Cohasset Associates

Veritas™ NetBackup™ Flex Scale

COMPLIANCE ASSESSMENT

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

Abstract

Veritas™ NetBackup™ Flex Scale is a hyperconverged, scale-out data protection solution that provides backup and recovery services for safeguarding digital content against catastrophic events such as unexpected business disruptions and security attacks. NetBackup Flex Scale captures point-in-time *Image*s of source system workloads (e.g., databases, files systems, virtual machines) and applies *Lockdown* retention controls that are designed to meet securities industry requirements for electronic recordkeeping.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of NetBackup Flex Scale (see Section 1.3, *NetBackup Flex Scale 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 NetBackup Flex Scale, when properly configured and used with the *Lockdown* retention feature in either *Compliance* or *Enterprise* mode, has functionality that meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). Additionally, the assessed functionality of NetBackup Flex Scale meets the principles-based requirements of CFTC Rule 1.31(c)-(d).

COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to our practice is the delivery of records management and information governance professional consulting services, and education and training. Cohasset's expert consulting services support regulated organizations, including those in financial services. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls to their organizations' business priorities, facilitating regulatory compliance and risk mitigation, while generating quantifiable business efficiency.

Cohasset assesses a range of electronic recordkeeping systems, each designed to meet the requirements of the Securities and Exchange Commission Rules 17a-4(f)(2) and 18a-6(e)(2) for record audit-trail and non-rewriteable, non-erasable record formats, considering the SEC 2001, 2003 and 2019 interpretations. For the non-rewriteable, non-erasable record, these interpretations authorize the use of erasable storage, conditioned on integrated software or hardware control codes, to prevent overwriting, erasing, or otherwise altering the records, during the applied retention period.

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

This Introduction *summarizes the regulatory environment pertaining to this assessment and the purpose and approach for Cohasset's assessment. It also provides an overview of Veritas NetBackup Flex Scale and the assessment scope.*

1.1 Overview of the Regulatory Requirements

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

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

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

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

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

1.1.2 FINRA Rule 4511(c) Requirements

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

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

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

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

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

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

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

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

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

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of NetBackup Flex Scale for preserving required electronic records, Veritas 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.

Veritas engaged Cohasset to:

- Assess the functionality of NetBackup Flex Scale, 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 NetBackup Flex Scale; 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, meets 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 NetBackup Flex Scale and its functionality or other Veritas 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 Veritas 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 NetBackup Flex Scale Overview and Assessment Scope

1.3.1 NetBackup Flex Scale Overview

NetBackup Flex Scale is a hyperconverged, scale-out data protection solution that provides backup and recovery services to safeguard digital content against catastrophic events such as unexpected business disruptions and security attacks.

NetBackup Flex Scale captures point-in-time *Images*[4] of source system workloads (e.g., databases, file systems, virtual machines) and retains them according to rules defined in backup policies. Integrated immutability[5] and indelibility[6] controls are applied within the storage subsystem during the backup process, to retain *Images* in compliance with securities industry electronic record-keeping requirements.

NetBackup Flex Scale is an appliance-based solution. The logical architecture of NetBackup Flex Scale, responsible for managing the storage of *Images*, is depicted in Figure 1, below.

Three primary architectural components, which are an integral part of the NetBackup Flex Scale appliance, are responsible for compliant storage:

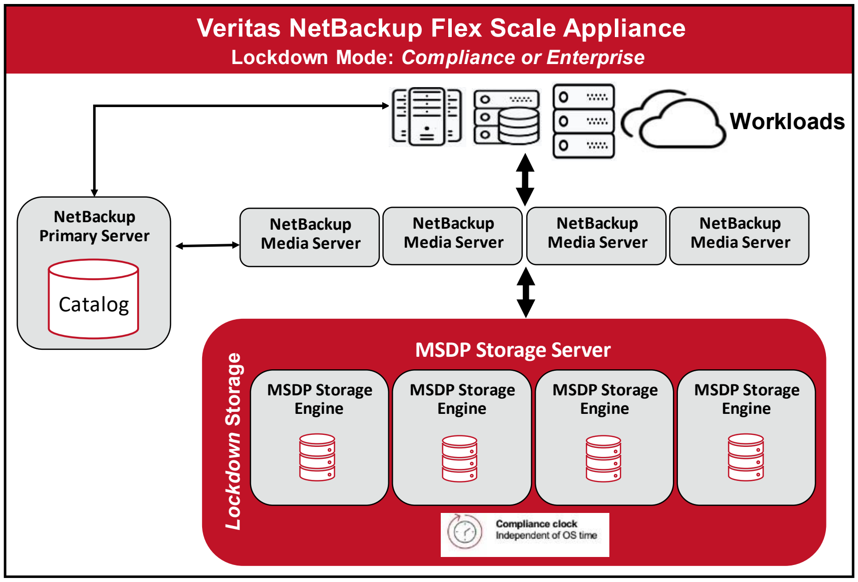

Figure 1: NetBackup Flex Scale Logical Architecture

NetBackup Primary Server – Provides scheduling, resource management, and the user interface control plane for managing retention policies and post-retention disposition. The Primary Server Catalog, maintained on Primary Server Storage, is the index of stored *Images* and is also managed by the Primary Server.

Media Server(s) – Are intelligent load-balancing gateways, or data movers, between the source system workloads and the MSDP[7] Storage Server (i.e., storage subsystem).

MSDP Storage Server – A single tenancy, scale-out deduplicated storage pool consisting of four to sixteen storage nodes, each with its own Intel-based CPU, memory, network and disks. All storage nodes are treated as a single entity by NetBackup. A configuration setting at the NetBackup Flex Scale appliance level, called *Lockdown* mode, determines the type of

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

[5] Immutability controls, also referred to as WORM (write-once, read-many) controls within Veritas NetBackup Flex Scale, ensure that an *Image* cannot be ***modified*** or ***overwritten*** by disallowing the use of any modifying commands or functions.

[6] Indelibility controls ensure that an *Image* cannot be ***deleted*** by any means, until expiration of applied retention rules.

[7] Veritas Media Server Deduplication Pool (MSDP) technology is embedded within the Flex Scale Appliance storage subsystem and is responsible for deduplicating data received from a client source prior to writing to storage.

integrated retention controls that will be made available for use within the MSDP Storage Server. *Lockdown* mode options include:

- *Compliance* mode – a highly-restrictive retention mode which applies strict, integrated control codes that extend to the storage subsystem and systemically disallow administrators from shortening or removing retention controls.
- *Enterprise* mode – a less-restrictive retention mode with software control codes that allow authorized administrators to shorten or remove retention controls applied to previously stored *Images*; *thus,* ***administrative procedures and monitoring are required to ensure compliant retention protections are enforced***.
- Normal mode – no retention mode controls are available.

