

Nutanix Files

COMPLIANCE ASSESSMENT

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

Abstract

Nutanix Files is a software-defined, scale-out file storage solution to store, manage and scale unstructured data and is part of the Nutanix Unified Storage[‡] offering. Nutanix Files provides WORM capabilities that allows immutable file locking and retention. This WORM feature enables integrated controls designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of Nutanix Files (see Section 1.3, *Nutanix Files 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 Nutanix Files, when properly configured with *WORM enabled* for the Share and *Locked* for the record status, 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 Nutanix Files meets the principles-based requirements of CFTC Rule 1.31(c)-(d).

[‡] Nutanix Unified Storage (NUS) is a software-defined storage solution that combines block, file and object storage into a single platform. Along with the Nutanix Cloud Platform, NUS provides a simple and flexible platform to build and run modern applications and services irrespective of where they are deployed - in the core, cloud or the edge.

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.

Table of Contents

- Abstract 1**
- Table of Contents 2**
- 1 • Introduction 3**
 - 1.1 Overview of the Regulatory Requirements 3
 - 1.2 Purpose and Approach 4
 - 1.3 Nutanix Files Overview and Assessment Scope 5
- 2 • Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e) 6**
 - 2.1 Record Audit-Trail 6
 - 2.2 Non-Rewriteable, Non-Erasable Record Format 7
 - 2.3 Record Storage Verification 12
 - 2.4 Capacity to Download and Transfer Records and Location Information 13
 - 2.5 Record Redundancy 14
 - 2.6 Audit System 16
- 3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) 18**
- 4 • Conclusions 21**
- 5 • Overview of Relevant Electronic Records Requirements 22**
 - 5.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) Electronic Recordkeeping System Requirements 22
 - 5.2 Overview of FINRA Rule 4511(c) Electronic Recordkeeping System Requirements 24
 - 5.3 Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements 25
- About Cohasset Associates, Inc. 26**

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 Nutanix Files 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 entities¹, 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 Section 5.1, *Overview of SEC Rules 17a-4(f) and 18a-6(e) Electronic Recordkeeping System Requirements*.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. 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 Section 5.3, *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 Nutanix Files for preserving required electronic records, Nutanix 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.

Nutanix engaged Cohasset to:

- Assess the functionality of Nutanix Files, 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 Nutanix Files; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*; and
- Prepare this Compliance Assessment Report, enumerating the assessment results.

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

This assessment represents the professional opinion of Cohasset and should not be construed as either an endorsement or a rejection, by Cohasset, of Nutanix Files and its functionality or other Nutanix 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 Nutanix 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 Nutanix Files Overview and Assessment Scope

1.3.1 Nutanix Files Overview

Nutanix Files is a software-defined, virtualized, scale-out file⁴ storage solution that provides a repository for unstructured data, such as home directories, user profiles, departmental shares, application logs, backups, and archives. Nutanix Files is a fully integrated, core component of the Nutanix platform. Nutanix Files can run on a dedicated cluster or be collocated on a cluster running user virtual machines (VMs). Nutanix Files includes native high availability and uses Nutanix distributed storage for intra-cluster data resiliency.

Nutanix Files architecture consists of the following components, as depicted in Figure 1.

- **File Server Virtual Machine (FSVM)** provides file service to NFS and SMB clients. A file server comprises of a cluster of three (3) or more FSVMs providing highly-available access. FSVM incorporates the security and hardening of the Nutanix Controller VM (CVM).
- **NFS** (Network File System) and **SMB** (Server Message Block) are communication protocols that enable a user to access files over a network.
- **Distributed Metadata Service** allows clients to see a single unified namespace, regardless of which FSVM the client is connected.
- **Data Service** implements the NFS and SMB protocol servers on top of a filesystem that is local to each FSVM. Additionally, it includes a distributed configuration service to set server parameters and tunables.
- **MinervaFS** is the filesystem which runs on each FSVM and is constructed out of a virtualized storage volume exported by Nutanix distributed storage. Each instance MinervaFS is responsible for a shard or a partition of the unified file system namespace.
- **Shares** store unstructured information, comprised of files, in a hierarchical filesystem namespace composed of directories.

