® environment or in a Kernel-based Virtual Machine (KVM) environment; both solutions must utilize Hitachi Vantara-recommended storage.

- This assessment ***excludes*** cloud-only deployments and cloud-tiered storage.

Throughout this report, the above described operating environments of HCP are being assessed.

2 | Assessment of Compliance with SEC Rule 17a-4(f)

This section presents Cohasset's assessment of the capabilities of the Hitachi Content Platform (HCP) in compliance mode, compared to the five requirements related to recording and non-rewriteable / non-erasable storage of electronic records and three requirements for an audit system, as stipulated in SEC Rule 17a-4(f).

For each of the eight relevant requirements in SEC Rule 17a-4(f), this assessment is organized into the following four topics:

- ***Compliance Requirement*** – Excerpt of each electronic storage requirement in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirement
- ***Compliance Assessment*** – Assessment of the relevant capabilities of HCP
- ***HCP Capabilities*** – Description of relevant capabilities
- ***Additional Considerations*** – Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities HCP, as described in Section 1.3, HCP Overview and Assessment Scope, relative to each pertinent requirement of SEC Rule 17a-4(f).

2.1 Non-Rewriteable, Non-Erasable Record Format

2.1.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(A)]

SEC 17a-4(f)(2)(ii)(A): Preserve the records exclusively in a non-rewriteable, non-erasable format.

As set forth in Section III (B) of the 2001 Interpretive Release, this requirement *"is designed to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in an unalterable form [for the required retention period]."*

The following statement in the 2003 Interpretive Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, meet the requirements of a non-rewriteable and non-erasable recording environment provided: (a) the storage solution delivers the prescribed functionality, and (b) the functionality is delivered via appropriate integrated control codes for the SEC designated retention period associated with the stored records.

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) 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.* [emphasis added]

Further, Section IV of the 2003 Interpretive Release places requirements on the storage system for retaining records beyond the SEC-established retention period when certain circumstances occur, such as a subpoena or legal hold:

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, 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.* [emphasis added]

This statement by the SEC clarifies that the storage system must have the capability to retain records beyond the retention period established at the time of initial recording when required for legal matters, external investigations or audits, or other similar circumstances.

2.1.2 Compliance Assessment

It is Cohasset's opinion that HCP, in *compliance mode,* meets this SEC requirement to retain records in non-rewriteable, non-erasable format for time-based[7] and event-based[8] retention periods and any applied legal hold, when (a) properly configured, as described in Section 2.1.3, and (b) the considerations described in Section 2.1.4 are satisfied.

2.1.3 HCP Capabilities

This section describes the capabilities of HCP that pertain to this SEC requirement for preserving electronic records (record objects) as non-rewriteable, non-erasable.

Overview

- HCP offers two *modes* for the retention of record objects in a given namespace: *enterprise* or *compliance*. When a namespace is set to *compliance mode*, the mode cannot be changed or removed, and more stringent retention protection and object management controls are employed. A namespace utilized for storing records in compliance with SEC Rule 17a-4(f) must be set to *compliance mode*.
  - A default retention setting is configured for each namespace.
  - Additionally, one or more *Retention Classes* (i.e., custom retention settings) may be configured for use within each namespace.
  - When a namespace is in *compliance mode*, *Retention Classes* cannot be deleted, nor can their retention duration be shortened.
- Retention is applied to each record object stored in the namespace. Each record object inherits the default retention setting for the namespace, unless a valid *Retention Class* (i.e., a Retention Class that is allowed for use within the namespace) or a specific retention attribute (i.e. an expiration date, retention offset period, etc.) is sent from the source application with the record object.

---

[7] Time-based retention periods require records to be retained for a specified contiguous period of time from the date and time created and stored.

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

- When a retention period is applied to a record object within a *compliance mode* namespace, integrated control codes are applied which:
  - Disable all write permissions for the content of the record object, thus protecting it against modification or overwrite for the specified retention period.
  - Prohibit deletion until the assigned retention period expires and any Legal Holds are removed.
  - Prohibit the *shortening* of the assigned retention period assigned to the record object.
  - Prohibit the deletion or renaming of a directory containing one or more record objects.

Record Object and Retention Controls

- Record objects are uploaded to an HCP namespace via user console or, programmatically, via standard protocols such as Hitachi API for Amazon S3 (Amazon S3-compliant API), HTTP/REST, SMTP, NFSv4, CIFS, and WebDAV.
- A record object within HCP is comprised of four elements:
  1. **Content:** The contents of the record object (i.e., document, image, video, database image, etc.).
  2. **System metadata:** Critical attributes for record object management such as:
     - *Immutable metadata*, such as record ID, object create/storage date and time and cryptographic hash value.
     - *Mutable metadata,* such as retention period (can be increased only), data protection level (number of replicas or duplicates) and hold attribute.
  3. **Custom metadata:** Optional information, called *annotations*, that are defined by the regulated entity for purposes of further identification or retrieval.
     - Changes to custom metadata for records under retention may be restricted by administrators of the namespace, as required.
  4. **Object Access Control List (ACL):** Simple per object access permissions managed by HCP to optionally define user permissions for various non-retention operations.
- HCP can optionally be configured to support:
  - *Versioning of record objects.* When retention is applied to a set of versioned objects, the retention controls apply only to the latest (most recent) version. Therefore, the top version is the only compliance version of the record object. Once retention is applied, HCP prohibits the creation of new versions of that record object.
    - Retention is not applied to prior versions; therefore, prior versions are not protected or stored for SEC compliance and may be deleted utilizing version pruning capabilities.
  - *Appending custom metadata (e.g., annotations and access control lists) to record objects,* which does not affect (i.e., modify) the original content.

