Cohasset Associates

Broadcom© CA 1™ Flexible Storage™

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

Broadcom© CA 1™ Flexible Storage™ stores, controls, and protects z/OS tape data sets and volumes. Storing archival records with retention and *Immutable* controls applied is designed to meet securities industry requirements for preserving records in non-rewriteable, non-erasable format for the applied retention period.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of CA 1 Flexible Storage (see Section 1.3, *CA 1 Flexible Storage Overview and Assessment Scope*) relative to the electronic records requirements, specified by multiple regulatory bodies, as follows:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)(2);
- SEC in 17 CFR § 240.18a-6(e)(2);
- Financial Industry Regulatory Authority (FINRA) in Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f); and
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d); 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 CA 1 Flexible Storage, when retention and *Immutable* controls are properly applied, has functionality that meets the requirements for electronic records set forth in the above Rules and supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3) and 18a-6(e)(3).

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.

March 2024

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

+1.312.527.1550 | www.cohasset.com

Table of Contents

1 • Introduction

Regulators, worldwide, establish explicit requirements for certain regulated entities that elect to electronically retain books and records. Given the prevalence of electronic books and records, these requirements apply to most broker-dealers, commodity futures trading firms and similarly regulated organizations.

This Introduction *summarizes the regulatory environment pertaining to this assessment and the purpose and approach for Cohasset's assessment. It also provides an overview of Broadcom* CA 1 *Flexible Storage and the assessment scope.*

1.1 Overview of the Regulatory Requirements

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

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

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 CA 1 Flexible Storage for preserving required electronic records, Broadcom 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.

Broadcom engaged Cohasset to:

- Assess the functionality of CA 1 Flexible Storage, in comparison to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and describe features that support the regulated entity in its compliance with SEC Rules 17a-4(f)(3) and 18a-6(e)(3); see Section 2, *Assessment of 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 CA 1 Flexible Storage; 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 CA 1 Flexible Storage; 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 CA 1 Flexible Storage and its functionality or other Broadcom 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 Broadcom 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 CA 1 Flexible Storage Overview and Assessment Scope

1.3.1 CA 1 Flexible Storage Overview

CA 1 Flexible Storage stores, controls, and protects z/OS tape data sets and volumes. It automates tape management tasks to enable storage data integrity, while protecting against the inadvertent destruction of Virtual Volumes, which are referred to as archival records[6] in this report. CA 1 Flexible Storage provides comprehensive tape library inventory and audit tracking, including offsite vaults and utilities for controlling tape and catalog maintenance activities. CA 1 Flexible Storage includes the capability to replicate the Tape Management Catalog (TMC) from one system or location to one or more remote active data centers by utilizing the replicated copy at a remote location.

The logical architecture of CA 1 Flexible Storage is depicted in Figure 1 and summarized as follows:

- **Host** is an IBM Z mainframe running z/OS.
- **Tape Management System (TMS)** provides retention protection for data sets, manages the Scratch Pool, verifies system integrity, provides reporting and auditing, and manages the library.
  - **Retention Data Set (RDS)** is a sequential file containing data set names and user-defined retention periods or expiration dates. The RDS is used to provide retention criteria for tape data sets created

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

without job control language (JCL) supplied by RETPD (Retention Period) EXPDT (Expiration Date) or ACCODE (Access Code) values.

- **Tape Management Catalog (TMC)** is the main database for CA 1 Flexible Storage. The TMC inventories and tracks all files in each Virtual Volume controlled by CA 1 Flexible Storage.
- **Vtape Virtual Volumes** may store backups, data, files, and objects, thus throughout this report, Cohasset uses the term archival records to encompass these different types, with each Virtual Volume housing an accumulation of distinct required archival records.

- **Connected storage** may be either (1) Storage Direct Access Storage Devices (DASD) or (2) Amazon S3 and may store backups, data, files, and objects. Throughout this report, Cohasset uses the term archival records to encompass these different types of records, with each archival record stored in a Virtual Volume and housing an accumulation of distinct required records.
- **Vantage GUI** is a graphical user interface search and reporting tool, which is an extra installation included with the CA 1 Flexible Storage license.

