Cohasset Associates

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

Veeam Backup & Replication

Abstract

Veeam® Backup & Replication™, version 11.0, is a comprehensive, enterprise-grade data protection and disaster recovery solution that protects a wide variety of workloads located on premises or in the cloud. The *Hardened Repository* feature is designed to meet securities industry requirements for preserving backup files in non-rewriteable, non-erasable format until the specified retention period has expired.

In this Report, Cohasset Associates, Inc. (Cohasset) assesses the capabilities of Veeam Backup & Replication (see Section 1.3, *Veeam Backup & Replication Overview and Assessment Scope*) relative to:

- The recording and non-rewriteable, non-erasable storage requirements for electronic records, as specified by:
  - 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).
- The principles-based electronic records requirements of the Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset's opinion that Veeam Backup & Replication, version 11.0, when properly configured, meets the five requirements related to the recording and non-rewriteable, non-erasable storage of electronic records in SEC Rule 17a-4(f) and FINRA Rule 4511(c). Additionally, the assessed capabilities of Veeam Backup & Replication meet the principles-based requirements of CFTC Rule 1.31(c)-(d).

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.

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 Veeam Backup & Replication 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 *Immutable Backup File* (versus *record*, *data*, or *file*) 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 Veeam Backup & Replication. 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 Veeam Backup & Replication, Veeam engaged Cohasset Associates, Inc. (Cohasset). As a highly-respected consulting firm, Cohasset has recognized expertise and more than 40 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.

Veeam engaged Cohasset to:

- Assess the capabilities of Veeam Backup & Replication in comparison to the five requirements of SEC Rule 17a-4(f) for the recording and non-rewriteable, non-erasable storage 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 Veeam Backup & Replication; 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 Veeam Backup & Replication and its capabilities or other Veeam 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 Veeam 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 Veeam Backup & Replication Overview and Assessment Scope

Veeam Backup & Replication, version 11.0, is a comprehensive, enterprise-grade data protection and disaster recovery solution that protects a wide variety of workloads located on premises or in the public cloud. When properly configured to utilize the *Hardened Repository* feature, Veeam Backup & Replication captures and retains backups of source workloads. Leveraging native capabilities of the Linux operating system, the immutability attribute is set for each backup file (hereinafter referred to as an *Immutable Backup File*), which assures the contents of the file and its associated metadata will be retained as non-rewriteable, non-erasable until expiration of an applied *Immutable Until Date*. Key components of the Veeam Backup & Replication architecture are depicted in figure 1, below.

Backup Server is the central management system used to define and retain backup configurations, schedules, and rules for retention and immutability in the Backup Configuration Database.

Backup Proxy or Veeam Agent interfaces between the Backup Server and other components of Veeam infrastructure, responsible for processing jobs and delivering backup traffic from source systems.

Hardened Repository Server is a Linux-based server, with the *Hardened Repository* feature enabled, used to retain *Immutable Backup File*s within a file system. An unlimited number of hardened repositories, in combination with normal repositories, may be connected to a Backup Server, to accommodate different retention needs.

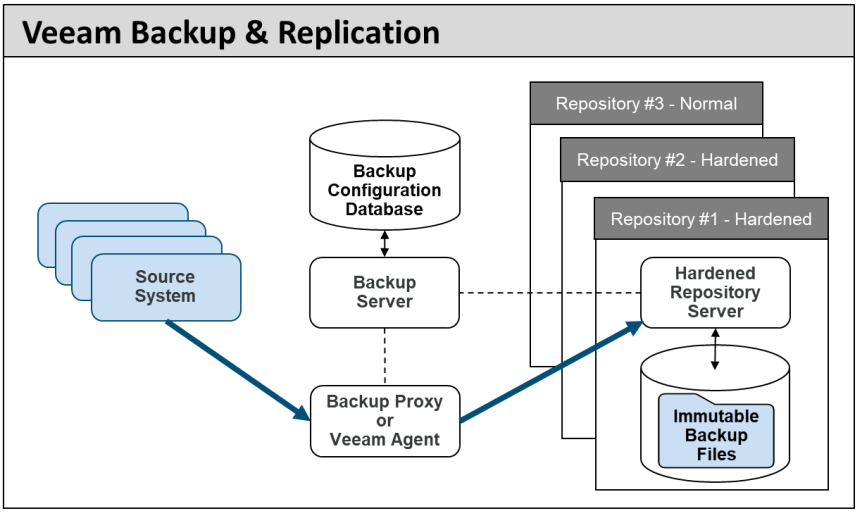

Figure 1: Veeam Architecture

The scope of this assessment is focused specifically on the compliance-related capabilities of Veeam Backup & Replication software, version 11.0, when used to backup VMware, Hyper-V, and agent-based Windows and Linux workloads, and deployed as follows:

- *Hardened Repositories* - deployed on (a) industry standard server hardware that meets or exceeds Veeam's minimum system requirements and (b) running a Veeam-qualified **Linux** 64-bit operating system with a filesystem (XFS is recommended) that supports the use of both extended attributes and chattr.
- All remaining Veeam Backup & Replication components - deployed on (a) industry standard hardware that meets or exceeds Veeam's minimum system requirements and (b) running Veeam-qualified, commercially available operating systems. *Note: Linux is required for the Hardened Repository but is not required for any other component.*

This assessment excludes (a) workload types not listed above, and (b) other Veeam products that are not part of Veeam Backup & Replication.

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

This section presents Cohasset's assessment of the capabilities of Veeam Backup & Replication for compliance with the five requirements related to the 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 Veeam Backup & Replication
- ***Veeam Backup & Replication 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 Veeam Backup & Replication, as described in Section 1.3, *Veeam Backup & Replication 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 Veeam Backup & Replication, with the *Hardened Repository* feature, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for time-based[3] 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 Veeam Backup & Replication Capabilities

This section describes the capabilities of Veeam Backup & Replication that directly pertain to this SEC requirement for preserving electronic records as non-rewriteable, non-erasable for the required retention period and any extended retention periods required to satisfy legal holds. In this report, Cohasset uses the term *Immutable Backup File* when referring to backup files stored with configurations required for compliance with SEC Rule 17a-4(f).

2.1.3.1 *Overview*

- To meet the requirements of SEC Rule 17a-4(f), a backup file requiring time-based retention must be stored, via a Backup Job, in a *Hardened Repository,* which ensures that (a) the *Immutability* attribute is set and (b) an appropriate retention period, i.e., *Immutable Until Date,* is applied to the backup file. These configurations establish the following stringent integrated controls:
  - The immutability attribute cannot be removed from the *Immutable Backup File*.
  - An *Immutable Backup File* and associated metadata cannot be modified, overwritten or deleted by any Veeam user, or system administrator until the applied *Immutable Until Date* has expired.
  - The *Immutable Until Date* applied to the *Immutable Backup File* cannot be shortened, only extended. For example, when litigation or a subpoena requires an *Immutable Backup File* to be preserved for a longer period, the *Immutable Until Date* can be extended for the duration of the hold.

[3] Time-based retention periods require records to be retained for a specified contiguous period of time from the date and time created and stored.

2.1.3.2 *Repository and Backup Job Configurations*

- Veeam Backup & Replication generates two types of backup files, with different methods of setting the *Immutable Until Date*.

  1. Recent Backups are a series of full and incremental backups that make up the current chain of restore points for a workload. The *Immutable Retention Period (*up to 9,999 days) configured for the ***Hardened Repository*** is used to calculate the *Immutable Until Date,* which is applied to Recent Backups during the storage process.
  2. GFS Backups are optional, long-term Grandfather-Father-Son backups which may be captured weekly, monthly and/or yearly. The *GFS Retention Period* (up to 999 years) is defined as part of the **Backup Job** configuration, with separate retention durations set for weekly, monthly and/or yearly GFS Backups. The longer of the *GFS Retention Period* and the *Immutable Retention Period* is used to calculate the *Immutable Until Date, which is applied to* GFS Backups during the storage process.

Repository and **Backup Job** configurations, as described in the following table, are required to generate *Immutable Backup Files* for compliance with Rule 17a-4(f):

1. Repository Configuration	A repository that is intended to retain *Immutable Backup Files* for compliance with SEC 17a-4(f) must be configured to utilize the *Hardened Repository* feature, as follows: ● A Linux-based server must be added to the Veeam Backup & Replication system as a hardened, managed server and assigned the repository role. (See *Section 2.1.3.7, Security,* for more information regarding repository hardening.) ◆ A *Hardened Repository* must be configured as a standalone backup repository. Scale-Out-Repositories (i.e., a logical grouping of multiple repositories, used to extend or tier stored backup files) are not compliant with the Rule. ● It is recommended that the name and description attributes for the repository include the word "immutable," when the *Hardened Repository* feature is enabled. ● The 'Make recent backups immutable for x days' option must be enabled for the repository and the number of days (up to a maximum of 9,999 days) must be set. The specified days represent the *Immutable Retention Period* which is used to calculate the *Immutable Until Date* for the following types of backups, during the storage process: ◆ Recent Backups, including scheduled and ad hoc backups, and ◆ GFS Backups, when the *Immutable Retention Period* is longer than the *GFS Retention Period*, as described in the following row.