- Note: Content cannot be appended, because this would create a new version, which is disallowed after retention is applied.

- To be compliant with the non-rewriteable, non-erasable requirement of SEC 17a-4(f), a record object must (1) be stored in a namespace that is configured in ***compliance mode*** and (2) have an appropriate **retention setting** applied.
- The following three types of retention settings are available for a namespace configured in *compliance mode*.

1. Retention Class: A *Retention Class* is a named configuration comprised of one of the following retention attributes.

Retention Attribute	Description
• Offset	An offset from the record object's create date/time, specified in terms of the number of years, months or days (i.e., retain for 6 years from create date). An offset may be configured to calculate the retention expiration date by adding the offset period to: • The time at which the object was added to the namespace • The current retention setting for the record object • The current time Optionally, a post-retention delete action may be defined for an offset Retention Class, which allows the *disposition service* for HCP to automatically delete expired record objects that are not subject to a legal hold.
• Fixed date	An explicit, fixed date in the future.
• Special value:	
○ Deletion Allowed	Allows the object to be deleted at any time. Accordingly, Deletion Allowed cannot be assigned for SEC Compliance.
○ Deletion Prohibited	Prevents the object from ever being deleted by means of a normal delete operation.
○ Initial Unspecified	Prevents the object from being deleted and allows its retention setting to be set in the future. When used for event-based retention, a governing value called *Minimum Retention After Initial Unspecified* (i.e., an offset value stated in terms of years, months, and/or days) may be defined for the namespace to ensure any future retention value exceeds the minimum value.

- Once a *Retention Class* is created and configured for a namespace in *compliance mode,* the following controls apply:
  - The *Retention Class* cannot be deleted.
  - A retention period defined for the *Retention Class* cannot be decreased or shortened, nor can an offset value be reduced or shortened.
  - An offset retention value cannot be changed to Deletion Allowed or Initial Unspecified.
  - A Deletion Prohibited value cannot be changed to an offset retention value.
  - A Deletion Prohibited value cannot be changed to Deletion Allowed.
  - A Deletion Allowed value *can be changed* to a specific retention date or offset.

2. Default Retention: When configured, the default retention period is assigned to any record object that does not have a specific retention attribute sent with the record object by the source application.

- The *Default Retention* setting may be configured with one of the Retention Attributes listed in the table above, or with a named *Retention Class*. It is important that the regulated entity configure the default retention setting to reflect the specific retention period (*or the longest retention period*) for the record objects to be stored in the namespace.

  Caution: If an explicit *fixed date* is used as the default retention setting, it must be set to a future date. When the explicit *fixed date* is in the past, the default setting of the namespace reverts to *Deletion Allowed*, which is not compliant with the Rule, since it allows objects to be deleted at any time.

3. **Synchronization of atime Attribute:** An HCP namespace can be configured to synchronize retention with a file system that uses the atime (last access time) attribute to store the retention expiration date. When configured, the retention expiration dates are synchronized, changing the retention expiration date in one storage solution will cause the same update in the other storage solution, subject to *compliance mode* restrictions for changing retention settings (i.e., the atime cannot be used to shorten a retention period once assigned).

- The mechanisms for **applying** a retention setting to an object in an HCP namespace are as follows:
  - *Retention Class*, which is applied when the source application sends the *Retention Class* as a metadata attribute for the record object to be stored in a specific namespace. When a *Retention Class* sent by the source application does not match one of the defined *Retention Classes* for the specified namespace, the record object is rejected by the application programming interface (API) and handled as an *error condition*.
  - *Specific Retention Attribute,* as described in the preceding table for Retention Classes, may be applied to a record object by the source application when storing the record object. When a *Specific Retention Attribute* is sent, HCP verifies it is a future date (past dates result in an *error condition*).
  - *Default retention setting:* The default retention setting will be applied to a record object when the source application does not send one of the above retention attributes when storing the record object.
- When a retention period is applied to a record object:
  - All write permissions for the content of the object are disabled, thereby not allowing the object to be modified, renamed, appended to or overwritten;
  - Versioning is automatically disabled; therefore, no new versions of the record object can be created, and no prior versions can be promoted.
  - Record objects and associated metadata cannot be deleted through any mechanism prior to the expiration of the associated retention period;
  - The retention period of a record object cannot be shortened, only lengthened; and
  - Deleting or renaming a directory containing one or more record objects is prohibited.
- For record objects requiring event-based retention, a retention setting of *Initial Unspecified* is applied when the record is first stored. This *Initial Unspecified* retention setting protects a record object for an indefinite period of time, until a "triggering event" occurs.

- When the "triggering event" occurs, the source application provides a new retention attribute which will be validated against the *Minimum Retention After Initial Unspecified governing* value defined for the namespace. The record object will be retained for the greater of the new retention value or the *required minimum*.

Legal Hold

When litigation or a subpoena requires record objects to be placed on hold, which could entail retaining them beyond their assigned retention period, the regulated entity must ensure the subject record objects are protected for the duration of the legal hold.

