Cohasset Associates

IBM TS7700 Virtual Tape

COMPLIANCE ASSESSMENT

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

Abstract

The IBM TS7700 Virtual Tape (TS7700) is a modular, scalable, and high-performing virtual tape solution for IBM Z mainframes. The architecture is a fully integrated, tiered storage hierarchy of disk, tape, and connected object stores.

The IBM TS7700 storage family includes several models and types, which rely on the same underlying architecture and virtual tape management compliance features.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of the IBM TS7700 Virtual Tape (see Section 1.3, *IBM TS7700 Virtual Tape Overview and Assessment Scope*) relative to the electronic records requirements, specified by multiple regulatory bodies, as follows:

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

It is Cohasset's opinion that the IBM TS7700 Virtual Tape, when properly configured and when the additional considerations are satisfied, meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 240.18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 240.18a-6(e)(3)(iii). Additionally, the assessed functionality of the TS7700 meets the principles-based requirements of CFTC Rule 1.31(c)-(d).

BENEFIT FROM 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 a multitude of 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.

January 2023

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

+1.312.527.1550 | www.cohasset.com

Table of Contents

1 • Introduction

Regulators, worldwide, establish explicit requirements for regulated entities that elect to electronically retain books and records[1]. 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 the IBM TS7700 Virtual Tape 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 securities broker-dealer industry and 17 CFR §§ 240.18a-5 and 240.18a-6 for nonbank SBS entities[2], the SEC stipulates recordkeeping requirements, including retention periods.

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

> *The Securities and Exchange Commission ("Commission") is adopting amendments to the recordkeeping rules applicable to broker-dealers, security-based swap dealers, and major security-based swap participants. The amendments modify requirements regarding the maintenance and preservation of electronic records***[3]* [emphasis added]

For additional information, refer to Section 5.1, *Overview of SEC Rules 17a-4(f) and 18a-6(e) Electronic Recordkeeping System Requirements*.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets and amended its rules to address security-based swaps (SBS).[4]

---

1 Regulators use the phrase *books and records* to describe information that must be retained for regulatory compliance. Cohasset uses the term *archival record* (versus *data* or *object*) to consistently recognize that the content is a required record.

2 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.

3 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).

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

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

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

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

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

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, which correlates the CFTC principles-based requirements with the capabilities of the TS7700. Section 5.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*, provides additional information on the requirements.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of the IBM TS7700 Virtual Tape for preserving regulated electronic records, IBM 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.

IBM engaged Cohasset to:

- Assess the functionality of IBM TS7700 Virtual Tape, in comparison to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and describe audit system features that support the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii); see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e);*
- Address FINRA Rule 4511(c); given FINRA explicitly defers to the requirements of SEC Rule 17a-4, see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e);*
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) with the assessed functionality of the IBM TS7700 Virtual Tape; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);* and
- Prepare this Compliance Assessment Report, enumerating the assessment results.

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

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection, by Cohasset, of the IBM TS7700 Virtual Tape and its functionality or other IBM products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral

discussions, (b) system documentation, (c) user and system administrator guides, and (d) related materials provided by IBM 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.

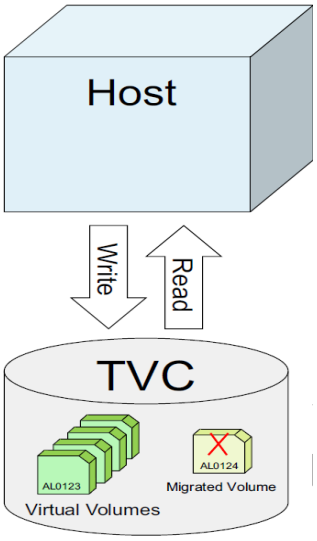
1.3 IBM TS7700 Virtual Tape Overview and Assessment Scope

1.3.1 IBM TS7700 Virtual Tape Overview

The IBM TS7700 Virtual Tape (TS7700) is a modular, scalable, and high-performing virtual tape solution for IBM Z mainframes. The architecture is a fully integrated, tiered storage hierarchy of disk, tape, and connected object stores. The IBM TS7700 storage family includes several models and types, which rely on the same underlying architecture and virtual tape management compliance features.

The TS7700 service is summarized as follows:

- **Host** is an IBM Z mainframe computing system.
- **Tape Volume Cache (TVC)** provides the ability to write, read and store virtual tape data (archival records) on emulated tape volumes (i.e., logical or virtual volumes).
  - Logical (virtual) volumes may be assigned a Data Class (policy used to automate storage management) with Logical Write-Once, Read-Many (*Standard LWORM*), which is less-restrictive, or the highly-restrictive *LWORM Retention* feature. Enabling and properly configuring *Standard LWORM* or *LWORM Retention* applies integrated control codes that place additional restrictions on the actions that can be performed on the volumes and associated archival records, to prevent overwrite or erasure prior to the expiration of an assigned retention period. A *Migrated Volume* exists only on physical tape or cloud connected to a particular TS7700 cluster.