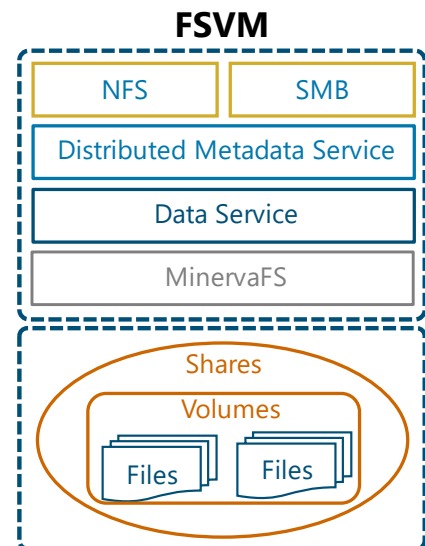


Figure 1

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related capabilities of Nutanix Files, Release 4.2.1, when Shares are properly configured with WORM enabled to store records and when the solution is running on on-premises Nutanix qualified hardware or as a virtual machine (VM) in the cloud.

Other deployments are excluded from this assessment.

⁴ The SEC uses the phrase *books and records* to describe information that must be retained for regulatory compliance. Cohasset uses the term *record* (versus file, object or data) to consistently recognize that the content is required for regulatory compliance.

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

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

For each 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 Nutanix Files
- **Nutanix Files 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 Nutanix Files, as described in Section 1.3, *Nutanix Files Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

2.1 Record Audit-Trail

2.1.1 Compliance Requirement

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

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

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

- (1) All modifications to and deletions of the record or any part thereof;
- (2) The date and time of actions that create, modify, or delete the record;
- (3) If applicable, the identity of the individual creating, modifying, or deleting the record; and
- (4) Any other information needed to maintain an audit-trail of the record in a way that maintains security, signatures, and data to ensure the authenticity and reliability of the record and will permit re-creation of the original record if it is modified or deleted

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

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

For clarity, the record 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.*⁶ [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed Nutanix Files in comparison to this requirement of the SEC Rules.

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

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

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

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

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

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 a process of integrated software and hardware codes and clarified that "a software solution that prevents the

⁵ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

⁶ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.”

In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.⁷ [emphasis added]

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

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

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of Nutanix Files, with WORM (Write Once, Read Many), meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based⁹ retention periods and legal holds, 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 assessed in Section 2.1.

2.2.3 Nutanix Files Capabilities

This section describes the functionality of Nutanix Files 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 and any applied legal holds.

2.2.3.1 Overview

- ▶ Nutanix Files offers WORM protection to retain records in a Share, for compliance with SEC Rule 17a-4(f).
 - When a Share is configured with *WORM enabled* and the record status is *Locked*, integrated control codes:
 - ◆ Prohibit deletion of the record, through any mechanism, until expiration of the *Retention period* inherited from the Share.
 - ◆ Disable all write privileges for the content of the record, thus protecting it against modification or overwrite for the specified retention period.
 - Additionally, integrated control codes prohibit both (a) removing or disabling the WORM protection and (b) *shortening* the Share *Retention period*.

