



SEC 17a-4(f) Compliance Assessment **IBM Virtualization Engine TS7700**

Prepared by
Cohasset Associates, Inc.

July 2010

Abstract

This technical report is a compliance assessment of the storage capabilities of the IBM Virtualization Engine TS7700 relative to the requirements and conditions of SEC Rule 17a-4(f).

Cohasset Associates' assessment concludes that the TS7700 meets all of the SEC requirements that are its direct responsibility for retaining and storing in digital form 17a-3 and 17a-4 records – pursuant to the requirements set forth in Rule 17a-4(f), which expressly allows records to be retained on electronic storage media.

Table of Contents

- 1. Introduction 3**
 - 1.1 The Electronic Storage Requirements of the Securities & Exchange Commission for 17a-4 Records3
 - 1.2 IBM Virtualization Engine TS77005
 - 1.3 Assessment and Technical Report.....6

- 2. Compliance Assessment with SEC Rule 17a-4(f) 7**
 - 2.1 Structure and Organization of Cohasset’s Assessment.....7
 - 2.2 Non-rewriteable, Non-erasable Format7
 - 2.3 Verify Automatically the Quality and Accuracy of the Recording Process 11
 - 2.4 Serialize the Original and Duplicate Units of Storage Media 13
 - 2.5 Store Separately a Duplicate Copy..... 14
 - 2.6 Other Requirements of the Rule 16

- 3. Conclusions 17**

- End Notes 18**

- Appendix A: Retention Management Options 19**

- Appendix B: Magnetic Disk Recording Quality and Accuracy..... 21**

- Appendix C: Other Non-applicable Rules 23**

- About Cohasset Associates, Inc. 26**

Prepared by:
Cohasset Associates, Inc.
3806 Lake Point Tower
505 North Lake Shore Drive
Chicago, IL 60611 USA
www.cohasset.com
312-527-1550
2.0

This technical report and the information contained in it are copyrighted and are the sole property of Cohasset Associates, Inc. Selective references to the information and text of this technical report are welcome, provided such references have appropriate attributions and citations. Permission is granted for in-office reproduction so long as the contents are not edited and the “look and feel” of the reproduction is retained.

1. Introduction

This section sets the context for this technical assessment. It identifies a) the SEC's regulatory foundation for allowing e-records to be retained on a variety of electronic storage media, and b) the storage system that is the subject of Cohasset's assessment against these SEC electronic storage media regulations.

1.1 The Electronic Storage Requirements of the Securities & Exchange Commission for 17a-4 Records

Records retention requirements for the U.S. securities broker-dealer industry are stipulated by the Securities & Exchange Commission ("SEC") Regulations 17 CFR 240.17a-3 and 17 CFR 240.17a-4 adopted on February 12, 1997. Within this regulation, Rule 17a-4(f) (the "Rule" or "Regulation") expressly allows records to be retained on electronic storage media, subject to meeting certain conditions.

Three foundational documents collectively define and interpret the 16 specific regulatory requirements that must be met in order to be SEC-compliant under Rule 17a-4(f). They are:

- The Rule itself,
- SEC Interpretive Release No. 34-44238, *Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with Respect to Rule 17a-4*, dated May 1, 2001 (the "2001 Release"), and
- SEC Interpretive Release No. 34-47806, *Electronic Storage of Broker-Dealer Records*, dated May 7, 2003 (the "2003 Release").

In the Rule and the two subsequent interpretative releases, the SEC clearly states that the use of electronic storage media and devices, to the extent that they can deliver the prescribed functionality, satisfy the stipulations of Rule 17a-4.

Rule 240.17a-4(f) specifically states that:

The records required to be maintained and preserved pursuant to § 240.17a-3 and § 240.17a-4 may be immediately produced or reproduced on “micrographic media” (as defined in this section) or by means of “electronic storage media” (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form [emphasis added].

(1) For purposes of this section:

* * * * *

(ii) *The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(1)(i) and f(1)(ii) of this section, which meets the applicable conditions set forth in this paragraph (f).*

The 2003 Release further clarifies that implementation of rewriteable and erasable media, such as magnetic tape or magnetic disk, may meet the requirements of a non-rewriteable, non-erasable recording environment – to the extent that they deliver the prescribed functionality so long as appropriate integrated control codes are in place. The 2003 Release states:

A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.