  - The TS7700 logical 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 archival record housing an accumulation of distinct required records.

1.3.2 Assessment Scope

This report assesses the IBM TS7700 Virtual Tape, Release 8.51.1.26, when the (a) *LWORM* or *LWORM Retention* is enabled and appropriately configured and (b) the TS7700 Policy is configured to apply 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.

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

This section presents Cohasset's assessment of the functionality of the IBM TS7700 Virtual Tape, for compliance with the electronic recordkeeping system requirements promulgated in SEC Rules 17a-4(f)(2) and 18a-6(e)(2), as well as describing how the solution supports the regulated entity in meeting the audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

For each of the compliance requirements described in this section, this assessment is organized as follows:

- ***Compliance Requirement*** – Excerpt of relevant regulatory requirement in SEC Rules 17a-4(f) and 18a-6(e) and Cohasset's interpretation of the specific requirement
  - Both SEC Rules 17a-4(f) and 18a-6(e) are addressed in this section, since the electronic recordkeeping system requirements (principles, controls and testable outcomes) are the same, though the Rules name their respective regulations and regulators and include semantic differences.
- ***Compliance Assessment*** – Summary statement assessing compliance of the IBM TS7700 Virtual Tape
- ***IBM TS7700 Virtual Tape 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 the TS7700, as described in Section 1.3, *IBM TS7700 Virtual Tape Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

2.1 Record Audit-Trail

2.1.1 Compliance Requirement

This regulatory requirement, adopted with the 2022 Rule amendments, allows regulated entities to use a combination of electronic recordkeeping systems, with each system meeting either (a) the 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 audit-trail requirement is designed to permit use of the regulated entities' business-purpose recordkeeping systems to achieve the required outcome without specifying any particular technology solution.

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

Preserve a record for the duration of its applicable retention period in a manner that maintains a complete time-stamped audit-trail that includes:

(1) All modifications to and deletions of the record or any part thereof;

(2) The date and time of actions that create, modify, or delete the record;

(3) If applicable, the identity of the individual creating, modifying, or deleting the record; and

(4) Any other information needed to maintain an audit-trail of the record in a way that maintains security, signatures, and data to ensure the authenticity and reliability of the record and will permit re-creation of the original record if it is modified or deleted

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

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

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

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

2.1.2 Compliance Assessment

Since the IBM TS7700 Virtual Tape is not a business-purpose recordkeeping system, Cohasset has not assessed it in comparison to this requirement of the SEC Rules.

For enhanced control, a separate host system may store the complete time-stamped audit-trail on the TS7700, with the features and controls described in Sections 2.2 through 2.6 of this report.

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

2.2 Non-Rewriteable, Non-Erasable Record Format

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

2.2.1 Compliance Requirement

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

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

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

[5] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
[6] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

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

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

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

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of the IBM TS7700 Virtual Tape, with *Standard LWORM* or *LWORM Retention*, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for time-based[9] retention periods and applied legal hold, when (a) properly configured, as described in Section 2.2.3 and (b) the considerations described in Section 2.2.4 are satisfied.

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

2.2.3 IBM TS7700 Virtual Tape Capabilities

This section describes the functionality of the TS7700 that directly pertains to this requirement to preserve electronic books and records (archival records) in a non-rewriteable, non-erasable format, for the required retention period and applied legal hold.

2.2.3.1 Overview

The TS7700, like other magnetic tape systems, is divided into logical volumes which contain archival records that are an accumulation of distinct required records. The TS7700 offers two compliance options: (1) *Standard LWORM*, a less-restrictive option, provides overwrite protection but requires administrative checks and balances to ensure compliant retention, as administrators are allowed to shorten or remove retention controls, or (2) *LWORM Retention*, a highly-restrictive option, which provides both overwrite protection and stricter retention controls.

---

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

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

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

The following table delineates the primary differences between *Standard LWORM* and *LWORM Retention* controls.

	Standard LWORM	***LWORM Retention***
Retention	*Delete Expire* (hold duration) together with the *Expire Hold* (set), provides the following controls: ● Prevents deletion until hold duration is in the past. ● Allows administrators, with appropriate permissions, to extend or shorten the hold duration or remove the *Expire Hold* attribute. ● Allows the volume to return to *Scratch Pool*. Prevents overwrites using the worldwide identifier and write-mount-count integrated controls.	*Retention Type* defines how retention is applied to the archival record, when written, and can be either: 1. Fixed duration or 2. HDR1 (an explicit expiration date), applied to an archival record when written. *Retention Duration*, which provides the following controls: ● Prevents deletion until the retain until date is in the past. ● Archival records may only be appended to a volume, which will either extend the retention duration or use the longest duration for the volume. ● Deny an early return to scratch, when configured. ● Once *Retention* has expired for a volume, the volume and associated archival records are managed as a *Standard LWORM* volume.
Legal Holds (Temporary Holds)	*Expire Hold* attribute, which provides the following controls: ● Prevents deletion until fixed hold duration *(Delete Expire)* is in the past. Note: The fixed hold duration *(Delete Expire)* may be extended for the Category, to meet the legal hold requirement. Alternatively, all or a subset of the archival record may be written to a new volume with an extended retention duration.	See *LWORM*