Lockdown retention controls, including an appropriate *WORM Retention Period*, are applied to *Images* during the recording process, according to rules defined in NetBackup Policies.

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the capabilities of the fully integrated, enterprise-grade NetBackup Flex Scale appliance (version 3.1), with:

- All necessary NetBackup services instantiated (e.g., NetBackup Primary Server, Media Servers, and MSDP Storage Server with a minimum of four storage nodes), and
- The *Lockdown* retention feature configured for the appliance in either *Compliance* (highly-restrictive) or *Enterprise* (less-restrictive) mode.

NOTES: The NetBackup Flex Scale appliance is available directly from Veritas-qualified third parties. Deployments utilizing storage subsystems other than the NetBackup Flex Scale appliance are outside of the scope of this Compliance Assessment Report.

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

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

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

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

2.1 Record and Audit-Trail

2.1.1 Compliance Requirement

This regulatory requirement, adopted with the 2022 Rule amendments, allows regulated entities to use a combination of electronic recordkeeping systems, with each system meeting either (a) the record and audit-trail requirement, as described in this section or (b) the non-rewriteable, non-erasable record format requirement, as explained in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*.

This record and audit-trail requirement is designed to permit use of the regulated entities' business-purpose recordkeeping systems to achieve the required outcome without specifying any particular technology solution.

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

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

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

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

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

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

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

> *[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*[8] [emphasis added]

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

> *[T]he audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6.*[9] [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed NetBackup Flex Scale in comparison to this requirement of the SEC Rules.

For enhanced control, a business-purpose recordkeeping system may store records and complete time-stamped audit-trails on NetBackup Flex Scale, with the features and controls described in Sections 2.2 through 2.6 of this report.

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

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

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

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

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

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

[8] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

[9] 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.*[10] [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.*[11] [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of NetBackup Flex Scale, with the *Lockdown* retention feature in either *Compliance* or *Enterprise* mode, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[12] retention periods, when (a) properly configured, as described in Section 2.2.3 and (b) the considerations described in Section 2.2.4 are satisfied.

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

2.2.3 NetBackup Flex Scale Capabilities

This section describes the functionality of NetBackup Flex Scale that directly pertains to this SEC requirement to preserve electronic books and records in a non-rewriteable, non-erasable format, for the required retention period.

2.2.3.1 Overview

- Each *Image,* in NetBackup Flex Scale, is a point-in-time backup copy of a specified source system workload and provides a recovery point to reestablish the ***collection of records*** included in the *Image*.
- The NetBackup Flex Scale appliance must be configured with the *Lockdown* retention feature in either *Compliance* or *Enterprise* mode.
  - *Compliance* mode is a highly-restrictive retention mode which applies strict, integrated control codes that extend to the storage subsystem and systemically disallow administrators from shortening or removing retention controls.

[10] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

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

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

- *Enterprise* mode is a less-restrictive retention mode with software control codes that allow authorized administrators to shorten or remove retention controls applied to previously stored *Images*; *thus,* ***administrative procedures and monitoring are required to ensure compliant retention protections are enforced when using Enterprise mode***.

- ▶ *Lockdown* retention controls, including an appropriate *WORM Retention Period*, are applied to *Images* during the recording process, according to rules defined in NetBackup Policies.
- ▶ The following table summarizes the *Lockdown* retention controls applied in *Compliance* versus *Enterprise* modes.

	Lockdown **retention controls, in highly-restrictive** ***Compliance*** **mode**	***Lockdown*** **retention controls, in less-restrictive** ***Enterprise*** **mode**
Protecting record content and immutable metadata	● By design, the contents of an *Image* and its immutable metadata <u>cannot</u> be modified for the lifespan of the stored *Image*.	
Restricting changes to ***Lockdown*** **retention controls**	● The *Lockdown* mode set for the appliance cannot be downgraded or removed while *Images* are retained in storage. ● The *Lockdown* mode applied to an *Image* <u>cannot</u> be removed or downgraded to *Enterprise* or *Normal* mode. ● *The WORM Retention Period* applied to an *Image* may <u>not</u> be reduced or deleted by any NetBackup users or administrators but may be extended at any time.	● The *Lockdown* mode set for the appliance cannot be downgraded or removed while *Images* are retained in storage but may be upgraded to *Compliance.* ● The *Lockdown* mode applied to an Image <u>cannot</u> be removed or downgraded to *Normal* mode. ● The *WORM Retention Period* applied to an *Image* may be*:* ○ Extended at any time. ○ Reduced or removed by a privileged Appliance Administrator only.
Restricting deletion of ***Images***	● Attempts by any user to **delete** the *Image* prior to the expiration of the *WORM Retention Period* are <u>rejected</u>.	● Images, and the associated records, may be deleted prior to the expiration of the *WORM Retention Period*, via a ***dual-approval*** process, which requires actions to be taken by two separate administrators, each with restricted privileges.

See the following subsections for information on how to configure the *Lockdown* retention feature in *Compliance* or *Enterprise* mode and details about the resulting integrated controls.

2.2.3.2 Flex Scale Appliance and NetBackup Primary Server Configurations

The following configurations are required within the (a) NetBackup Flex Scale appliance and (b) the NetBackup Primary Server to enable the use of integrated *Lockdown* retention controls, which are designed to retain *Images* (i.e., collections of required records) in compliance with the non-rewriteable, non-erasable record format requirement of the SEC Rules.

- ▶ The <u>**NetBackup Flex Scale appliance**</u> comes preconfigured as described in Section *1.3 NetBackup Flex Scale Overview and Assessment Scope*. All necessary NetBackup services (e.g., NetBackup Primary Server, Media Servers, and MSDP Storage Server with a minimum of four storage nodes) are instantiated automatically on the appliance. By default, the appliance is set to operate in *Normal* mode, which does <u>not</u> support the application of *Lockdown* retention controls (i.e., immutability and indelibility controls are <u>not</u> supported in *Normal* mode).