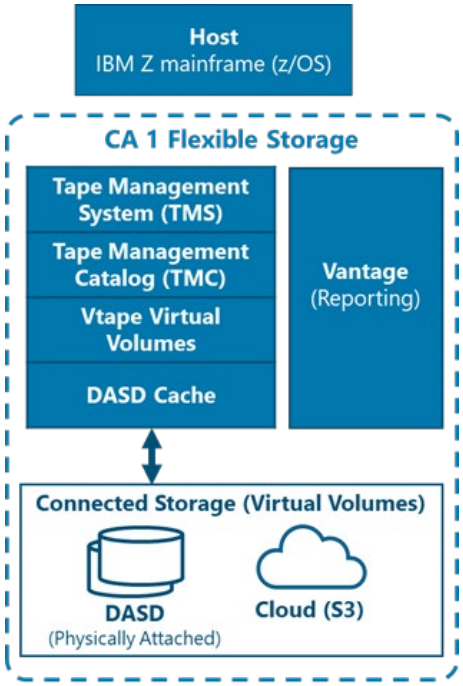

Figure 1: Logical Architecture

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related capabilities of CA 1 Flexible Storage, Release 15.0, when the (a) *Immutable* feature is appropriately configured and (b) the *Expiration Date* applies an appropriate retention control. When properly configured, these features are designed to meet the requirements for SEC Rules 17a-4(f)(2) and18a-6(e)(2), to preserve archival records as non-rewriteable, non-erasable for the required retention period.

Notes:

(1) The *Immutable* feature is only applicable for CA Vtape; therefore, the CA Vtape system must be the virtual tape system used for compliance with the Rule.

(2) When using a cloud provider for storage, this Compliance Assessment Report only evaluates the Amazon S3 cloud service, when retention controls are aligned with CA 1 Flexible Storage., Other cloud providers and configurations are outside the scope of this assessment, since retention is not aligned with CA 1 Flexible Storage.

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

This section presents Cohasset's assessment of the functionality of Broadcom CA 1 Flexible Storage, for compliance with the electronic recordkeeping system requirements promulgated in SEC Rules 17a-4(f)(2) and 18a-6(e)(2), as well as describes how the solution supports the regulated entity in meeting the requirements of SEC Rules 17a-4(f)(3) and 18a-6(e)(3).

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

- ***Compliance Requirement*** – Excerpt of relevant regulatory requirement in SEC Rules 17a-4(f) and 18a-6(e) and Cohasset's interpretation of the specific requirement
  - Both SEC Rules 17a-4(f) and 18a-6(e) are addressed in this section, since the electronic recordkeeping system requirements (principles, controls and testable outcomes) are the same, though the Rules specify their respective regulations and regulators and include semantic differences.
- ***Compliance Assessment*** – Summary statement assessing compliance of CA 1 Flexible Storage
- ***CA 1 Flexible Storage Capabilities*** – Description of assessed functionality
- ***Additional Considerations*** – Additional clarification related to meeting the specific requirement

The following sections document Cohasset's assessment of the capabilities of CA 1 Flexible Storage, as described in Section 1.3, *CA 1 Flexible Storage 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.*[7] [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.*[8] [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed CA 1 Flexible Storage 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 CA 1 Flexible Storage, with the features and controls described in Sections 2.2 through 2.6 of this report.

Reminder: This requirement is an alternative to the non-rewriteable, non-erasable record format requirement (i.e., write-once, read-many or WORM requirement), which is assessed in Section 2.2.

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

SEC 17a-4(f)(2)(i)(B) and 18a-6(e)(2)(i)(B):
Preserve the records exclusively in a non-rewriteable, non-erasable format

This regulatory requirement was first adopted in 1997. In the 2022 Rule amendments, regulated entities are allowed to use a combination of electronic recordkeeping systems, to comply with each system meeting either (a) the non-rewriteable, non-erasable record format requirement described in this section or (b) the complete time-stamped record audit-trail requirement described in Section 2.1, *Record and Audit-Trail*.

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

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

7 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

8 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

> *a process of integrated software and hardware codes and clarified that "a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule."*
> *****
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.*[9] [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.*[10] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of CA 1 Flexible Storage, with retention and *Immutable* controls applied to Virtual Volumes containing archival records, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[11] and event-based[12] retention periods, when (a) properly configured, as described in Section 2.2.3 and (b) the considerations described in Section 2.2.4 are satisfied.

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

2.2.3 CA 1 Flexible Storage Capabilities

This section describes the functionality of CA 1 Flexible Storage 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.

2.2.3.1 Overview

CA 1 Flexible Storage, utilizes Vtape Virtual Volumes (Virtual Volumes) to store archival records, which are an accumulation of distinct required records. CA 1 Flexible Storage offers retention controls and an *Immutable* feature, a highly-restrictive option, which provides both overwrite protection and stricter retention controls.

---

9 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

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

12 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.

The following table summarizes the controls resulting from applying retention and *Immutable* controls. See the subsections below the following table, for information on how to apply the retention and *Immutable* features and details about the resulting integrated controls.