2.2.3.2 *Standard LWORM* – Configuration and Controls

- In the administrative setup of the TS7700 each Data Class policy must be defined, named and configured with the LWORM attribute set to Yes. Logical volumes assigned to the Data Class then inherit the LWORM setting which prevents archival records from being overwritten.
  - The regulated entity can reset the Data Class policy to enable or remove the *LWORM* attribute.
  - When changing the *LWORM* attribute from Yes to No (non-*LWORM)*, the WORM status for existing volumes and associated archival records are unchanged and the applied *Delete Expires and Expire Hold* configurations continue to apply. However, new volumes will not include the LWORM attribute, though the volume may continue to be protected by *Delete Expire* and *Expire Hold* as part of any Category setting that may apply.
- For *Standard LWORM*, the Category (which is a grouping of logical volumes) must have the Expires configurations set by assigning both: (1) *Delete Expires* (hold duration) and (2) *Expire Hold* features.

1. The hold duration (denoted as *Expires*, in the Add Category excerpt to the right) assigns a fixed period of time to the volume and associated archival records are kept in the *Scratch Pool*. It may be set in hours, days or years (up to 2000 years).

   - The hold duration counter starts when a volume is sent to the *Scratch Pool*; thus, volumes containing archival records are retained in the scratch status for the hold duration (retention period).
   - The hold duration is reset (the count starts over) each time the volume is sent to the *Scratch Pool*. Thus, if a volume is returned to a Private volume (Normal Use), then returned to the *Scratch Pool* from Private, the hold duration restarts.
   - The hold duration (retention period) may be changed (extended or shortened). Any changes to the hold duration will be honored. To reduce opportunities for misuse, dual-access control should be configured for this feature; dual-access requires two users to configure the feature.
   - Once the hold duration passes, the volume is a candidate for re-use and automatic expiration (deletion).

2. The *Expire Hold* setting must be enabled on the Category to disallow the volumes from early deletion (reclamation of storage), ejection or reuse in advance of the hold duration (retention period) ending. Thus, enabling the *Expire Hold* setting ensures the applied hold duration (retention period) is honored.
   - When the hold duration is assigned and the *Expire Hold* feature is unselected (unchecked) it allows the volume to be offered up (overwritten) if storage space is needed. Thus, unselecting (unchecking) *Expire Hold* flag is not compliant with the Rules.
   - The *Expire Hold* feature can be reset or removed. To reduce opportunities for misuse, dual-access control should be configured for this feature; dual-access requires two users to configure the feature.

- In conjunction with the Data Class *LWORM* setting, the TS7700 employs the following two integral control codes to prevent overwrite:
   1. Worldwide identifier (WWID), a unique identifier that is cryptographically generated and temporarily assigned to each logical volume in a Data Class with the *LWORM* attribute at the time the logical volume is initially mounted. The WWID is bound to each logical volume at the point in time when the initial block of data is recorded. The process of binding stores the WWID in (a) the TS7700 volume management metadata and (b) the protected header information area of each logical volume. Once the WWID is bound to a virtual volume, subsequent recording of data can only be appended after the point at which the previous recording ended. Therefore, previously recorded data cannot be overwritten or erased.
   2. Write-Mount-Count (WMC), is used to track the number of times a logical volume has been mounted for recording purposes.

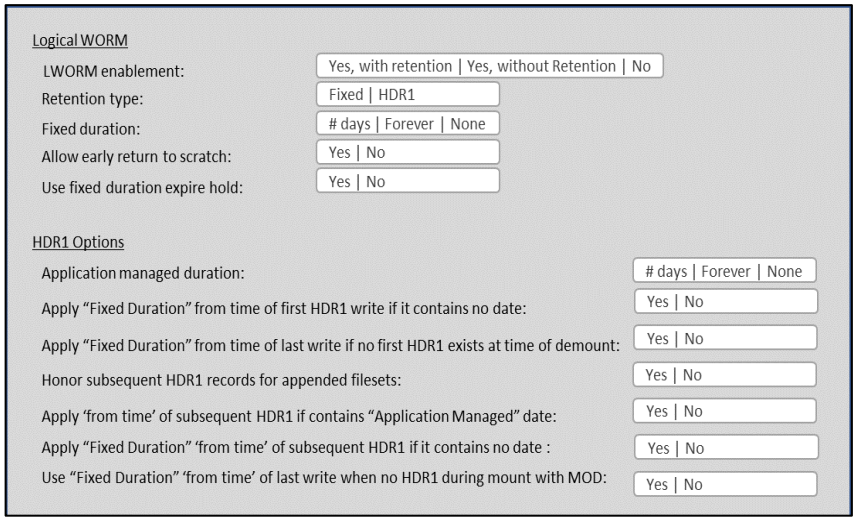
- For each LWORM logical volume, the *LWORM* Data Class name, the WWID and WMC are recorded to the TS7700 management metadata and to the volume header information. Additionally, the control codes are made available to the host operating system (e.g., IBM Z/OS/DFSMS) and passed to the removable media management system for storage, tracking and comparison purposes.
- When a recording process is initiated, both the WWID and the WMC of the virtual volume specified for recording by the host operating system must agree with: (a) the WWID stored by the removable media management system, (b) the WWID stored in the virtual volume metadata on the TS7700, and (c) the WWID stored in the header information of the virtual volume. This ensures that all elements of the recording chain are in agreement that the correct virtual volume is being used for an LWORM recording process.

