Cohasset Associates

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

NetApp StorageGRID

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.

NetApp® StorageGRID®, version 11.5, is a software-defined, scalable, object storage solution that provides intelligent policy-driven data management. The StorageGRID *S3 Object Lock* feature, based on the Amazon Simple Storage Service (S3) protocol, is designed to meet securities industry requirements for preserving record objects in a non-rewriteable, non-erasable format. StorageGRID, with *S3 Object Lock* enabled, applies integrated control codes to prevent stored objects from being modified, overwritten, or deleted until the specified retention period has expired and any legal holds have been released.

In this Assessment Report, Cohasset Associates, Inc. (Cohasset) assesses the capabilities of StorageGRID (see Section 1.3, *StorageGRID 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 regulation 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset's opinion that the capabilities of StorageGRID, version 11.5, 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 StorageGRID 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 NetApp StorageGRID 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 *record object* (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 StorageGRID. 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 StorageGRID, NetApp 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.

NetApp engaged Cohasset to:

- Assess the capabilities of StorageGRID, with the *S3 Object Lock* feature, 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 StorageGRID; 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 StorageGRID and its capabilities or other NetApp 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 documentation, and (d) other directly-related materials provided by NetApp 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 StorageGRID Overview and Assessment Scope

NetApp® StorageGRID®, version 11.5, is a software-defined, scalable object storage solution that provides intelligent policy-driven data management. The StorageGRID *S3 Object Lock* feature, based on the Amazon Simple Storage Service (S3) protocol for *Object Lock* in *Compliance* mode, is designed to meet securities industry requirements for preserving record objects in a non-rewriteable, non-erasable format until the specified retention period has expired and any legal holds have been released. At the time this report was prepared, StorageGRID exclusively offers the *Compliance* mode setting for *S3 Object Lock*. Therefore, throughout this report, references to *S3 Object Lock* refer to *S3 Object Lock* in *Compliance* mode.

The logical architecture of StorageGRID is depicted in Figure 1 and summarized as follows:

- A StorageGRID system must have the system-wide **S3 Object Lock** setting enabled to make the *S3 Object Lock* feature available.
- **Tenants** provide authorized access to the storage environment by client applications, using either Amazon S3 REST application programming interface (APIs) or Swift REST APIs. Tenants may be used to segregate the storage environments for a business entity (e.g., different departments within an organization). *For compliance with SEC Rule 17a-4(f), a Tenant must be configured for use with Amazon S3 REST APIs (hereafter referred to as a StorageGRID S3 Tenant).*

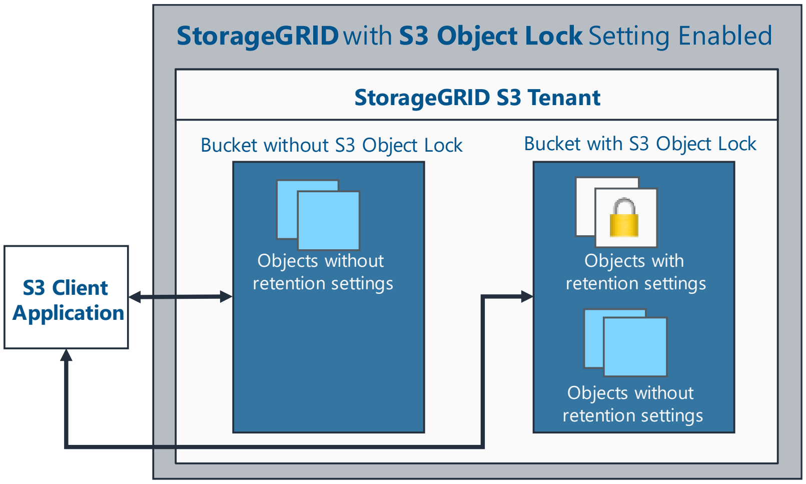
StorageGRID with S3 Object Lock Setting Enabled
StorageGRID S3 Tenant
Bucket without S3 Object Lock
Bucket with S3 Object Lock
Objects without retention settings
Objects with retention settings
Objects without retention settings
S3 Client Application

Figure 1: StorageGRID Logical Architecture

- Within a StorageGRID S3 Tenant, ***S3 Object Lock Buckets*** (i.e., S3 Buckets created with the *S3 Object Lock* feature enabled) are used to retain record objects and their associated system and custom metadata. Stringent retention protection and object management controls are employed to meet the requirements of SEC Rule 17a-4(f).