- Authorized users identify record objects that are subject to the hold, via the HCP search console, and set a *Hold* attribute for each identified object.
- While subject to a *Hold*:
  - No new versions are allowed for the object;
  - No changes are allowed to retention settings;
  - Custom metadata may continue to be modified; and
  - An object cannot be deleted by any means, even if past its retention period.
- The *Hold* attribute can be removed for one or multiple records, via the HCP search console or the API, when the hold is no longer required. Thereafter, immutability controls for the record object are governed by the retention setting assigned to the record object.

Deletion Controls

- The record object must meet the following conditions to be eligible for deletion:
  - The retention period applied to the record object must be in the past, and
  - A *Hold* must not be assigned to the record object.
- Disposition or deletion of *eligible* record objects may be initiated by HCP or by the source application.
  - The *disposition service* for HCP, when configured for use within a namespace, periodically runs to identify and automatically delete *expired* record objects that (1) are past their retention expiration date, (2) are not subject to a Hold, and (3) have the automatic deletion flag enabled.
    - Objects with a special value retention setting, such as Deletion Prohibited or Initial Unspecified are excluded from the *disposition service*.
  - The source application must explicitly initiate the disposition process for record objects that do not meet the requirements listed above, for the *disposition service*, but are otherwise eligible for deletion.
- Special queries are available to produce a time-ordered report of record object activities, such as, objects processed by the *disposition service*.
- *Shredding* (i.e., secure deletion) can be configured as part of the deletion process. When configured, HCP overwrites the spaces where objects and metadata were stored to assure the deleted record object cannot be reconstructed.

- Privileged delete is not allowed for a namespace in *compliance mode*. Accordingly, the administrative deletion of a record object (prior to the expiration of the retention period and prior to the release of any associated legal hold) is prohibited.
- A namespace in *compliance mode* cannot be deleted by any mechanism if it contains any record objects.
- A tenant that contains one or more namespaces in *compliance mode* cannot be deleted through any mechanism.

Clock Management

- To protect against the possibility of premature deletion of record objects that could result from accelerating the system time clock, every HCP system clock that is controlling a namespace in *compliance mode,* including all systems within a replication topology, must be configured to synchronize with multiple external time servers, e.g., network time protocol (NTP) clocks. 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 an HCP namespace time clock that could result in the premature deletion of record objects.
- Additionally, HCP prevents "sudden clock jumps" that may result from misconfigured external time servers, thus preventing clock manipulation by corrupted or compromised time servers.

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 record objects.

- The HCP system executes on a fully-customized Fedora operating system, which has (a) all unused modules and extensions removed and (b) regularly updated security hardening.
- Role-Based Access Control (RBAC), set at both system and tenant levels, provide the means to constrain access to functionality for both 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 HCP 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 record objects is available as follows:
    - Hypertext transport-layer encryption (HTTPS) and Secure Sockets Layer (SSL) 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.

2.1.4 Additional Considerations

The following considerations for configuration and usage of HCP in *compliance mode* are provided to help ensure that the non-rewriteable, non-erasable requirements of the Rule are met. The regulated entity is responsible for:

- Configuring *compliance mode* for namespaces that will store books and records required by regulation, thereby establishing the foundation for meeting the requirements of the Rule.
- Ensuring the appropriate retention class or appropriate retention value is stored with the record object, since only objects with retention applied meet the SEC requirements.
  - Note: The Deletion Allowed retention value is not allowed for compliance with the Rule, since it allows the object to be deleted at any time.
- Setting a *Minimum Retention After Initial Unspecified* governing value for event-based retention to ensure any future retention value exceeds the minimum value and appropriately managing event-based retention attributes.
- Applying legal holds to record objects that require preservation for legal matters, government investigations, external audits and other similar circumstances, and removing the legal holds when the applicable action is completed.
- Setting appropriate security controls to (1) restrict network ports and protocol access, (2) establish roles-based access, (3) encrypt data in transit and while at rest.
- Synchronizing HCP system clocks with an external time source to prevent tampering that could result in the premature deletion of record objects.
- Disallowing cloud-only and cloud-tiered storage (e.g., Amazon S3, Google Cloud Storage, Microsoft Azure) for the official or replica of the record objects, 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.

2.2 Accurate Recording Process

2.2.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(B)]

SEC 17a-4(f)(2)(ii)(B): Verify automatically the quality and accuracy of the storage media recording process.

The intent of this requirement is to ensure both the accuracy and quality of the recording process such that the records read from the storage media are precisely the same as those that were recorded. This requirement includes both a quality verification of the recording process and post-recording verification processes.

2.2.2 Compliance Assessment

Cohasset asserts that the capabilities of HCP, in conjunction with the inherent capabilities of advanced magnetic storage technology, meet this SEC requirement for accurate recording and post-recording verification.

2.2.3 HCP Capabilities

HCP is a self-monitoring, self-healing system that alerts users to identified integrity issues. The capabilities described below address both the initial recording and the post-recording verification processes.

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.
  - Record objects are recorded using RAID6 which provides for recovery of record object data.
  - Namespace storage quotas are verified prior to recording record objects. Should insufficient space exist, the write operation is rejected, and an error notification is issued.
- During upload, a cryptographic hash may be calculated and sent by the source application to validate transmission. Upon receipt HCP recalculates the hash value and either (a) writes the record object only if the hash values match or (b) returns the hash value to the source application for validation that HCP received and stored the record object correctly.
- HCP stores the cryptographic hash value as metadata for each record object and subsequently uses the hash value for post-recording, periodic quality and integrity checks and for automated record object repair.