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

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

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

2.2.3.2 Nutanix Files Configurations and Controls

- ▶ Within Nutanix Files, a record is stored in a Share and is comprised of two elements:
 1. **Content:** The contents of the record (i.e., document, image, video, database image, snapshot, etc.).
 2. **Immutable metadata:**
 - ◆ Critical attributes for record management, e.g., unique identifier, commit time (the timestamp when the record transitioned to a *Locked* state), and a cryptographic hash value.
 - ◆ Metadata becomes immutable, when the record is committed and remains immutable during the lifespan of the record, with the exception of permitting metadata modifications at the conclusion of the retention period to allow the record to expire, after which the record is eligible for deletion.
- ▶ Nutanix Files supports both NFS (Network File System) and SMB (Server Message Block) protocols.
- ▶ When configuring a new Share, using either a Command line interface (CLI) or REST APIs (application programming interfaces), for compliance with Rule 17a-4(f), the following configurations are mandatory:
 1. WORM must be enabled (*WORM_enabled* is *true*) as a Share-level property, and *WORM_type* must be set to *ShareLevel*.
 2. The Share *Retention period*, i.e., the duration of time each record is kept from the date the file is committed to *Locked* state, must be set to a period of time that meets regulatory requirements.
 - ◆ *The Retention period* is configured in seconds; the default is 31449600 seconds (approximately 1 year).
 - ◆ *The Retention period* is applied to every record on the Share, by adding the *Retention period* to the commit time (the timestamp when the record transitioned to a *Locked* state). **Note:** File level retention expiration dates transmitted as an attribute of the record are not supported.
 3. The *Cooloff_interval*, i.e., the delay between last modified time and transition to a *Locked* status, which applies WORM controls, must be set.
 - *Cooloff_interval* is configured in seconds; the default is 600 seconds (10 minutes), when a custom parameter is not specified.
 4. Autocommit must be enabled (*true*). This indicates that a record will automatically transition to a *Locked* state once the *Cooloff_interval* has passed.
- ▶ When a Share is configured with *WORM enabled* (*WORM_enabled* is *true*) the following controls apply to the Share:
 - The WORM configurations (*WORM_enabled* and *WORM_type*) applied to the Share cannot be modified or removed.
 - The *Retention period* applied to the Share cannot be shortened or removed, though it may be extended.
 - ◆ The Share *Retention period* automatically applies the time-based retention period to records in the Share, when the file is transitioned to the *Locked* status.

- The *Cooloff_interval* can be shortened, but cannot be extended, which assures that the lag for automatically transitioning files to a *Locked* status is not extended.
 - Autocommit cannot be disabled (set to false or null).
- ▶ Records in a WORM Compliance Share may be in one of the following three states:
1. *Unlocked* is the initial state of a new record. When a record is in an *Unlocked* state, it can be modified, overwritten or deleted. Any file updates or metadata updates, prior to a record being *Locked*, will update the *ctime* (change time) and delay the commit. A record in the *Unlocked* state is not compliant with the Rule.
 2. *Locked* state is set when the record is automatically transitioned from *Unlocked* to *Locked*.
 - ◆ Records automatically transition to *Locked* state when the last change time (*ctime*) plus the *Cooloff_interval* is less than the current time. Alternatively, records may be systemically transitioned to *Locked* state by setting the Read-Only attribute as enabled for SMB clients or by removal of the write mode for NFS clients.
 - ◆ Once a record is *Locked*, the *Retention period* for the Share applies and access privileges are changed to read-only in SMB or write mode is removed in NFS.
 - ◆ When a record is in a *Locked* state, it cannot be modified or deleted, until *Expired*.
 - ◆ Only records in a *Locked* state are compliant with the Rule.
 3. *Expired* state is assigned when the *Retention period* is in the past and the records are transitioned from the *Locked* state. *Expired* records remain immutable for their lifespan and can only be deleted.
- ▶ To verify the WORM status of a record, users can query for a record using CLI commands. The *Retention period* is exposed to clients through the file *atime* attribute.

2.2.3.3 Legal Holds (Temporary Holds)

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

- ▶ A Share-level *Override* attribute may be set, which prevents deletion of all records on the Share, even if the record is *Expired* and otherwise eligible for deletion (i.e., retention period is in the past) until the *Override* is removed. Once the *Override* is removed, *Locked* records are managed in accordance with the Share *Retention period* applied to each record.

2.2.3.4 Deletion Controls

- ▶ When a record is eligible for deletion, the record transitions from the *Locked* state to the *Expired* state. A record in an *Expired* state cannot be modified, but can be deleted.
- Disposition or deletion of *Expired* records is initiated by the source system.

- ▶ For a filesystem configured with *WORM*, privileged delete is disabled for all system users or administrators. Accordingly, the regulated entity administrative deletion of a record in a *Locked* state is prohibited.
- ▶ A Share configured with *WORM enabled* cannot be deleted by any mechanism if it contains any *Locked* records.

