Cohasset Associates

Nutanix Objects

COMPLIANCE ASSESSMENT

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

Abstract

Nutanix Objects, deployed and managed as part of the Nutanix™ Enterprise Cloud Platform, is a software-defined, hardware agnostic, scalable object storage solution designed with an S3-compatible REST API interface to handle large volumes of unstructured data.

The *Bucket Lock* and *Object Lock* features are designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format, for records.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of Nutanix Objects (see Section 1.3, *Nutanix Objects 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 Objects, when properly configured and used with a default *Bucket Retention Period* that applies *Bucket Lock* and *Object Lock*, 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 Objects meets the principles-based requirements of CFTC Rule 1.31(c)-(d).

May 2023

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.

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 Nutanix Objects 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 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 Objects 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 Objects, 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 Objects; 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 Objects 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.

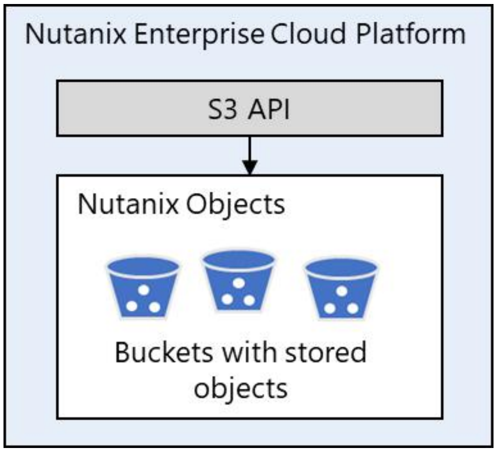
1.3 Nutanix Objects Overview and Assessment Scope

1.3.1 Nutanix Objects Overview

Nutanix Objects deployed and managed as part of the Nutanix Enterprise Cloud Platform, is a software-defined, hardware agnostic, scalable object[4] storage solution designed with an S3-compatible REST API interface to handle large volumes of unstructured data from a single namespace.

Nutanix Objects architecture (illustrated in the diagram) consists of the following components:

- **Nutanix™ Enterprise Cloud Platform** is a private cloud platform deployed on industry-leading infrastructure
- Amazon S3-compatible application programming interface (**S3 API**) is used to store, retrieve and retain records in Nutanix Objects
- **Nutanix Objects** is a simple, scalable S3-compatible object storage solution
- **Buckets** are storage resources available in Nutanix Objects to retain objects, which are comprised of the content and its metadata attributes


Nutanix Enterprise Cloud Platform
S3 API
Nutanix Objects
Buckets with stored objects

Cohasset assessed the capabilities of Nutanix Objects, Release 3.1, when *Bucket Lock* and *Object Lock* are properly applied to stored records. Specifically, when using Nutanix Objects S3 API, *Object Lock* may be applied, which exclusively uses *Compliance m*ode (stricter retention setting with no bypass feature).

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on Cohasset assessed the compliance-related capabilities of Nutanix Objects, when deployed on-premises and running on Nutanix qualified hardware.

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 object, file 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 Objects, 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 Objects
- ***Nutanix Objects 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 Objects, as described in Section 1.3, *Nutanix Objects 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 Objects 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 Objects, 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

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 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 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 Objects, with *Bucket Lock* and *Object Lock*, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based[9] 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 Objects Capabilities

This section describes the functionality of Nutanix Objects 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

- To meet the non-rewriteable, non-erasable requirements of SEC Rule 17a-4(f), Nutanix Objects offers two retention features:
  - *Bucket Lock,* when properly configured, automatically applies time-based retention controls to all records stored in the bucket.
  - *Object Lock* is optionally used to apply an explicit retention period that is longer than the bucket default retention duration to the record.
- A *Legal Hold* may be placed on a record to protect against modification, overwrite and deletion until the *Legal Hold* is released. Once the *Legal Hold* is released, immutability and retention are governed by the records default *Bucket Lock* or explicit *Object Lock* controls.

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

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

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

- With the above settings, Nutanix applies the following stringent integrated controls to the record:
  - The record and its immutable metadata cannot be modified, overwritten or deleted by any process or user, including the system administrator, until both (a) the applied retention duration has expired, and (b) any assigned *Legal Hold* has been released.
  - *Bucket Lock Enable WORM* configuration cannot be modified or removed from the bucket and subsequently protects all records stored in the bucket.
  - The *Bucket Lock Retention* duration cannot be shortened, only extended if necessary.