- The Appliance Administrator must configure NetBackup Flex Scale appliances, intended to store required *Images,* to operate in *Compliance* or *Enterprise* mode as follows:

Appliance Level Configurations	
***Lockdown* Mode**	● Configure either *Compliance* or *Enterprise Lockdown* mode for the appliance during initial setup or at any time thereafter. ○ ***Compliance*** mode is a highly-restrictive configuration which applies strict, integrated control codes that extend to the storage subsystem and systemically disallow all users and administrators from reducing or removing retention controls. ○ ***Enterprise*** mode is a less-restrictive configuration that allows privileged administrators to reduce or remove retention controls. See Section 2.2.3.3 *Records and Retention Controls* for more information on *Compliance* and *Enterprise* modes. ● The *Lockdown* mode configured for the appliance applies to the entire MSDP Storage Server pool, meaning that all nodes within the MSDP Storage Server pool are capable of storing *Images* in a non-rewriteable, non-erasable format (hereinafter referred to as *Lockdown Storage*). Policies within NetBackup dictate whether the *Lockdown* retention controls are applied to each *Image* as it is written. ● The *Lockdown* retention mode for the appliance can be changed by a privileged Appliance Administrator from less restrictive to more restrictive at any time (i.e., changed from *Enterprise* to *Compliance*). Retention controls are applied to new *Images* according to NetBackup Policies, however: ○ When changing the appliance from *Normal* to either *Enterprise* or *Compliance* mode, previously stored *Images* remain unprotected. ○ When moving from *Enterprise* to *Compliance* mode, *Compliance* Mode Controls are automatically applied to previously stored *Images* and as such, premature deletion of those *Images* is prohibited. ● The *Lockdown* retention mode for the appliance may be changed to a less restrictive mode only when all existing protected *Images* have expired and are removed from storage. ● New nodes added to the MSDP Storage Server pool automatically inherit the existing Lockdown retention mode of the appliance.
Min/Max Retention Values	Set allowable Min/Max retention values (i.e., ranging between 1 hour and 60 years) as guardrails for *Lockdown Storage*. When an *Image* is written to *Lockdown Storage* with a retention value outside the established Min/Max values, the write process fails and an error message is generated.
Restricted Remote Access	Enable the *Restricted Remote Access* feature to limit Appliance Administrator capabilities to an approved set of non-destructive operations when remotely using IPMI infrastructure. Once the *Restricted Remote Access* feature is enabled for an appliance, configured in either *Compliance* or *Enterprise* mode, the feature cannot be disabled.
NetBackup Primary Server Level Configurations	
Storage Unit	A Storage Unit is a storage construct or label, referenced within NetBackup Policies that points to or identifies the specific physical storage pool to be used for retaining *Images*. ● For compliance with the Rules, a Storage Unit must be configured to support the application of *Lockdown retention controls* (hereinafter referred to as *Lockdown*-enabled) by (a) pointing to a WORM-capable Disk Pool[13] *(Lockdown Storage)* and (b) requiring WORM controls be applied (*Lockdown retention controls*). If these two requirements are not met, recorded *Images* **will not have *Lockdown retention controls* applied** and, therefore, the *Images* will **not** comply with the requirements of the Rules.

[13] *The NetBackup Primary Server utilizes different terminology than the NetBackup Flex Scale Appliance when referring to retention controls. Two examples are: (1) the phrase* **WORM-capable Disk Pool** is *used by the NetBackup Primary Server rather than* **Lockdown Storage** *and (2) the phrase* **WORM controls** is used in lieu of **Lockdown retention controls**.

	● When NetBackup is initially instantiated on the NetBackup Flex Scale appliance, one default Storage Unit is automatically created within NetBackup. ○ When the appliance *Lockdown* mode is set to *Compliance* or *Enterprise*, the default Storage Unit is automatically updated to properly point to a WORM-capable Disk Pool. ○ Additional Storage Units may be configured that point to a WORM-capable Disk Pool, with or without requiring the application of WORM controls. Accordingly, *Images* written via a Storage Unit **that does not require** WORM controls be applied, are recorded on *Lockdown Storage* without *Lockdown* retention controls applied. ● Once a Storage Unit is designated as *Lockdown*-enabled, it cannot be changed. ● Ideally, the names of both the Storage Unit and the *Lockdown Storage* it points to will contain the words COMPLIANCE WORM or ENTERPRISE WORM, for reference purposes. ● NetBackup Administrators must always verify that a Storage Unit points to properly configured *Lockdown* Storage via the MSDP Storage Server Properties screen on the NetBackup user interface.

2.2.3.3 Records and Retention Controls

- Digital content is transmitted from the source system according to scheduled or on-demand policies (described, below).
  - The source system workload (i.e., file system, database, virtual machine, applications, etc.) is copied via a stream, or multiple parallel streams of data, to the designated NetBackup Flex Scale MSDP Storage Server pool.
- A record in NetBackup is defined as an *Image* (i.e., a full, incremental, synthetic, or accelerator backup copy of a specified source system workload) along with system metadata associated with that *Image*.
  - System metadata includes critical attributes for records management, such as the unique backup ID (including the date and time backup was initiated at the source system), copy number, Immutable flag (Y/N), Indelible flag (Y/N), *WORM Retention Period* (in seconds), name of backup policy, type of backup policy, calculated *Retain Until Date*, content index, and checksum.
- *Lockdown* retention controls are **applied** to *Images* when the backup process executes, according to rules established in (1) NetBackup Policies and/or (2) *Storage Lifecycle Policies*:
  1. **A *<u>NetBackup Policy</u>*** is a predefined ruleset/schedule, created by the NetBackup Administrator, whereby a specified source system *workload* is copied to *Lockdown Storage* for data protection purposes.
     - *Lockdown* retention control settings must be defined for a policy that is intended to govern required *Images*, as follows:
       - Target storage is selected for retaining backup copies that is either (a) a *Lockdown*-enabled Storage Unit or (b) a link to a *Storage Lifecycle Policy* that specifies a *Lockdown*-enabled Storage Unit.
       - A *WORM Retention Period* (i.e., an expiry period for *Images*, sometimes referred to as *Retention Period or WORM Lock Time)* is assigned by (a) entering a retention value in terms of days, weeks, months or years and ensuring that the entered value falls within the allowable min/max range for the selected *Lockdown Storage* or (b) associating the *NetBackup Policy* with a *Storage Lifecycle Policy* that specifies a *WORM Retention Period* for the *Image*.

    - Each *NetBackup Policy* includes additional attributes, or rules, which govern the backup, including the frequency/schedule and backup type (i.e., full, incremental, synthetic, or accelerator).

        - Full and incremental backups are linked together via attributes to facilitate recovery. However, full and associated incremental backups are treated as separate, individual *Images,* each with its own retention controls.

        - A synthetic backup is one that combines a prior full backup with one or more recent incremental backups to produce a new consolidated *Image*. The consolidated *Image* is a separate *Image*, with its own unique ID and retention controls.

        - An accelerator backup is a streamlined version of synthetic backup. As changes are made within the source system workload, those changes are backed up and used to immediately assemble a new full backup (i.e., no incremental will exist). This newly assembled full backup is a separate *Image*, with its own unique ID and retention controls.