The scope of this assessment is focused specifically on the compliance-related capabilities of StorageGRID, version 11.5, operating under the following configurations and deployments:

- The S3 Object Lock setting is enabled at the StorageGRID system level, thereby allowing *S3 Object Lock Buckets* to be created within StorageGRID S3 Tenants.
- One of following three software/hardware environments is configured:
  - *NetApp StorageGRID appliances*: Fully integrated software and hardware storage solutions provided by NetApp as an enterprise-grade turnkey object storage appliance which provides fully integrated logical and physical storage management and administrative and user controls.

- *VMWare/vSphere*: StorageGRID operates as a virtual appliance in an environment managed by VMWare/vSphere. StorageGRID continues to manage all compliance-related administrative actions via grid[3] and tenant administrators. Record objects are protected in the same manner as the NetApp StorageGRID appliance, as storage volumes are exclusively allocated to StorageGRID.
- *NetApp-qualified open-source operating systems running on bare metal:* StorageGRID operates as a software application in an environment managed by a third-party open-source operating system. StorageGRID continues to manage all compliance-related administrative actions via grid and tenant administrators. Record objects are protected in the same manner as the NetApp StorageGRID appliance, as storage volumes are exclusively allocated to StorageGRID.

Throughout this assessment, the above-described operating environments of StorageGRID are being assessed. Note: In version 11.5 of StorageGRID, information lifecycle policies (ILM) used for tiering objects to external storage (e.g., cloud storage, tape) have automatic safeguards to prevent record objects stored in *S3 Object Lock Buckets* (with or without retention and/or legal hold settings) from being archived to external storage. However, this does not preclude the use of ILM-based tiering for other Buckets that do not have *S3 Object Lock* enabled.

[3] StorageGRID utilizes a grid architecture for the storage of objects. Copies of object data are distributed throughout the grid. If any part of the grid fails, another part immediately takes over, providing optimized durability and performance.

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

This section presents Cohasset's assessment of the capabilities of NetApp StorageGRID 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 StorageGRID
- ***StorageGRID 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 StorageGRID, with the *S3 Object Lock* feature, as described in Section 1.3, *StorageGRID 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 StorageGRID, with the *S3 Object Lock* feature, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for time-based[4] retention periods and any applied legal hold, 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 StorageGRID Capabilities

In this subsection, StorageGRID capabilities are assessed regarding their ability to meet the requirements of SEC Rule 17a-4(f) for preserving electronic records (record objects) as non-rewritable and non-erasable, for the required retention period and any associated legal hold time periods.

2.1.3.1 *Enabling Compliance*

To meet the requirements of SEC Rule 17a-4(f), the following three (3) baseline requirements must be met:

1. **Enabling the system-level S3 Object Lock setting**. This setting establishes an environment whereby the *S3 Object Lock* feature is made available for use.
    - Only an authorized Grid administrator can enable the S3 Object Lock setting.
    - StorageGRID utilizes metadata-driven information lifecycle management (ILM) policies to define and direct the execution of functions, such as replication, geo-distribution and data protection. Enabling the system-level S3 Object Lock setting is only allowed if the active Information Lifecycle (ILM) Policy has a default rule that satisfies the data protection requirement for managing record objects protected by the *S3 Object Lock* feature. (See Section 2.5, *Duplicate Copy of the Records Stored Separately*, for more

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

information on data protection ILM rules.) If a compliant data protection default rule does not exist, the attempt to enable the S3 Object Lock setting will be rejected.