2.2.3.3 *LWORM Retention* – Configuration and Controls

When the *LWORM* attribute is enabled (Yes), *LWORM Retention* inherits the *LWORM* functions (described in Section 2.2.3.2), plus additional capabilities related to retention which cannot be achieved using the *LWORM* function alone.

- *LWORM Retention* configurations and subsequent changes to the settings must be performed by IBM Support. The *LWORM Retention* settings may be applied to: (1) specific Data Class(es), (2) default Data Class, or (3) all Data Classes.
- During the configuration, numerous settings allow for customized behaviors. The three (3) primary settings that define how the *LWORM Retention* functions are: (1) *Retention Type*, (2) *Retention Duration*, and (3) *Retention Return-To-Scratch*.

1. ***Retention Type*** may be configured as (a) Fixed or (b) HDR1 (Header1).
   - **Fixed:** A *Fixed duration* of time is applied to the volume and associated archival records, and the retention date is calculated using the timestamp when data was last written or appended to the logical volume. When *Fixed duration* is applied to a volume, any retention dates encoded in the HDR1 are ignored.
   - **HDR1:** An explicit retention expiration date may be transmitted in the HDR1 associated with the archival record. Further, the HDR1 feature provides *HDR1 Extended Options* which explicitly define how retention is applied.



2. ***Fixed Duration*** is used to calculate the retain until date for the volume and associated archival records for the Fixed retention type and may be utilized by the HDR1 retention type, if no retention expiration date is transmitted in the HDR1. The *Fixed duration* must be configured as (a) a specified number of days or (b) Forever.

3. When using the **HDR1** *Retention Type*, the archival retention time is based on the value transmitted in the HDR1 by the host system. The transmitted value may be any of the following three options:
   - Option 1 (valid date in the future): The explicit future date is applied to the archival record for retention expiration.
   - Option 2 (special application managed date, i.e., 99365 or 99366): The *Application Managed Duration* is applied, based on the configuration. Note: This option is not assessed in this Compliance Assessment Report, since the retention controls are maintained by the host system. However, once a valid date is sent by the application, the controls described in Option 1, above, would apply.
   - Option 3 (invalid date, e.g., date in the past, all zeros or all spaces): The *Fixed Duration* is applied.
4. ***Retention Return-To-Scratch*** configuration provides two independent settings that define the behavior when the host system sends a request to return-to-scratch: (1) *Allow early return to scratch* (Yes/No) and (2) *Use fixed duration expire hold* (Yes/No). For both configurations, either option (Yes or No) are acceptable, since the *Retention Type* and retention duration manages the length of retention and immutability of the volume and associated archival records.
   - The *Allow early return to scratch* feature impacts the storage status, but does not impact the applied retention controls:
     - If *Allow early return to scratch* is enabled, the volume may be sent to the *Scratch Pool* before retention expires. The *LWORM Retention* feature assures the volume and associated archival records continue to be retained in the *Scratch Pool*, until its retention expires. A command can be issued to transition the volume back to a Private state, where the remainder of the retention duration will continue to be honored
     - If *Allow early return to scratch* is disabled, attempts to transition the volume to the *Scratch Pool* are denied.
     - If the *Return-To-Scratch* event is allowed and the *Expire-Hold* is enabled, the greater of the following two retentions takes precedence: (1) remaining retention duration or (2) *Expire-Hold* duration.

- The applied *LWORM Retention* date can only be extended (never decreased). Multiple *LWORM Retention* settings may apply to a single volume. When multiple retentions are applied to the volume and associated archival records, the longest retention takes precedence.
- Content may be appended to the end of the volume (without changing the content of the previously stored archival records). However, stored archival record content and metadata cannot be modified until retention has passed; the volume is protected from: (1) overwrites, (2) unexpected appends (i.e., higher than expected Write Mount Count), and (3) early expiration of the volume and associated archival records.
  - When content is appended to a volume, the retention will either: (1) automatically extend, when using *Fixed duration* or (2) the longest retention expiration date will apply, when using the appended HDR1.