    Note: The Storage Unit and *WORM Retention Period* defined for a *NetBackup Policy* may be overridden during the creation of the backup schedule to allow flexibility on how certain types of *Images* are retained (i.e., incremental backups may <u>not</u> require WORM storage or may be kept for a shorter retention period than a full backup).

2. ***<u>Storage Lifecycle Policies</u>*** allow NetBackup Administrators to create a storage plan for a *set of* NetBackup Policies, such as:

    - Establishing the *Lockdown* retention control settings (i.e., *Lockdown*-enabled Storage Unit and the *WORM Retention Period)*, if not already assigned by an individual *NetBackup Policy*, and

    - Establishing duplication, replication, or other post backup operations. Note: Each *Storage Lifecycle Policy* operation that will produce required *Images*, must have its own *Lockdown* retention control settings defined.

    Note: The Storage Unit and *WORM Retention Period* referenced within NetBackup Policies and *Storage Lifecycle Policies* can be modified at any time; however, the new values apply to new *Images* only.

- When NetBackup executes a backup job, based on policies as described above, integrated *Lockdown* retention controls are applied to retain *Images* in accordance with the non-rewriteable, non-erasable requirements of the Rules.

    - At run time, through a series of Open Storage Technology (OST) API commands, the NetBackup Flex Scale system verifies it can immutably store the source system workload for the requested *WORM Retention Period.* If able to meet the storage request (i.e., sufficient storage space is available and the *WORM Retention Period* falls within the allowable Min/Max range) the backup will proceed. If the storage request cannot be supported, the operation fails and an error is issued.

    - When a successful write-to-disk is complete:

        - The current value of the Compliance Clock (i.e., the elapsed run-time value for the system, in seconds) is added to the *Image* as metadata. Additionally, the *WORM Retention Period* is translated into the total number of seconds the *Image* is to be retained and that value is stored as metadata. ***Lockdown Storage*** **controls retention and determines deletion eligibility by comparing the elapsed time (i.e., using the Compliance Clock) since the** ***Image*** **was stored to the WORM Retention Period (i.e., total number of seconds to be retained).**

- Additionally, an approximate *Retain Until Date* is calculated for each *Image* by adding the assigned *WORM Retention Period* to the storage timestamp, according to the NetBackup Primary Server system clock. The calculated *Retain Until Date* is retained as a mutable attribute in the Primary Server Catalog. Note: The approximate *Retain Until Date* in the Primary Server Catalog is not confirmed by or aligned with *Lockdown Storage* and, therefore, does not control retention of the *Image*; it is used to facilitate queries and govern automated post retention delete requests.

- The following table describes the integrated retention controls that are applied to *Images* (i.e., collections of *records*) when the appliance is configured in either (1) *Compliance* mode or (2) *Enterprise* mode.

	Retention Controls – *Compliance* Mode	**Retention Controls – *Enterprise* Mode**
Protecting record content	● By design, the contents of an *Image* cannot be modified or overwritten for the lifespan of the stored *Image*.	
Protecting immutable metadata	● Changing *Image* metadata that is critical for records management is prohibited, including the unique Backup ID together with the date and time backup was initiated at the source system, copy number, name of backup policy, type of backup policy, and checksum.	
Restricting changes to *Lockdown* retention mode	● The *Lockdown* mode configured for the appliance and applied to stored *Images* cannot be removed and cannot be downgraded to *Enterprise* or *Normal* mode.	● The *Lockdown* mode configured for the appliance and applied to stored *Images* cannot be removed or downgraded, however, ○ A privileged Appliance Administrator may upgrade the *Lockdown* mode for the appliance from *Enterprise* to *Compliance* at any time. *Compliance* Mode Controls are then retroactively applied to all existing *Images* and to all new *Images* as they are recorded.
Extending *WORM Retention Period*	● The *WORM Retention Period* assigned to an *Image* may be extended as needed. The NetBackup Primary Server sends the number of additional seconds required for retention to *Lockdown Storage*, where the *Image's* lock time is extended accordingly.	
Shortening *WORM Retention Period*	● The WORM Retention Period may not be reduced or deleted by any NetBackup users, including Appliance Administrators, who have no access to the root account or operating system of the appliance.	● The WORM Retention Period may be shortened or removed by a privileged Appliance Administrator. As such, administrative procedures and monitoring are required to ensure compliant retention protections are enforced when using *Enterprise* mode.
Restricting deletion	● The *Image* is protected against deletion for the duration of the applied *WORM Retention Period*. ● *Lockdown* retention controls in *Compliance* mode cannot be unlocked, removed or circumvented by any user or administrator. ● See Section 2.2.3.5, *Deletion Controls*, for additional information.	● The *Image* is protected against deletion for the duration of the applied *WORM Retention Period.* However, *Lockdown* retention controls in *Enterprise* mode may be circumvented: ○ Using a dual-approval process, which requires actions be taken by two separate administrators, each with restricted privileges, an *Image* can be deleted prior to expiration of its WORM Retention Period. As such, administrative

	Retention Controls – *Compliance* Mode	Retention Controls – *Enterprise* Mode
		procedures and monitoring are required to ensure compliant retention protections are enforced when using *Enterprise* mode. ● See Section 2.2.3.5, *Deletion Controls*, for additional information.
Copying *Images*	● An *Image* may be copied up to 10 times via rules defined within a *Storage Lifecycle Policy*. All copies are tracked within the Primary Server Catalog. ● The original *Image* remains unchanged and protected by the *Lockdown* retention controls for the specified *WORM Retention Period*. ● The copy is assigned its own unique *Image* ID (i.e., the original *Image* ID with an appended sequential copy number). *Lockdown* retention controls, including the *WORM Retention Period,* will not carry over to the copy and, therefore, must be applied independently by the *Storage Lifecycle Policy*, if required.	
Moving *Images*	● *Images* cannot be moved.	

2.2.3.4 Legal Holds (Temporary Holds)

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

- ▶ The *WORM Retention Period* may be extended for select *Images* (and any secondary copies) that are subject to the hold. If the initial extension of the *WORM Retention Period* is insufficient, the *WORM Retention Period* must continue being extended to meet the legal hold timeframe.
  - When *Compliance* mode retention controls are applied to an *Image*, the *WORM Retention Period* cannot be shortened. Therefore, Cohasset recommends extending the *WORM Retention Period* in shorter increments to avoid excessive retention, after the legal hold is released.
- ▶ Additionally, a Hold Name and Yes/No Hold attribute may be set for the primary *Image* (and any secondary copies) within the Primary Server Catalog, to facilitate searches and to prevent the Primary Server Catalog from issuing automated post-retention delete requests.
  - The Hold attribute is not transferred to *Lockdown Storage*, and therefore, will not provide immutability and indelibility protection to *Images* that are past their assigned WORM Retention Period.
  - The Hold attribute may be removed from the Primary Server Catalog for an *Image* when no longer required.

