Cohasset Associates

SEC 17a-4(f), FINRA 4511(c), CFTC 1.31(c)-(d)
Compliance Assessment

# Veritas™ NetBackup™ Flex Scale

## Abstract

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to Cohasset's practice is its delivery of records management and information governance professional consulting services, education and training. Cohasset's expert consulting services are tailored to support a multitude of regulated organizations, including those in the financial services industry. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls with their organizations' business priorities and facilitating regulatory compliance and risk mitigation, all the while generating measurable business efficiencies.

Cohasset has assessed the spectrum of storage technologies and systems designed to meet the requirements of the Securities and Exchange Commission Rule 17a-4(f), as defined by 1) the No Action Letter in 1993 (allowing broker dealers to use non-rewriteable, non-erasable digital storage media); 2) the issuance of the Rule in 1997; and 3) the Interpretive Release in 2003, which authorizes the use of erasable storage, conditioned on integrated control codes, to prevent premature deletion of records.

Veritas™ NetBackup™ Flex Scale is a hyperconverged, scale-out data protection solution that provides backup and recovery services which safeguard data and objects against catastrophic events such as unexpected business disruptions and security attacks. NetBackup Flex Scale captures point-in-time *Image*s of source workloads and applies *Compliance Mode Controls* that are designed to meet securities industry requirements for preserving electronic records in a non-rewriteable, non-erasable format.

In this Report, Cohasset Associates, Inc. (Cohasset) assesses the capabilities of NetBackup Flex Scale (see Section 1.3, *NetBackup Flex Scale Overview and Assessment Scope*) relative to the following regulations:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset's opinion that NetBackup Flex Scale (version 3.0), when properly configured, meets the five requirements related to the recording and the non-rewriteable, non-erasable storage of electronic records in SEC Rule 17a-4(f) and FINRA Rule 4511(c). Additionally, the assessed capabilities of NetBackup Flex Scale meet the principles-based requirements of CFTC Rule 1.31(c)-(d).

# Table of Contents

# 1 | Introduction

*Regulators, world-wide, establish explicit requirements for regulated entities that elect to retain books and records[1] on electronic storage media. Given the prevalence of electronic books and records, these requirements apply to most broker-dealer and commodity futures trading firms and other organizations with similarly regulated operations.*

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

## 1.1 Overview of the Regulatory Requirements

### 1.1.1 SEC Rule 17a-4(f) Requirements

In 17 CFR §§ 240.17a-3 and 240.17a-4, the SEC stipulates recordkeeping requirements, including retention periods, for the securities broker-dealer industry. On February 12, 1997, the SEC adopted amendments to 17 CFR § 240.17a-4 (the Rule or Rule 17a-4). These amendments to paragraph (f) expressly allow books and records to be retained on electronic storage media, subject to explicit standards.

> *The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4.*[2] [emphasis added]

Further, the SEC issued two Interpretive Releases (No. 34-44238 on May 1, 2001, and No. 34-47806 on May 7, 2003), which pertain specifically to the electronic storage media requirements of paragraph (f).

For additional information, refer to Section 5.1, Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements.

### 1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to the format and media requirements of SEC Rule 17a-4, for the 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.*

[1] Regulators use the phrase *books and records* to describe information about certain business transactions, customers, personnel and other administrative activities that must be retained. Accordingly, Cohasset has used the term *Image* (versus *data* or *object*) to consistently recognize that the content is a required record.

[2] Exchange Act Release No. 38245 (Feb. 5, 1997), 62 FR 6470 (Feb. 12, 1997) ("Adopting Release").

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

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

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, which correlates the CFTC principles-based requirements to the capabilities of NetBackup Flex Scale. Additionally, refer to 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 NetBackup Flex Scale, Veritas engaged Cohasset Associates, Inc. (Cohasset). As a highly-respected consulting firm, Cohasset has recognized expertise and more than 50 years of experience with the legal, technical and operational issues associated with the records management practices of companies regulated by the SEC and CFTC. Additional information about Cohasset is provided in the last section of this report.

Veritas engaged Cohasset to:

- Assess the capabilities of NetBackup Flex Scale in comparison to the five requirements of SEC Rule 17a-4(f) for the recording and non-rewriteable, non-erasable storage and retention of electronic records; see Section 2, *Assessment of Compliance with SEC Rule 17a-4(f);*
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of NetBackup Flex Scale; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);* and
- Prepare this Assessment Report, enumerating the results of its assessment.

*In addition to applying the information in this Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the capabilities of implemented electronic recordkeeping solutions, 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 NetBackup Flex Scale and its capabilities or other Veritas products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) system documentation, (c) user and system administrator guides, and (d) other directly-related materials provided by Veritas or obtained from publicly available resources.

The content and conclusions of this assessment are not intended, and must not be construed, as legal advice. Relevant laws and regulations constantly evolve, and legal advice is tailored to the specific circumstances of the organization. Therefore, nothing stated herein should be substituted for the advice of competent legal counsel.

## *1.3* NetBackup Flex Scale Overview and Assessment Scope

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

NetBackup Flex Scale captures a point-in-time *Image*[3] of a source workload (i.e., a database, file system, virtual machine, etc.) and retains it according to rules defined in a backup policy. Integrated immutability[4] and indelibility[5] controls are applied within the storage subsystem during the backup process, to retain the *Image* in compliance with the non-rewriteable, non-erasable storage requirements of SEC Rule 17a-4(f).

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

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

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

**Media Server(s)** – Are intelligent load-balancing gateways, or data movers, between the clients and the MSDP[6] Storage Server (i.e., storage subsystem). Media Servers communicate with the MSDP Storage Server via Open Storage Technology (OST) commands (i.e., an application programming interface published by Veritas).