2. Backup Job Configuration	Backup Jobs are a predefined set of rules and schedules, configured on the Backup Server to manage individual or recurring backups. To generate *Immutable Backup File*s for compliance with Rule 17a-4(f), one or more Backup Jobs must be configured as follows: ● Specify a supported source workload to be backed up (refer to Section 1.3, *Veeam Backup & Replication Overview and Assessment Scope* for a list of workloads that are supported by the *Hardened Repository* feature). Note: If an unsupported workload is specified, it will be backed up according to the Backup Job, however, the backup files will not be immutably retained and no error message will be generated. ● Select a *Hardened Repository* that will serve as the target storage location for the *Immutable Backup File*s. The *Hardened Repository* must have sufficient space allocated to accommodate storage of the source workloads. Note: If space is inadequate, the backup file will not be stored. ● Select one of the two backup methods supported by the *Hardened Repository*: (1) forward incremental with active full backup or (2) forward incremental with synthetic full backup. ● If GFS Backups are to be retained, define the *GFS Retention Period* (up to 999 years). The *GFS Retention Period* is used to calculate the *Immutable Until Date* for GFS Backups, when it is longer than the *Immutable Retention Period*. ● A *Retention Policy* must be configured for the Backup Job which specifies either (a) the number of restore points or (b) the number of days (i.e., all restore points created in the last N days) to be maintained, thereby establishing the Recent Backup chain. The *Retention Policy* is used by automated post-retention disposition services only and does not control the immutable retention of backup files. ◆ As described above, in *1. Repository Configuration*, the *Immutable Retention Period* configured for the *Hardened Repository* is designed for compliance with the Rule and sets the immutable retention duration for Recent Backups. ◆ The *Retention Policy* specified in the Backup Job must be equal to or longer than the *Immutable Retention Period* set for the *Hardened Repository*. If the *Retention Policy* is less than the *Immutable Retention Period* set for the *Hardened Repository*, informational messages will result when (a) the *Retention Policy* has expired and (b) Veeam Backup & Replication attempts to automatically delete a Recent Backup that is protected by a longer *Immutable Retention Period*. ● The *Configure Secondary Destinations for this Job* setting must be selected, which links the Backup Job to an appropriately configured Backup Copy Job, assuring a duplicate backup file is automatically generated upon completion of each primary backup (refer to Section 2.5.3, *Duplicate Copy of Records Stored Separately*, for more details regarding the configuration of Backup Copy Jobs).