2.2.3.5 Deletion Controls

- ▶ The following table summarizes actions taken to delete *Images* and associated metadata, when the *Lockdown* retention controls are set to *Compliance* or *Enterprise* modes.

	Retention Controls – *Compliance* Mode	Retention Controls – *Enterprise* Mode
Determining eligibility for deletion	● An *Image*, together with its metadata and the records retained within the *Image*, is eligible for deletion when both: ○ Its *WORM Retention Period* is in the past, and ○ A Hold attribute is not assigned to the *Image* in the Primary Server Catalog. Note: The Primary Server Catalog attribute applies to automated disposition only.	

	Retention Controls – *Compliance* Mode	Retention Controls – *Enterprise* Mode
Restricting deletion	● Deletion of each *Image*, and its associated immutable metadata, is prohibited until the *Image*'s *WORM Retention Period* is in the past. ○ When set to *Compliance* mode, the *Lockdown* retention controls cannot be unlocked, removed or circumvented by any user or administrator.	● For standard users, deletion of each *Image* and its associated immutable metadata are prohibited until the *Image's WORM Retention Period* is in the past. ● Administrators with elevated privileges may delete an *Image* before the *WORM Retention Period* is in the past (i.e., Privileged Delete). The privileged delete process requires ***dual-approval*** to execute. Two separate administrators, each with separate, restricted privileges, are required to complete the following: ○ The Appliance Administrator removes the *WORM Retention Period* for the *Image*. ○ The Backup Administrator then deletes the *Image*. Accordingly, procedural controls and monitoring are required to scrutinize user and administrator actions taken to bypass *Lockdown* retention controls.
Deleting eligible Images	● Delete requests are part of an automated job on the NetBackup Primary Server, which typically runs every 12 hours to remove *Image*s eligible for deletion. Additionally, delete requests may be triggered manually. ○ Delete requests are based on the stored *Retain Until Date*, according to the Primary Server system time. ○ Upon receipt of a delete request, *Lockdown Storage* verifies deletion eligibility based on the elapsed retention time, as calculated by the Compliance Clock. If the storage subsystem determines that the *WORM Retention Period* has not yet expired, it denies the request, however, index information associated with the *Image* will be removed from the Primary Server Catalog. An automated background *Image Cleanup* process periodically attempts deletion of eligible *Images* from *Compliance Storage* until successful. ▪ To add index data for the *Image* back into the Primary Server Catalog, a re-import is required and the Primary Server Catalog will then contain the updated *Retain Until Date* provided by the storage subsystem.	
Preventing deletion of *Lockdown Storage*	● *Lockdown Storage* cannot be deleted if it contains immutable *Images*	

2.2.3.6 Security

NetBackup Flex Scale is designed to meet stringent enterprise security and compliance requirements.

- NetBackup Flex Scale utilizes Roles Based Access Controls (RBAC) to restrict privileges of users.
- NetBackup Flex Scale is hardened at operating system and appliance layers, according to Security Technical Implementation Guide (STIG) standards.
  - Firewalls are utilized to protect internal services.
  - A secured, authorized process via temporary, password-protected support key, is required for access by Veritas Support. Note: this secure process is required only when the NetBackup Flex Scale appliance is locked down in either *Compliance or Enterprise* mode.
  - *Image*s are only accessible via OST API's.

  - Custom VxOS shell is utilized for MSDP Storage Engines and appliance Command-Line Interface (CLI) commands and provides no operating system or root access.
  - *Lockdown Storage* is segregated from protocol services such as NFS and CIFS.
  - SELinux labelling is automatically employed for file systems to provide segregation. Additionally, SELinux protections include default RedHat policies to protect the core operating system.
- Two factor authentication is required for administrative access to the NetBackup Flex Scale appliance.
- When the *Restricted Remote Access* feature is enabled on the NetBackup Flex Scale appliance, Appliance Administrator capabilities are limited to an approved set of non-destructive operations. Appliance Administrators are prohibited from using iLO/iDRAC and IPMI console interfaces to remotely boot from an unsecure device.
- The NetBackup Flex Scale appliance operating system runs in Federal Information Processing Standard (FIPS) mode by default. This ensures only FIPS validated algorithms are used by the operating system and its core services.
  - All appliance management and MSDP Storage Server communications are fully encrypted as per FIPS 140-2 standard. MSDP Storage Server also employs FIPS 140-2 compliant encryption for data at-rest, utilizing the provided NetBackup Key Management System (KMS) or an external KMS.

2.2.3.7 Clock Management

- To protect against the possibility of premature deletion of *Images*, *Lockdown Storage* utilizes a Compliance Clock that is independent of NTP or the system clock, deployed on the storage layer of the hardened NetBackup Flex Scale appliance. The Compliance Clock tracks *elapsed system run-time*, in seconds, rather than wall-clock time. This approach resolves a common security attack vector that involves changing system time for a server.
- Flex Scale tracks the number of seconds remaining for a *WORM Retention Period* by comparing an *Image*'s assigned retention duration (in seconds) to the time elapsed since the *Image* was committed to *Lockdown Storage*.
  - During the initial write of an *Image*, the Compliance Clock is used to calculate and store a *Retain Until Date* in *Lockdown Storage*. The Primary Server Catalog also maintains a *Retain Until Date* based on server time. These two, independent *Retain Until Dates* are not synchronized. As such, the *Retain Until Date* within *Lockdown Storage* takes precedence.
- The Compliance Clock cannot be accessed or altered by any user, including the root user.
- The Compliance Clock is not affected by hardware outages such as node failures.

2.2.4 Additional Considerations

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

- Deploying the NetBackup Flex Scale appliance (version 3.1) as described in Section 1.3.

- Appropriately configuring the NetBackup Flex Scale appliance for use in either *Compliance* or *Enterprise Lock Down* mode with the *Restricted Remote Access* feature enabled.
  - Implementing necessary administrative procedures and monitoring to ensure compliant retention protections are enforced when used in *Enterprise* mode.
- Setting appropriate Min/Max Retention range values as guardrails for *Lockdown Storage*.
- Creating *Lockdown*-enabled Storage Units that point to *Lockdown Storage* and mandate the use of WORM controls.
- Applying *Lockdown retention controls* to required *Images* by establishing NetBackup Policies and/or *Storage Lifecycle Policies* that reference *Lockdown*-enabled Storage Units and setting appropriate *WORM Retention Period*s.
- Appropriately protecting source system workloads, until the *Images* have been successfully written to *Lockdown Storage*, particularly in cases where the size of the *workload* will result in a multi-day process to complete.
- Extending the retention duration for *Images* and secondary copies that must be kept longer than the assigned *WORM Retention Period*, to effectuate a legal hold for subpoenas, litigation, government investigations, external audits and other similar circumstances.
- Re-importing index data from the storage subsystem into the Primary Server Catalog as needed to ensure alignment.
- Storing *Image*s requiring event-based[14] retention in a separate compliance system, since NetBackup Flex Scale does not natively support event-based retention.