Post-Recording Verification Process:

- During retrieval of a record object, HCP recalculates the hash value for the record object 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 object from a local copy or replica. If the recovery methods are unsuccessful, HCP sends an error message to the source application 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.

2.2.4 Additional Considerations

Cohasset recommends that the integrity of each record object transmitted from the source application to HCP be validated, whereby the source application will calculate a hash value of the record object 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 application to determine if HCP correctly received and stored the record object.

2.3 Serialize the Original and Duplicate Units of Storage Media

2.3.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(C)]

This requirement, according to Section III(B) of the SEC's 2001 Interpretive Release, *"is intended to ensure both the accuracy and accessibility of the records by indicating the order in which records are stored, thereby making specific records easier to locate and authenticating the storage process."*

SEC 17a-4(f)(2)(ii)(C): Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media.

When the SEC Rule was issued in 1997, this requirement was thought to be more pertinent to tracking the individual units of removable media related to micrographic or optical storage. This requirement for non-unitized electronic storage may be satisfied by capturing and storing immutable metadata, associated with each electronic record, to *uniquely* identify the record and the *date and time of recording*.

2.3.2 Compliance Assessment

It is Cohasset's opinion that HCP meets this SEC requirement to serialize the original and duplicate records.

2.3.3 HCP Capabilities

- HCP requires the source application to submit a name with each record object being created, that uniquely identifies it within the tenant. The object's name is retained as immutable metadata for the record object.
  - If a record object is created with a name that is already stored in the tenant, then the record object is not stored, and an error message is returned to the source application.
- During the write process, HCP assigns a unique global identifier to the record object, which is stored as immutable metadata for the record object.
- The date and time each record object is stored to the HCP namespace is recorded as the create date/time in the system metadata.
- The combination of (a) unique object name sent with a storage request, (b) unique HCP global identifier, and (c) create date/time stored with the system metadata represent a serialization of the record object in both space and time.

2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

2.4 Capacity to Download Indexes and Records

2.4.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(D)]

This requirement necessitates an adequate capacity to readily download records and associated indexes, in a format and on a medium acceptable under the Rule and as specified by the SEC or self-regulatory organization. This allows the SEC or self-regulatory organizations to take possession of the downloaded records and indexes.

SEC 17a-4(f)(2)(ii)(D): Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.

2.4.2 Compliance Assessment

It is Cohasset's opinion that HCP meets this SEC requirement to readily download records and indexes (metadata attributes), 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 support the capacity to search and download record objects and metadata (index) attributes:

- *HCP search console* is a web application that utilizes a *metadata query engine* to query namespace contents. *(Note: the query engine is also available for use separately, as an API.)* Alternatively, the HCP search console can be configured to use the Hitachi Data Discovery Suite (HDDS) query engine, which is a separate query product that is not part of HCP, but which offers enhanced search capabilities.
  - Searching must be enabled for the namespace, which causes the query engine to create and maintain an index of objects contained within a namespace. 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 namespace, 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**: 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**: Provides the ability to combine different search criteria and operators to further refine search results.
  - A list of objects matching the search criteria is 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 object metadata, depending on the search performed. A maximum of 102,000 search results may be included in the export.
- *HCP browser* is a web application that may be used to (1) list directories within the namespace, (2) view a list of all objects contained within a directory including metadata such as record object name, storage date, *Retention Class*, etc., and (3) view and/or retrieve objects. The HCP browser application downloads object data and opens 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.
- *HCP data migrator* is a utility that, among other operations, copies record objects between two locations in a single namespace or a local file system, where local application capabilities may be used to view, reproduce or transfer the record objects to a medium acceptable under the Rule.
- Industry Standard Protocols, such as Hitachi's API for Amazon S3 (Amazon S3-compliant API), HTTP/REST, SMTP, NFSv4, CIFS, and WebDAV, may be used in lieu of the HCP search console or HCP browser, to programmatically search for and export selected record objects. Once the record objects have been retrieved,

local application capabilities may be used to view, reproduce or transfer the record objects to a medium acceptable under the Rule.

- Hitachi Content Intelligence is a separate data discovery and transformation product that may be used to execute HCP content searches. Hitachi Content Intelligence extracts content from both Hitachi and third-party repositories, whether located on-premises or in the cloud, unifies, classifies and categorizes the content, then makes it available from a central user interface. Advanced search capabilities are provided to search for, view and reproduce record objects. Once identified, selected record objects may be transferred to a medium acceptable under the Rule.

2.4.4 Additional Considerations

The regulated entity is responsible for (a) assuring that hardware and software capacity allows for ready access to the record objects and metadata (index) attributes and that the appropriate data protection level has been established within the HCP system, (b) maintaining its HCP licensing in good standing, (c) authorizing necessary user access, and (d) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the record objects and metadata (index) attributes, in the requested format and medium.

2.5 Duplicate Copy of the Records Stored Separately

2.5.1 Compliance Requirement [SEC 17a-4(f)(3)(iii)]

The intent of this requirement is to provide an alternate source for accessing the records, should the primary source be compromised, i.e., lost or damaged.

> **SEC 17a-4(f)(3)(iii):** Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required.

Note: A *duplicate copy* is defined as a persistent copy that allows the complete and accurate record to be reestablished from data stored on a compliant storage system or medium. Whereas, a *backup copy* is defined as a non-persistent copy that is overwritten as it is *rotated* on a periodic basis, resulting in a much shorter retention period than the original.