2.2.3.2 Nutanix Bucket Configurations

- For each Nutanix Objects bucket that will retain records required to comply with SEC Rule 17a-4(f), *Bucket Lock* must be configured by (a) selecting *Enable WORM* and (b) setting a *Bucket Lock Retention Period* (retention duration, e.g., 7 years).
  - The *Bucket Lock Enable WORM* feature may be configured at any time after the bucket is created.
  - *Bucket Lock Retention Period* is specified in seconds, days, months and years.
  - A 24-hour period must lapse for these controls to permanently apply to the bucket.
    - During the first 24-hours of enabling *Bucket Lock*, Nutanix Objects allows the creator of the bucket to remove the *Bucket Lock* and the applicable retention controls provided by the *Bucket Lock* feature.
    - After 24-hours has passed the *Bucket Lock* configuration is permanently applied to the bucket:
      - The *Bucket Lock Enable WORM* feature cannot be suspended or cleared (null) by any user, including the system administrator.
      - The *Bucket Lock Retention Period* may only be extended to retain records for a longer period of time, but cannot be not be shortened (i.e., a retention duration of five (5) years may be extended to six (6) years, but cannot be shortened to four (4) years). When the *Bucket Lock Retention Period* is extended, the new retention duration applies to previously stored, as well as new records.
    - Therefore, to be compliant with the Rule, an appropriate *Bucket Lock Retention Period* must be configured, and records may only be stored in a bucket after the *Bucket Lock* features are permanent (24 hours after *Bucket Lock Enable WORM* is set).
- Optionally, versioning may be enabled on any bucket that uses *Bucket Lock*, which means records that are updated are stored as new versions. When versioning is enabled, each version of a record is separately managed.

2.2.3.3 Record Definition and Retention Controls

- Throughout this report, the term 'record' pertains to either a unique stored object or a specific version of an object, when versioning is enabled.
- Each record is comprised of:
  - Complete content of the object,

  - Immutable metadata, which includes, but is not limited to, unique *Key* name, version identifier (*VersionID*), unique *Object ID*, *creation timestamp* (last modified timestamp), and user-defined custom metadata (key-value pairs), and
  - Mutable metadata, which includes the *Retain Until Date*, which may be extended but not shortened, and *Legal Hold* status, which may be set to On or Off.

- The *Bucket Lock Retention Period,* as described in *Nutanix Bucket Configurations,* above, serves two purposes:
  1. It applies a default retention duration for records stored in the bucket, and
  2. It applies a minimum retention duration, when the *Object Lock* feature, described in the next bullet, is utilized.
- The fundamental capabilities of Nutanix Objects, when *Bucket Lock* is enabled, immutably store records and metadata, assuring that records are not overwritten.
- In addition to the *Bucket Lock* retention feature, Nutanix Objects S3 API supports *Object Lock*, exclusively using the *Compliance mode* (stricter retention setting with no bypass feature). Applying *Object Lock* controls is optional.
  - To apply *Object Lock* controls to a record, the source system may transmit, with the record, an explicit *Object Lock Retain Until Date* and *Object Lock* mode of *Compliance*.
    - When an explicit *Object Lock Retain Until Date* is transmitted with the record, the *Bucket Lock Retention* duration is added to the record creation timestamp to calculate the minimum retention period for the record. This date is then compared to the explicit *Object Lock Retain Until Date* and is stored as the records *Retain Until Date,* if it is longer than the minimum retention period calculated using the *Bucket Lock Retention Period*.
    - For records stored with an explicit *Retain Until Date,* the date may only be extended to a future date but cannot be shortened or cleared (null), by any user, including the account root user.
    - When versioning is enabled, extending the *Retain Until Date* does not create a new version of the record.
  - *Object Lock* mode of *Governance,* a less stringent mode which allows authorized users to remove *Object Lock* from an object, is currently not supported, and results in an error message being returned to the source system.
  - If the source system sends a record with *Object Lock* mode of *Compliance* and *Bucket Lock* is not *enabled*, the write will be denied, and an error message returned to the source system.
- Each record is protected from deletion, by any users, until:
  - The *Object Lock Retain Until Date* that was explicitly applied to the record is in the past.
  - The **current** *Bucket Lock Retention Period* added to the creation timestamp is in the past.
    - Note: If the *Bucket Lock Retention Period* is extended, the longer period will be used to determine eligibility for deletion.
  - The *Legal Hold* status of the record is released (Off).