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

Examples of integrated control codes that could be applied towards providing a non-rewriteable, non-erasable recording process are:

- Specific identifiers or attributes and program logic which allow records to be protected against erasure or overwrite,
- A retention period during which records cannot be erased,

- A unique record identifier that differentiates each record from all other records, and
- The date/time of recording (the date/time of recording and the unique identifier serve in combination to “serialize” a record).

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

An important associated requirement of Rule 17a-4(f)(2)(i) is that a member, broker or dealer wanting to store its 17a-3 and 17a-4 records electronically must notify its “examining authority” ninety (90) days prior to employing any technology other than write-once-read-many (“WORM”) optical media. Examining authorities are self-regulatory organizations (“SROs”) under the jurisdiction of the SEC such as the New York Stock Exchange (“NYSE”) and the Financial Industry Regulatory Authority (“FINRA”).

1.2 IBM Virtualization Engine TS7700

The IBM Virtualization Engine TS7700 (“TS7700”) is designed to provide a higher-performance storage environment by combining high-performance magnetic disk storage with optional magnetic tape drives to offer a virtual magnetic tape storage solution.

The TS7700 provides a virtual magnetic tape management system in that electronic records¹ are written to a “virtual volume”² (either on magnetic disk only or on a combination of magnetic disk storage and magnetic tape media) that emulates the characteristics of recording to physical magnetic tape volumes (i.e. magnetic tape cartridges).

With Release 1.6, the TS7700 provides the capabilities that prevent any erasure or overwrite of electronic records by embedding control codes which are integral and unique to a) a specially defined Data Class³ and b) individual virtual volumes related to that specific Data Class.

There are two models of the TS7700:

- TS7720 – records virtual volumes only to magnetic disk storage and
- TS7740 – records virtual volumes to magnetic disk storage and to IBM magnetic tape drives and cartridges.

1.3 Assessment and Technical Report

To obtain an independent and objective assessment of the TS7700's capabilities to meet the requirements set forth in SEC Rule 17a-4(f), IBM Corporation ("IBM") engaged Cohasset Associates, Inc. ("Cohasset"), a highly respected consulting firm with specific knowledge, recognized expertise, and more than 30 years of experience regarding the legal technical and operational issues associated with the records management practices of companies regulated by the SEC and SROs.

Cohasset's assignment was to:

- Assess the ability of the TS7700's capabilities to meet the requirements of all the relevant conditions of Rule 17a-4(f), and
- Prepare this technical report regarding that assessment.

This assessment represents the professional opinion of Cohasset Associates and should not be construed as an endorsement or rejection by Cohasset of the TS7700 and its capabilities, or other IBM products. The information utilized by Cohasset to conduct this assessment consisted of a) oral discussions, b) system design documents, c) user documentation, and d) other directly related materials provided by IBM.

The content and conclusions of this assessment are not intended and should not be construed as legal advice. Relevant laws and regulations are constantly evolving and legal advice must be tailored to the specific circumstances of the laws and regulations for each organization. Therefore, nothing stated herein should be substituted for the advice of competent legal counsel. Additional information about Cohasset Associates is provided on page 26 of this report.

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

This section presents Cohasset's assessment of the TS7700's capabilities that are relevant in meeting the electronic records storage requirements of SEC Rule 17a-4(f).

2.1 Structure and Organization of Cohasset's Assessment

The assessment of each relevant requirement in Rule 17a-4(f) is organized into four parts:

Compliance Requirement – Definition of the specific SEC regulatory requirements that must be met in order to utilize electronic records storage media in the retention of 17a-3 and 17a-4 records,

Compliance Assessment – Cohasset's assessment of the degree to which TS7700 capabilities comply with the Rule,

TS7700 Capabilities – Description of the TS7700 capabilities that enable them to meet the specific 17a-4(f) requirement, and

Other Considerations – Identification of actions (if any exist) that may need to be performed in order to meet the requirements of the Rule.

2.2 Non-rewriteable, Non-erasable Format

2.2.1 Compliance Requirement 17a4(f)(2)(ii)(A)

Preserve the records exclusively in a non-rewriteable, non-erasable format.

As set forth in Section III(B) of the 2001 Release, this requirement “is designed to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in unalterable form.”

The following statement in the 2003 Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, would meet the requirements of a non-rewriteable, non-erasable recording environment provided a) they deliver the prescribed functionality, and b) that functionality is delivered for as long as appropriate integrated control codes are in place:

A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.