2.5.2 Compliance Assessment

Cohasset affirms that HCP meets this SEC requirement for a persistent duplicate copy of the record objects when properly configured, as described in Section 2.5.3.

2.5.3 HCP Capabilities

There are three primary options for meeting the conditions of this requirement to separately store a duplicate copy:

- When configured with a S series node, erasure coding is utilized, which stores segments of the record object across multiple disks. This assures that a replica can be accurately regenerated from the erasure coded data should an error occur in one segment of the data.
  - The erasure coded data segments are retained for the full retention period and any applied Legal Holds.

- The Data Protection Level (DPL) of a namespace 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 object be in error or not be available, the record object can be accessed from the duplicate. The record object in error can then be restored from the duplicate. HCP automatically generates duplicates, as defined for the namespace, to ensure that the required number of duplicates is maintained.
- Multiple HCP systems 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 namespace in *compliance mode*, where a duplicate of each record object and associated metadata can be asynchronously recorded. Should one HCP namespace become inaccessible, the record object can then be retrieved from a duplicate stored on another system. A record object found in error on one HCP *compliance mode* system can be restored from a replica.

2.5.4 Additional Considerations

Additionally, record objects may be tiered to another storage location, such as HCP S series node, Amazon S3 or Microsoft Azure; however, these tiered copies are for operational use and are only compliant with the Rule when SEC-compliant protections are separately applied to the tiered storage location.

2.6 Audit System

2.6.1 Compliance Requirement [SEC 17a-4(f)(3)(v)]

Meeting this provision requires an audit system which provides accountability (e.g., when, by whom and what action was taken) for both initially inputting and tracking changes made to the original and duplicate records and associated retention metadata.

> **SEC 17a-4(f)(3)(v):** The member, broker, or dealer 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 and 240.17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

2.6.2 Compliance Assessment

Cohasset asserts that HCP meets this SEC requirement for an audit system.

2.6.3 HCP Capabilities

- The following record object compliance events are logged in HCP *internal access logs* and include the requesting IP address, username, date/time/time zone, full record object name, status code, size, namespace name, and tenant name:
  - Initial capture of record objects,
  - Assignment and extension of retention attributes,
  - Assignment or removal of Legal Holds,

- Deletion of eligible record objects (i.e., record objects with a retention expiration date in the past and no assigned legal hold attribute). Privileged delete actions, which are allowed only in namespaces in *enterprise mode*, are also captured in the *access log*.

- All Retention Class activity (i.e., add Retention Class, modify Retention Class) for a namespace is captured in the HCP's *tenant log* and includes the requesting user or service ID, date/time and description of the event. The *tenant log* is available via the tenant management console.

2.6.4 Additional Considerations

The regulated entity is responsible for retaining audit log activity (see Section 2.8, *Preservation of Audit Results*).

2.7 Availability of Audit System for Examination

2.7.1 Compliance Requirement [SEC 17a-4(f)(3)(v)(A)]

The intent of this requirement is to ensure that the audit trail is available for examination, upon request, by the SEC or self-regulatory organizations.

> **SEC 17a-4(f)(3)(v)(A):** At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.

2.7.2 Compliance Assessment

Cohasset asserts that HCP supports this SEC requirement to make the audit system available to the regulated entity for submission to the SEC or self-regulatory organization.

2.7.3 HCP Capabilities

- *Tenant log* events can be viewed via the HCP tenant management console. Events are displayed in reverse chronological order and may be viewed in summary or expanded (detail) mode.

- A list of *internal access log* events can be generated for download in a single .zip file. Authorized administrators can filter the events by date range to minimize the scope/size of the download, thereby reducing the demand on the HCP system.

- 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.

2.7.4 Additional Considerations

- The regulated entity is responsible for (a) capturing audit trail activity in HCP (see Section 2.8., Preservation of Audit Results), (b) conducting searches to locate requested audit trail data, (c) printing, downloading or otherwise producing audit trail data, in the requested format and medium, and (d) providing the produced audit trail data to the regulator, self-regulatory organization or designated examining authority.

2.8 Preservation of Audit Results

2.8.1 Compliance Requirement [SEC 17a-4(f)(3)(v)(B)]

It is the intent of this requirement to ensure that the audit trail information is preserved for the same period of time as the associated records.

SEC 17a-4(f)(3)(v)(B): The audit results must be preserved for the time required for the audited records.

2.8.2 Compliance Assessment

Cohasset asserts that HCP meets this SEC requirement to retain the audit results for the same time period as the audited records.

2.8.3 HCP Capabilities

- Record object-level compliance events retained in the *internal access log* are retained for 90 days by default. To meet the requirement for preserving audit trail entries for the same period of time as the associated records, the regulated entity may either:
  - Extend the retention duration longer than the default, which requires a service call to HCP, or,
  - Export the *internal access log* data to the regulated entity's internal (non-HCP) security information event management tool, and then use that tool and data to retain the audit trail events for the required retention period.
- Tenant-level compliance events logs (i.e., events related to Retention Classes) are retained on HCP permanently.

2.8.4 Additional Considerations

The regulated entity is responsible for either: (a) extending the default duration for the access log through HCP service, or (b) exporting access log events from HCP, during the period of time they are available, and storing the audit log for the required retention period.

3 | Summary Assessment of Compliance with MiFID II Durable Medium Requirements for Recordkeeping

The objective of this section is to document Cohasset's assessment of the capabilities of HCP, as described in Section 1.3, *HCP Overview and Assessment Scope*, in comparison to the MiFID II requirements.