- If the user attempts any of the following actions, the action is rejected:
  - Disable the *Enable WORM* functionality after 24-hours of configuration, when it is permanently applied to the bucket.
  - Shorten or remove the *Bucket Lock Retention Period*.
  - Shorten or remove a records explicit *Object Lock Retain Until Date*.
  - Delete a record before it is eligible for deletion.
- The *Retain Until Date* for a record can be verified by either: (a) get object *HEAD* command or (b) issuing 'get-object-retention' through the S3 API.

2.2.3.4 Legal Holds

When litigation, regulatory investigation, or a subpoena requires records to be placed on hold, which could entail preserving the record beyond the assigned retention period, the regulated entity must ensure the subject records are preserved for the duration of the Legal hold.

- The *Legal Hold* (On/Off) status may be applied to any record stored in a bucket with the *Bucket Lock* feature enabled.
  - The *Legal Hold* status attribute is applied separately to each record.
  - When the records *Legal Hold* status is set (On), it prohibits deleting the record until the *Legal Hold* status is removed (Off).
  - When the *Legal Hold* status is removed (Off), this attribute no longer mandates preservation of the record; however other retention controls continue to apply to the record.
- When versioning is enabled, setting the *Legal Hold* status does not create a new version of the record.
- The *Legal Hold* status for a record can be verified by the object *HEAD* command through the S3 API.

2.2.3.5 Deletion Controls

- The *Retain Until Date* and *Legal Hold* status determine if the record is eligible for deletion (eligibility for deletion does not cause automatic deletion). The following criteria must be met for a record to be eligible for deletion:
  - The *Object Lock Retain Until Date* that was explicitly applied to the record is expired.
  - The **current** *Bucket Lock Retention Period* added to the creation timestamp is expired.
    - Note: If the *Bucket Lock Retention Period* is extended, the longer period will be used to determine expiration and eligibility for deletion.
  - The *Legal Hold* status must be removed (Off).
- A Lifecycle action may be configured to automatically delete eligible record.
- The bucket cannot be deleted, until the bucket is empty.

2.2.3.6 Security

- Nutanix is designed to meet Enterprise security and compliance requirements.
- Nutanix provides data encryption via the following options: (a) native software-based (SW) encryption (FIPS-140-2 Level-1), (b) self-encrypting drives (SED) (FIPS-140-2 Level-2), or (c) software + hardware encryption Dual encryption. Both SED and SW based encryption can be activated at the same time.
  - Nutanix software encryption provides native AES-256 data-at-rest encryption, which can either interact with any Key Management Interoperability Protocol or Trusted Computing Group compliant external Key Management System server (Vormetric, SafeNet, etc.) or the Nutanix native Key Management service.
- Micro-segmentation with a distributed stateful firewall (Flow) enables granular network monitoring and enforcement between entities.
- Nutanix Objects may be configured to protect data in-transit (data traveling to and from Nutanix Objects) using Secure Sockets Layer (SSL).
- Granular identity and access management (IAM), where the user is identified by access key and policy to allow S3 API (Application Programming Interface) calls. The privileges for each user are controlled through IAM Policies.
- Security Technical Implementation Guide (STIG) – defines the self-healing security configuration providing a point-in-time security baseline checking to a continuous monitoring/self-remediating baseline.

2.2.3.7 Clock Management

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

- Nutanix Objects must be configured to enable NTP and regularly check the time of the external source (NTP) and resynchronize time. During initial configuration, the application server is synced with NTP and all users are restricted from modifying system time once the sync has occurred. These controls prevent or correct any inadvertent or intentional administrative modifications of the system clock, which could allow for premature deletion of records.