	Archival Records when Retention and *Immutable* controls are applied
Retention controls	For time-based retention, an *Expiration Date* applies the retention controls to archival records by defining the date when a Virtual Volume can be moved to Scratch[13] (i.e., is eligible for deletion). When an *Expiration Date* is applied to a volume: ● The volume cannot be moved to Scratch until the *Expiration Date* is in the past. ● The *Expiration Date* of the volume may be delayed (deferred to a later date) but cannot be expedited or removed. For event-based retention, either "catalog control" or "EDM controlled" retention controls may be applied for the initial retention until the event or condition occurs; thereafter, the Virtual Volume is uncatalogued, which sends the Virtual Volume to Scratch where it is held for the duration of the preconfigured *Immutable-Hold* time period. During the *Immutable-Hold* the Virtual Volume may be moved from Scratch and a time-based retention period manually applied to the Virtual Volume.
Immutability	The *Immutable* feature sets a Virtual Volume to the *Immutable* state when the volume is dismounted. ● While in the *Immutable* state, the volume is read-only, which assures that: ○ New files cannot be appended to the volume. ○ Volume contents cannot be modified or deleted. ● The *Immutable* state and read-only controls apply to the volume even if CA 1 Flexible Storage is shutdown or removed. ● The *Immutable* state and read-only controls expire only after the volume is moved to Scratch, which is allowed only after the *Expiration Date* is in the past. (See the *Retention controls* row, above.)
Legal Holds (Temporary Holds)	The *Expiration Date,* as described in the *Retention controls* row, may be delayed on volumes that are subject to the hold.

2.2.3.2 Record Definition and Retention and *Immutable* Controls

CA 1 Flexible Storage is divided into Virtual Volumes which contain archival records that house an accumulation of distinct required records. Specifically, each Virtual Volume is considered a separate record and is comprised of:

- The complete content of the archival record, which is an accumulation of distinct required records, each with its attributable metadata. This content is stored immutably until the *Expiration Date* is in the past, when the contents become mutable.
- Immutable attributes, including unique VOLSER (volume serial number), file name and creation/storage timestamp.
- Mutable attributes, including *Expiration Date* and Scratch indicator.

These Virtual Volumes and associated archival records may be protected by applying retention and *Immutable* controls, described as follows.

[13] Scratch or a Scratch Pool describes Virtual Volumes that do not contain any data that needs to be retained, instead the Virtual Volumes are designated as available to be overwritten.

- Retention of Virtual Volumes and associated archival records is controlled by the volume *Expiration Date* stored in the Tape Management Catalog (TMC). A Virtual Volume cannot be moved to Scratch (i.e., made available for overwrite), until its *Expiration Date* is in the past.
- Setting an *Expiration Date* applies the retention control for an archival record by defining the date when a Virtual Volume can be moved to Scratch (i.e., is eligible for deletion).
  - The following two methods of assigning an *Expiration Date* for time-based retention are compliant with the Rule:
    1. The *Expiration Date* can be set using the JCL (job control language) and can be defined as either an:
       - Explicit Date (EXPDT), or
       - Retention Period (RETPD), which is converted and stored as an *Expiration Date*.
    2. If the *Expiration Date* is not specified in the JCL, the *Default Retention Period* (RP), if configured, is used to calculate and store the *Expiration Date*.
       - As noted above, the job submission timestamp may be different than the time the volume is created and stored.
       - The *Default Retention Period* must be defined on installation as an RP system option. A status indicator in the TMC reflects the assignment of the *Default Retention Period*.
       - The *Default Retention* values are stored in the Retention Data Set (RDS), which is a sequential file containing data set names and user-defined retention periods or expiration dates. The RDS is used to provide retention criteria for tape data sets created without JCL supplied retention values
  - For event-based retention, "Catalog-Control" and "EDM-Controlled" retention settings (LABEL=99000) are applied. When the retention event occurs (i.e., with the retention condition is met), either (1) the Virtual Volume is uncatalogued or (2) the volume is released from the owning EDM system. Either of these two actions sends the Virtual Volume to Scratch where it is held for the duration of the preconfigured *Immutable-Hold* time period. During the *Immutable-Hold* the Virtual Volume may be moved from Scratch and a time-based retention period manually applied to the Virtual Volume.
  - Other methods of setting retention (e.g., 88uuu, 90ddd, 99ccc, etc.) in the JCL are available, but they do not provide the ability to assign a strict *Expiration Date* to the volume; therefore, they are **not** compliant with the Rule.
  - The *Expiration Date* may be delayed using one of two manual methods: (1) file-by-file, or (2) volume-by-volume.
  - The *Expiration Date* cannot be expedited or removed. Any attempt to expedite an *Expiration Date* applied to a Virtual Volume will result in an error and the *Expiration Date* will not be changed.
- Further, when using the Amazon S3 cloud for storage, CA 1 Flexible Storage is "aligned," which means that CA 1 Flexible Storage sets and manages the Amazon S3 object retention by (1) setting Compliance mode and (2) applying and delaying an explicit Retain Until Date on each volume stored as an object in the Amazon S3

cloud service. Once the Compliance mode and Retain Until Date are set on the object, Amazon S3 features provide retention and immutability protections. See Cohasset's Amazon S3 Compliance Assessment Report for additional information.