The concept of durable medium, as an alternative to paper, was first introduced in the European Union on May 20, 1997, in the *Distance Selling Directive 97/7/EC*. Since 1997, many EU regulations have adopted the concept of durable medium. The definition of durable medium recognizes the evolution of technology and the interests of both customers and service providers to have the ability to transition from paper to electronic storage.

The MiFID II definition of durable medium focuses on storability, accessibility, retention and immutable reproduction:

> *(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]

MiFID II was further supplemented by *Commission Delegated Regulation (EU) 2017/565*. Article 72(1) specifies recordkeeping practices for the retention of records:

> *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.*

Both the EU definition of durable medium and the above paragraph (e) recognize the technology evolution and defines requirements or conditions for regulated entities that retain records electronically. The approach is consistent with the SEC, which also set forth standards that the electronic storage media must satisfy to be considered acceptable.

Cohasset has leveraged its assessment of the capabilities of HCP, as described in Section 2 and correlated HCP, in *compliance mode*, to the requirements for (a) *durable medium* in MiFID II and (b) retention of records in the *Delegated Regulation,* which supplements MiFID II. For each of the four requirements, which are highlighted in the light blue rows, the following table summarizes the results of Cohasset's analysis:

- The two left-hand columns list key requirements specified in (a) the definition of *durable medium* in MiFID II and (b) the retention of records in the *Delegated Regulation*, which supplements MiFID II, respectively. The focal element for each row is underlined for clarity.
- The right-hand column provides Cohasset's compliance assessment and an analysis of capabilities of HCP, relative to these requirements.

Regulatory excerpts that are pertinent to each of the four specific requirements		Compliance Assessment and Analysis of HCP, in compliance mode, Relative to the MiFID II *Directive* and the Supplementing *Delegated Regulation*
***Directive 2014/65/EU* (MiFID II) Article 4(1)(62)**	***Commission Delegated Regulation (EU) 2017/565, Article 72(1),* which supplements MIFID II**	
Requirement #1: **Store record for the required retention period**		
(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 ***** [emphasis added]	(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: ***** [emphasis added]	While this requirement pertains to the client of the regulated entity, the regulated entity itself would have a similar need to store the record for the required retention period. It is Cohasset's opinion that HCP, when configured in *compliance mode*. has features that apply a retention period to a record object and its core metadata, as described in **Section 2.1 *Non-Rewriteable, Non-Erasable Record Format***. The associated integrated control codes: ● Disable all write permissions for the content of the object, thus protecting it against modification or overwrite for the specified retention period. ● Prohibit deletion, through any mechanism, until the assigned retention period expires and any Legal Holds are removed. ● Prohibit the shortening of the retention period assigned to the record object. ● Prohibit the deletion or renaming of a directory containing one or more record objects. Further, HCP in *compliance mode* assures the accurate recording (storage) of the record content and associated metadata, as explained in **Section 2.2 *Accurate Recording Process***. The quality and accuracy of the recording process is verified: (a) during the initial recording of the object record; (b) using post-recording verification during read-back; and, (c) by conducting periodic consistency and integrity checking.

Regulatory excerpts that are pertinent to each of the four specific requirements		Compliance Assessment and Analysis of HCP, in compliance mode, Relative to the MiFID II *Directive* and the Supplementing *Delegated Regulation*
***Directive 2014/65/EU* (MiFID II) Article 4(1)(62)**	***Commission Delegated Regulation (EU) 2017/565, Article 72(1),* which supplements MIFID II**	
Requirement #2: **Assure immutable record content**		
(62) 'durable medium' means any instrument which: ***** (b) allows the unchanged reproduction of the information stored [emphasis added]	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: ***** (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; ***** [emphasis added]	It is Cohasset's opinion that the features of HCP in *compliance mode* to achieve non-rewriteable, non-erasable storage meet this requirement to assure that record content is unchangeable. See **Section 2.1 Non-Rewriteable, Non-Erasable Record Format** for additional information. If the regulated entity corrects or amends a record, it must store each rendition as a separate record object. The features for assuring a non-rewriteable, non-erasable format assure that the original record is not modified. Further, HCP in *compliance mode* stores a cryptographic hash value for each record object during the recording process and subsequently uses it for post-recording quality and integrity checks and for automated record object repair, as described in **Section 2.2 Accurate Recording Process.**
Requirement #3: **Provide access to and reproduce the stored records**		
(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 (b) allows the unchanged reproduction of the information stored [emphasis added]	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; ***** (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 ***** [emphasis added]	Cohasset asserts that HCP in *compliance mode* provides three methods of retrieving records: 1. HCP search console 2. HCP browser, which is a web application 3. Industry Standard Protocols may be used in lieu of the HCP search console or HCP browser The selected records may be downloaded and local capabilities may be used to view or print the records. See ***Section 2.4 Capacity to Download Indexes and Records*** for additional information. Further, HCP ensures that records are readily available by storing a duplicate copy of each record on different nodes during the initial recording process and/or by configuring replication to a second, equivalently configured HCP system. See ***Section 2.5 Duplicate Copy of the Records Stored Separately*** for additional information.