2.2.2 Compliance Assessment

It is Cohasset Associates' opinion that the TS7700 meets this requirement of the Rule, provided certain recommendations stated in subsection 2.2.4, "Other Considerations," are performed.

2.2.3 TS7700 Capabilities

TS7700 Release 1.6 uses multiple control codes that are integral to a) a defined Data Class and b) virtual volumes associated with that defined Data Class. The integral control codes are designed to protect records against erasure or overwrite and thereby meet the requirements of the Rule for non-rewriteable, non-erasable recording.

In the administrative setup of the TS7700 each Data Class must be defined, named and configured with the Logical WORM ("LWORM") attribute set to "Yes." Once set, the LWORM functionality automatically ensures that electronic records written to virtual volumes associated with an LWORM-configured Data Class will be protected against subsequent erasure or overwrite.

In conjunction with the Data Class LWORM setting, the TS7700 employs other integral control codes to prevent overwrite. The primary control code is the worldwide identifier ("WWID") – a unique identifier that is cryptographically generated and temporarily assigned to each virtual volume in a Data Class with the LWORM attribute at the time the virtual volume is initially mounted. The WWID then is "bound" to each virtual 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 virtual 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. A second integrated control code, a Write-Mount-Count (“WMC”), is used to track the number of times a virtual volume has been mounted for recording purposes.

The LWORM Data Class name, the WWID, and WMC (for each LWORM virtual volume) are recorded to the TS7700 management metadata and to the volume header information. The control codes also are made available to the host operating system (e.g., IBM z/OS/DFSMS) and passed to the removable media management system (e.g., IBM DFSMSrmm or Computer Associates CA-1) 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.

Once the retention period (controlled externally from the TS7700) for all data records on a virtual volume has expired, the LWORM virtual volume may be released (into a scratch pool⁴) for reuse.⁵ Note: The TS7700 does not provide retention management capabilities because it is emulating a physical magnetic tape storage system, which does not provide for retention management. See the additional information in the sub-sections on “Retention Management” and “Legal Hold” below.

The status of a Data Class can be modified administratively at any time by setting the LWORM attribute to “no” or non-LWORM. All virtual volumes of electronic records recorded up to the time of a status change will continue to be protected as non-rewritable and non-erasable. See additional information in sub-section “Other Considerations.”

Because the TS7700, like all magnetic tape storage systems, operates only at the volume management level and has no knowledge of the content or context of the individual electronic records or data sets stored, Cohasset’s believes there is no possibility that individual electronic records or sets of electronic stored records could be erased or overwritten by the TS7700 itself.

Retention Management

Retention management must be accomplished at the level of the individual electronic record or data set, but, because all magnetic tape systems (both virtual and physical) intrinsically have

no content-level knowledge of the information being stored, all magnetic tape systems have no capability to manage the retention of the individual electronic records or data sets they store. Accordingly, since the TS7700 emulates a physical magnetic tape storage system (WORM magnetic tape), the TS7700 also has no capability of providing retention management.

Ensuring that required retention periods are applied to the virtual volumes stored in a TS7700 is therefore the responsibility of the member, broker, or dealer. Two ways that retention management of records stored in a TS7700 could be accomplished are:

- Using procedures and tools as defined and executed by the member, broker or dealer, or
- Employing the electronic record retention management capabilities provided by a content or records management application such as the IBM Object Access Method or by the volume management capabilities of the removable media management system (e.g., IBM DFSMSrmm or Computer Associates CA-1).

The second way is preferable since it is the most automated and therefore the least prone to human error or possible malfeasance.

See Appendix A for additional information regarding IBM product capabilities for managing retention.

Legal Hold

It is the member, broker or dealer that has the responsibility of ensuring that virtual volumes of electronic records are preserved in accordance with a legal discovery order or a regulatory audit “hold.”

To support organizations in meeting their legal/audit “hold” requirements, the TS7700 administrator has the capability to place records on “hold” by setting a “hold” on an LWORM virtual volume when it is released to scratch status by the host operating system or the removable media management system.

As long as the “hold” condition is active, the released scratch virtual volumes cannot be mounted for reuse. This allows TS7700 LWORM virtual volumes to be retained, as necessary, beyond the required retention period for as long as a legal hold order or other longer-term regulatory hold is active.