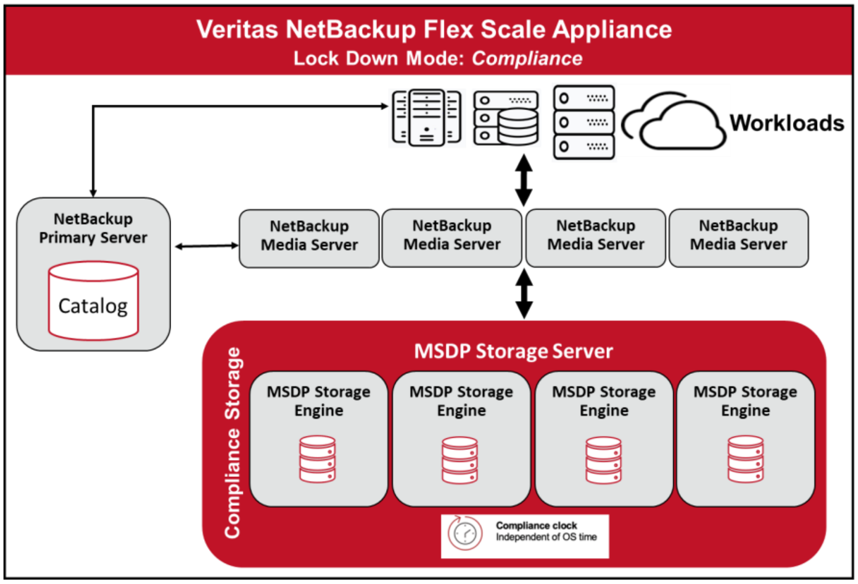

Figure 1: NetBackup Flex Scale Logical Architecture

**MSDP Storage Server** – A single tenancy, scale-out deduplicated storage pool consisting of four to sixteen storage nodes, each with its own Intel-based CPU, memory, network and disks. All storage nodes are treated as a

[3] Regulators use the phrase *books and records* to describe information about certain business transactions, customers, personnel and other administrative activities that must be retained. Accordingly, Cohasset has used the term *Image* (versus *data* or *object*) to consistently recognize that the content is a required record.

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

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

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

single entity by NetBackup. A configuration setting at the NetBackup Flex Scale appliance level, called *Lock Down Mode*, determines the type of integrated controls that will be made available for use within the MSDP Storage Server. *Lock Down Mode* options include:

- Compliance Mode
- Enterprise Mode
- Normal Mode

Only NetBackup Flex Scale appliance storage configured in *Compliance Mode* (hereinafter referred to as ***Compliance Storage***) meets the strict non-rewriteable, non-erasable storage requirements of the Rule by providing integrated immutability and indelibility controls (hereinafter referred to as ***Compliance Mode Controls***).

The scope of this assessment is focused specifically on the capabilities of the fully integrated, enterprise-grade NetBackup Flex Scale appliance (version 3.0), with:

- All necessary NetBackup services instantiated (e.g., NetBackup Primary Server, Media Servers, and MSDP Storage Server with minimum of four storage nodes), and
- Configured in *Compliance Mode.*

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

Throughout this report, the above-described operating environment of NetBackup Flex Scale are assessed.

# 2 | Assessment of Compliance with SEC Rule 17a-4(f)

*This section presents Cohasset's assessment of the capabilities of Veritas NetBackup Flex Scale for compliance with the five requirements related to recording and non-rewriteable, non-erasable storage of electronic records, as stipulated in SEC Rule 17a-4(f).*

For each of the five relevant requirements in SEC Rule 17a-4(f), this assessment is organized into the following four topics:

- ***Compliance Requirement*** – Excerpt of each electronic storage requirement in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirement
- ***Compliance Assessment*** – Assessment of the relevant capabilities of NetBackup Flex Scale
- ***NetBackup Flex Scale Capabilities*** – Description of relevant capabilities
- ***Additional Considerations*** – Additional considerations related to meeting the specific requirement

The following subsections document Cohasset's assessment of the capabilities of NetBackup Flex Scale, as described in Section 1.3, *NetBackup Flex Scale Overview and Assessment Scope*, relative to each pertinent requirement of SEC Rule 17a-4(f).

## 2.1 Non-Rewriteable, Non-Erasable Record Format

### 2.1.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(A)]

**SEC 17a-4(f)(2)(ii)(A):** Preserve the records exclusively in a non-rewriteable, non-erasable format

As set forth in Section III(B) of the 2001 Interpretive Release, this requirement *"is designed to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in an unalterable form [for the required retention period]."*

The following statement in the 2003 Interpretive Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, meet the requirements of a non-rewriteable, non-erasable recording environment provided: (a) the storage solution delivers the prescribed functionality and (b) the functionality is delivered via appropriate integrated control codes for the SEC designated retention period associated with the stored records.

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

Further, Section IV of the 2003 Interpretive Release places requirements on the storage system for retaining records beyond the SEC-established retention period when certain circumstances occur, such as a subpoena or legal hold:

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, 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.* [emphasis added]

This statement by the SEC clarifies that the storage system must have the capability to retain records beyond the retention period established at the time of initial recording when required for legal matters, external investigations or audits, or other similar circumstances.

### 2.1.2 Compliance Assessment

It is Cohasset's opinion that NetBackup Flex Scale, with *Compliance Mode Controls*, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for time-based[7] retention periods, when (a) properly configured, as described in Section 2.1.3 and (b) the considerations described in Section 2.1.4 are satisfied.

### 2.1.3 NetBackup Flex Scale Capabilities

This section describes the capabilities of NetBackup Flex Scale that directly pertain to this SEC requirement for preserving electronic records (*Images*) as non-rewriteable, non-erasable for the required retention period and any associated legal holds.

#### 2.1.3.1 Overview

- A record in NetBackup Flex Scale is defined as a backup *Image* (i.e., a backup copy of a specified source workload) along with system metadata associated with that *Image*.
- To meet the non-rewriteable, non-erasable requirements of SEC Rule 17a-4(f), an *Image* requiring time-based retention, must be stored in *Compliance Storage* via a policy that (a) requires the application of *Compliance Mode Controls* and (b) sets an appropriate *WORM*[8] *Retention Period* for the *Image*.
- When litigation or a subpoena requires an *Image* to be preserved beyond its currently assigned *WORM Retention Period*, the *WORM Retention Period* is extended to ensure the *Image* is immutably retained for the duration of the hold. Additionally, a hold attribute may be set for the *Image* within the Primary Server Catalog, to facilitate searches and to prevent the Primary Server Catalog from issuing automated post-retention delete requests.

[7] Time-based retention periods require records to be retained for a specified contiguous period of time from the date and time created (i.e., storage date).

[8] WORM is a common acronym for *write-once, read-many* and refers to the type of retention controls applied by NetBackup Flex Scale.

- With the above settings, NetBackup Flex Scale applies the following stringent integrated controls to the *Image*:
  - The *Image* and its immutable metadata cannot be modified, overwritten or deleted by any mechanism, NetBackup Flex Scale user, or NetBackup Flex Scale Appliance Administrator until the applied *WORM Retention Period* has expired.
  - *Compliance Mode Controls*, once established, cannot be modified for *Compliance Storage* (i.e., *Lock Down Mode* cannot be changed to Enterprise or Normal) nor removed from the *Image*.
  - The *WORM Retention Period* cannot be shortened, only extended, if necessary.

### 2.1.3.2 *Flex Scale Appliance and NetBackup Primary Server Configurations*

The following configurations are required within the (a) NetBackup Flex Scale appliance, and (b) the NetBackup Primary Server to enable the use of integrated *Compliance Mode Controls*, which are designed to retain regulated *Images* in compliance with SEC Rule 17a-4(f).