- Volumes and associated archival records cannot be deleted prior to the end of the applied retention. Once *LWORM Retention* is expired for a volume, it is managed as a *Standard LWORM* volume until it's either (a) reused or (b) appended to which may result in the re-enablement of a retention period.

2.2.3.4 Legal Holds (Temporary Holds)

The regulated entity may need to preserve records beyond the applied retention period, in the event of litigation or a subpoena. For volumes using as either *LWORM* or *LWORM Retention*, the following two options may be employed to preserve archival records for a legal hold.

1. The *Delete Expires* configurations may be set for a category (which is an attribute of a volume), by assigning both: (1) hold duration and (2) *Expire Hold* flag. See Section 2.2.3.2, *LWORM – Configuration and Controls,* for information on applying these controls.
   - To support a legal hold, the hold duration may be extended to a future date (e.g., 100 years). When the legal hold is released, the hold duration may then be shortened. If no other retention controls apply to the volume, it will be unprotected and eligible for overwrite or deletion.
   - When the *Expire Hold* feature is enabled (checked) and associated hold duration is set for a category, the volume and associated archival records are preserved for the defined hold duration. The *Expire Hold* feature can be reset, removed, extended or shortened. To reduce opportunities for misuse, dual-access control should be configured for this feature (dual-access requires two users to configure the feature).
2. The archival records (all or a subset) can be written to a new volume, that has an extended *Retention Duration* or *Delete Expire* hold duration (i.e., using a different category).

2.2.3.5 Deletion Controls

Volumes and associated archival records and metadata may be deleted by either:

1. The *auto-delete expiring*, which is a background asynchronous process that deletes volumes from the *Scratch Pool*, containing the associated archival record and metadata, when the hold duration (*LWORM*) or *Retention Duration* (*LWORM Retention*) is in the past.
2. The host system can *eject* a scratch volume, if it is past the *Retention Duration*. Ejecting a scratch volume will delete the volume containing the associated archival records and metadata.

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.

The system time of the two (2) lowest TS7700 clusters in the grid to act as NTP servers for the grid, two or more physically separated TS7700s, and optionally, may synchronize to an external NTP server. The internal NTP servers tolerate minor discrepancies in time variance and auto resynchronize micro variations. If one of the internal NTP servers presents a large variance in time, it will be ignored by the other clusters in the grid. Neither end users nor system administrators are able to manipulate system time. These controls prevent or correct inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of archival record.

2.2.3.7 Security

In addition to the stringent retention protection and management controls described above, the TS7700 provides the following security capabilities, which support the authenticity and reliability of the archival records.

- Auditing & Compliancy, Cloud Tier and Physical Tape Tier
  - Disaster recovery (DR) testing
    1. Flash Copy DR Testing – Provides a way for customers to test their disaster recovery plan and ensures data integrity after a DR simulation for data stored on TS7700 cache.
    2. Cloud Export Recovery – Provides a way to test and restore from the loss of an entire TS7700 grid and where the only surviving data is stored in the cloud.
    3. Tape Copy Export Recovery – Provides a way to test and restore from the loss of an entire TS7700 grid and where the only surviving data is stored in a physical tape library.
    4. Cloud Pool Retention – Provides a way for users to enable a retention period to hold older versions of a tape logical volume in the cloud for potential PIT (point-in-time) recovery for air gap recovery or single volume recovery.
- User Auditing
  1. Remote System for Log processing (RSYSLOG) – Tamperproof logging that is sent out to an external server. Captures tasks/operations performed by TS7700 administrators.
  2. Simple Network Management Protocol (SNMP) – Audit traps for any TS7700 user interface or Service panel modification action. (Note: Users can also see any transactions for the last 90 days on a task page on the graphical user interface).
- Management Interface Security
  - Dual Control – Requires two people (i.e., a maker and a checker) to submit commands that may cause data integrity issues, e.g., changing Category Expire Hold setting.
  - Multi-factor authentication using either (a) LDAP with RACF (Resource Access Control Facility) protection for Tivoli LDAP Servers or (b) an authentication proxy such a Cisco Duo for Microsoft Active Directory.
- 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.
- Other
  - Select Device Access Control (SDAC) – Provides a way to assign logical volumes to a range of devices. Logical partitions (LPARS) are assigned certain device ranges and, if they are only allowed to use certain logical volumes, it prevents other LPARS from being able to mount volumes it does not own.
  - TS7700 Grid – provides a way to replicate data to up to eight (8) geographically dispersed clusters, segregating data into different regions of the world, using asynchronous replication.