2.2.4 Other Considerations

The member, broker, or dealer should consider the following to ensure that the TS7700 is appropriately configured and managed to protect electronic records against erasure or overwrite:

- The TS7700 must be at Release 1.6, since prior releases do not support the non-rewriteable, non-erasable functionality. All operating systems (e.g., z/OS/DFSMS) and removable tape management systems (e.g., DFSMSrmm) must be at a release level that supports TS7700 Release 1.6 LWORM capabilities.
- The TS7700 must be administratively configured so that the Data Classes defined for storing regulated electronic records have the LWORM attribute set to “yes.”
- The host operating system and the removable media management system must be configured to write regulated records only to LWORM Data Classes and associated virtual volumes.
- Cohasset Associates recommends that the member, broker, or dealer establish administrative procedures that do not allow the LWORM attribute of a defined Data Class to be modified from “yes” to “no” or to non-LWORM.

Although modifying the status of a Data Class from LWORM to non-LWORM does not compromise the virtual volumes of electronic records previously recorded, to ensure that regulated records are not (unintentionally or intentionally) written to virtual volumes in a non-LWORM Data Class, all such modifications must be carefully coordinated so the correct Data Class is assigned.

- To meet the SEC’s requirements for record retention, the member, broker, or dealer must put in place appropriate procedures or, preferably, utilize automated records management capabilities such as those detailed in Appendix B.

2.3 Verify Automatically the Quality and Accuracy of the Recording Process

2.3.1 Compliance Requirement 17a-4(f)(2)(ii)(B)

Verify automatically the quality and accuracy of the storage media recording process.

The intent of SEC Rule 17a-4(f)(2)(ii)(B) is to ensure that the media recording process is accurate to a very high degree and, therefore, the recorded information is of the highest quality. The

objective of this subsection of the Rule is to provide the utmost confidence that all records read from the storage media are precisely the same as those recorded.

2.3.2 Compliance Assessment

Cohasset believes that the TS7700 has the capabilities to meet the SEC requirement to verify the accuracy and completeness of the recording process. See additional comments in subsection 2.3.4, “Other Considerations.”

2.3.3 TS7700 Capabilities

The TS7700 relies on state-of-the-art magnetic disk and, optionally, magnetic tape recording technologies to meet the quality and accuracy requirements of the Rule.

The following TS7700 capabilities directly support the verification of the quality and accuracy of the recording process:

- The use of cyclical redundancy checks (“CRC”)⁶ to verify the quality and accuracy of the recording process.

A CRC of the electronic record data set is generated by the host operating system (e.g., z/OS) channel recording component and sent to the TS7700. The TS7700, in turn, recalculates and checks the CRC to ensure that the information sent by the host operating system has been completely and accurately received.

The TS7700 then calculates a separate CRC based on the content of the electronic record data set, which then is recorded with the related electronic record data sets to a virtual tape volume.

- When an electronic record data set is read-back as part of the information retrieval process, the following two-step quality and accuracy check is executed.

First, the TS7700 reads the electronic record data set from magnetic disk or magnetic tape with the stored CRC, then recalculates the CRC and compares it to the stored CRC.

Second, the TS7700 calculates a new CRC that it sends with the electronic record data set to the host operating system channel component, which then recalculates the CRC and compares it to the one sent by the TS7700.

Both of these CRC validations are performed to ensure that no errors have occurred during storage or retrieval. If the CRC comparisons do not agree, the recording or read-back process is aborted. The read-back process then is attempted multiple times. If also unsuccessful, an error message is generated so that an administrative recovery can be initiated.

2.3.4 Other Considerations

Cohasset Associates believes that state-of-the-art magnetic disk and magnetic tape recording technologies meet both the letter and the spirit of the SEC Rule for these reasons:

- They provide quality and accuracy checks and monitoring during the magnetic storage recording process (such as CRCs) and, where applicable, direct read-after-write bit recording verification in the magnetic tape drives.
- They have advanced techniques for detecting and correcting both minor and relatively major data errors during read back, and
- They are relied upon by private and public entities, in the regular course of their business operations, to store critical business and regulatory electronic data with the highest levels of accuracy.

See Appendix B for additional discussion regarding verification of recording quality and accuracy using magnetic and disk magnetic tape technologies.

2.4 Serialize the Original and Duplicate Units of Storage Media

2.4.1 Compliance Requirement 17a-4(f)(2)(ii)(C)

Serialize the original, and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media.