- The **NetBackup Flex Scale appliance** comes preconfigured as described in section *1.3 NetBackup Flex Scale Overview and Assessment Scope*. All necessary NetBackup services (e.g., NetBackup Primary Server, Media Servers, and MSDP Storage Server with a minimum of four storage nodes) are instantiated automatically on the appliance. By default, the appliance is set to operate in *Normal Mode*, which does not support the application of WORM (i.e., immutability and indelibility) retention controls. As such, a NetBackup Flex Scale appliance that is intended to store regulated *Images,* must be configured by the Appliance Administrator as follows:

  1. Enable *Compliance Mode* for the appliance, via the Appliance Management Console, during initial setup or at any time prior to storing regulated *Images*. *Compliance Mode* applies to the entire MSDP Storage Server pool, meaning that all nodes within the MSDP Storage Server pool are ***capable*** of storing *Images* in a non-rewriteable, non-erasable format (hereinafter referred to as *Compliance Storage*). Policies within NetBackup dictate whether the *Compliance Mode Controls* are **applied** to each *Image* as it is written.
     - Note: NetBackup Flex Scale also supports *Enterprise Mode*. If set to *Enterprise Mode*, *Images*, including system metadata, cannot be modified or overwritten by any user. However, *Images* may be deleted prior to the expiration of the *WORM Retention Period* by a secured, authorized process. As such, *Enterprise Mode* is non-compliant and outside the scope of this assessment. Only *Compliance Mode* allows regulated *Image*s to be stored in compliance with SEC Rule 17a-4(f).
     - The appliance mode can be changed from less restrictive to more restrictive at any time (i.e., changed from *Enterprise* to *Compliance*). Retention controls are applied to **new** *Images* according to NetBackup policies, however:
       - When moving from *Normal* to either *Enterprise* or *Compliance* mode, previously stored *Images* remain unprotected.
       - When moving from *Enterprise* to *Compliance* mode, *Compliance Mode Controls* are automatically applied to previously stored *Images* and as such, premature deletion of those *Images* is prohibited.

- The appliance mode may be changed to a less restrictive mode only when all existing protected *Images* have expired and are removed from storage.
- New nodes added to the MSDP Storage Server pool automatically inherit the existing mode of the appliance.

2. Set allowable Min/Max retention values (i.e., ranging between 1 hour and 60 years) as guardrails for the MSDP Storage Server pool. When an *Image* is written to *Compliance Storage* with a retention value outside the established Min/Max values, the write process fails and an error message is generated.
3. Enable the *Restricted Remote Access* feature, which limits Appliance Administrator capabilities to an approved set of non-destructive operations when remotely using IPMI infrastructure. Once the *Restricted Remote Access* feature is enabled for an appliance configured in *Compliance Mode*, the feature cannot be disabled.

- **The NetBackup Primary Server** must have one or more Storage Units (i.e., a storage construct or label, referenced within backup policies, identifying the specific physical storage pool to be used for retaining *Images*) configured to allow *Images* to be retained on *Compliance Storage*. *Note: the NetBackup Primary Server utilizes different terminology than the NetBackup Flex Scale Appliance when referring to retention controls. For example, the phrase* WORM-capable Disk Pool i*s used by the NetBackup Primary Server rather than* Compliance Storage.
  - A Storage Unit must be *Compliance-Enabled* by (a) specifying the use of *Compliance Storage* and (b) requiring WORM controls be applied (*Compliance Mode Controls*). If these two requirements are not met, recorded *Images* **will not have *Compliance Mode Controls* applied**.
  - When NetBackup is initially instantiated on the NetBackup Flex Scale appliance, one default Storage Unit is automatically created within NetBackup, with the same mode as the appliance.
    - When the appliance mode is set to Compliance, the default Storage Unit is automatically updated to Compliance-Enabled.
    - Additional Storage Units may be configured for *Compliance Storage*, with or without requiring the application of WORM controls. Accordingly, *Images* written via a Storage Unit **that does not require** WORM controls, are recorded on *Compliance Storage* without *Compliance Mode Controls* applied.
  - Once a Storage Unit is designated as Compliance-Enabled, it cannot be changed.
  - Ideally, the names of both the Storage Unit and the *Compliance Storage* it references will contain the words COMPLIANCE or COMPLIANCE WORM, for reference purposes.
  - NetBackup Administrators must always verify that a Storage Unit points to properly configured *Compliance Storage* via the MSDP Storage Server Properties screen on the NetBackup user interface.

#### 2.1.3.3 *Images and Retention Controls*

- Data and/or objects are transmitted from the source system, via NetBackup client software, according to scheduled or on-demand policies (described, below).
  - The *Workload* (i.e., file system, database, virtual machine, applications, etc.) from the source system is copied via a stream, or multiple parallel streams of data, to the designated NetBackup Flex Scale MSDP Storage Server pool.
- A record in NetBackup is defined as a backup *Image* (i.e., a full, incremental, synthetic, or accelerator copy of a specified source workload) along with system metadata associated with that *Image*.
  - System metadata includes critical attributes for records management, such as the unique backup ID (including the date/time backup was initiated at the source system), copy number, Immutable Y/N flag, Indelible Y/N flag, WORM Retention Period (in seconds), name of backup policy, type of backup policy (i.e., workload), calculated *Retain Until* Date, content index, and checksum.
- *Compliance Mode Controls* are **applied** to *Images* when the backup process executes, according to rules established in (1) *NetBackup Policies* and/or (2) *Storage Lifecycle Policies*:
  1. **A *NetBackup Policy*** is a predefined ruleset/schedule, created by the NetBackup Administrator, whereby a specified source *workload* is copied to *Compliance Storage* for data protection purposes.
     - *Compliance Mode Controls* settings must be defined for a policy that is intended to govern regulated *Images*, as follows:
       - Target storage is selected for retaining backup copies that are either (a) a *Compliance-Enabled* Storage Unit or (b) a link to a *Storage Lifecycle Policy* that specifies a *Compliance-Enabled* Storage Unit.
       - A *WORM Retention Period* (i.e., sometimes referred to as *Retention Period or WORM Lock Time)* is assigned by (a) entering a retention value in terms of days, weeks, months or years and ensuring that the entered value falls within the allowable min/max range for the selected *Compliance Storage*, (b) selecting the desired retention value from a list of pre-defined Retention Levels (i.e., a logical construct for easier access to commonly used retention periods), or (c) associating the *NetBackup Policy* with a *Storage Lifecycle Policy* that specifies a *WORM Retention Period* for the *Image*.
     - Each *NetBackup Policy* includes additional attributes, or rules, which govern the backup, including the frequency/schedule and backup type (i.e., full, incremental, synthetic, or accelerator).
       - Full and incremental backups are linked together via attributes to facilitate recovery. However, full and associated incremental backups are treated as separate, individual *Images* and as such, each may have different retention requirements.
       - A synthetic backup is one that combines a prior full backup with one or more recent incremental backups to produce a new consolidated backup *Image*. The consolidated *Image* is a separate *Image*, with its own unique ID and retention controls.