2.2.3.5 Security

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

- ▶ User Authentication and Authorization protocol access: Windows Active Directory and LDAP.
- ▶ **Network segmentation:** VLAN-based, data-driven segmentation.
- ▶ **Security Policy Management:** Policy driven security framework for traffic inspection.
- ▶ **Data Security and Integrity:** Cluster access control, SSL certificate management, data-at-rest encryption (AES-256), data in transit protocol-level (SMB/NFS) encryption.

2.2.3.6 Clock Management

- ▶ Nutanix Files must be configured to enable NTP (Network Time Protocol), which regularly checks the time of the external source (NTP) and resynchronizes system clock. During initial configuration, the application server is synced with NTP and users are restricted from modifying system time once the sync has occurred.
 - The clock controls prevent any inadvertent or intentional administrative modifications of the system clock, which could allow for premature deletion of records.

2.2.4 Additional Considerations

To assure compliance with the non-rewriteable, non-erasable requirement of the SEC Rules, the regulated entity is responsible for:

- ▶ Configuring *WORM enabled* (*WORM_enabled* is *true*) for Shares that will store books and records required by regulation, thereby establishing the foundation for meeting the requirements of the Rule.
- ▶ Ensuring records required to comply with the Rule are *Locked* and an appropriate retention period is applied.
- ▶ Configuring the *Auto-Commit* feature and *Cooloff_interval* to ensure that records are *Locked* when they are unmodified after a specified period of time. Under normal circumstances, Cohasset recommends locking records within 24 hours of last change time.
- ▶ Storing records requiring event-based¹⁰ retention periods in a separate compliance system, since Nutanix Files does not currently support event-based retention periods.
- ▶ Setting the Share-level *Override* attribute to override the Share *Retention period* for records that require preservation for legal matters, government investigations, external audits and other similar circumstances, and periodically reviewing the legal holds to determine if the *Override* must remain set.

¹⁰ 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.

Additionally, when Nutanix Files is running on a virtual machine (VM) in the cloud, the regulated entity is responsible for: (a) maintaining its cloud account in good standing and paying for appropriate services to protect Shares and allow records to be retained until the applied retention periods and holds have expired or until the records have been transferred to another compliant storage system, (b) authorizing user privileges; and (c) maintaining the appropriate technology, encryption keys, and other information and services needed to retain the records.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

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.

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

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

2.3.2 Compliance Assessment

Cohasset affirms that the functionality of Nutanix Files 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 Nutanix Files Capabilities

The recording and post-recording verification processes of Nutanix Files are described below.

2.3.3.1 Recording Process

- ▶ Nutanix Files calculates and stores a checksum for each record written to the Share.
- ▶ Nutanix Files utilizes advanced electronic recording technology which applies a combination of checks and balances to assure that records are written in a high quality and accurate manner.

2.3.3.2 Post-Recording Verification Process

- ▶ Integrity of the record is validated, during retrieval, by comparing the calculated checksum to the original stored checksum.
- ▶ Nutanix files employs a background scrubbing process that runs automatically or initiated manually to scan the data blocks of records to detect and repair errors. If a data block is corrupt, a recovery process is initiated to rebuild the data block from the other valid data blocks.

2.3.4 Additional Considerations

The source system is responsible for transmitting the complete contents of the required record and Nutanix Files ensures the transmitted record is accurately recorded.

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 either a:

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

The downloaded records and information 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 Audit-Trail*.

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]

2.4.2 Compliance Assessment

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

2.4.3 Nutanix Files Capabilities

The following capabilities relate to the requirement for capacity to download and transfer records and the information needed to locate the records.

- ▶ Each record in Nutanix Files is assigned a unique identifier, which facilitates findability. Specifically, Nutanix Files captures the following metadata for each record and immutably retains this metadata for the duration of the applied retention period.
 - Unique identifier, which is comprised of generation number and inode.
 - System-managed *commit* timestamp, which is captured when the record is *Locked*.
- ▶ The directory of records, including the record name, date stored and other directory attributes can be viewed by the source system through the standard NFS and SMB protocols.
- ▶ The appropriate records can be identified, retrieved and downloaded, whereupon they can be transferred using local capabilities to any medium acceptable under the Rule.