2.2.4 Additional Considerations

Additionally, the regulated entity is responsible for:

- Enabling *LWORM* (for less-restrictive retention controls) or collaborating with IBM Support to enable *LWORM Retention* (for highly-restrictive retention controls). Additionally, the host system and the removable media management system must be configured to write required archival records only to properly configured Data Classes and associated logical volumes.
  - When using *LWORM* only, Cohasset recommends the regulated entity (a) establish administrative procedures to limit opportunities for the *LWORM* attribute for a Data Class to be changed from *Yes* to *No* (which is non-*LWORM*) and (b) set Dual Control to restrict access privileges that allow modifications to the *Expire Hold* feature and the *Delete Expires* hold duration.
  - Configuring appropriate *LWORM Retention* options, including the *Retention Type* and *Retention Duration,* to ensure the volumes and associated archival records are stored immutably for the required period of time and extending retention, when necessary.
- Assuring the retention controls apply the required retention period. Important Note: For LWORM Retention, the **Fixed Duration** cannot be configured with **None** to be compliant with the Rule.
- Storing LWORM, WWID and WMC control codes in the metadata or header information to prevent overwriting the volume during the applied retention. See Section 2.2.3.2 for additional information.
- Assuring erasable physical tape media used by the TS7700 is under the exclusive control of the TS7700 and is stored in a secure robotic tape library.
- Assuring any S3 compatible Object Store used by the TS7700, and the objects it creates, are under the exclusive control of the TS7700.
- Applying and removing the Expire Hold feature for a category to preserve the volume and associated archival records for legal matters, government investigations, external audits and similar circumstances. Alternatively, writing the archival records (all or a subset) to a new volume, that has an extended *Retention Duration* or *Delete Expire* hold duration.

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 a 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 the IBM TS7700 Virtual Tape, in conjunction with the inherent capabilities of advanced magnetic storage technology, meets this SEC requirement for complete and accurate recording and post-recording verification, when the considerations identified in Section 2.3.4 are satisfied.

2.3.3 IBM TS7700 Virtual Tape Capabilities

The recording and post-recording verification processes of the TS7700 are described below for the archival records, which are an accumulation of distinct required records.

2.3.3.1 Recording Process

- A combination of checks and balances in the advanced magnetic recording technology, e.g., inter-component and inter-step cyclic redundancy checks (CRCs), as well as write-error detection and correction, assure the archival records are written in a high-quality and accurate manner.
  - A CRC of the electronic archival record is generated by the host system and sent to the TS7700. The TS7700, in turn, recalculates and checks the CRC to ensure that the information sent by the host system has been completely and accurately received and captured. If the CRC comparisons do not match, the recording process is aborted, an error message is generated, and the host system must resend the archival record for storage.
  - Subsequently, the TS7700 calculates a separate CRC for the archival record, which is recorded in the logical volume with the related archival record.

2.3.3.2 Post-Recording Verification Process

- To validate the retrieval process, the TS7700 reads the archival record with its stored CRC, then calculates a new CRC and compares the two values.
  - If the CRC values match, the archival record is retrieved.
  - If the CRC values do not match, the TS7700 automatically aborts the retrieval process. When the host system sends a subsequent retrieval request, the TS7700 checks a different copy of the volume. After multiple attempts, if the retrieval is unsuccessful, an error message is generated, which alerts the system administrator to manually initiate recovery.
- Additionally, a CRC calculated by the TS7700 during retrieval is transmitted with the archival record for the host system to use to validate the downloaded content.

2.3.4 Additional Considerations

The host system is responsible for transmitting the complete contents of required records included in the archival record and the TS7700 ensures the transmitted archival record is accurately recorded.

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 either a:

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

The downloaded records and information 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 audit-trails applies only when this alternative is utilized; see Section 2.1, *Record Audit-Trail*.

2.4.2 Compliance Assessment

It is Cohasset's opinion that the functionality of the IBM TS7700 Virtual Tape meets this SEC requirement for the capacity to readily download and transfer the records and the information to locate the archival records (e.g., unique identifier, index, or properties) stored in the TS7700, when the considerations described in Section 2.4.4 are satisfied.

2.4.3 IBM TS7700 Virtual Tape Capabilities

The following capabilities support the capacity to download and transfer the archival records and the information to locate the records (e.g., unique identifier, index, or properties).

- The Bulk Volume Information Retrieval (BVIR) data containing location information for the archival record, including volume, WWID, WMC, creation timestamp, and modified timestamp is provided to facilitate locating archival records.
  - Using local tools, the data generated by the BVIR is analyzed to identify the archival records for retrieval.
  - Using Library commands, the archival records can be readily made available for download by mounting a logical volume and reading its content. Thereafter, since the TS7700 retains the archival records, which are an accumulation of distinct required records, the host system must be used to locate specific records, for downloading and transferring as requested by the regulator.

2.4.4 Additional Considerations

The regulated entity is responsible for:

- Maintaining the necessary hardware and software to access and use the TS7700.
- Maintaining the host system and the information retained by the host system to locate, read and interpret the downloaded copy of the archival records from the TS7700.