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

While this requirement is more pertinent to tracking the individual units of removable media related to micrographic or optical storage, this SEC Rule requirement can be satisfied for all other types of electronic records storage systems by capturing index or metadata associated with

each record or volume of records that: a) “uniquely” identifies the record file, and b) associates a “date of recording” with each record or volume.

2.4.2 Compliance Assessment

Cohasset believes that IBM’s TS7700 meets the SEC requirement to serialize both the original record and each duplicate copy stored.

2.4.3 TS7700 Capabilities

The TS7700 automatically performs serialization and tracking of electronic records to virtual volumes using the following capabilities:

- The TS7700 serializes each virtual volume by recording a header (containing the volume serial number as well as the unique WWID and WMC) at the beginning of each virtual volume.
- The TS7700 maintains a metadata database that includes serialization and tracking information, specifically, the volume serial number, as well as the WWID and the WMC attributes for each virtual volume.
- The TS7700’s identification and serialization information (including the virtual volume serial number, as well as the WWID and the WMC attributes) are made available to the operating system and are stored and tracked by the removable media management system.

2.4.4 Other Considerations

There are no other considerations related to this requirement.

2.5 Store Separately a Duplicate Copy

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

Store separately from the original a duplicate copy of the record stored on any medium acceptable under 240.17a-4 for the time required.

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

Note: A “duplicate copy” is different from a backup copy. A duplicate copy is the recording of

each electronic record data set to a second compliant storage system or media. Such a duplicate then is retained as a non-rewriteable, non-erasable copy for the same period of time as the originally stored record. Backup copies, on the other hand, are typically overwritten as they are “rotated” on a periodic basis – usually a much shorter period of time than the retention time of the electronic record data sets (and related duplicate copies) preserved according to the Rule.

2.5.2 Compliance Assessment

It is Cohasset’s opinion that the TS7700 complies with this SEC requirement.

2.5.3 TS7700 Compliance Capabilities

The following capabilities of the TS7700 facilitate meeting this SEC requirement:

- When electronic records are written to virtual volumes on a primary TS7700 cluster, a duplicate copy of those records can be written automatically to a second TS7700 cluster. When this occurs, the LWORM Data Class information, as well as the WWID and WMC, is recorded automatically with the copy. Such duplicate copies can be produced either synchronously (immediately when recording of the primary virtual volume is complete) or asynchronously (at a designated point subsequent to completion of the recording of the primary virtual volume).
- Duplicate copies of TS7720 virtual volumes can only be recorded to a second TS7700 cluster because the TS7720 does not support the attachment of magnetic tape drives.
- Model TS7740 duplicate copies can be recorded to a second TS7700 cluster or to the magnetic tape drives and cartridges configured on the Model T7740. The TS7740 does not provide for the use of WORM magnetic cartridges. However, all LWORM control code information (e.g., WWID), are recorded to duplicate copies recorded to a physical magnetic tape cartridge, thereby meeting the non-rewriteable, non-erasable requirements of the Rule.

2.5.4 Other Considerations

If a second TS7700 cluster is not configured, or if a TS7700 is not configured with magnetic tape drives, the member, broker, or dealer must ensure that appropriate procedures and duplicate copy capabilities are provided in order to create the duplicate copies necessary to meet the requirements of the Rule.

2.6 Other Requirements of the Rule

A number of other requirements of SEC 17a-4(f) are not the direct responsibility of the TS7700 virtual tape storage system. These other requirements of the Rule must be met by other product capabilities or by procedures and processes provided by the member, broker, or dealer in order for the overall electronic records management environment that utilizes the TS7700 to meet all of the requirements of the Rule.

The other requirements fall into areas such as:

- Providing, managing and retaining index information for search and retrieval of individual electronic records,
- Reproducing a copy of each individual electronic record,
- Providing and retaining an audit trail that logs events affecting the life cycle of individual electronic records, and
- Providing procedures to be followed by the member, broker or dealer to assure that access to electronic records is provided in the case of a disaster.

Appendix C lists each of the other requirements that are beyond those for which the TS7700 is directly responsible.

3. Conclusions

This technical assessment has addressed whether the functional capabilities of the TS7700 meet the requirements and conditions of SEC Rule 17a-4(f) for which it is directly responsible.