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

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

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

    - Establishing the *Compliance Mode Controls* settings (i.e., Compliance-Enabled Storage Unit and the *WORM Retention Period)*, if not already assigned by an individual *NetBackup Policy*, and

    - Establishing duplication, replication, or other post backup operations. Note: Each *Storage Lifecycle Policy* operation that will produce regulated *Images*, must have its own *Compliance Mode Controls* defined (i.e., Compliance-Enabled Storage Unit and *WORM Retention Period*).

- When NetBackup executes a backup job, based on policies as described above, integrated *Compliance Mode Controls* are applied by *Compliance Storage* to retain *Images* in accordance with the non-rewriteable, non-erasable requirements of the Rule.

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

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

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

        - The *Image* is locked and protected against modification and overwrites for the life of the *Image* and protected against deletion for the duration of the *WORM Retention Period*.

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

- The *WORM Retention Period* assigned to an *Image* under *Compliance Mode Controls* may be extended via the command line interface or Java user interface, as needed. The NetBackup Primary Server sends the number of additional seconds required for retention to Compliance Storage, where the *Image's* lock time is extended accordingly.
  - The *WORM Retention Period* retained within *Compliance Storage* may **not** be reduced or deleted by any NetBackup users, including Appliance Administrators who have no access to the root account or operating system within *Compliance Storage*.
- *The* Storage Unit and *WORM Retention Period* referenced within *NetBackup Policies* and *Storage Lifecycle Policies* can be modified at any time; however, the new values apply to new *Image*s only.
- An *Image* that is stored with *Compliance Mode Controls* may be copied up to 10 times via rules defined within a *Storage Lifecycle Policy*. All copies are tracked within the Primary Server Catalog.
  - The original *Image* remains unchanged and protected by the *Compliance Mode Controls* for the specified *WORM Retention Period*.
  - The copy is assigned its own unique *Image* ID (i.e., the original *Image* ID with an appended sequential copy number). *Compliance Mode Controls,* including the *WORM Retention Period,* will <u>not</u> carry over to the copy and, therefore, must be applied independently by the *Storage Lifecycle Policy*, if required.

#### 2.1.3.4 *Legal Hold*

- When litigation or a subpoena requires an *Image* to be preserved beyond its currently assigned *WORM Retention Period*, the *WORM Retention Period* must be extended on the primary *Image* (and any secondary copies) to ensure the *Image* is immutably retained for the duration of the hold.
  - Additionally, a Hold Name and Yes/No Hold attribute may be set for the primary *Image* (and any secondary copies) within the Primary Server Catalog, to facilitate searches and to prevent the Primary Server Catalog from issuing automated post-retention delete requests. *Note: The Hold attribute is <u>not</u> transferred to* Compliance Storage*, and therefore, will not provide immutability and indelibility protection to* Images *that are past their assigned* WORM Retention Period.
  - The Hold attribute may be removed from the Primary Server Catalog for an *Image* when no longer required.

#### 2.1.3.5 *Deletion Controls*

- In NetBackup Flex Scale, an *Image* is eligible for deletion when the following conditions are met:
  - The assigned *WORM Retention Period* has expired, and
  - A Hold attribute is <u>not</u> assigned to the *Image* in the Primary Server Catalog. Note: The Primary Server Catalog attribute applies to automated disposition only.

- Delete requests are part of an automated job on the NetBackup Primary Server, which typically runs every 12 hours to remove *Image*s eligible for deletion. Additionally, delete requests may be triggered manually.
  - Delete requests are based on the stored *Retain Until Date*, according to Primary Server system time.
  - Upon receipt of a delete request, *Compliance Storage* verifies deletion eligibility based on the elapsed retention time, as calculated by the Compliance Clock. If the storage subsystem determines that the *WORM Retention Period* has <u>not</u> yet expired, it denies the request, however, index information associated with the *Image* will be removed from the Primary Server Catalog. An automated background *Image Cleanup* process periodically attempts deletion of eligible *Images* from *Compliance Storage* until successful.
    - To add index data for the *Image* back into the Primary Server Catalog, a re-import is required and the Primary Server Catalog will then contain the updated *Retain Until Date* provided by the storage subsystem.
- *Compliance Storage* cannot be deleted if it contains immutable *Images*.

#### 2.1.3.6 *Clock Management*

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

#### 2.1.3.7 *Security*

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

  - *Image*s are only accessible via OST API's.
  - Custom VxOS shell is utilized for MSDP Storage Engines and appliance CLI commands and provides no operating system or root access.
  - Compliance Storage is segregated from protocol services such as NFS and CIFS.
  - SELinux labelling is automatically employed for file systems to provide segregation. Additionally, SELinux protections include default RedHat policies to protect the core operating system.

- When the *Restricted Remote Access* feature is enabled on the NetBackup Flex Scale appliance, Appliance Administrator capabilities are limited to an approved set of non-destructive operations. Appliance Administrators are prohibited from using iLO/iDRAC interfaces to remotely boot from an unsecure device.
- The NetBackup Flex Scale appliance operating system runs in Federal Information Processing Standard (FIPS) mode by default. This ensures only FIPS validated algorithms are used by the operating system and its core services.
  - All appliance management and MSDP Storage Server communications are fully encrypted as per FIPS 140-2 standard. MSDP Storage Server also employs FIPS 140-2 compliant encryption for data at-rest, utilizing the provided NetBackup Key Management System (KMS) or an external KMS.

### *2.1.4 Additional Considerations*

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

- Deploying the NetBackup Flex Scale appliance (version 3.0) as described in section 1.3.
- Appropriately configuring the NetBackup Flex Scale appliance for use in *Compliance Lock Down Mode* (i.e., create *Compliance Storage*) with the *Restricted Remote Access* feature enabled.
- Setting appropriate Min/Max Retention range values for *Compliance Storage*.
- Creating Compliance-Enabled Storage Units that point to *Compliance Storage* and mandate the use of WORM controls.
- Applying *Compliance Mode Controls* to *Images* requiring compliant retention by establishing *NetBackup Policies* and/or *Storage Lifecycle Policies* that reference Compliance-Enabled Storage Units and setting appropriate *WORM Retention Period*s.
- Appropriately protecting source workloads, until the *Images* have been successfully written to Compliance Storage, particularly in cases where the size of the workload will result in a multi-day process to complete.
- Extending the retention duration for *Images* and secondary copies that must be kept longer than the assigned *WORM Retention Period*, to effectuate a legal hold for subpoenas, litigation, government investigations, external audits and other similar circumstances.
- Re-importing index data from the storage subsystem into the Primary Server Catalog as needed to ensure alignment.