Additionally, the regulated entity is responsible for: (a) authorizing user privileges, (b) managing encryption keys, if not utilizing the NetBackup KMS, and (c) maintaining appropriate technology and other information and services needed to retain the records.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

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

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

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

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

2.3.2 Compliance Assessment

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

2.3.3 NetBackup Flex Scale Capabilities

The recording and post-recording verification processes of NetBackup Flex Scale are described below.

2.3.3.1 Recording Process

- When an *Image* is written to NetBackup Flex Scale storage:
  - The *Image* is divided into separate fragments during the write process.
  - A checksum is calculated for each fragment of data and stored as immutable metadata at the individual fragment level, for post-recording validation.
  - Once NetBackup Flex Scale verifies that all fragments have been successfully written, acknowledgement of a successful write is returned to the source system. If a write failure occurs at any stage, an error message is returned to the source system for corrective action and the write operation is stopped to prevent corrupted data from being written to NetBackup Flex Scale storage.

2.3.3.2 Post-Recording Verification Process

- During automated background consistency checks, magnetic disk error detection and correction are applied to correct any in-error data on the magnetic disk. Should the magnetic disk error detection and correction fail to correct the data, the data is flagged as corrupt and the regulated entity must work with NetBackup Flex Scale support personnel to correct it.
- During every read back of the *Image,* NetBackup Flex Scale validates the accuracy of all fragments by recalculating each fragment's checksum and comparing it to the checksum originally calculated and stored with the fragment.
  - If the checksums do not match, magnetic disk error detection and correction are applied to correct any corrupt data on the disk.
  - Should the magnetic disk error detection and correction fail to correct the data, the data is flagged as corrupt and the regulated entity must work with NetBackup Flex Scale support personnel to correct it.

2.3.4 Additional Considerations

The source system is responsible for transmitting the complete contents of the required *Images* and NetBackup Flex Scale validates the accuracy of the recording process.

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

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

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

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]

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

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

2.4.2 Compliance Assessment

It is Cohasset's opinion that the functionality of NetBackup Flex Scale meets this SEC requirement to maintain the capacity to readily download and transfer the records and the information used to locate them, when the considerations described in Section 2.4.4 are satisfied.

2.4.3 NetBackup Flex Scale Capabilities

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

- NetBackup Flex Scale assures each *Image*, regardless of how it originates (i.e., full, incremental, or synthetic backup), is assigned a unique ID. The unique *Image* ID is a combination of the following attributes:
  - A *Backup ID*, which is comprised of (a) source system name and (b) backup timestamp.
    - Backups may span multiple days due to the size of the workload, therefore, the timestamp represents the time at which the backup *started on the source system*.
  - A *Copy Number*, which is an incremental number assigned to each sequential execution of a given *NetBackup Policy*.
- The *Backup ID* and *Copy Number* for each *Image* are recorded as part of the system metadata and protected from alteration for the duration of the *WORM Retention Period* associated with the *Image*.
- The NetBackup Flex Scale Primary Server Catalog acts as the index for all *Images* stored in Flex Scale storage. Due to the critical service it performs, multiple protections are in place, including:
  - The Primary Server Catalog storage environment is 3-way mirrored across three independent disks, assuring continued access should a single disk fail.

- Point-in-time *Images* (checkpoints) of the catalog are periodically and frequently taken at the file system level.
- Data in the catalog is backed up for disaster recovery purposes every four hours, to separate storage.
- The full catalog is replicated to a disaster recovery site, continuously, as new data is written to it.

The combination of these protections assures rapid recovery of the catalog and/or failover to an alternate catalog in the event of a Primary Server Catalog storage hardware failure.

- Additionally, should the Primary Server Catalog ever become out of synch with the MSDP storage environment, NetBackup Administrators may perform a resynchronization process to assure every *Image* is indexed and searchable.
- The NetBackup Administrator's Console (a Java-based graphical user interface) provides NetBackup Administrators the ability to list the *Image*s under retention management within the Primary Server domain, filtered by metadata such as policy, copy number, type of backup, source system, date range, etc. *Note: NetBackup is storage agnostic in that it searches through all Images being managed by the NetBackup Flex Scale Primary Server Catalog, whether the Images are stored in Flex or NetBackup Flex Scale appliances*.
  - The search results screen is configurable and may include metadata such as: Unique ID, NetBackup policy name, backup policy type, media server, lock status, *WORM Retention Period,* source system name and timestamp, etc.
  - From the search results screen, the following operations are available:
    - Copy (duplicate) a select *Image* (i.e., make a full copy of the backup *Image*) to another location.
    - Verify consistency of the *Image* on the disk volume.
    - Browse through the contents of the NetBackup *Image*. The level of viewable content varies by type of workload.
- Alternatively, the command line interface (CLI) may be used to programmatically search the Primary Server Catalog. The resulting list may be exported via flat file, then imported into a CSV file and viewed and/or transferred to a medium acceptable under the Rule.
- NetBackup Flex Scale allows for *Images* to be:
  - Restored, via the NetBackup Administrator's Console, to a specified source system where content may then be viewed and/or reproduced or transferred to a medium acceptable under the Rule; or
  - Programmatically exported, via CLI.
- Programmatic interfaces (i.e., CLI or Restful APIs), as well as supported third party query tools, may be used to search and restore/retrieve *Image*s from NetBackup storage. Once retrieved, content may be viewed by source system software and reproduced or transferred to a medium acceptable under the Rule.

2.4.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) authorizing user privileges, (b) maintaining appropriate technology and resource capacity, and other information and services needed to use NetBackup Flex Scale to readily access, download, and transfer the records and the information needed to locate the records, (c) maintaining its encryption keys, if not utilizing the NetBackup KMS, and (d) providing requested information to the regulator, in the requested format.

2.5 Record Redundancy

2.5.1 Compliance Requirement

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

(A) Include a backup electronic recordkeeping system that meets the other requirements of this paragraph [(f) or (e)] and that retains the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and in accordance with this section in a manner that will serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible; or

(B) Have other redundancy capabilities that are designed to ensure access to the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and this section

The intent of 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).