- When using Amazon S3 for required records, the bucket must be manually configured with Bucket Lock enabled and versioning enabled. Note: CA 1 Flexible Storage does not create versions, though Amazon S3 requires versioning to be enabled.

- As described above, Retention controls are separately applied to each Virtual Volume and are based on either (a) the retention programmed in the JCL or (b) the system default retention.
- The following table describes the integrated retention controls that protect archival records, which house an accumulation of distinct required records, and record metadata by applying *Retention* and *Immutable* controls to the volume.

	Retention and *Immutable* controls applied to archival records
Protecting record content and associated metadata	● By design, Virtual Volumes, with the *Immutable* feature applied, are inherently read-only and cannot be overwritten or modified during their lifespan, even after they are moved to Scratch. Therefore, the archival record and the distinct records and associated metadata, stored as content of these Virtual Volumes, are protected from overwrite and modification for their lifespan. ● Specifically, the *Immutable* feature sets the Virtual Volume to *Immutable* upon dismount processing and applies the following controls: ○ If any file is marked *Immutable*, the volume itself will be marked as *Immutable* upon dismount processing. ○ An *Immutable* volume is set as read-only, which prevents new files from being appended to the volume and prevents modifications or deletion of volume contents. ○ The *Immutable* state and read-only controls apply to the volume even if CA 1 Flexible Storage is shutdown or removed. ○ The *Immutable* and read-only controls apply even after the volume is moved to Scratch, which is allowed only after the *Expiration Date* is in the past. (See the *Restricting deletion* row, below.) ● The *Immutable* feature cannot be removed from a Virtual Volume, once applied. ● The Virtual Volume's unique identifier (i.e., VOLSER and file sequence number) and timestamp are immutable for the lifespan of the volume and associated archival record. ● Mutable volume metadata includes the *Expiration Date*, which may be delayed (deferred to a later date) but not expedited (set to an earlier date).
Modifying or removing retention controls	● When retention controls (i.e., *Expiration Date* and *Immutable* feature) are assigned to a volume, the *Expiration Date* cannot be expedited (set to an earlier date) but may be delayed (deferred to a later date). ● When using Amazon S3 for cloud storage, the Object (i.e., volume) is aligned and managed by the TMS. The TMS sets Compliance mode and manages (i.e., sets and delays) the Amazon S3 Retain Until Date for the object. Refer to Cohasset's Amazon S3 Compliance Assessment Report for an explanation of the Amazon S3 compliance capabilities.
Modifying legal holds	● The *Expiration Date* may be extended, manually, for select files or volumes that are subject to the hold. ● See Section 2.2.3.3, *Legal Holds (Temporary Holds),* for additional information.

	Retention and *Immutable* controls applied to archival records
Restricting deletion	● Each volume is protected from deletion, by users or by lifecycle policies, until the volume is in Scratch ○ For time-based retention, the volume cannot be moved to Scratch until the *Expiration Date* is in the past. ○ For event-based retention, the volume cannot be moved to Scratch while it is under catalogue control or the volume is released from the owning EDM system. When the volume is uncatalogued or released, the Virtual Volume is sent to Scratch where it is held for the duration of the preconfigured *Immutable-Hold* time period. During the *Immutable-Hold* the Virtual Volume may be moved from Scratch and a time-based retention period manually applied to the Virtual Volume. ● A specific volume and its associated archival records, are eligibility for deletion (Scratch) only when the *Expiration Date* applied to the volume is in the past. ● Any attempt to delete a volume that is not eligible is rejected. ● See Section 2.2.3.4, *Deletion Controls*, for additional information.
Copying Virtual Volumes	● A Virtual Volume can be copied. ○ The creation timestamp of the copy of the Virtual Volume reflects the date and time that the copy operation was completed. ○ A separate and unique VOLSER (volume serial number) and file name are assigned to the copy.
Moving Virtual Volumes	● A Virtual Volume cannot be moved, it can only be copied.
Displaying retention controls	● To aid the user, the *Expiration Date* be viewed using either the command line for DASD storage or the Vantage GUI (graphical user interface) for either the cloud or DASD storage.
Accessing records	● To access the contents (archival records) stored within a volume, the volume needs to be restored. ● When the TMC is backed up, the VOLSER (volume serial number) of the backup tape is automatically recorded. If a restore is necessary, this VOLSER is checked against the tape mounted for the restore to assure that the most current backup tape is used. ● Also see Section 2.4, *Capacity to Download and Transfer Records and Location Information*.