2.1.3.3 *Backup Files and Retention Controls*

- Source workloads are retrieved according to Backup Jobs defined in the Backup Server. Source workloads to be backed up are then transported to the *Hardened Repository* by the Veeam Transport Service.
- An *Immutable Backup File* in Veeam Backup & Replication includes the content as well as critical metadata, such as source system name and ID, backup completion timestamp, the immutability flag, and checksums.
- Immutable retention controls are applied to the backup file when the source workload is successfully backed up to the target *Hardened Repository*.
  - Veeam Backup & Replication leverages native capabilities of Linux to set the immutability attribute for each *Immutable Backup File*, which assures the *backup file,* including its associated metadata, are retained as non-rewriteable, non-erasable until the assigned *Immutable Until Date* has expired.
  - The *Immutable Until Date* is calculated for each *Immutable Backup File* by adding the applicable *Immutable Retention Period* or *GFS Retention Period* to the backup completion timestamp. The *Hardened Repository* stores the applied *Immutable Until Date* in two locations:
    - The *Immutable Until Date* (user.immutable.until) for the backup file is immutably stored as an extended attribute in the file system.
    - The *Immutable Until Date* (ImmutableTillUtc) for the backup file is stored in an XML .lock file. This date can be changed, as long as it is equal to or greater than the *Immutable Until Date* (user.immutable.until) date described above. Accordingly, the date stored in the XML .lock file may be used to extend retention for purposes of legal holds. (See Section 2.1.3.4, *Legal Holds (Temporary Holds),* below, for more detail.)
- The *Immutable Retention Period* configured for the *Hardened Repository* and the *GFS Retention Period* configured for a Backup Job, may be modified at any time (i.e., extended or shortened), however, the changed values only apply to new backups generated in the future.
  - Note: All backups that are part of a Recent Backup chain (i.e., the initial full backup plus daily incrementals that are performed prior to the next full backup) must share the same *Immutable Retention Period*. Therefore, if the *Immutable Retention Period* is **extended** prior to the next full backup, the new *Immutable Retention Period* will apply retroactively to any existing (dependent) incrementals within the active chain.
- An *Immutable Backup File* may be **copied** from a *Hardened Repository*, via a Backup Copy Job, to a different repository. The duplicate backup file is stored on the target repository *without* the retention controls of the primary *Immutable Backup File*.
  - If the target repository is a *Hardened Repository*, the immutable attribute is set for the duplicate backup file. An *Immutable Until Date* is calculated and applied, based on the copy completion timestamp and:
    - For duplicate **Recent Backups**, the *Immutable Retention Period* of the target *Hardened Repository*.
    - For duplicate **GFS Backups**, the longer of the *GFS Retention Period*, as configured in the Backup Copy Job, or the *Immutable Retention Period* for the target *Hardened Repository*.
- An *Immutable Backup File* may not be **moved** once it is stored in a *Hardened Repository*.

2.1.3.4 *Legal Holds (Temporary Holds)*

When litigation or a subpoena requires *Immutable Backup File*s to be placed on hold, which could entail retaining them beyond their assigned *Immutable Until Date*, the regulated entity must ensure the subject backup files are protected for the duration of the legal hold.

- Authorized users must identify the backup files (and any duplicate copies) that are subject to the hold and via PowerShell commands, extend the ImmutableTillUtc attributes in the XML .lock file to a future date. If the duration of the hold is unknown, the ImmutableTillUtc attribute may continue to be extended as many times as necessary.

2.1.3.5 *Deletion Controls*

- To be eligible for deletion, both *Immutable Until Dates* (user.immutable.until and ImmutableTillUtc) for the *Immutable Backup File* must be in the past.
- Disposition or deletion of eligible *Immutable Backup File*s may be initiated manually by authorized users or automatically by post-retention deletion jobs running on the repository.
- Privileged delete is not allowed for a *Hardened Repository*. Accordingly, attempts by the system administrator to delete an *Immutable Backup File* prior to the expiration of both *Immutable Until Dates* is prohibited.
- A *Hardened Repository* that contains *Immutable Backup File*s can be removed from the Veeam Backup & Replication Configuration Database, however, the *Immutable Backup File*s remain intact on the *Hardened Repository*.
    - The *Hardened Repository* may be re-added to the Configuration Database, however, the *Immutable Backup File*s it contains will appear as orphaned files that are no longer managed by Veeam Backup & Replication. The original *Immutable Until Dates* are stored permanently for the *Immutable Backup File*s and no manual or automated disposition is allowed.

2.1.3.6 *Clock Management*

- To protect against the possibility of premature deletion of backup files that could result from accelerating the system time clock, the Linux operating system of every Veeam *Hardened Repository* must be configured to synchronize with a secure time source, e.g., a secure internal network time protocol (NTP) clock. Once configured and synchronized, the time of the *Hardened Repository* clock should be regularly, e.g., every 5 minutes, checked against the secure time source and resynchronized as required. This constant synchronization prevents, or immediately corrects, any inadvertent or intentional administrative modifications to a time clock that could result in the premature deletion of backup files.

2.1.3.7 *Security*

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

- The Linux-based repository, used to immutably store backup files, is a hardened minimal installation, such that:
    - Only two services are allowed to run on the *Hardened Repository* server:

  - **Veeam Transport Service** – receives the backup data and instructs the Veeam Immureposvc Service to set the *Immutable Until Dates*.
  - **Veeam Immureposvc Service** – sets the immutable flag for the backup files, monitors the *Immutable Until Dates* and removes the immutable flag once expired.
- When no backups or restores are running, only one port is open on the *Hardened Repository* to allow the Veeam Transport Service to communicate with other Veeam components. Certificate based authentication is established between the Backup Server and the Veeam Transport Service. The Veeam Transport Service opens additional ports, temporarily, to allow data to be received from the Proxy servers during backup and restore processes.
- Secure Shell (SSH) access is deactivated for the repository and no root passwords are required for normal operations.