- 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.[15] [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.[16] [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 NetBackup Flex Scale meets both paragraphs (A) and (B) of this SEC requirement by retaining a persistent duplicate copy of the records or alternate source to reestablish the records, when (a) properly configured as described in Section 2.5.3 and (b) the considerations described in Section 2.5.4 are satisfied.

[15] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

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

2.5.3 NetBackup Flex Scale Capabilities

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

2.5.3.1 Redundant Set of Records

- NetBackup Flex Scale offers the following two options for retaining full, duplicate copies of records:
  1. **Auto *Image* Replication (AIR)** - creates a copy of an *Image* onto a remote, geographically dispersed storage device in a different Primary Server domain. This results in the original and replica *Images* being managed by two separate Primary Server Catalogs.
  2. **Duplication** - creates a copy of an *Image* on a separate NetBackup Flex Scale appliance, typically within the same data center, which can be used for disaster recovery purposes in addition to meeting compliance requirements. Original and duplicate *Images* can be managed by a single NetBackup Flex Scale Primary Server Catalog when configured to do so.
  - Duplication and Auto *Image* Replication (AIR) are configured via *Storage Lifecycle Policies* that (a) identify the *NetBackup Policy*, or rather, the resulting *Images created by a NetBackup Policy* that require replication, (b) assign target storage for the duplicates/replicas by specifying a *Lockdown*-enabled Storage Unit with appropriate storage capacity, and (c) assign a *WORM Retention Period* that is identical to the original *Image*.
    - Additionally, duplication may be initiated manually via the NetBackup Administrator's Console or programmatically via command line interface (CLI).
  - Once configured via a *Storage Lifecycle Policy*, duplication/replication occurs automatically, each time the primary *NetBackup Policy* executes.
    - NetBackup can catalog up to 10 copies of a single *Image*, however, each copy must reside on a separate NetBackup Flex Scale appliance. *Note: the original Image is considered the first copy*.
  - The content of the duplicated/replicated *Image* is an exact copy of the original, however, metadata associated with the secondary *Image* is different:
    - The secondary *Image* has a unique Backup ID and Copy number.
    - The *WORM Retention Period* associated with the secondary *Image* is not kept synchronized with the primary *Image*. Therefore, if the *WORM Retention Period* is extended on the primary *Image* (i.e., when litigation or a subpoena requires an *Image* to be preserved beyond its currently assigned *WORM Retention Period)* the *WORM Retention Period* associated with the secondary *Image* must be manually extended as well.

2.5.3.2 Other Redundancy Capabilities

- NetBackup Flex Scale provides self-healing, enterprise-level durability by recording data utilizing erasure coding 8:4. During the write process, data is deduplicated, then broken into equal slices. Erasure coding is then applied to each slice of data, further dividing the data into fragments that are written across separate nodes and disks within the NetBackup Flex Scale cluster. In the event of data corruption or a system failure (i.e., a node or disk failure), a replica of an *Image* can be automatically and accurately regenerated from the erasure coded data fragments.

2.5.4 Additional Considerations

If electing to use replication or duplication, to augment erasure coding, the regulated entity is responsible for: (a) properly configuring compliant storage for the duplicate copies/replicas and (b) validating that the *Lockdown* retention controls applied to both the primary and secondary copies remain identical.

2.6 Audit System

2.6.1 Compliance Requirement

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

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

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

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

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

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

2.6.2 Compliance Assessment

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

2.6.3 NetBackup Flex Scale Capabilities

The regulated entity is responsible for an audit system, and compliance is supported by NetBackup Flex Scale.

- When recording *Images* (whether the *Image* originates as a full, incremental, or synthetic backup), NetBackup Flex Scale assigns a unique ID. The unique *Image* ID is a combination of the following attributes:
  - A *Backup ID*, which is comprised of (a) source system workload name and (b) backup timestamp.
    - Backups may span multiple days due to the size of the workload, therefore, the backup timestamp represents the time at which the backup *started on the source system*.
  - A *Copy Number*, which is an incremental number assigned to each sequential execution of a given *NetBackup Policy*.

The *Backup ID* and *Copy Number* for each *Image* are recorded as part of the system metadata and protected from alteration for the duration of the *WORM Retention Period* associated with the *Image*.

- By design, the contents of an *Image*, including immutable system metadata, cannot be modified for the lifespan of the stored *Image*. Therefore, tracking of the inputting of changes made is not relevant to NetBackup Flex Scale.
- In addition to the immutable system metadata, the following operations related to *Images* are captured in either the NetBackup Log or the MSDP Log:
  - Adding new *Images* to *Lockdown Storage*.
  - Modifying *Images* with applied *Lockdown* retention controls.
  - Deleting eligible *Images*.
- Attributes captured as part of each logged event include, but are not limited to, operation timestamp, user ID, the operation performed, status of operation (success/failure), source IP, destination IP, and Unique ID.
- NetBackup Logs may be automatically forwarded to Splunk or other security information and event management tools for long-term retention. MSDP Logs may be manually downloaded to an alternate system for long-term retention.
- By default, both NetBackup and MSDP Logs are retained in the Flex Scale storage environment for 30 days, but the retention duration may be shortened or extended as needed.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records. In addition to relying on the immutable metadata, the regulated entity may utilize NetBackup Flex Scale logging and export features alone or in conjunction with another system.

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

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

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

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

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

In Section 2 of this report, Cohasset assesses two compliance options: (1) *Lockdown* retention controls in *Compliance* mode, which is highly-restrictive and provides both overwrite protection and strict retention controls, and (2) *Lockdown* retention controls in *Enterprise* mode, a less-restrictive option, which provides overwrite protection but requires administrative procedures and monitoring to ensure compliant retention, as administrators are allowed to shorten or remove retention controls. (See Subsection 2.2.3.1, *Overview*, for a summary of controls for *Compliance* and *Enterprise Lockdown* modes.)

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

[17] 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)**
(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 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;*	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records[18] with time-based retention periods, are met by the functionality of NetBackup Flex Scale, with *Lockdown* retention controls in either *Compliance* or *Enterprise* mode. This report describes the functionality of NetBackup Flex Scale, with *Lockdown* retention controls, 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 information to access, search and display records, as well as data on records creation, formatting and modification: *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:* *(i) Any data necessary to access, search, or display any such books and records; and* *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added] NetBackup Flex Scale retains immutable metadata attributes (e.g., Backup ID with date/timestamp, and Copy Number), as an integral component of the record (*Image*). The system metadata are subject to the same retention protections as the associated record (*Image*). These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records. Further, the NetBackup Log or the MSDP Log tracks audit events and provides storage options for retaining this additional audit system information for longer retention periods. For additional information, see Section 2.6, *Audit System*.
(ii) Systems that ensure the records entity is able to produce electronic regulatory records in accordance with this section, and ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems; and	It is Cohasset's opinion that NetBackup Flex Scale capabilities described in Section 2.5, *Record Redundancy*, including methods for a persistent duplicate copy or erasure coding which provides an alternate source to reestablish the 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*.
(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).