2.4.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing, when using virtual machines (VMs) in the cloud, (b) authorizing user privileges, (c) maintaining

appropriate technology and resource capacity, encryption keys, and other information and services needed to use Nutanix Files to readily download, and transfer the records and the information needed to locate the records, and (c) providing requested information to the regulator, in the requested format.

2.5 Record Redundancy

2.5.1 Compliance Requirement

The intent of this requirement is to retain a persistent alternate source to reestablish an accessible, complete and accurate record, should the original electronic recordkeeping system be temporarily or permanently inaccessible.

The 2022 final Rule amendments promulgate two redundancy options, paragraphs (A) or (B).

- ▶ 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.¹¹ [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.¹² [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 asserts that the functionality of Nutanix Files 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.

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

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

¹² 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

2.5.3 Nutanix Files Capabilities

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

2.5.3.1 Redundant Set of Records

For compliance with paragraph (A), to maintain a duplicate set of records, Nutanix Files must be configured with Prism Central for asynchronous replication between two file servers, as follows:

- ▶ Using Prism Central, replication is configured between a local file server and a remote file server at the Share level.
 - Primary Share level configuration is replicated to the Target Share at the time of creation, ensuring retention controls for the Target Share are consistent with the Primary Share. Subsequent share updates, such as retention hold, are performed separately on the Primary and Target shares.
 - Record changes on the primary filesystem are asynchronously replicated to the target filesystem. In the event the target is unavailable, all changes since last successful write will be sent in the next replication.
 - In the event that replication is paused or disassociated, all records on the target WORM Share in a *Locked* state will be protected for the applied *Retention period*.
- ▶ The duplicate copy can be utilized when the primary copy is not accessible, to either: (a) restore the primary copy or (b) retrieve records.

2.5.3.2 Other Redundancy Capabilities

For compliance with paragraph (B), Nutanix Files uses erasure coding (EC) to store data blocks of record redundantly across multiple nodes. In the event of a disk or node failure, the original record can be regenerated.

- ▶ Nodes can be spread across multiple blocks and racks.
- ▶ A record is regenerated from the erasure coded data.
- ▶ The erasure coded data segments are retained for the full retention period and any applied Legal Holds.

2.5.4 Additional Considerations

When using *Replication*, the regulated entity must ensure that a primary and target filesystems remain associated, to continue duplicating the records.

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing, when using virtual machines (VMs) in the cloud, (b) ensuring that the primary and target file systems remain associated, to continue duplicating the records, when using Prism Central for asynchronous replication, (c) maintaining the technology, storage capacity, encryption keys, and other information and services needed to use Nutanix Files and permit access to the redundant records.

2.6 Audit System

2.6.1 Compliance Requirement

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

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

2.6.2 Compliance Assessment

Cohasset asserts that Nutanix Files supports the regulated entity's efforts to meet this SEC audit system requirement.

2.6.3 Nutanix Files Capabilities

The regulated entity is responsible for complying with this audit system requirement and compliance is supported by Nutanix Files.

- ▶ For each record stored in Nutanix Files, it retains the following audit information.
 - When inputting records, Nutanix Files (a) systematically generates and stores an immutable unique identifier (generation number plus inode) and (b) a system-managed *commit* timestamp, which is assigned when the record is *Locked*. These attributes are immutable, chronologically account for each input record and are retained for the lifespan of the record.
- ▶ Each record is immutably stored over its lifespan; therefore, no changes can be input once the record is stored.
- ▶ In addition to the immutable record metadata, Nutanix File delivers real-time notifications of share-related events. These events include file creation, deletion and write operations among other activities.
 - The Syslog is used to send configured share-level audit events, as part of normal file system operations. Subsequently, the log files may then be filtered for specific WORM compliance activities.
 - Alternatively, the Nutanix Files Monitoring and Auditing APIs may be used to receive notifications for specified file operations (e.g., create, delete and write). The APIs are currently in beta and can be utilized through Prism.