2.2.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for:

- Enabling the *Bucket Lock* (enabling WORM) and configuring an appropriate *Bucket Lock Retention Period* for buckets that will store records required for compliance with SEC Rule 17a-4(f). These configurations will assure that all records are stored with retention controls.
- When initially configuring *Bucket Lock* (one-time action per bucket), the *Bucket Lock* settings are permanent after the 24-hour modification window has lapsed; thereafter the *Bucket Lock* feature cannot be removed, and the *Bucket Lock Retention Period* cannot be shortened (though it may be extended). While records can be written to the bucket during the 24-hour modification window, it is recommended to start writing after the initial 24-hour modification window has lapsed to ensure the desired record/data protection.

- Setting a *Legal Hold* status to On, as needed, to preserve records for legal matters, government investigations, external audits and other similar circumstances; and, setting the *Legal Hold* status to Off, when preservation is no longer required.
- Storing records requiring event-based[10] retention periods in a separate compliance system, since Nutanix Objects does not currently support event-based retention periods.
- Setting appropriate security controls to (a) restrict network ports and protocol access, (b) establish roles-based access, and (c) encrypt data in transit and while at rest.

Additionally, the regulated entity is responsible for: (a) authorizing user privileges, and (c) maintaining appropriate technology', encryption keys, and other information and services needed to retain the records.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

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

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

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

2.3.2 Compliance Assessment

Cohasset affirms that the functionality of Nutanix Objects 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 Objects Capabilities

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

2.3.3.1 Recording Process

- An MD5 checksum must be transmitted with the record from the source system at the time of record creation. The record will be stored only if the MD5 checksum value calculated by Nutanix Objects matches the uploaded checksum. If it does not match, an error is reported, and the record must be re-uploaded.
- Nutanix Objects 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.

[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.

2.3.3.2 Post-Recording Verification Process

- Integrity of the record, during retrieval, is validated by comparing the calculated checksum to the original stored checksum.
- Nutanix Objects uses erasure coding to split the record into strips of data blocks and calculates parity. Integrity of the record is maintained by leveraging the parity to calculate any missing data blocks.
  - Nutanix Objects employs a background healing process that scans the data blocks of a record for checking and correcting errors. If a data block is corrupt, an automatic recovery process is initiated to rebuild the data block from the other valid data and parity blocks.

2.3.4 Additional Considerations

The source system is responsible for transmitting the complete contents of the required records and Nutanix Objects validates the accuracy of the transmission and the recording processes.

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

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

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

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

The downloaded records and information 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*.

2.4.2 Compliance Assessment

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

2.4.3 Nutanix Objects 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 Objects is assigned a unique identifier, which facilities findability. Specifically, Nutanix Objects captures the following metadata for each record and immutably retains this metadata for the duration of the applied retention period.
  - Unique *Key* name and *VersionID* at the time of creation, and
  - System-managed creation (storage) timestamp (last modified timestamp).
- Records and metadata attributes may be identified using the Nutanix Objects S3 API.
  - List all the buckets that contain records.
  - List the records, including each version and the date eligible for deletion, which is the longer of: (a) the date calculated by adding the creation timestamp to the *Bucket Lock Retention Period,* and (b) the stored *Object Lock Retain Until Date*.
- Selected records and the associated metadata, or only the metadata, may be downloaded to a designated storage location.

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, encryption keys, and other information and services needed to use Nutanix Objects to readily access, 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).

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

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

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

- The intent of paragraph (A) is:

  [B]ackup electronic recordkeeping system must serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible because, for example, it is impacted by a natural disaster or a power outage.[11] [emphasis added]

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

- 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

It is Cohasset's opinion that the functionality of Nutanix Objects 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 additional consideration in 2.5.4 are satisfied.

2.5.3 Nutanix Objects 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 Objects must be configured with uni-directional geo replication.

- When configuring geo replication, the *Bucket Lock* settings must be manually configured with the same settings on both buckets.
  - If the *Bucket Lock* settings need to be changed, the system administrator must disassociate replication, then change the bucket configurations on both buckets and reenable replication.
- When the *Bucket Lock Retention* or *Object Lock Retain Until Date* is modified or *Legal Hold* is set on the record on the primary storage, the attributes will be propagated between the buckets by the replication process.

2.5.3.2 Other Redundancy Capabilities

For compliance with paragraph (B), Nutanix Objects uses erasure coding (EC) to store data blocks of records 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 encoded data.
- The erasure coded data segments are retained for the full retention period and any applied Legal Holds.

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

2.5.4 Additional Considerations

When using geo replication, the regulated entity must ensure that the initial configuration is the same across the primary and secondary storage.