- Storing *Image*s requiring event-based retention in a separate compliance system, since NetBackup Flex Scale does not natively support event-based retention.
- Managing encryption keys if utilizing a third-party or NetBackup KMS.

## 2.2 Accurate Recording Process

### 2.2.1 *Compliance Requirement [SEC 17a-4(f)(2)(ii)(B)]*

**SEC 17a-4(f)(2)(ii)(B):** Verify automatically the quality and accuracy of the storage media recording process

The intent of this requirement is to ensure both the accuracy and quality of the recording process such that the records read from the storage media are precisely the same as those that were recorded. This requirement includes both a quality verification of the recording process and post-recording verification processes.

### 2.2.2 *Compliance Assessment*

Cohasset affirms that the capabilities of NetBackup Flex Scale, in conjunction with the inherent capabilities of advanced magnetic storage technology, meet this SEC requirement for accurate recording and post-recording verification.

### 2.2.3 *NetBackup Flex Scale Capabilities*

NetBackup Flex Scale has a combination of recording and post-recording verification processes, which are described in the following subsections.

#### 2.2.3.1 *Recording Process:*

- A combination of checks and balances in the advanced magnetic recording technology – such as inter-component and inter-step cyclical redundancy checks (CRCs), as well as write-error detection and correction – are relied upon to ensure that the *Image*s are written in a high-quality and accurate manner.
- When an *Image* is written to NetBackup Flex Scale storage:
  - The *Image* is divided into separate fragments during the write process.
  - A checksum is calculated for each fragment of data and stored as immutable metadata at the individual fragment level, for post-recording validation.
  - Once NetBackup Flex Scale verifies that all fragments have been successfully written, acknowledgement of a successful write is returned to the source system. If a write failure occurs at any stage, an error message is returned to the source for corrective action and the write operation is stopped to prevent corrupted data from being written to NetBackup Flex Scale storage.

#### 2.2.3.2 *Post-Recording Verification Process:*

- During automated background consistency checks, magnetic disk error detection and correction are applied to correct any in-error data on the magnetic disk. Should the magnetic disk error detection and correction fail to correct the data, the data is flagged as corrupted and the regulated entity must work with NetBackup Flex Scale support personnel to correct it.

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

### 2.2.4 Additional Considerations

There are no additional considerations related to this requirement.

## 2.3 Serialize the Original and Duplicate Units of Storage Media

### 2.3.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(C)]

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

**SEC 17a-4(f)(2)(ii)(C):** Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media

When the SEC Rule was issued in 1997, this requirement was thought to be more pertinent to tracking the individual units of removable media related to micrographic or optical storage. This requirement for non-unitized electronic storage may be satisfied by capturing and storing immutable metadata, associated with each electronic record, to *uniquely* identify the record and the *date and time of recording*.

### 2.3.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of NetBackup Flex Scale meet this SEC requirement to serialize the original and duplicate records.

### 2.3.3 NetBackup Flex Scale Capabilities

- NetBackup Flex Scale assures each *Image*, regardless of how it originates (i.e., full, incremental, or synthetic backup), is assigned a unique ID. The unique *Image* ID is a combination of the following attributes:
  - A *Backup ID*, which is comprised of (a) source system name and (b) date and time stamp.
    - Backups may span multiple days due to the size of the workload, therefore, the date and time stamp represents the time at which the backup *started on the source system*.
  - A *Copy Number*, which is an incremental number assigned to each sequential execution of a given *NetBackup Policy*.
- The combination of the *Backup ID* and *Copy Number* serialize the *Image* in both space and time.

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

### 2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

## 2.4 Capacity to Download Indexes and Records

### 2.4.1 Compliance Requirement [SEC 17a-4(f)(2)(ii)(D)]

This requirement necessitates an adequate capacity to readily download records and associated indexes, in a format and on a medium acceptable under the Rule and as specified by the SEC or self-regulatory organization. This allows the SEC or self-regulatory organizations to take possession of the downloaded records and indexes.

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

### 2.4.2 Compliance Assessment

It is Cohasset's opinion that the capabilities of NetBackup Flex Scale meet this SEC requirement to readily download *Images* and Indexes (metadata attributes) when the considerations described in Section 2.4.4 are addressed.

### 2.4.3 NetBackup Flex Scale Capabilities

NetBackup Flex Scale capabilities that support the capacity to download *Image*s and associated metadata include:

- The NetBackup Administrator's Console (a Java-based graphical user interface) provides NetBackup Administrators the ability to list the *Image*s under retention management within the Primary Server domain, filtered by metadata such as policy, copy number, type of backup, source system, date range, etc. *Note: NetBackup is storage agnostic in that it searches through all Images being managed by the NetBackup Flex Scale Primary Server Catalog, whether the Images are stored in Flex or NetBackup Flex Scale appliances.*
  - The search results screen is configurable and may include metadata such as: *Image* ID, NetBackup policy name, backup policy type, media server, lock status, *WORM Retention Period,* source system name and time stamp, etc.
  - From the search results screen, the following operations are available:
    - Copy (duplicate) a select *Image* (i.e., make a full *Image* copy) to another location.
    - Verify consistency of the *Image* on the disk volume.
    - Browse through the contents of the NetBackup *Image*. The level of viewable content varies by type of workload.

- Alternatively, the command line interface (CLI) may be used to programmatically search the Primary Server Catalog. The resulting list may be exported via flat file, then imported into a CSV file and viewed and/or transferred to a medium acceptable under the Rule.
- NetBackup Flex Scale allows for *Images* to be:
  - Restored, via the NetBackup Administrator's Console, to a specified source system where content may then be viewed and/or reproduced or transferred to a medium acceptable under the Rule; or
  - Programmatically exported, via CLI.
- Programmatic interfaces (i.e., CLI or Restful APIs), as well as supported third party query tools, may be used to search and restore/retrieve *Image*s from NetBackup storage. Once retrieved, content may be viewed by source system software and reproduced or transferred to a medium acceptable under the Rule.

### *2.4.4 Additional Considerations*

The regulated entity is responsible for (a) assuring that hardware and software capacity allows for ready access to the *Image*s and Indexes (metadata attributes) within NetBackup, (b) maintaining its NetBackup licensing in good standing, (c) maintaining its encryption keys, if not utilizing the NetBackup KMS, and (d) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the *Image*s and Indexes (metadata attributes) in the requested format and medium.