Regulatory excerpts that are pertinent to each of the four specific requirements		Compliance Assessment and Analysis of HCP, in compliance mode, Relative to the MiFID II *Directive* and the Supplementing *Delegated Regulation*
***Directive 2014/65/EU* (MiFID II) Article 4(1)(62)**	***Commission Delegated Regulation (EU) 2017/565, Article 72(1),* which supplements MIFID II**	
Requirement #4: **Provide access to and reproduce the stored records**		
N/A	*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:* ***** *(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used.* ***** [emphasis added]	Cohasset asserts that HCP provides three methods of retrieving and then exporting record objects: 1. HCP search console can be used to export a list of record objects as a comma-separated-values (CSV) or XML file. 2. HCP browser, which is a web application, can be used to export and save the record objects. 3. Industry Standard Protocols may be used to export selected record objects. The selected records may be exported and local capabilities may be used to view, reproduce or transfer the record objects to another medium. See ***Section 2.4 Capacity to Download Indexes and Records*** for additional information. As may be required, the regulated entity may transfer records to other media or migrate record objects to new file formats, in advance of technological obsolescence.

The focus of this assessment pertains to namespaces configured to utilize *compliance mode* retention features, which are highly restrictive and assure that the storage solution applies controls to (a) protect the immutability of the record content and certain metadata and (b) prevent deletion over the applied retention period.

In this section, Cohasset correlates the *compliance mode* capabilities to the durable medium definition in MiFID II and retention of records requirements in Article 72(1) of the Delegated Regulation. Additionally, Cohasset contends that namespaces configured to utilize *enterprise mode* retention features meet the MiFID II and EU durable medium requirements, *when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be changed or deleted prior to expiration of the retention period*. This less restrictive *enterprise mode* provides flexibility to shorten retention periods, which may be beneficial for compliance with privacy and data protection requirements.

4 | Conclusions

Cohasset assessed the capabilities of HCP in *compliance mode*, in comparison to the five requirements related to recording and non-rewriteable / non-erasable storage of record objects and associated metadata and the three audit system requirements, set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. (See Section 1.3, *HCP Overview and Assessment Scope*.)

Cohasset determined that HCP, when properly configured, has the following capabilities, which meet the regulatory requirements:

- Maintains record objects and immutable record object metadata in a non-rewriteable, non-erasable format for time-based and event-based retention periods and any applied Legal Hold.
- Prohibits deletion of a record object and its immutable metadata until the retention period for the record object, and any Legal Hold on the Bucket, has expired.
- Verifies the accuracy and quality of the recording process through cryptographic hash values and HCP validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- Uniquely serializes each record object and duplicate copies with an object ID and a date/time stamp.
- Synchronously records a minimum of two (and up to four) duplicates of each record object on separate local storage nodes, which allows for automatic recovery of record objects that become lost or damaged. Additionally, supports a replication topology for asynchronous, geographically dispersed replication of record objects.
- Provides the capacity and tools to (a) search for record objects, (b) list the object names, and (c) download the record objects and associated metadata attributes for a browser or other local tool to render as a human-readable image.
- Captures and preserves an audit log for all compliance-related events for at least the same period as the record objects. Additionally, HCP provides the ability to export compliance events from the HCP audit system for storage in other non-HCP security information event management solutions.

In Section 3, Cohasset correlates the assessed capabilities of HCP, in *compliance mode,* to the *durable medium* definition in MiFID II and retention of records requirements in Article 72(1) of the *Delegated Regulation*. Further, Cohasset contends that namespaces configured to utilize *enterprise mode* retention features meet the MiFID II and EU requirements, *when the regulated entity applies appropriate procedural controls to oversee operations that allow changes or deletion prior to expiration of the retention period*.

Accordingly, Cohasset concludes that HCP, when properly configured, meets the five requirements related to recording and non-rewriteable / non-erasable storage of electronic records as well as the three requirements for an audit system, as specified in SEC Rule 17a-4(f) and FINRA Rule 4511(c). In addition, the assessed capabilities meet the requirements defined in the MiFID II Directive and the supplementing Delegated Regulation.

5 | Overview of Relevant Regulatory 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 allowing electronic records to be retained on a variety of compliant electronic storage media.

5.1 Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements

Recordkeeping requirements for the securities broker-dealer industry are stipulated by the United States Securities and Exchange Commission (SEC) Regulations, including 17 CFR §§ 240.17a-3 and 240.17a-4. Specifically, SEC Rule 17a-4(f), when adopted on February 12, 1997, expressly allow books and records to be retained on electronic storage media, subject to meeting certain conditions.

Three separate foundational documents collectively define and interpret the specific regulatory requirements that must be met for an electronic storage system to be compliant with SEC Rule 17a-4(f). These are:

- The Rule itself, as modified over time by the SEC. These modifications to the original Rule have not affected the requirements for electronic storage media, which are the basis of this assessment. However, certain Interpretive Releases have clarified the context and meaning of certain requirements and conditions of the Rule.
- SEC Interpretive Release No. 34-44238, *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)*, dated May 1, 2001 (the 2001 Interpretive Release).
- SEC Interpretive Release No. 34-47806, *Electronic Storage of Broker-Dealer Records*, dated May 7, 2003 (the 2003 Interpretive Release).