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

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(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 NetBackup Flex Scale has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in. ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System*

4 • Conclusions

Cohasset assessed the functionality of NetBackup Flex Scale[19] 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 NetBackup Flex Scale, when properly configured, has the following functionality, which meets the regulatory requirements:

- Immutably retains *Images* (i.e., collections of records) and immutable system metadata in a non-rewriteable, non-erasable format for time-based retention periods by applying *Lockdown* retention controls in either highly-restrictive *Compliance* mode or less-restrictive *Enterprise* mode.
- Permits *WORM Retention Periods* to be extended, as needed, to retain *Images* for regulatory compliance or to satisfy a legal hold.
- Prohibits deletion of an *Image* and its immutable system metadata until the *WORM Retention Period* for the *Image* has expired.
- Verifies the accuracy of the recording process through cryptographic hash values and NetBackup Flex Scale validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- Provides authorized users with the capacity and tools to readily (a) search for records (*Images*), (b) list the *Images*, and (c) download the *Images* and associated metadata attributes for a browser or other local tool to produce a human-readable view and in a reasonably usable electronic format.
- Maintains records redundancy utilizing erasure coding to provide high durability of *Image*s. Additionally, provides the ability to asynchronously record a duplicate of each *Image* to a separate storage device, which allows for the recovery of *Images* that may become lost or damaged. Additionally, supports geographically dispersed, asynchronous replication of *Images*.
- Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that NetBackup Flex Scale, when properly configured and the additional considerations are satisfied, meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with the audit system requirements in 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).

[19] See Section 1.3, *NetBackup Flex Scale Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

Appendix A • Overview of Relevant Electronic Records Requirements

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

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

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

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments[20] 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.*[21] [emphasis added]

These 2022 amendments (a) provide a record and complete time-stamped audit-trail alternative and (b) allow regulated entities to continue using the electronic recordkeeping systems they currently employ to meet the non-rewriteable, non-erasable (i.e., WORM or write-once, read-many) requirement.

> *Under the final amendments, broker-dealers and nonbank SBS Entities have the flexibility to preserve all of their electronic Broker-Dealer Regulatory Records or SBS Entity Regulatory Records either by: (1) using an electronic recordkeeping system that meets either the audit-trail requirement or the WORM requirement; or (2) preserving some electronic records using an electronic recordkeeping system that meets the audit-trail requirement and preserving other electronic records using an electronic recordkeeping system that meets the WORM requirement.*[22] [emphasis added]

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

A.1.1 Record and Audit-Trail Alternative

The objective of this requirement is to allow regulated entities to keep required records and complete time-stamped record audit-trails in business-purpose recordkeeping systems.

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

[21] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

[22] 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.*[23] [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.*[24] [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."*[25] [emphasis added]

A.1.2 Non-Rewriteable, Non-Erasable Record Format Alternative

With regard to the option of retaining records in a non-rewriteable, non-erasable format, the adopting release clarifies that the previously released interpretations to both SEC Rules 17a-4(f) and 18a-6(e) still apply.

> *The Commission confirms that a broker-dealer or nonbank SBS Entity can rely on the 2003 and 2019 interpretations with respect to meeting the WORM requirement of Rule 17a-4(f) or 18a- 6(e), as amended.*
>
> *****
>
> *In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance. Moreover, because Rule 18a-6(e) is closely modelled on Rule 17a-4(f), it also is consistent with the ESIGN Act****[26] [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).

[23] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

[24] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

[25] 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

[26] 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.*[27] [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.*[28] [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.*[29] [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 NetBackup Flex Scale related to each requirement.

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

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. Additionally, FINRA adopted amendments clarifying the application of FINRA rules to security-based swaps (SBS).[30]

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.*

[27] 2003 Interpretative Release, 68 FR 25282.

[28] 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).

[29] 2003 Interpretative Release, 68 FR 25283.

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

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

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 (CFTC Rule) to modernize and make technology-neutral the form and manner in which to keep regulatory records. This resulted in less-prescriptive, principles-based requirements.

> *Consistent with the Commission's emphasis on a less-prescriptive, principles-based approach, proposed § 1.31(d)(1) would rephrase the existing requirements in the form of a general standard for each records entity to retain all regulatory records in a form and manner necessary to ensure the records' and recordkeeping systems' authenticity and reliability.*[31] [emphasis added]

The following definitions in 17 CFR § 1.31(a) confirm that recordkeeping obligations apply to all *records entities* and all *regulatory records*. Further, for *electronic regulatory records*, paragraphs (i) and (ii) establish an expanded definition of an electronic regulatory record to include information describing data necessary to access, search and display records, as well as information describing how and when such books and records were created, formatted, or modified.

> *Definitions. For purposes of this section:*
>
> *Electronic regulatory records means all regulatory records other than regulatory records exclusively created and maintained by a records entity on paper.*
>
> *Records entity means any person required by the Act or Commission regulations in this chapter to keep regulatory records.*
>
> *Regulatory records means all books and records required to be kept by the Act or Commission regulations in this chapter, including any record of any correction or other amendment to such books and records, provided that, with respect to such books and records stored electronically, regulatory records shall also include:*
>
> > *(i) Any data necessary to access, search, or display any such books and records; and*
> >
> > *(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added]

The retention time periods for required records includes both time-based and event-based retention periods. Specifically, 17 CFR § 1.31(b) states:

> *Duration of retention. Unless specified elsewhere in the Act or Commission regulations in this chapter:*
>
> *(1) A records entity shall keep regulatory records of any swap or related cash or forward transaction (as defined in § 23.200(i) of this chapter), other than regulatory records required by § 23.202(a)(1) and (b)(1)-(3) of this chapter, from the date the regulatory record was created until the termination, maturity, expiration, transfer, assignment, or novation date of the transaction and for a period of not less than five years after such date.*
>
> *(2) A records entity that is required to retain oral communications, shall keep regulatory records of oral communications for a period of not less than one year from the date of such communication.*
>
> *(3) A records entity shall keep each regulatory record other than the records described in paragraphs (b)(1) or (b)(2) of this section for a period of not less than five years from the date on which the record was created.*
>
> *(4) A records entity shall keep regulatory records exclusively created and maintained on paper readily accessible for no less than two years. A records entity shall keep electronic regulatory records readily accessible for the duration of the required record keeping period.* [emphasis added]

For a list of the CFTC principles-based requirements and a summary assessment of NetBackup Flex Scale in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

[31] 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.