## 2.5 Duplicate Copy of the Records Stored Separately

### *2.5.1 Compliance Requirement [SEC 17a-4(f)(3)(iii)]*

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

**SEC 17a-4(f)(3)(iii):** Store separately from the original, a duplicate copy of the record stored on any medium acceptable under § 240.17a-4 for the time required

Note: A *duplicate copy* is defined as a persistent copy that allows the complete and accurate record to be reestablished from data stored on a compliant storage system or medium. Whereas, a *backup copy* is defined as a non-persistent copy that is overwritten as it is *rotated* on a periodic basis, resulting in a much shorter retention period than the original.

### *2.5.2 Compliance Assessment*

Cohasset affirms that NetBackup Flex Scale meets this SEC requirement for a persistent duplicate copy of the *Images*, when (a) properly configured, as described in Section 2.5.3, and (b) the considerations described in Section 2.5.4 are satisfied.

### *2.5.3 NetBackup Flex Scale Capabilities*

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

- In addition to erasure coding, which is capable of regenerating stored *Images*, NetBackup Flex Scale offers the following two options for retaining full, duplicate copies of *Images*:

  1. **Auto *Image* Replication (AIR)** - creates a copy of an *Image* onto a remote, geographically dispersed storage device in a different Primary Server domain. This results in the original and replica *Images* being managed by two separate Primary Server Catalogs.

  2. **Duplication** - creates a copy of an *Image* on a separate NetBackup Flex Scale appliance, typically within the same data center, which can be used for disaster recovery purposes in addition to meeting compliance requirements. Original and duplicate *Images* can be managed by a single NetBackup Flex Scale Primary Server Catalog when configured to do so.

  - Duplication and Auto *Image* Replication (AIR) are configured via *Storage Lifecycle Policies* that (a) identify the *NetBackup Policy*, or rather, the resulting *Images created by a NetBackup Policy,* that require replication, (b) assign target storage for the duplicates/replicas by specifying a Compliance-Enabled Storage Unit with appropriate storage capacity, and (c) assign a *WORM Retention Period* that is identical to the original *Image*.

    - Additionally, duplication may be initiated manually via the NetBackup Administrator's Console or programmatically via command line interface (CLI).

  - Once configured via a *Storage Lifecycle Policy*, duplication/replication occurs automatically, each time the primary *NetBackup Policy* executes.

    - NetBackup can catalog up to 10 copies of a single *Image*, however, each copy must reside on a separate NetBackup Flex Scale appliance. *Note: the original Image is considered the first copy*.

  - The content of the duplicated/replicated *Image* is an exact copy of the original, however, metadata associated with the secondary *Image* is different:

    - The secondary *Image* has a unique Backup ID and Copy number.

    - The *WORM Retention Period* associated with the secondary *Image* is not kept synchronized with the primary *Image*. Therefore, if the *WORM Retention Period* is extended on the primary *Image* (i.e., when litigation or a subpoena requires an *Image* to be preserved beyond its currently assigned *WORM Retention Period)* the *WORM Retention Period* associated with the secondary *Image* must be manually extended as well.

### 2.5.4 Additional Considerations

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

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

The objective of this section is to document Cohasset's assessment of the capabilities of NetBackup Flex Scale, as described in Section 1.3, *NetBackup Flex Scale Overview and Assessment Scope*, in comparison to the CFTC requirements.

The individual relevant requirements cited in Section 2, *Assessment of Compliance with SEC Rule 17a-4(f)*, are based on the wording in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirements, given the associated SEC Interpretive Releases. Specifically, the SEC's 2003 Interpretive Release reiterates that the Rule sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under SEC Rule 17a-4:

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

Accordingly, it is Cohasset's opinion that the requirements set forth in SEC Rule 17a-4(f) are *technology-neutral* and apply to any electronic solution with (a) integrated control codes that extend to the electronic storage system and (b) features that deliver capabilities that meet the requirements of the Rule.

The August 28, 2017, amendments to CFTC Rule 1.31 establish *technology-neutral*, *principle-based* requirements. As illustrated in the table in this section, it is Cohasset's opinion that the requirements of the modernized CFTC Rule may be achieved by meeting the SEC requirements.

When comparing the capabilities of NetBackup Flex Scale that align with the SEC requirements to the *principles-based* CFTC requirements, it is essential to recognize that the SEC Rule separately describes requirements for index data and audit trail, whereas the CFTC in 17 CFR § 1.31(a) establishes an expanded definition of an *electronic regulatory record* to include the information as specified in paragraph (i) and (ii) below.

> ***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 focus of Cohasset's assessment, presented in Section 2, pertains to NetBackup Flex Scale, configured with *Compliance Mode Controls*, which is a highly restrictive configuration that assures the storage solution applies controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied *WORM Retention Period*.

In the following table, Cohasset correlates the capabilities of NetBackup Flex Scale, with *Compliance Mode Controls,* to the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. In addition, Cohasset contends that NetBackup Flex Scale when configured in *Enterprise Mode*, meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be modified or deleted prior to expiration of the *WORM Retention Period*. This less restrictive *Enterprise Mode* configuration allows *Images* to be deleted by a secured, authorized process, which may be beneficial for compliance with privacy and data protection requirements.

The left-hand column lists the *principles-based* CFTC requirements. The middle column also provides Cohasset's analysis and opinion regarding the ability of NetBackup Flex Scale to meet the requirements for electronic regulatory records in CFTC Rule 1.31(c)-(d). In addition, for ease of reference, the right-hand column lists the correlated SEC requirements.

| CFTC 1.31(c)-(d) Requirement | Compliance Assessment Relative to CFTC 1.31(c)-(d) | SEC 17a-4(f) Requirements Listed in the Referenced Sections |
|---|---|---|
| **(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:<br>(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.<br>(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:<br>(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 NetBackup Flex Scale capabilities, utilized with *Compliance Mode Controls*, as described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for *Images*.<br>Additionally, for *records stored electronically*, the CFTC has expanded the definition of *regulatory records* in 17 CFR § 1.31(a) to include metadata:<br>*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:*<br>*(i) Any data necessary to access, search, or display any such books and records; and*<br>*(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.* [emphasis added]<br>● It is Cohasset's opinion that NetBackup Flex Scale retains immutable system metadata (e.g., Backup ID with date/time stamp, and Copy Number), as an integral part of the *Image* itself. The *Image* system metadata are subject to the same retention protections as the associated *Image*.<br>● To satisfy this requirement for other essential data related to how and when the *Images* were created, formatted, or modified, the regulated entity must retain this data in a compliant manner. | **Section 2.1 *Non-Rewriteable, Non-Erasable Record Format***<br>*Preserve the records exclusively in a non-rewriteable, non-erasable format*<br>**Section 2.2 *Accurate Recording Process***<br>*Verify automatically the quality and accuracy of the storage media recording process*<br>**Section 2.3 Serialize the Original and Duplicate Units of Storage Media**<br>*Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media.*<br>***Section 2.4 Capacity to Download Indexes and Records***<br>*Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member* |