2.2.3.3 Legal Holds (Temporary Holds)

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

- The *Expiration Date* may be delayed, manually, on files or volumes that are subject to the hold.
- If the initial extension of the *Expiration Date* is insufficient, the *Expiration Date* must continue being delayed to meet the Legal Hold timeframe.

2.2.3.4 Deletion Controls

- When the *Expiration Date* is in past, the volume is eligible to be Scratched, which is an automatic deletion, via TMS clean process, of the volume and associated archival records. TMSCLEAN reads the complete Tape Management Catalog (TMC) or specified ranges of volumes looking for eligible (expired) volumes and passes the VOLSERS to a subroutine, TMSSCR, that performs the Scratch process.
- When setting the *Immutable* feature, an *Immutable-Hold* may be applied, which will delay the deletion of the volume until the configured number of days has passed. The volume will be in the "Pending Scratch" state while on hold and may be removed from Pending Scratch and assigned a new *Expiration Date*.

- Volumes in an *Immutable-Hold* Status are uncatalogued and cannot be read.
- Once the assigned number of *Immutable-Hold* days has passed the volume and associated archival records will be Scratched and the Virtual Volume is eligible for re-use.

- When using Amazon S3 in aligned mode for storage, the TMS will notify Amazon S3 that the Object is eligible for deletion on Amazon S3. Note**:** On Amazon S3, a Virtual Volume is stored as an object.

2.2.3.5 Security

In addition to the stringent retention protection and management controls described above, CA 1 Flexible Storage provides the following security capabilities, which support the authenticity and reliability of the archival records.

- For user authentication and access control, CA 1 requires one of the following external security programs be installed: (1) IBM Resource Access Control Facility (RACF), (2) Broadcom Top Secret, or (3) Broadcom Access Control Facility (ACF2).
- Encryption for archival records and metadata include:
  - Secure Data Transfer using AES256 encryption.
  - AES256, as the data is stored, ensuring confidentiality of data-at-rest.

2.2.3.6 Clock Management

To meet the requirements of the Rule, Cohasset asserts that every system clock must synchronize to an external time server, e.g., a network time protocol (NTP) clock.

- For CA 1 Flexible Storage, clock management is performed by z/OS, which may be configured to synchronize with an external NTP server. The internal NTP servers tolerate minor discrepancies in time variance and auto resynchronize minor variations. Through procedural controls, the end users and system administrators must be prevented from accessing and manipulating the system clock. These controls prevent or correct inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of the volume and associated archival records.

2.2.4 Additional Considerations

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

- Enabling the *Immutable* feature for highly-restrictive retention controls, which prevents appending files to the volume, when closed, and prevents shortening the volume *Expiration Date*. Additionally, the host system and the tape management system must be configured to write required archival records only to properly configured Virtual Volumes.
- Assuring the retention controls apply the required *Expiration Date* to the volume. Important Note: Cohasset recommends configuring a system *Default Retention Period* (RP) to ensure an *Expiration Date* is applied to all archival records, even when one is not supplied in the JCL.

- When storing records requiring event-based[14] retention periods the regulated entity must ensure an *Expiration Date* is applied when the Virtual Volume is uncatalogued and while still in the *Immutable-Hold* state to ensure an appropriate time-based retention period.
- Maintaining procedural controls, when using cloud storage, to restrict the storage configuration to Amazon S3 to ensure appropriate retention controls are maintained for the archival records, since Amazon S3 is currently the only supported cloud option for CA 1 Flexible Storage to manage the retention controls.
- Assuring that any Amazon S3 Object Store used by CA 1 Flexible Storage, is configured with Bucket Lock enabled, versioning enabled. Additionally, an appropriate retention is set for each object.
- Delaying the *Expiration Date* to preserve the volume and associated archival records for legal matters, government investigations, external audits and similar circumstances.
- 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

SEC 17a-4(f)(2)(ii) and 18a-6(e)(2)(ii):
Verify automatically the completeness and accuracy of the processes for storing and retaining records electronically

The electronic recordkeeping system must automatically verify the completeness and accuracy of the processes for storing and retaining records electronically, to ensure that records read from the system are precisely the same as those that were captured.

This requirement includes both quality verification of the recording processes for storing records and post-recording verification processes for retaining complete and accurate records.

2.3.2 Compliance Assessment

Cohasset affirms that the functionality of CA 1 Flexible Storage meets this SEC requirement for complete and accurate recording of records and post-recording verification processes, when the considerations identified in Section 2.3.4 are satisfied.

2.3.3 CA 1 Flexible Storage Capabilities

The recording and post-recording verification processes of CA 1 Flexible Storage are described below.

2.3.3.1 Recording Process

- Encryption and compression may be used to ensure the accuracy of recording.
- During the recording process a series of checksums are created for use in ensuring ongoing data accuracy.