Cohasset's conclusion is that the capabilities of the TS7700, Release 1.6:

- Meet the requirements of the Rule for preserving electronic records in a non-rewriteable, non-erasable format when a) the Data Class recording mode is set to LWORM and b) the WWID and WMC attributes are generated by the TS7700, stored in the metadata of the TS7700 and the virtual volume header, obtained by the operating system and stored by the removable media management system.
- Meet the letter of the Rule relating to the automatic verification of the accuracy and quality of the recording process – because the TS7700 relies on trusted quality and accuracy checks inherent in state-of-the-art magnetic disk and magnetic tape recording technology.
- Uniquely identify and serialize the original and duplicate copy of each LWORM volume stored - by generating and binding a unique WWID to each virtual volume and duplicate copy that identifies them as non-rewriteable, non-erasable LWORM.
- Support multiple methods for storing a compliant duplicate copy of each record.

Note: TS7700 users (members, brokers, or dealers) must ensure a) the LWORM parameter (for each TS7700 Data Class where regulated records are to be stored) is set to “yes,” b) appropriate secondary clusters of model TS7740 or TS7720 are configured to automatically create a duplicate copy or put in place other compliant procedures and that duplicate copy capabilities are provided, and c) procedures are established so the LWORM attribute in a previously defined Data Class cannot be reset to “no.”

Cohasset Associates' conclusion: The TS7700 meets all of the SEC requirements that are its direct responsibility for retaining and storing in digital form 17a-3 and 17a-4 records – pursuant to the requirements set forth in Rule 17a-4(f), which expressly allows records to be retained on electronic storage media.

End Notes

1. The terms “electronic record,” “electronic record data set,” “record” and “data record” are used in this technical report as interchangeable terms to describe an electronic file of data- or document-based information that is defined and regulated by SEC Rules 17a-3 or 17a-4. In the terminology of magnetic tape storage, an “electronic record” would be recorded as part of a data set; there may be one or multiple data sets recorded on a volume of media.
2. A “volume” is a distinct unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. A virtual volume is a tape volume that resides in a tape volume cache or a virtual tape server. (Source: IBM Globalization Terminology.) For purposes of this technical report, the terms “volume” and “virtual volume” are intended to mean a storage space equivalent to and managed so that it emulates a physical magnetic tape cartridge volume.
3. A Data Class defines a particular set of electronic records that likely are related from a business operations perspective, e.g., confirms, broker e-mail, etc., and that are to be similarly managed by the TS7700.
4. A scratch volume is a virtual or physical tape volume (or a set of tape volumes - a scratch pool) that “is either blank or contain no valid data, that is not currently defined, and that is available for use (IBM Globalization Terminology).”
5. Allowing the reuse (overwrite) of a released LWORM TS7700 volume of magnetic tape (whether a physical cartridge media volume or a virtual volume on magnetic disk media) is no different than allowing for the manual destruction (erasure) of a physical magnetic tape cartridge that affords inherent WORM overwrite or erasure protection. In either case, the electronically stored information on the physical or virtual volume is destroyed. In both cases, a host operating system or application is managing the retention period of the data records and associated magnetic tape volumes and, therefore, has the responsibility in conjunction with procedures of the member, broker or dealer to retain the data records for the required period of time before releasing the media for reuse or destruction.
6. Cyclic redundancy check (“CRC”) – A redundancy check in which the check key is generated by a cyclic algorithm (Source: IBM Terminology). A CRC is a non-secure hash function designed to detect accidental changes to raw computer data, and is commonly used in digital networks and storage devices such as hard disk drives. A CRC-enabled device calculates a short, fixed-length binary sequence, known as the CRC code or just CRC, for each block of data and sends or stores them both together. When a block is read or received, the device repeats the calculation. If the new CRC does not match the one calculated earlier, the block contains a data error and the device may take corrective action such as rereading or requesting the block be re-sent. Otherwise the data is assumed to be error free. (Source: Wikipedia).

Appendix A: Retention Management Options

Retention management must be accomplished at either a) the volume level or b) the electronic record (object) sets of electronic records, which is frequently referenced as the data set-level. Managing retention at the electronic record/data set level is not possible with virtual (or physical) magnetic tape storage systems, such as the TS7700, since they have no content-level knowledge of the information being stored. Ensuring that the required retention period is applied therefore must be provided outside of the TS7700. This can be done in either of two ways:

- Volume retention management capabilities provided by a removable media management system (e.g., IBM DFSMSrmm or Computer Associates CA-1) or,
- Electronic record retention provided by an application-level records management capability (e.g., through IBM Object Access Method).