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

- ▶ Audit events, from Syslog or Nutanix Files Monitoring and Auditing APIs, may be downloaded and subsequently imported into an external application, such as security information and event management tools, to meet the required retention period in alignment with the associated records.

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and may utilize Nutanix Files 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 Nutanix Files, as described in Section 1.3, *Nutanix Files 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 audit-trail and (2) non-rewriteable, non-erasable, a.k.a. WORM, are more likely to achieve this objective because each alternative requires the specific and testable outcome of accessing and producing modified or deleted records, in their original form, for the required retention period.

The proposed amendments to Rules 17a-4 and 18a-6 and the [CFTC] principles-based approach recommended by the commenters share an objective: ensuring the authenticity and reliability of regulatory records. However, the audit-trail requirement is more likely to achieve this objective because, like the existing WORM requirement, it sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.¹³ [emphasis added]

Cohasset's assessment, in Section 2, pertains to Nutanix Files, with *WORM enabled*, which is a highly restrictive configuration that assures the storage solution applies integrated controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied retention period.

In the following table, Cohasset correlates the functionality of Nutanix Files, using *WORM enabled*, 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 Nutanix Files to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d).

¹³ 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)
<p><i>(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:</i></p> <p><i>(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the <u>authenticity and reliability</u> of such regulatory records in accordance with the Act and Commission regulations in this chapter.</i></p> <p><i>(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the <u>authenticity and reliability</u> of electronic regulatory records, including, without limitation:</i></p> <p><i>(i) Systems that maintain the security, signature, and data as necessary to ensure the <u>authenticity</u> of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;</i></p>	<p>It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records¹⁴ with time-based retention periods, are met by the functionality of Nutanix Files, with <i>WORM</i>, as described in:</p> <ul style="list-style-type: none"> ● Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i> ● Section 2.3, <i>Record Storage Verification</i> ● Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i> ● Section 2.6, <i>Audit System</i> <p>Additionally, for <u>records stored electronically</u>, the CFTC definition of <u>regulatory records</u> in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification:</p> <p><u>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:</u></p> <p><u>(i) Any data necessary to access, search, or display any such books and records; and</u></p> <p><u>(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.</u> [emphasis added]</p> <p>Nutanix Files retains immutable metadata attributes (e.g., unique identifier and commit timestamp) as an integral component of the records, and, therefore, these attributes are subject to the same retention protections as the associated record. These immutable attributes support both (a) records access, search and display and (b) audit system and accountability for inputting the records.</p> <p>Further, Nutanix File in conjunction with the inherent Syslog capabilities and Nutanix Files auditing API's track audit events and provides storage options for retaining this additional audit system information for the same time period as the record. For additional information, see Section 2.6, <i>Audit System</i>.</p>
<p><i>(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 <u>emergency or other disruption</u> of the records entity's electronic record retention systems; and</i></p>	<p>It is Cohasset's opinion that Nutanix Files capabilities described in Section 2.5, <i>Record Redundancy</i>, including options for a persistent duplicate copy or alternate source to reestablish the records and associated system metadata, meet the CFTC requirements (c)(2)(ii) to <u>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.</u></p>
<p><i>(iii) The creation and maintenance of an <u>up-to-date inventory</u> that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.</i></p>	<p>The regulated entity is required to create and retain an <i>up-to-date inventory</i>, as required for compliance with 17 CFR § 1.31(c)(iii).</p>

¹⁴ If Nutanix Files retains the regulatory record content and core metadata attributes but does not necessarily retain other information needed to satisfy this definition of a regulatory record (such as information to augment search and data on how and when the records were created, formatted, or modified), the regulated entity is responsible for retaining and managing this other information in a compliant manner.