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

2.3.3.2 Post-Recording Verification Process

- In CA 1 Flexible Storage, when errors are encountered, RAID6[15] error correction is performed for complete and accurate recovery.
- When using encryption and compression, the file accuracy is verified based on the checksums created during recording. If an error is detected and Vtape made multiple copies, it will automatically fail-over to another copy. If Vtape only made a single copy to replicated direct-access storage device (DASD), a manual process is performed to recover from the replicated copy on DASD.

2.3.4 Additional Considerations

- The host (i.e., IBM Z mainframe) is responsible for storing the complete contents of the required records and CA 1 Flexible Storage validates the accuracy of the recording process.
- The regulated entity must use encryption and compression to ensure the accuracy of the recording process.
- Cohasset recommends creation of multiple copies on Vtape to facilitate the automatic fail-over should an error be encountered on retrieval.

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

SEC 17a-4(f)(2)(iv) and 18a-6(e)(2)(iv):
Have the capacity to readily download and transfer copies of a record and its audit-trail (if applicable) in both a human readable format and in a reasonably usable electronic format and to readily download and transfer the information needed to locate the electronic record, as required by the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity]

This requirement calls for an adequate capacity to readily download records and information needed to locate the record in both a:

- Human readable format that can be naturally read by an individual, and
- Reasonably usable electronic format that is compatible with commonly used systems for accessing and reading electronic records.

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

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

[15] 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. RAID 6 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.

2.4.2 Compliance Assessment

Cohasset asserts that the functionality of CA 1 Flexible Storage meets this SEC requirement to maintain capacity to readily download and transfer the records and information used to locate the records, when the considerations described in Section 2.4.4 are satisfied.

2.4.3 CA 1 Flexible Storage Capabilities

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

- The TMC keeps track of all the files on the volume.
  - Each archival record in CA 1 Flexible Storage is assigned a unique identifier or VOLSER (volume serial number) plus the file sequence number, which facilitates findability.
  - Further, the distinct records housed in the archival record includes both the contents of the record and associated metadata written by the host system.
- Vantage GUI, which is an extra installation included on the CA 1 Flexible Storage license, provides a graphical user interface for search. Vantage MTC-M provides user-driven features to view, analyze, filter, sort, zoom, and run actions on selected entries.
- Alternatively, the TMC may be used to list archival record using the command line. Note: When storing archival records on the cloud, the command line will not show the cloud object name.
- A list of volumes and associated archival records can be viewed using an inventory command to identify archival records to be recovered.
  - When using Amazon S3 for storage the inventory command lists the object name, which contains the volume and associated archival records. An inventory CSV (comma-separated values) may be setup when the Amazon account is setup to generate an inventory CSV file on a daily basis that includes the retention of every object in the bucket.
    - The cloud object name can be derived by using the archival record name to find that volume the archival record is stored in and the associated object name,
    - Using the Vantage product the file information can be joined with the cloud inventory CSV file, which can be exported in MS Excel format or viewed online via a web browser.
- For retrieval and download, when a job submitted to read the file on the z/OS, a copy of the file is returned to the DASD cache on z/OS and then returned to the application requesting the file.
  - Once the file is returned, it can be exported for delivery to the regulator using local tools.

2.4.4 Additional Considerations

The regulated entity is responsible for: (a) authorizing user privileges, (b) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use CA1 Flexible Storage (and to Amazon S3, if utilized) to readily access, download, and transfer the archival records and the information needed to locate the archival 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.[16] [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.[17] [emphasis added]

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

2.5.2 Compliance Assessment

Cohasset upholds that the functionality of CA 1 Flexible Storage meets the requirement in SEC Rules 17a-4(f)(2)(v)(A) and 18a-6(f)(2)(v)(A) by retaining a persistent duplicate copy of the records, when (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 CA 1 Flexible Storage Capabilities

- For compliance with paragraph (A) to maintain a redundant copy of required records, the Vtape must be configured to replicate the archival records on two virtual tape storage devices or to an Amazon S3 cloud configured to support replication.
  - If the write operation fails for any reason, the original copy is maintained and the write operation is repeated until it is successful. If the write operation fails more than twice, error messages are issued to the administrator.

16 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

17 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

- For additional information regarding Amazon S3 cloud capabilities, refer to the following link: https://aws.amazon.com/compliance/secrule17a-4f/.

2.5.4 Additional Considerations

The regulated entity is responsible for: (a) properly configuring replication to two DASD storage devices or to the Amazon S3 cloud, (b) monitoring to ensure the required redundant copies are created, and (c) when using Amazon S3, ensuring the retention controls are appropriately configured on the bucket and object.

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 CA 1 Flexible Storage supports the regulated entity's efforts to meet this SEC requirement for an audit system.