- Once the system-level S3 Object Lock setting is enabled:
  - All StorageGRID S3 Tenants in the grid can utilize the *S3 Object Lock* feature. At the time of this report, StorageGRID offers only *S3 Object Lock* in *Compliance* mode. If other modes, such as Governance[5] mode, are subsequently available, these other modes have not been assessed for compliance with the Rule.
  - The S3 Object Lock setting cannot be disabled by the Grid administrator or by any other means.
  - The default rule for the ILM policy cannot be changed to a non-compliant rule.

2. **Creating a StorageGRID S3 Tenant**. Each StorageGRID system may have one or more tenant accounts, each with its own federated or local groups, users, and logical units of storage for record objects.
   - StorageGRID supports the use of Amazon S3 REST APIs and Swift REST APIs. However, for compliance with SEC Rule 17a-4(f), a tenant **must be configured to use Amazon S3 APIs**. Only this setting enables the use of *S3 Object Lock Buckets* for storing record objects.
   - StorageGRID S3 Tenants can be created by a Grid administrator before or after enabling the system-level S3 Object Lock setting.
   - A StorageGRID S3 Tenant cannot be deleted if *S3 Object Lock Buckets* exist within the Tenant.

3. **Creating *S3 Object Lock Buckets* with versioning enabled**. Buckets are logical units of storage for retaining record objects.
   - The *S3 Object Lock* feature must be enabled for any Bucket intended to store record objects in compliance with the Rule. When S3 Object Lock is enabled for a Bucket, StorageGRID automatically enables versioning. *Note: The* S3 Object Lock *setting can only be enabled for new Buckets during the creation process*.
   - The client application or user can create *S3 Object Lock Buckets*, with versioning enabled, using the StorageGRID Tenant Manager or S3 API. They can then store, retrieve and delete objects to/from the Bucket using S3 APIs.
   - Once the *S3 Object Lock Bucket* is created, neither its S3 Object Lock setting nor versioning can be disabled.
   - Both *S3 Object Lock Buckets* and non-compliance enabled Buckets can be configured for use within a single StorageGRID S3 Tenant.

[5] StorageGRID has been designed for compatibility with Amazon S3 APIs. For clarity, Amazon S3 offers both *Compliance* and *Governance* modes, though only *Compliance* Modes was designed for compliance with the SEC requirements.

2.1.3.2 *Record Objects and Retention*

- Record objects are comprised of the complete content of the object, as well as associated metadata. The term record object is defined as a ***version*** of an object.
  - *Immutable* metadata, which includes, but is not limited to: unique Bucket name, S3 Object Key, version identifier, creation/storage (ingest) timestamp and user-defined custom metadata.
  - *Mutable* metadata for a record object, which includes, but is not limited to: *Retain Until Date*, legal hold status and S3 object tags.
- Record objects are transmitted by the client application for storage in *S3 Object Lock Buckets* via S3 API commands and are protected when the client application explicitly transmits <u>both</u> (a) an *S3 Object Lock* mode of *Compliance* and (b) an appropriate *Retain Until Date.*
  - Integrated *S3 Object Lock* retention controls are applied to the specified version of the object only, to prevent the deletion of that version and its associated metadata, by any mechanism or user, until the assigned *Retain Until Date* has expired and any legal hold is released (see Section 2.1.3.3, Legal Holds for more information.)
  - New versions of the object may continue to be created and, when necessary, must have *S3 Object Lock* retention controls and/or legal holds applied separately.
  - Note: Object versions can never be modified or overwritten, whether or not they have an applied retention mode attribute and *Retain Until Date*.
- The retention period set for a record object can be extended, but it cannot be shortened. Any attempt to delete or shorten the retention period will be rejected.
- StorageGRID supports multipart uploads of record objects and enforces Amazon Web Services size limits for such operations. When the multipart upload operation completes:
  - *S3 Object Lock* attributes, if included as part of the Initiate Multipart Upload request, will be applied.
  - A new record object version identifier is assigned.
- A record object may be <u>copied</u> from an *S3 Object Lock Bucket* to another bucket, resulting in the creation of a new object with its own unique metadata. A *Retain Until Date* and *S3 Object Lock* retention mode can be assigned to the copy if the destination Bucket is an *S3 Object Lock Bucket*. The original record object and its metadata remains unaltered in the original *S3 Object Lock Bucket*.
- A record object cannot be <u>moved</u> between *S3 Object Lock Buckets*.