DFSMSrmm Removable Media Management System

In DFSMSrmm, retention can be managed by establishing one or more vital record specifications that define retention policies for electronic record data sets (such as a computer report, large e-mail archive or a contiguous set of document-based information) or virtual volumes. The electronic record data set vital record specifications then apply to the volume on which the electronic record data set resides. Volume vital record specifications assume nothing about the content of the electronic record data sets on the volume.

IBM Object Access Method (OAM)

OAM has three electronic records management capabilities that are available with the OAM Archive Retention Enhancement support in z/OS V1R11.

1. **Retention-protection.** Retention-protection provides OAM's most stringent protection to ensure that an object has not been modified or deleted prior to its expiration date. When retention-protection is enabled for a given object, OAM will not allow that

object to be deleted prior to its expiration date. Additionally, OAM will not allow the expiration date to be changed to an earlier date. It will however, allow the expiration date to be changed to a later date. If an object is stored into an object storage group that has retention-protection enabled, that object is considered retention-protected for the life of the object. Installations cannot disable retention-protection for a retention-protected object.

2. **Event-based-retention.** When an object is in event-based-retention mode, its expiration date is not calculated until OAM has received notification that an external event has occurred. The external event notification event is received by OAM via the OAM application programming interface (“API”) for triggering event-based retention period calculation.
3. **Deletion-hold.** When an object is in deletion-hold mode, it cannot be deleted from the OAM. Deletion holds are set and released using OAM’s APIs.

The retention management capabilities of OAM are utilized by IBM OnDemand content management applications, such as OnDemand for Enterprise Report Management.

Other Retention Options

Electronic record retention management also can be implemented using specialized applications such as IBM Records Manager or IBM FileNet Records Manager.

Appendix B: Magnetic Disk Recording Quality and Accuracy

In the early 1990s, when the SEC first was considering the use of digital media for storing regulated records, the only non-rewritable, non-erasable media available was write-once, read-many (“WORM”) optical disk. At that time, WORM optical disk required either a) a direct read after write (“DRAW”) capability or b) a second rotation of the media with a read-back and comparison operation to verify the quality and accuracy of the recording process. Optical recording technology was in its early stages and, therefore, was deemed to require a more thorough, read-after-write check to ensure recording accuracy.

When the Rule was promulgated in 1997, no specific methodology or time requirement for accomplishing the verification of recording quality and accuracy is mentioned in Rule 17a-4(f)(2)(ii)(B). As it relates to the spirit in which the initial Rule was developed, Cohasset’s interpretation of this requirement is that automatic verification of the media recording process should be done as close to the recording event as possible. In this context, magnetic disk and magnetic tape technologies are ideal in that they provide quality and accuracy checks in real time – as the recording process is being executed.

Today, when evaluating the level of recording quality and accuracy provided by state-of-the-art magnetic disk technology, these points should be considered:

- Magnetic disk technology has produced significant advances in the electronic controls, checks, and monitoring capabilities that are designed to provide a high degree of accuracy during the recording process.
- The degree to which a) the accuracy and quality of recording data or records is accomplished and b) the recording process can ensure that data or records are not lost (and can be fully corrected or recovered if found later in error) is critical to the reputation and the livelihood of the electronic information storage industry.
- The largest corporate and public entities have relied on the quality and accuracy of magnetic recording (appropriately backed up for recovery) for many decades. During

this period, the systems employing magnetic recording have shown that mission-critical, vital business and regulatory records can be preserved and retained over time as well as readily retrieved on demand.

- Significant error correction advances, such as the RAID 6 (redundant array of inexpensive disks), have been made in detecting and correcting errors that are encountered when reading records back from magnetic disk media.

Cohasset Associates believes state-of-the-art magnetic tape technologies meet the letter and spirit of the SEC Rule for these reasons:

- The IBM Total Storage 3592 magnetic tape drive and the IBM System Storage TS1120 and TS1130 magnetic tape drives automatically perform a bit-level write verification check as an integral part of its recording operation. A separate read/write head is positioned immediately behind the primary write head that reads back and verifies that the bit-level information intended to be recorded has indeed been accurately written.
- A multi-level error correction capability (“ECC”), which is an inherent part of the magnetic tape format, ensures that all data written to tape are written with no uncorrectable errors so, when read back, the data will be an accurate and complete representation of what was written.
- Additionally, data path integrity checks within the drive and between the drive and the media ensure that no external error situations cause data to be written incorrectly to the media.