- Roles Based Access Controls (RBAC) are utilized to define permissions for accessing retention and repository settings.
- Encryption of backup files is available as follows:
  - As part of a Backup Job, Veeam Backup & Replication can use 256-bit AES block cypher encryption.
  - Data in transit may also be encrypted via 256-bit AES encryption.

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 Veeam Backup & Replication (version 11.0) as described in Section 1.3, *Veeam Backup & Replication Overview and Assessment Scope*.
- Appropriately configuring the *Hardened Repository* feature on repositories that will store books and records required by regulation and enabling the 'Make recent backups immutable' with a retention period that meets regulatory requirements for Recent Backups, thereby establishing the foundation for meeting the requirements of the Rule.
- Ensuring all workloads required to be retained for compliance with the SEC Rule are uploaded to a properly configured *Hardened Repository*; Cohasset recommends uploading within 24 hours of creation or storing in an SEC-compliant protected storage system until they are uploaded to a Veeam *Hardened Repository*.
- Applying immutable retention controls to backup files requiring compliant retention by:
  - Establishing Backup Jobs that utilize *Hardened Repositories* to store backup files and
  - Setting appropriate *GFS Retention Periods* for GFS Backups.
- Extending the retention duration of backup files (and duplicate backup files) via PowerShell command, when the backup files must be kept longer than the applied *Immutable Until Dates,* to effectuate a legal hold for subpoenas, litigation, government investigations, external audits and other similar circumstances. If the

anticipated duration of a hold is unknown, care must be taken to extend retention in smaller increments to avoid over-retention, since *Immutable Until Dates* cannot be shortened.

- Ensuring proper separation of duties by assigning management of *Hardened Repositories* to a user other than the Backup Administrator.
- Establishing clear policies to prevent the deletion of *Hardened Repositories* until all *Immutable Backup Files* are past their applied *Immutable Until Dates*.
- Storing backup files requiring event-based retention in a separate compliance system, since Veeam Backup & Replication does not natively support event-based retention.
- Synchronizing the Linux operating system time of all *Hardened Repositories* with an external time source to prevent tampering that could result in the premature deletion of backup files.

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 Veeam Backup & Replication, in conjunction with the inherent capabilities of advanced magnetic storage technology, meet this SEC requirement for accurate recording and post-recording verification, when the considerations described in Section 2.2.4 are addressed.

2.2.3 Veeam Backup & Replication Capabilities

The recording and the post-recording verification processes for Veeam Backup & Replication 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 assure that the backup files are written in a high-quality and accurate manner.
- During the recording process, the source workload is divided into blocks of data. A checksum is computed by the Backup Proxy or Veeam Agent for each block, validated by the *Hardened Repository*, and recorded as metadata inside the backup file, for use in post recording validation processes. Once the entire source workload is successfully written to the *Hardened Repository*, the immutable flag is set for the backup file.

- A single Backup Job may encompass multiple source machines. For example, if a Backup Job attempts to backup ten virtual machines, but only nine are successful, those nine will be written to the *Hardened Repository* and flagged as immutable. The system will automatically attempt to capture the remaining virtual machine (i.e., the system defaults to three retries) but if unsuccessful, no portion of the failed virtual machine will be written to the *Hardened Repository*. Error messages will be issued and the Backup Administrator must take corrective action.

2.2.3.2 *Post-Recording Verification*

- When configured, Veeam Backup & Replication performs regularly scheduled storage level health checks. The system recalculates the checksum for each block of data and compares it to checksums stored with the backup file. Should an error be detected, the Backup Administrator is notified and must replace the corrupted block from a duplicate copy. Note: Auto heal functionality is currently not available for *Hardened Repositories*.
- During the restore process, Veeam recalculates the checksum for each block of data and compares it to the checksum stored as part of the backup file. If the checksum values do not match, the restore fails and must be reattempted from a duplicate copy.

2.2.4 Additional Considerations

Cohasset recommends that the regulated entity configure Veeam Backup & Replication to regularly perform storage level health checks and assure procedures are established for Backup Administrators to monitor backups to resolve any errors and assure completion.

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 Veeam Backup & Replication meet this SEC requirement to serialize the original and duplicate records.