- Assuring that the regulator receives downloads of the requested records and the information to locate the records (including the information from both the TS7700 and the host system), in the requested format and medium.

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)(iv):

(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.[10] [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.[11] [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 the IBM TS7700 Virtual Tape meets the requirement in SEC Rules 17a-4(f)(2)(v)(A) and 18a-6(f)(2)(v)(A) by retaining a persistent redundant copy of the archival 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 IBM TS7700 Virtual Tape Capabilities

In compliance with paragraph (A) to maintain a redundant copy of required records, the TS7700 must be configured, as follows:

- Replication policy must be configured when the volume is created. The target TS7700 will synchronize the policy.

[10] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.
[11] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

- When archival records are written to logical volumes on a primary TS7700 cluster, a redundant set of records can be written automatically to a target (secondary) TS7700 cluster that is sufficiently geographically separated. When this occurs, the *LWORM Retention* (if applicable), *LWORM* Data Class information, the WWID and WMC, are recorded automatically with the redundant copy.
  - Redundant copies can be produced either synchronously (immediately when recording of the primary logical volume is complete) or asynchronously (at a designated point subsequent to completion of the recording of the primary logical volume). For regulated archival records, it is recommended to configure the TS7700 with synchronous replication.
  - If the secondary TS7700 is unavailable, asynchronous replication will queue and track that the cluster is down. When the cluster returns, it will reconcile and queue up archival records for replication, as required.
- Alternatively, or in addition to replication between two TS7700's, redundant copies of logical volumes can be recorded to rewriteable magnetic tape drives and cartridges.
  - If physical rewriteable magnetic tape media are used, the media must be (a) overwrite-protected by storing the *LWORM*, WWID and WMC control codes in the tape header information, (b) under the exclusive control of the TS7700, and (c) housed in a secure tape library.

2.5.4 Additional Considerations

The regulated entity must ensure that appropriate procedures and redundant copy capabilities are utilized to ensure the required redundant copies are created.

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.

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

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

2.6.2 Compliance Assessment

Cohasset asserts that the IBM TS7700 Virtual Tape supports the regulated entity's efforts to meet this SEC audit system requirement.

2.6.3 IBM TS7700 Virtual Tape Capabilities

The regulated entity is responsible for complying with this audit system requirement. The TS7700 retains the archival records, which are an accumulation of distinct required records.

- For each archival record stored in the TS7700, it retains the following audit information.
  - The unique identifier for the archival record, which is a combination of the logical volume serial number, the assigned WWID and the WMC. Additionally, this unique identifier is transmitted to the host system.
  - The date the archival record was stored (date of inputting) and the last modified timestamp (date of last update), which are system-generated and cannot be modified by a user.
  - The CRC value when the archival record was stored (input), to both validate the recording process and confirm no changes were made to the archival record. See Section 2.3, *Record Storage Verification*, for additional information.
  - These attributes are *immutably* stored for the lifespan of the archival record and are produced together with the archival record.
- The archival record is immutable, meaning changes are disallowed; therefore, tracking of the inputting of changes made is not relevant to the TS7700.

2.6.4 Additional Considerations

In addition to the audit information retained for the volume and associated archival records, the regulated entity is responsible for retaining any other required audit system information, which may include information (a) transferred with the distinct records within the archival record, (b) retained by the host system or (c) stored in a security information event management tool.

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

This section contains a summary assessment of the functionality of the IBM TS7700 Virtual Tape, as described in Section 1.3, *IBM TS7700 Virtual Tape Overview and Assessment Scope*, in comparison to CFTC electronic regulatory record requirements. Specifically, this section associates the features described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e),* to the principles-based requirements of CFTC Rule 1.31(c)-(d).

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

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

> *The proposed amendments to Rules 17a-4 and 18a-6 and the [CFTC] principles-based approach recommended by the commenters share an objective: ensuring the authenticity and reliability of regulatory records. However, the audit-trail requirement is more likely to achieve this objective because, like the existing WORM requirement, it sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[12] [emphasis added]

In the following table, Cohasset correlates the functionality of the TS7700 designed to meet SEC requirements 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 the IBM TS7700 Virtual Tape 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 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*	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records with time-based retention periods, are met by the TS7700 capabilities, including *Standard LWORM* and *LWORM Retention,* as described in: ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.3, *Record Storage Verification* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System* Additionally, for *records stored electronically*, the CFTC definition of *regulatory records* in 17 CFR § 1.31(a) includes metadata:

[12] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

CFTC 1.31(c)-(d) Regulation [emphasis added]	Compliance Assessment Relative to CFTC 1.31(c)-(d)
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;*	*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] It is Cohasset's opinion that the TS7700 retains immutable metadata (e.g., WWID, WMC and storage timestamp) as an integral part of the archival record, and therefore these attributes are subject to the same retention protections as the associated archival record. To satisfy this requirement for other essential data that is not retained in the TS7700 (such as separate indices to facilitate search and data on how and when the distinct required records accumulated in the archival record were created, formatted, or modified), the regulated entity must retain this other data in a compliant manner.
(ii) Systems that ensure the records entity is able to produce electronic regulatory records[13] 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 the TS7700 capabilities described Section 2.5, *Record Redundancy*, including options for replicating the archival records and associated system metadata, meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems*. To satisfy this requirement for other essential data that is not retained in the TS7700 (such as separate indices), the regulated entity must retain this other data in a compliant manner.
(iii) The creation and maintenance of an up-to-date inventory that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).
*(d) **Inspection and production of regulatory records**. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must produce or make accessible for inspection all regulatory records in accordance with the following requirements:* *(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.* *(2) Production of **paper** regulatory records. **** *(3) Production of **electronic** regulatory records.* *(i) A request from a Commission representative for electronic regulatory records will specify a reasonable form and medium in which a records entity must produce such regulatory records.* *(ii) A records entity must produce such regulatory records in the form and medium requested promptly, upon request, unless otherwise directed by the Commission representative.* *(4) Production of **original** regulatory records. ****	It is Cohasset's opinion that the TS7700 has features that support the regulated entity's efforts to comply with requests for inspection and production of records and associated system metadata (i.e., index attributes). Specifically, it is Cohasset's opinion that: ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format,* assures that immutable records are retained. ● Section 2.4, *Capacity to Download and Transfer Records and Location Information*, describes the use of the TS7700 to list and restore (download) archival records and associated system metadata retained by the TS7700. As noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the archival record and associated metadata, in the form and medium requested. ● Section 2.6, *Audit System,* pertains to the information on how and when records were created, formatted, or modified.

[13] 17 CFR § 1.31(a) includes indices (*Any data necessary to access, search, or display any such books and records*) in the definition of regulatory records.

4 • Conclusions

Cohasset assessed the functionality of the IBM TS7700 Virtual Tape[14] in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described audit system features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

Cohasset determined that the TS7700, when properly configured, has the following functionality, which meets the regulatory requirements:

- Maintains archival records and immutable archival record metadata in non-rewriteable, non-erasable format for time-based retention periods. (Archival records are an accumulation of distinct required records.)
- Preserves archival records as immutable and prohibits deletion or overwrites, while the *Expire Hold* and *Delete Expires* (hold duration) is active.
- Prohibits deletion of an archival record and its immutable metadata until either: (1) the *Retention Duration* (*LWORM Retention*) or (2) *Expire Hold* (*LWORM*), for the archival record has expired.
- Verifies the completeness and accuracy of the recording process through cryptographic hash values and IBM validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- Maintains a minimum of two duplicates of each archival record with either (a) a primary and secondary TS7700 or (b) a primary TS7700 and an exported copy on physical tape, which allows for lost or damaged archival records to be restored.
- Synchronously or asynchronously stores a minimum of two duplicates on separate local or remote TS7700s or physical tape media, which allows for automatic recovery of archival records that become lost or damaged.
- Provides the capacity and tools to: (a) list and view archival records and (b) ability to download the associated archival records and associated metadata attributes.

Additionally, the TS7700 supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records by storing and downloading immutable metadata related to inputting each archival record.

Accordingly, Cohasset concludes that the IBM TS7700 Virtual Tape, when properly configured and utilized to retain time-based records, meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c) and supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d).

[14] See Section 1.3, *IBM TS7700 Virtual Tape Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

5 • Overview of Relevant Electronic Records Requirements

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

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

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

On October 12, 2022, the U.S. Securities and Exchange Commission (SEC) adopted amendments[15] 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.*[16] [emphasis added]

These 2022 amendments (a) provide an 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.*[17] [emphasis added]

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

5.1.1 Record Audit-Trail Alternative

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

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

[16] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[17] 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.*[18] [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.*[19] [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."*[20] [emphasis added]

5.1.2 Non-Rewriteable, Non-Erasable Format 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****[21] [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).

[18] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
[19] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.
[20] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.
[21] 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.*[22] *[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.*[23] [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.*[24] [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 the TS7700 related to each requirement.

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

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. Additionally, FINRA adopted amendments clarifying the application of FINRA rules to security-based swaps (SBS).[25]

FINRA Rule 4511(c) explicitly defers to the electronic recordkeeping system requirements of SEC Rule 17a-4.

> *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.*

---

[22] 2003 Interpretative Release, 68 FR 25282.

[23] 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] 2003 Interpretative Release, 68 FR 25283.

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

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

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 (CFTC Rule) to modernize and make technology neutral the form and manner in which to keep regulatory records. This resulted in adopting 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.*[26] [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 regulated 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 the TS7700 in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

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

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.