COMPLIANCE ASSESSMENT REPORT

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

CFTC 1.31(c)-(d) Regulation [emphasis added]	Compliance Assessment Relative to CFTC 1.31(c)-(d)
<p><i>(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:</i></p> <p><i>(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.</i></p> <p><i>(2) Production of paper regulatory records. ***</i></p> <p><i>(3) Production of electronic regulatory records.</i></p> <p><i>(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.</i></p> <p><i>(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.</i></p> <p><i>(4) Production of original regulatory records. ***</i></p>	<p>It is Cohasset's opinion that Nutanix Files has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in.</p> <ul style="list-style-type: none">● Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i>● Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i>● Section 2.6, <i>Audit System</i>

4 • Conclusions

Cohasset assessed the functionality of Nutanix Files¹⁵ 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 Nutanix Files, when properly configured, has the following functionality, which meets the regulatory requirements:

- ▶ Retains the records and immutable system metadata in non-rewriteable, non-erasable format for time-based retention periods, by applying WORM controls.
- ▶ Preserves all records in Shares as immutable and prohibits deletion or overwrites, while a Share-level override attribute is applied for Legal Holds.
- ▶ Prohibits deletion of a record and its immutable metadata until the retention period for the record is in the past and the record has transitioned to an *Expired* state.
- ▶ Verifies the accuracy of storing and retaining the records, using cryptographic hash values.
- ▶ Provides authorized users with the capacity and tools, such as standard NFS and SMB protocols, to (a) search for records, (b) list the file names, and (c) download the records and associated metadata attributes for a local tool to render as a human-readable image and produce in the requested electronic format.
- ▶ Maintains records redundancy by asynchronously recording a minimum of two duplicates of each record on separate local filesystems or between local filesystems and a remote filesystem, which allows for automatic recovery of records that become lost or damaged. Additionally, erasure coding is utilized to store data blocks of records redundantly across multiple nodes.
- ▶ Supports the regulated entity's obligation to retain an audit system for non-rewriteable, non-erasable records.

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

¹⁵ See Section 1.3, *Nutanix Files Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

5 • Overview of Relevant Electronic Records Requirements

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

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

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

Effective January 3, 2023, the U.S. Securities and Exchange Commission (SEC) promulgated amendments¹⁶ 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.*¹⁷ [emphasis added]

These 2022 amendments (a) provide a record 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.*¹⁸ [emphasis added]

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

5.1.1 Record Audit-Trail Alternative

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

¹⁶ The compliance dates are May 3, 2023, for 17 CFR § 240.17a-4, and November 3, 2023, for 17 CFR § 240.18a-6.

¹⁷ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

¹⁸ 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.¹⁹ [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.²⁰ [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."²¹ [emphasis added]*

5.1.2 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.²² [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 SBS/MSBSP Recordkeeping Adopting Release).*

¹⁹ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

²⁰ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

²¹ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

²² 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.²³ [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.²⁴ [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.²⁵ [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 Nutanix Files related to each requirement.

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

Financial Industry Regulatory Authority (FINRA) rules regulate member brokerage firms and exchange markets. Additionally, FINRA adopted amendments clarifying the application of FINRA rules to security-based swaps (SBS).²⁶

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.

²³ 2003 Interpretive Release, 68 FR 25282.

²⁴ 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).

²⁵ 2003 Interpretive Release, 68 FR 25283.

²⁶ FINRA, Regulatory Notice 22-03 (January 20, 2022), FINRA Adopts Amendments to Clarify the Application of FINRA Rules to Security-Based Swaps.

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

Effective August 28, 2017, the Commodity Futures Trading Commission (CFTC) amended 17 CFR § 1.31 (CFTC Rule) to modernize and make technology-neutral the form and manner in which to keep regulatory records. This resulted in 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.²⁷ [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 Nutanix Files in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

²⁷ 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.

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.

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*

©2023 Cohasset Associates, Inc.

This Compliance Assessment Report and the information contained herein are copyrighted and the sole property of Cohasset Associates, Inc. Selective references to the information and text of this Compliance Assessment Report are permitted, provided such references have appropriate attributions and citations. Permission is granted for in-office reproduction so long as the contents are not edited and the look and feel of the original is retained.