In the Rule and in the two subsequent interpretative releases, the SEC authorizes the use of electronic storage media and devices to satisfy the recordkeeping requirements of SEC Rules 17a-3 and 17a-4, when the system delivers the prescribed functionality. Specifically, SEC Rule 17a-4(f)(1)(ii) states:

> *(f) The records required to be maintained and preserved pursuant to §§ 240.17a-3 and 240.17a-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form.*
> *(1) For purposes of this section:*
> *(ii) The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(1)(i) and (f)(1)(ii) of this section, that meets the applicable conditions set forth in this paragraph (f).* [emphasis added]

The February 12, 1997, Federal Register issued the final rule allowing broker-dealers to use electronic storage media. When issuing the rule, the SEC recognized that technology evolves; and, it set forth standards that the

electronic storage media must satisfy, rather than prescribing specific technology, as specified in the following excerpts:

> ***SUMMARY:*** *The Securities and Exchange Commission ("Commission") is amending its broker-dealer record preservation rule to allow broker-dealers to employ, under certain conditions, electronic storage media to maintain records required to be retained. The amendments reflect a recognition of technological developments that will provide economic as well as time-saving advantages for broker-dealers by expanding the scope of recordkeeping options while at the same time continuing to require broker-dealers to maintain records in a manner that preserves their integrity. The Commission is also issuing an interpretation of its record preservation rule relating to the treatment of electronically generated communications.*
> ***
> ***II. Description of Rule Amendments***
> ***A. Scope of Permissible Electronic Storage Media***
> ****The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4. Specifically, because optical tape, CD–ROM, and certain other methods of electronic storage are available in WORM and can provide the same safeguards against data manipulation and erasure that optical disk provides, the final rule clarifies that broker-dealers may employ any electronic storage media that meets the conditions set forth in the final rule.*[9] [emphasis added]

The 2003 Interpretive Release further clarifies that implementation of rewriteable and erasable media, such as magnetic tape or magnetic disk, meets the requirements of a non-rewriteable, non-erasable recording environment, if the system delivers the prescribed functionality and appropriate **integrated control codes** are in place. The 2003 Interpretive Release states:

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) 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.* [emphasis added]

The key words within this statement are '*integrated*' and '*control codes*'. The term '*integrated*' means that the method used to achieve a non-rewriteable, non-erasable recording environment must be an integral part of the recording hardware and software. The term '*control codes*' indicates the acceptability of using attribute codes (metadata), which are integral to the hardware and software of the recording process, to protect against overwriting or erasure of any records.

Examples of integrated control codes relevant to a non-rewriteable, non-erasable recording process are:

- A retention period during which the record cannot be erased, overwritten or otherwise modified;
- A unique record identifier that differentiates each record from all other records; and
- The date and time of recording, which in combination with the unique identifier "serializes" the record.

[9] Exchange Act Release No. 38245 (Feb. 5, 1997), 62 FR 6469 (Feb. 12, 1997) ("Adopting Release").

The 2003 Interpretive Release specifically notes that recording processes or applications which merely mitigate the risk of overwrite or erasure (rather than prevent them), such as relying solely on access control security, will not satisfy the requirements of SEC Rule 17a-4(f).

Further, the 2003 Interpretive Release requires the storage system to be capable of retaining records beyond the SEC-established retention period, when required by a subpoena, legal hold or other similar circumstances. In *Section IV. Discussion*, the 2003 Interpretive Release states:

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, 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.* [emphasis added]

An important associated requirement of SEC Rule 17a-4(f)(2)(i) is that a member, broker or dealer electing to electronically store its records required by SEC Rules 17a-3 or 17a-4, must notify its designated examining authority at least ninety (90) days prior to employing any technology other than write-once read-many (WORM) optical media. Examining authorities are self-regulatory organizations (SROs) or designated examining authorities (DEAs) under the jurisdiction of the SEC, such as the Financial Industry Regulatory Authority (FINRA).

See Section 2, *Assessment of Compliance with SEC Rule 17a-4(f),* for a list of the *five* SEC requirements relevant to the recording and non-rewriteable / non-erasable storage of electronic records and the *three* audit system requirements, together with a description of the capabilities of HCP related to each requirement.

5.2 Overview of FINRA Rule 4511(c) Electronic Records Storage Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to SEC Rule 17a-4(f), by stipulating:

> *(c) 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.*

5.3 Overview of MiFID II Durable Medium Requirements for Recordkeeping

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]

The concept of *durable medium* was first introduced on 20 May 1997 in the *Distance Selling Directive 97/7/ EC* as an alternative to paper as the support or medium for information. Since 1997, various European Union (EU) regulatory provisions require that a firm must provide certain information to a client in writing, either on paper or in another *durable medium*. Examples include, but not limited to:

- *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC*, Article 4(35)
- *Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast),* Article 2(1)(18)
- *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*, Article 3(1)
- *Commission Directive 2010/42/EU of 1 July 2010 implementing Directive 2009/65/EC of the European Parliament and of the Council as regards certain provisions concerning fund mergers, master-feeder structures and notification procedure,* Article 7

Further, with the implementation of the revised MiFID II, investment firms must arrange for records to be kept of 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 *Delegated Regulation,* supplementing MiFID II, defines record keeping and recording requirements, in Section 8, *Record-keeping*, Article 72, *Retention of records*, paragraph 1, which 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.*

See Section 3, *Summary Assessment of Compliance with MiFID II Durable Medium Requirements for Recordkeeping* for a summary assessment of the capabilities of HCP in relation to requirements for (a) *durable medium* in MiFID II and (b) retention of records in the *Delegated Regulation,* which supplements MiFID II.

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is recognized as a leading professional consulting firm, specializing in records management and information governance. Drawing on more than forty 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, engaging in implementation activities to promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

Cohasset has been 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.

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 assists with the implementation of information lifecycle practices that avoid the cost and risk associated with over-retention*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

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.