| CFTC 1.31(c)-(d) Requirement | Compliance Assessment Relative to CFTC 1.31(c)-(d) | SEC 17a-4(f) Requirements Listed in the Referenced Sections |
|---|---|---|
| (ii) Systems that ensure the records entity is able to produce electronic regulatory records[9] in accordance with this section, and *ensure the availability of such regulatory records in the event of an emergency or other disruption* of the records entity's electronic record retention systems; and | It is Cohasset's opinion that NetBackup Flex Scale capabilities described in Section 2.5, including erasure coding and options for duplicating or replicating the *Images*, 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*.<br>● To satisfy this requirement for other essential data related to how and when the *Images* were created, formatted, or modified, the regulated entity must retain this data in a compliant manner. | ***Section 2.5 Duplicate Copy of the Records Stored Separately***<br>*Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required* |
| (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). | N/A |
| **(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:<br>(1) *Inspection*. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.<br>(2) *Production of **paper** regulatory records*. ***<br>(3) *Production of **electronic** regulatory records*.<br>(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.<br>(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.<br>*(4) Production of **original** regulatory records.* *** | It is Cohasset's opinion that NetBackup Flex Scale has features that support the regulated entity's efforts to comply with requests for inspection or production of *Images* and associated Index (i.e., metadata attributes).<br>Specifically, it is Cohasset's opinion that Section 2.4, *Capacity to Download Indexes and Records*, describes use of NetBackup Flex Scale to retrieve and download the *Images* and the metadata retained by NetBackup Flex Scale. As noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the *Images* and associated metadata, in the form and medium requested.<br>If the regulator requests additional data related to how and when the *Images* were created, formatted, or modified, the regulated entity will need to provide this information from appropriate source systems | ***Section 2.4 Capacity to Download Indexes and Records***<br>*Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member* |

[9] 17 CFR § 1.31(a) includes indices (*Any data necessary to access, search, or display any such books and records*) in the definition of regulatory records.

# 4 | Conclusions

Cohasset assessed the capabilities of NetBackup Flex Scale, version 3.0, with *Compliance Mode Controls*, in comparison to the five requirements related to the recording and the non-rewriteable, non-erasable storage of electronic records, as set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. (See Section 1.3, *NetBackup Flex Scale Overview and Assessment Scope*.)

Cohasset determined that NetBackup Flex Scale, when properly configured, has the following capabilities, which meet the regulatory requirements:

- Immutably maintains *Images* and associated system metadata for time-based retention periods.
- Prohibits deletion of an *Image* and its immutable system metadata until the *WORM Retention Period* for the *Image* has expired.
- Permits *WORM Retention Periods* to be extended, as needed, to retain records for regulatory compliance or to satisfy a legal hold.
- Verifies the accuracy and quality of the recording process through cryptographic hash values and NetBackup Flex Scale validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- Uniquely serializes each *Image* and all duplicate copies with a *Backup ID* (including date/time stamp) and a Copy Number.
- Records *Image*s utilizing erasure coding to provide high durability of *Image*s. Additionally, provides the ability to asynchronously record a duplicate of each *Image* to a separate storage device, which allows for the recovery of *Images* that may become lost or damaged. Additionally, supports geographically dispersed, asynchronous replication of *Images*.
- Provides the capacity and tools to (a) search for *Images*, (b) list the *Images*, and (c) download the *Images* and associated metadata attributes for a local tool to render as a human-readable *Image*.

Cohasset also correlated the assessed capabilities of NetBackup Flex Scale, with *Compliance Mode Controls,* to the principles-based electronic records requirements in CFTC Rule 1.31(c)-(d).

Accordingly, Cohasset concludes that NetBackup Flex Scale, when properly configured and utilized to retain time-based records, meets the five requirements of SEC Rule 17a-4(f) and FINRA Rule 4511(c), which relate to the recording and non-rewriteable, non-erasable storage of electronic records. In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d).

# 5 | Overview of Relevant Regulatory 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 allowing electronic records to be retained on a variety of compliant electronic storage media.*

## 5.1 Overview of SEC Rule 17a-4(f) Electronic Records Storage Requirements

Recordkeeping requirements for the securities broker-dealer industry are stipulated by the United States Securities and Exchange Commission (SEC) Regulations, including 17 CFR §§ 240.17a-3 and 240.17a-4. Specifically, SEC Rule 17a-4(f), when adopted on February 12, 1997, expressly allow books and records to be retained on electronic storage media, subject to meeting certain conditions.

Three separate foundational documents collectively define and interpret the specific regulatory requirements that must be met for an electronic storage system to be compliant with SEC Rule 17a-4(f). These are:

- The Rule itself, as modified over time by the SEC. These modifications to the original Rule have not affected the requirements for electronic storage media, which are the basis of this assessment. However, certain Interpretive Releases have clarified the context and meaning of certain requirements and conditions of the Rule.
- SEC Interpretive Release No. 34-44238, Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with Respect to Rule 17a-4(f), dated May 1, 2001 (the 2001 Interpretive Release).
- SEC Interpretive Release No. 34-47806, Electronic Storage of Broker-Dealer Records, dated May 7, 2003 (the 2003 Interpretive Release).

In the Rule and in the two subsequent interpretative releases, the SEC authorizes the use of electronic storage media and devices to satisfy the recordkeeping requirements of SEC Rules 17a-3 and 17a-4, when the system delivers the prescribed functionality. Specifically, SEC Rule 17a-4(f)(1)(ii) states:

> *(f) The records required to be maintained and preserved pursuant to §§ 240.17a-3 and 240.17a-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form.*
> *(1) For purposes of this section:*
> *(ii) The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(1)(i) and (f)(1)(ii) of this section, that <u>meets the applicable conditions set forth in this paragraph (f)</u>.* [emphasis added]

The February 12, 1997, Federal Register issued the final rule allowing broker-dealers to use electronic storage media. When issuing the rule, the SEC recognized that technology evolves; and, it set forth standards that the electronic storage media must satisfy, rather than prescribing specific technology, as specified in the following excerpts:

> ***SUMMARY:*** *The Securities and Exchange Commission (''Commission'') is amending its broker-dealer record preservation rule to allow broker-dealers to employ, under certain conditions, electronic storage media to maintain records required to be retained. The amendments reflect a recognition of technological developments that will provide economic as well as time-saving advantages for broker-dealers by expanding the scope of recordkeeping options while at the same time continuing to require broker-dealers to maintain records in a manner that preserves their integrity. The Commission is also issuing an interpretation of its record preservation rule relating to the treatment of electronically generated communications.*
> ***
> ***II. Description of Rule Amendments***
> ***A. Scope of Permissible Electronic***
> ***Storage Media***
> ****The Commission is adopting a rule today which, instead of specifying the type of storage technology that may be used, sets forth standards that the electronic storage media must satisfy to be considered an acceptable method of storage under Rule 17a–4. Specifically, because optical tape, CD–ROM, and certain other methods of electronic storage are available in WORM and can provide the same safeguards against data manipulation and erasure that optical disk provides, the final rule clarifies that broker-dealers may employ any electronic storage media that meets the conditions set forth in the final rule.*[10] [emphasis added]

The 2003 Interpretive Release further clarifies that implementation of rewriteable and erasable media, such as magnetic tape or magnetic disk, meets the requirements of a non-rewriteable, non-erasable recording environment, if the system delivers the prescribed functionality and appropriate **integrated control codes** are in place. The 2003 Interpretive Release states:

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

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

Examples of *integrated control codes* relevant to a non-rewriteable, non-erasable recording process are:

- A retention period during which the record cannot be erased, overwritten or otherwise modified;
- A unique record identifier that differentiates each record from all other records; and
- The date and time of recording, which in combination with the unique identifier “serializes” the record.

[10] Exchange Act Release No. 38245 (Feb. 5, 1997), 62 FR 6469 (Feb. 12, 1997) ("Adopting Release").

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

Further, the 2003 Interpretive Release requires the storage system to be capable of retaining records beyond the SEC-established retention period, when required by a subpoena, legal hold or other similar circumstances. In *Section IV. Discussion*, the 2003 Interpretive Release states:

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, 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.* [emphasis added]

An important associated requirement of SEC Rule 17a-4(f)(2)(i) is that a member, broker or dealer electing to electronically store its records required by SEC Rules 17a-3 or 17a-4, must notify its designated examining authority at least ninety (90) days prior to employing any technology other than write-once read-many (WORM) optical media. Examining authorities are self-regulatory organizations (SROs) or designated examining authorities (DEAs) under the jurisdiction of the SEC, such as the Financial Industry Regulatory Authority (FINRA).

**Important Note**: In the December 1, 2021, Federal Register[11], the SEC issued proposed changes to Rule 17a-4 which would both (a) provide an audit-trail alternative and (b) allow broker-dealers to continue using the electronic recordkeeping systems they currently employ to meet the non-erasable, non-rewritable (a.k.a. WORM or write-once, read-many) requirement, as clarified in the May 7, 2003, Interpretive Release:

> **** the Commission is proposing amendments to Rules 17a-4(f) and 18a-6(e) that would provide firms with the option of using electronic recordkeeping systems that meet either the audit-trail requirement or the WORM requirement. Moreover, as discussed above, the Rule 17a-4(f) Interpretation, which is extant, clarifies that Rule 17a-4(f) does not mandate the use of optical disk to meet the WORM requirement.* [emphasis added]
> *****
> *Under the proposed amendments, broker-dealers could potentially continue to use the electronic recordkeeping systems they currently employ to meet the WORM requirement. ***** Moreover, some broker-dealers may choose to use their existing WORM-compliant electronic recordkeeping systems rather than adopt a new technology. Further, some broker-dealers may choose to retain existing electronic records on a legacy WORM-compliant electronic recordkeeping system, including software-based systems that are designed to follow the Rule 17a-4(f) Interpretation rather than transfer them to an electronic recordkeeping system that would meet the proposed audit-trail requirement. However, these firms could decide to preserve new records on an electronic recordkeeping system that would meet the proposed audit-trail requirement.*

These proposed updates also remove the requirement to submit a 90-day letter to the DEA. The comment period for the proposed changes closed on January 3, 2022, and a final Rule has **not** yet been promulgated.

[11] Exchange Act Release No. Release No. 34-93614; File No. S7-19-2 (Nov. 18, 2021), 86 FR 68300-01 (Dec. 1, 2021) ("Proposed rule").

See Section 2, *Assessment of Compliance with SEC Rule 17a-4(f),* for a list of the five SEC requirements relevant to the recording and non-rewriteable, non-erasable storage of electronic records and a description of the capabilities of NetBackup Flex Scale related to each requirement.

## 5.2 Overview of FINRA Rule 4511(c) Electronic Records Storage Requirements

Financial Industry Regulatory Authority (FINRA) Rule 4511(c) explicitly defers to SEC Rule 17a-4(f), by stipulating:

> *(c) 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.*

## 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 define principles-based requirements for organizations electing to retain electronic regulatory records. The CFTC requirements for electronic regulatory records evolved through amendments to Rule 1.31. The most substantive changes included:

- The June 28, 1999, amendment first implemented the technical provisions regarding the use of electronic storage media for required books and records.
- The November 2, 2012, amendment clarified the retention period for certain oral communications.
- The August 28, 2017, amendments modernize and make technology-neutral the form and manner in which regulatory records, including electronic regulatory records, must be retained and produced.

To address the transition to electronic regulatory records, the CFTC amended and modernized its recordkeeping regulation to adopt principles-based standards that are less prescriptive. This resulted in rephrasing and modernizing the requirements previously defined in 1999, as explained in the August 28, 2017, Federal Register in *III. Final Rules, D. Regulation 1.31(c): Form and Manner of Retention*:

> *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. The Commission proposed to adopt § 1.31(d)(2) to set forth additional controls for records entities retaining electronic regulatory records. The Commission emphasized in the Proposal that the proposed regulatory text does not create new requirements, but rather updates the existing requirements so that they are set out in a way that appropriately reflects technological advancements and changes to recordkeeping methods since the prior amendments of § 1.31 in 1999.* [emphasis added]

The definitions established in 17 CFR § 1.31(a) are paramount to applying the CFTC requirements.

> *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]

These definitions establish that recordkeeping obligations apply to (a) all *records entities*, without exception, and (b) 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.

The retention time periods for regulated records includes both time-based and event-time-based retention periods. Specifically, 17 CFR § 1.31(b)(1)-(b)(3) 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.* [emphasis added]

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

# About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is recognized as a leading professional consulting firm, specializing in records management and information governance. Drawing on more than forty 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, engaging in implementation activities to promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

Cohasset has been described as *the only management consulting firm in its field with its feet in the trenches and its eye on the horizon*. 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.

***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 assists with the implementation of information lifecycle practices that avoid the cost and risk associated with over-retention*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*

**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.