Additionally, the regulated entity is responsible for maintaining the technology, storage capacity, encryption keys, and other information and services needed to use Nutanix Objects 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.

> **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 Nutanix Objects supports the regulated entity’s efforts to meet this SEC audit system requirement.

2.6.3 Nutanix Objects Capabilities

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

- When inputting records, Nutanix Objects retains the following audit information: (a) unique *Key* name, (b) Version identifier (*VersionID*), and (c) system-managed creation (storage) timestamp (last modified timestamp). These attributes are immutable, chronologically account for each inputted 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 audit events, as part of normal system operations. Subsequently, the log files may then be filtered for specific compliance activities.
  - Alternatively, the Nutanix Objects APIs may be configured and used to receive notifications for specified operations (e.g., create, delete and write). The APIs are currently in beta and can be utilized through Prism.

- Audit events, from Syslog or Nutanix Objects APIs, may be downloaded and subsequently imported into an external applications, 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 Objects 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 Objects, as described in Section 1.3, *Nutanix Objects 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 Objects, with *Bucket Lock* and *Object Lock*, 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 Objects, with *Bucket Lock* and *Object Lock*, 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 Objects 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)**
(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[14] with time-based retention periods, are met by the functionality of Nutanix Objects, with *Bucket Lock* and *Object Lock*, as described in: ● Section 2.2, *Non-Rewriteable, Non-Erasable Record Format* ● Section 2.3, *Record Storage Verification* ● Section 2.4, *Capacity to Download and Transfer Records and Location Information* ● Section 2.6, *Audit System* Additionally, for *records stored electronically*, the CFTC definition of *regulatory records* in 17 CFR § 1.31(a) includes 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] Nutanix Objects retains immutable metadata attributes 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. Immutable metadata attributes include the following: ● Unique *Key* name, ● *VersionID* (when versioning enabled), ● Creation/storage (last modified) timestamp, and ● User-defined custom metadata (key-value pairs). Additionally, mutable (changeable) metadata stored for a record include retention controls and Legal Hold status. The most recent values of mutable metadata are retained for the same time period as the associated record. Further, Nutanix Objects, in conjunction with the inherent Syslog capabilities and Nutanix Objects APIs, tracks 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, *Audit System.*

[14] If Nutanix Objects 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.

CFTC 1.31(c)-(d) Regulation [emphasis added]	**Compliance Assessment Relative to CFTC 1.31(c)-(d)**
(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 Nutanix Objects capabilities described in Section 2.5, *Record Redundancy*, including methods for a persistent duplicate copy or 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).
(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 Nutanix Objects 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 Nutanix Objects[15] 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 Objects, when properly configured, has the following functionality, which meets the regulatory requirements:

- Retains records and immutable system metadata in a non-erasable and non-rewriteable format for time-based retention periods, when (a) *Bucket Lock* is enabled and the default *Bucket Lock Retention* duration is applied or (b) an explicit Object Lock *Retain Until Date* is transmitted together with the *Object Lock* mode of *Compliance*.
- Allows a *Legal Hold* status to be applied to records subject to preservation requirements, which retains the records as immutable and prohibits deletion or overwrites until the *Legal Hold* status is removed.
- Prohibits deletion of a record and its immutable metadata until (a) the applied *Bucket Lock* and *Object Lock* retention periods have expired and (b) the *Legal Hold* status is removed (Off).
- Verifies the accuracy of the process for storing and retaining records, using the MD5 checksum, which is stored as a metadata attribute and utilized for post-recording verification.
- Provides authorized users with the capacity and tools to readily find and download the records and information needed to locate the records for local tools to render a human readable view and produce in the requested format.
- Regenerates an accurate replica of the records and metadata from redundant data, should data be lost or damaged. Optionally, *Geo Replication* provides near synchronous replication of records and associated metadata between source and destination buckets, resulting in duplicate copies.
- Supports the regulated entity’s obligation to retain an audit system for non-rewriteable, non-erasable records.

Accordingly, Cohasset concludes that Nutanix Objects, 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).

[15] See Section 1.3, *Nutanix Objects 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 amendments[16] 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 SBSD/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 Objects 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 Interpretative 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 Interpretative 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 Objects 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.

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.