Appendix C: Other Non-applicable Rules

Appendix C contains those provisions of Rule 17a-4(f) that are not applicable to the functionality provided by the IBM TS7700 virtual tape storage solution. These other requirements of the Rule must be met by other product capabilities or by procedures and processes provided by the member, broker, or dealer in order for the overall electronic records management environment that utilizes the TS7700 to meet all of the requirements of the Rule.

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

17a-4(f)(3)(i) At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images.

17a-4(f)(3)(ii) Be ready at all times to provide, and immediately provide, any facsimile enlargement which the Commission or its representative may request.

17a-4(f)(3)(iv) Organize and index accurately all information maintained on both original and any duplicate storage media.

17a-4(f)(3)(iv)(A) At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.

17a-4(f)(3)(iv)(B) Each index must be duplicated, and the duplicate copies must be stored separately from the original copy of each index.

17a-4(f)(3)(iv)(C) Original and duplicate indexes must be preserved for the time required for the indexed records.

17a-4(f)(3)(v) The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to 240.17a-3 and 204.17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

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

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

17a-4(f)(3)(vi) The member, broker, or dealer must maintain, keep current, and provide promptly upon request by the staffs of the Commission or the self-regulatory organizations of which the member, broker, or broker-dealer is a member all information necessary to access records and indexes stored on the electronic storage media; or place in escrow and keep current a copy of the physical and logical file format of the electronic storage media, the field format of all different information types written on the electronic storage media and the source code, together with the appropriate documentation and information necessary to access records and indexes.

17a-4(f)(3)(vii) For every member, broker, or dealer using electronic storage media for some or all of its record preservation under this section, at least one third party (“the undersigned”), who has access to and the ability to download information from the member’s, broker’s, or dealer’s electronic storage media to any acceptable medium under this section, shall file with the designated examining authority for the member, broker, or dealer the following undertakings with respect to such records:

The undersigned hereby undertakes to furnish promptly to the U.S. Securities and Exchange Commission (“Commission”), its designees or representatives, upon reasonable request, such information as is deemed necessary by the Commission’s or designee’s staff to download information kept on the broker’s or dealer’s electronic storage media to any medium acceptable under Rule 17a-4.

Furthermore, the undersigned hereby undertakes to take reasonable steps to provide access to information contained on the broker’s or dealer’s electronic storage media, including, as appropriate, arrangements for the downloading of any record required to be maintained and preserved by the broker or dealer pursuant to Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 in a format acceptable to the Commission’s

staff or its designee. Such arrangements will provide specifically that in the event of a failure on the part of a broker or dealer to download the record into a readable format and after reasonable notice to the broker or dealer, upon being provided with the appropriate electronic storage medium, the undersigned will undertake to do so, as the Commission's staff or its designee may request.

About Cohasset Associates, Inc.

[Cohasset Associates, Inc.](http://www.cohasset.com) (www.cohasset.com), is one of the nation's foremost consulting firms specializing in records and information management. Now in its fourth decade of serving clients throughout the United States, Cohasset Associates provides award-winning professional services in three areas: management consulting, education and legal research.

Management Consulting: The focus of Cohasset Associates' consulting practice is improving the programs, processes and systems that manage document-based information. Cohasset works to provide its clients with cost-effective solutions that will both achieve their business objectives and meet their legal/regulatory responsibilities. This ranges from establishing effective corporate records management programs to planning state-of-the-art electronic records systems.

Education: Cohasset Associates is renowned for its longstanding leadership in records management education. Today, Cohasset's educational work is centered on its annual National Conference for Managing Electronic Records ([MER](http://www.merconference.com)), which addresses the operational, technical and legal issues associated with managing the complete life cycle of electronic records (www.merconference.com). The MER sessions also are available at [RIM on Demand](http://www.rimeducation.com/videos/rimondemand.php) (www.rimeducation.com/videos/rimondemand.php).

Legal Research: Cohasset Associates is nationally respected for its leadership on records management legal issues – from retention schedules to the use of alternative media to paper for storing document-based information.

For more than twenty years, Cohasset Associates has been a “thought leader” in records and information management. Cohasset has been described as *the only management consulting firm in its field with its feet in the trenches and its eye on the horizon*. It is this blend of practical experience and a clear vision of the future that, combined with Cohasset Associates' commitment to excellence, has resulted in Cohasset Associates' extraordinary record of accomplishments and innovation.