2.6.3 CA 1 Flexible Storage Capabilities

The regulated entity is responsible for an audit system, and compliance is supported by CA 1 Flexible Storage.

The regulated entity is responsible for and the following CA 1 Flexible Storage functionality supports the regulated entity in meeting this audit system requirement.

- For each archival record stored in CA 1 Flexible Storage, it retains the following audit information.
  - The unique identifier for the archival record, which is a combination of the VOLSER and the file name.
  - The date the archival record was recorded, which are system-generated and cannot be modified by a user.
  - These attributes are immutably stored for the lifespan of the archival record and are produced together with the archival record.

- The distinct records housed in the archival record are retained immutably and include both the contents of the record and associated metadata written by the host system.
- The volume and associated archival records are immutable, meaning changes are disallowed to the volume, the archival record and the distinct records houses in the archival record; therefore, tracking of the inputting of changes made are not relevant to the CA 1 Flexible Storage.
- The Audit data set provides complete TMC integrity. Archival record metadata cannot be modified in the TMC without a corresponding record being written to the Audit data set.
- The audit files may be exported in CSV format using the reporting utility.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records. In addition to relying on the immutable metadata, the regulated entity may utilize CA 1 Flexible Storage features alone or in conjunction with another system.

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

This section contains a summary assessment of the functionality of CA 1 Flexible Storage, as described in Section 1.3, *CA 1 Flexible Storage Overview and Assessment Scope*, in comparison to CFTC electronic regulatory record requirements. Specifically, this section associates the features described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* 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.*[18] [emphasis added]

In Section 2 of this report, Cohasset assesses CA 1 Flexible Storage, with *Immutable feature*, which is a highly restrictive configuration that assures the storage solution applies integrated controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied retention period.

In the following table, Cohasset correlates the functionality of CA 1 Flexible Storage, using *Retention and Immutable controls*, with the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. The first column enumerates the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the ability of CA 1 Flexible Storage to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d).

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(c) Form and manner of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter, all regulatory records must be created and retained by a records entity in accordance with	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records[19] with time-based and event-based retention periods, are met by the functionality of CA 1 Flexible Storage, with

[18] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

[19] The regulated entity is responsible for retaining and managing any additional required information, such as information to augment search and data on how and when the records were created, formatted, or modified, in a compliant manner.

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
the following requirements: *(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the authenticity and reliability of such regulatory records in accordance with the Act and Commission regulations in this chapter.* *(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the authenticity and reliability of electronic regulatory records, including, without limitation:* *(i) Systems that maintain the security, signature, and data as necessary to ensure the authenticity of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;*	*Retention and Immutable controls*. The functionality that supports retention, authenticity and reliability of electronic records are described in the following sections of this report: ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.3, *Record Storage Verification* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System* Additionally, for *records stored electronically*, the CFTC definition of *regulatory records* in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:* *(i) Any data necessary to access, search, or display any such books and records; and* *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added] CA 1 Flexible Storage retains immutable metadata (e.g., VOLSER, file name and creation/storage timestamp) as an integral component of the records, and, therefore, these attributes are subject to the same retention controls as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. Additionally, mutable metadata stored for records include retention controls. The most recent values of mutable metadata are retained for the same time period as the associated records.
(ii) Systems that ensure the records entity is able to produce electronic regulatory records in accordance with this section, and ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems; and	It is Cohasset's opinion that CA 1 Flexible Storage capabilities to retain a persistent duplicate copy of the records and associated system metadata, as described in Section 2.5, *Record Redundancy*, meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems.*
(iii) The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must produce or make accessible for inspection all regulatory records in accordance with the following requirements: *(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.* *(2) Production of **paper** regulatory records. **** *(3) Production of **electronic** regulatory records.* *(i) A request from a Commission representative for electronic regulatory records will specify a reasonable form and medium in which a records entity must produce such regulatory records.* *(ii) A records entity must produce such regulatory records in the form and medium requested promptly, upon request, unless otherwise directed by the Commission representative.* *(4) Production of **original** regulatory records. ****	It is Cohasset's opinion that CA 1 Flexible Storage has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in. ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System*

4 • 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 CA 1 Flexible Storage, as described in Section 1.3, *CA 1 Flexible Storage 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 the following table, Cohasset correlates specific MiFID II requirements for electronic records with the functionality of CA 1 Flexible Storage using the *Immutable feature*. 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 functionality of CA 1 Flexible Storage, relative to these requirements.