2.3.3 Veeam Backup & Replication Capabilities

- Each backup file is assigned a unique file name, which consists of the source system name and ID, the backup completion timestamp, and a unique hexadecimal value. The combination of these elements serializes the backup file in both space and time.
- The file name is recorded as part of the system metadata and protected from modification for the duration of the *Immutable Until Dates* (user.immutable.until and ImmutableTillUtc) associated with the backup file.

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 Veeam Backup & Replication meets this SEC requirement to readily download records and indexes (metadata attributes) when the considerations described in Section 2.4.4 are addressed.

2.4.3 Veeam Backup & Replication Capabilities

The following capabilities support the capacity to download backup files and index (metadata attributes):

- The Veeam Backup Console provides the ability to search by file name, within Veeam backup files. Selected backup files and their metadata may be restored, resulting in the contents of those backup files being made available to view online or copy to a new location.
- The Extract Utility, available on Linux and Microsoft Windows machines and accessible via graphical user interface (GUI) or command line interface (CLI), maintains an index of all backup files and provides the ability to:
  - List all machines included in a backup.
  - Independently (i.e., without any interaction with Veeam Backup & Replication) restore the contents from a single machine, or all machines contained within the backup file, to a target location.
- If the 'enable guest file system indexing' option is configured for a Backup Job, a catalog (i.e., advanced index) of guest files is created, which provides advanced search capabilities against all restore points for a selected machine backup:

- Search options include location, last modified time, backup time, file owner, type, and size.

- PowerShell commands may be utilized to list all backup files stored on a *Hardened Repository* and export selected backup files to a target location.
- Veeam ONE, a separate licensed product, provides the ability to list all backup files stored on a *Hardened Repository*. One or more files can then be selected for export to a local system.
- Once retrieved, content of backup files 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 backup files and indexes (metadata attributes), (b) maintaining its Veeam licenses in good standing, (c) maintaining its encryption keys, and (d) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the backup files 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 the capabilities of Veeam Backup & Replication meet this SEC requirement for a persistent duplicate copy of the *Immutable Backup Files*, when properly configured, as described in Section 2.5.3, when the considerations described in Section 2.5.4 are addressed.

2.5.3 Veeam Backup & Replication Capabilities

Veeam Backup & Replication provides the ability to maintain a persistent duplicate copy of each *Immutable Backup File* as follows:

- The *Configure Secondary Destinations for this Job* setting, available on the Backup Job storage screen, must be selected which links the Backup Job to a Backup Copy Job, assuring a duplicate backup file is automatically generated upon completion of each primary backup.

- A Backup Copy Job must be configured (a) to utilize the Immediate Copy (Mirroring) option and (b) with GFS backup settings (i.e., *GFS Retention Periods*) that are *exactly the same as those configured for the primary Backup Job*.

- The immutable flag and *Immutable Until Date* attributes are not copied as part of the duplication process. Therefore, for compliance with the Rule:
  - The target repository must be a *Hardened Repository*, configured with the same *Immutable Retention Period* as the primary *Hardened Repository*.
  - An *Immutable Until Date* is calculated and applied to the duplicate backup file, based on the copy completion timestamp and:
    - For duplicate **Recent Backups**, the *Immutable Retention Period* for the target *Hardened Repository*.
    - For duplicate **GFS Backups**, the longer of the *GFS Retention Period*, as configured in the Backup Copy Job, or the *Immutable Retention Period* for the target *Hardened Repository*.

    Note: the *Immutable Until Date* applied to the duplicate *Immutable Backup File* will never be shorter than that of the primary *Immutable Backup File*.

- The unique file name of the duplicate *Immutable Backup File* is comprised of the same source system name and ID as the primary *Immutable Backup File*, combined with the copy completion timestamp and a unique 4-digit hexadecimal number.
- If a legal hold is placed on an original *Immutable Backup File,* it must be manually applied to the duplicate *Immutable Backup File,* as well.
- Post-retention disposition of duplicate *Immutable Backup Files* may be initiated manually by authorized users.
- The contents of the duplicate *Immutable Backup File* are an exact replica of the primary. Restoration of the *Immutable Backup File* from a duplicate can be accomplished manually by the Backup Administrator.

2.5.4 Additional Considerations

- The regulated entity is responsible for (a) properly configuring Backup Jobs to automatically generate a duplicate of each *Immutable Backup File,* (b) ensuring the target repository is configured identical to the primary *Hardened Repository*, and (c) extending the *Immutable Until Date* for the source and duplicate *Immutable Backup Files,* when a legal hold applies.
- Cohasset recommends that the target repository be geographically separated from the primary repository.