Regulatory excerpts of MiFID II media requirements [emphasis added]	**Compliance assessment and analysis of CA 1 Flexible Storage relative to these MiFID II media requirements**
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *(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* ***** **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)** *(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:* *****	While this requirement pertains to the client of the regulated entity, the regulated entity itself would have a similar need to store the archival record for the required retention period. It is Cohasset's opinion that CA 1 Flexible Storage has features that apply time-based and event-based retention periods to archival records and associated system and custom metadata. The retention controls associated with *Immutable feature,* as described in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*: ● Prohibit modification and overwrites for the lifespan of the archival record. ● Prohibit deletion, through any mechanism, until the assigned retention period expires. ● Prohibit the shortening of the retention value assigned to the archival record. Further, CA 1 Flexible Storage assures the accurate recording (storage) of the record content and associated metadata, as explained in Section 2.3, *Record Storage Verification*. The quality and accuracy of the recording process is verified: (a) during the initial recording of the record, and (b) using post-recording verification during read-back.
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *(62) 'durable medium' means any instrument which:* ***** *(b) allows the unchanged reproduction of the information stored;* **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)** *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;* *****	It is Cohasset's opinion that the features of CA 1 Flexible Storage with *Expiration Date* and *Immutable feature,* achieve the non-rewriteable, non-erasable storage requirements necessary to assure that record content is unchangeable. See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for additional information. If the regulated entity corrects or amends a record in the source system, it must store each rendition as a new archival record. The features for non-rewriteable, non-erasable format assure that the original record is not modified. Further, CA 1 Flexible Storage calculates checksums during the recording process, when using encryption and compression, and subsequently uses it for post-recording quality and integrity checks and for archival record repair, as described in Section 2.3, *Record Storage Verification*.

Regulatory excerpts of MiFID II media requirements [emphasis added]	**Compliance assessment and analysis of CA 1 Flexible Storage relative to these MiFID II media requirements**
Directive 2014/65/EU (MiFID II) Article 4(1)(62) *(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;* **Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)** *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* *****	Cohasset asserts that CA 1 Flexible Storage provides the following methods of retrieving records: ● Direct searches of the TMC via command line ● Vantage GUI, which is a separate CA 1 Flexible Storage application, and ● Third-party search tools The selected records may be restored and local capabilities may be used to view, filter, print or produce the records in an acceptable format and medium. See Section 2.4, *Capacity to Download and Transfer Records and Location Information*, for additional information. Further, CA 1 Flexible Storage ensures that records are readily available by writing redundant copies of each archival record on different DASD storage device or cloud provider during the initial recording process. See Section 2.5, *Record Redundancy*, 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)** *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.* *****	Cohasset asserts that CA 1 Flexible Storage provides the following methods of retrieving records: ● Direct searches of the TMC via command line ● Vantage GUI, which is a separate CA 1 Flexible Storage application, and ● Third-party search tools 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, *Capacity to Download and Transfer Records and Location Information*, 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 CA 1 Flexible Storage[20] in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3) and 18a-6(e)(3).

Cohasset determined that CA 1 Flexible Storage, when properly configured, has the following functionality, which meets the regulatory requirements:

- Maintains the volume and associated archival records and immutable metadata in non-rewriteable, non-erasable format for time-based and event-based retention periods. (Note: Archival records are an accumulation of distinct required records; accordingly, the required records and associated metadata are immutably retained for the retention period applied to the volume.)
- Prohibits deletion of the volume and associated archival record and its immutable metadata until the *Expiration Date* for the volume has expired.
- Verifies the completeness and accuracy of the recording process through cryptographic hash values, when using encryption and compression, in addition to the inherent capabilities of advanced magnetic storage technology.
- Maintains a minimum of two duplicates of each volume and associated archival record with either (a) a primary and secondary DASD (direct access storage device) or (b) Amazon S3 cloud storage, which allows for lost or damaged archival records to be restored.
- Provides authorized users with the capacity and tools to (a) list and view the volume and associated archival records and (b) ability to download the associated the volume and associated archival records and metadata attributes.
- Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that CA 1 Flexible Storage, when properly configured and the additional considerations are satisfied, meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3) and 18a-6(e)(3). In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d) and the medium and *retention of records* requirements of the *MiFID II Delegated Regulation(72)(1)*.

[20] See Section 1.3, *CA 1 Flexible Storage Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

Appendix A • Overview of Relevant Electronic Records Requirements

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

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

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

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments[21] 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.*[22] [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.*[23] [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.

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

[22] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[23] 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.*[24] [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.*[25] [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."*[26] [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****[27] [emphasis added]

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

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

---

24 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
25 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
26 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
27 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.*[28] [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.*[29] [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.*[30] [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 CA 1 Flexible Storage 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).[31]

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.*

---

28 2003 Interpretative Release, 68 FR 25282.

29 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).

30 2003 Interpretative Release, 68 FR 25283.

31 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.*[32] [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 CA 1 Flexible Storage in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

[32] 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 CA 1 Flexible Storage 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.

For domestic and international clients, Cohasset:

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

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