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 Veeam Backup & Replication, as described in Section 1.3, *Veeam Backup & Replication 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 Veeam Backup & Replication 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 Veeam Backup & Replication, with the *Hardened Repository* feature, 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 retention period.

In the following table, Cohasset correlates the capabilities of Veeam Backup & Replication, with the *Hardened Repository* feature, to the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*.

The left-hand column lists the *principles-based* CFTC requirements. The middle column provides Cohasset's analysis and opinion regarding the ability of Veeam Backup & Replication 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: (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 Veeam Backup & Replication capabilities, utilized with the *Hardened Repository* feature as described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for *Immutable Backup Files*. Additionally, for *records stored electronically*, the CFTC has expanded the definition of *regulatory records* in 17 CFR § 1.31(a) to include metadata: *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] It is Cohasset's opinion that Veeam Backup & Replication retains immutable metadata attributes (e.g., Source Name and ID, backup completion date/time and *Immutable Until Date*), as an integral part of the backup file. The *Immutable Backup File* attributes are subject to the same retention protections as the *Immutable Backup File* contents. To satisfy this requirement for other essential data related to how and when the content of the backup files 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*** *Preserve the records exclusively in a non-rewriteable, non-erasable format* **Section 2.2 *Accurate Recording Process*** *Verify automatically the quality and accuracy of the storage media recording process* **Section 2.3 Serialize the Original and Duplicate Units of Storage Media** *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* ***Section 2.4 Capacity to Download Indexes and Records*** *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[4] 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 Veeam Backup & Replication capabilities described Section 2.5, including options to duplicate the *Immutable Backup Files* 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*. To satisfy this requirement for other essential data that is not retained in Veeam Backup & Replication (such as separate indices), the regulated entity must retain this other data in a compliant manner.	***Section 2.5 Duplicate Copy of the Records Stored Separately*** *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: (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 Veeam Backup & Replication has features that support the regulated entity's efforts to comply with requests for inspection or production of *Immutable Backup Files* and associated metadata. ● Specifically, it is Cohasset's opinion that Section 2.4, *Capacity to Download Indexes and Records*, describes use of Veeam Backup & Replication to retrieve and download the *Immutable Backup Files* and associated metadata retained by Veeam Backup & Replication. As noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the *Immutable Backup File* and associated metadata, in the form and medium requested. ● If the regulator requests additional data related to how and when the content of the *Immutable Backup Files* was 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*** *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*

[4] 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 Veeam Backup & Replication, version 11.0, with the *Hardened Repository* feature, in comparison to the five requirements related to the recording and 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, *Veeam Backup & Replication Overview and Assessment Scope*.)

Cohasset determined that Veeam Backup & Replication, when properly configured, has the following capabilities, which meet the regulatory requirements:

- Maintains backup files and associated metadata in non-rewriteable, non-erasable format for time-based retention periods.
- Allows for the extension of the *Immutable Until Date* to effectuate a legal hold, when the backup file must be kept longer for subpoenas, litigation, government investigations, external audits and other similar circumstances.
- Prohibits deletion of an *Immutable Backup File* and associated metadata until its *Immutable Until Date* has expired.
- Verifies the accuracy and quality of the recording process through the use of checksums and Veeam Backup & Replication validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- Uniquely serializes each *Immutable Backup File* and all duplicate copies with a unique file name, including source system name and ID, backup completion date/time, and a 4-byte unique hexadecimal value.
- Provides the ability to asynchronously write a duplicate of each *Immutable Backup File* to a separate *Hardened Repository*, which allows for the recovery of *Immutable Backup Files* that may become lost or damaged.
- Provides the capacity and tools to (a) search for *Immutable Backup Files*, (b) list the *Immutable Backup Files*, and (c) download the *Immutable Backup Files* and associated metadata attributes for a local tool to render as a human-readable image.

Cohasset also correlated the assessed capabilities of Veeam Backup & Replication, with the *Hardened Repository* feature, to the principles-based electronic records requirements in CFTC Rule 1.31(c)-(d).

Accordingly, Cohasset concludes that Veeam Backup & Replication, 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 meets the applicable conditions set forth in this paragraph (f).* [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.*[5] [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.

[5] 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).

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 Veeam Backup & Replication 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 Veeam Backup & Replication 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.