2.1.3.3 *Legal Hold*

- When litigation or a subpoena requires record objects to be placed on hold, which could entail retaining them beyond their assigned retention period, the regulated entity must ensure the subject record objects are protected for the duration of the hold. This is accomplished by setting a legal hold status attribute for each relevant object version, via S3 API.

  - The legal hold status is independent of the object's *Retain Until Date* and *S3 Object Lock* retention mode; therefore, a legal hold status may be applied to any object version in an *S3 Object Lock Bucket*, including objects with no applied *Retain Until Date* or *S3 Object Lock* retention mode.

- While the legal hold status is set for an object version:
  - Overwrite or deletion is prohibited,
  - Object tags may be modified, and
  - The *Retain Until Date* may be extended as necessary.
- When the legal hold status is cleared, this attribute no longer mandates preservation of the object version and retention control is returned to the applied *Retain Until Date*, if one exists.

2.1.3.4 *Deletion*

- A record object is eligible for deletion when (a) the *Retain Until Date* has expired and (b) any legal hold has been released.
  - When deleting a record object *without* also specifying the version identifier, a delete marker is added as the top-level version. The delete marker does not affect the stored versions of the record object (i.e., no versions are actually removed). Further, delete markers may be added and removed, as appropriate. See Section 2.4, *Capacity to Download Indexes and Records*, for information on the implications of delete markers on search and retrieval.
  - When deleting a record object by version identifier, *S3 Object Lock* protections apply, and only eligible versions are deleted. If the version is ineligible for deletion, an error message is communicated, and the deletion operation fails.
- S3 Lifecycle configuration rules may be set on *S3 Object Lock Buckets* to trigger automatic deletion of *eligible* record objects. Alternatively, deletion may be initiated manually by authorized users, including client applications. Deletion requests will be rejected if the record object is not eligible for deletion or the attempt is made by a user who does not have the required permission.
- An *S3 Object Lock Bucket* cannot be deleted if record objects are contained in the Bucket; and a StorageGRID S3 Tenant cannot be deleted if *S3 Object Lock Buckets* exists within the Tenant.

2.1.3.5 *Clock Management*

To protect against the possibility of premature deletion of record objects that could result from accelerating the system time clock, StorageGRID ensures that: (a) a minimum number and stratum of NTP sources are enforced, (b) tampering of NTP settings is disallowed, and (c) more than one NTP time sources are reachable and are consistent before setting the system clock on a node. Further, StorageGRID uses NTP version 4 daemon processes and algorithms to adjust system clock time and frequency on a continued basis.

2.1.3.6 *Security*

The StorageGRID system provides the following security capabilities to protect against unauthorized users or sources compromising the retention of stored record objects:

- Root login over SSH (Secure_Shell) is disabled on all Grid nodes.
- Internal public key infrastructure and node certificates are used to authenticate and encrypt internode communications. Internode communication is secured by TLS (Transport Layer Security).
- Separate networks are available for Client, Admin and internal Grid traffic.
- The base operating system of StorageGRID appliances and virtual nodes is hardened; unrelated software packages are removed.
- Object data can be encrypted using server-side encryption with customer-provided encryption keys (SSE-C) as defined by Amazon S3 REST APIs.
- StorageGRID supports data encryption on disk using external key managers that support the Key Management Interoperability Protocol (KMIP).

2.1.4 Additional Considerations

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

- Appropriately assigning permissions required to manage record objects.
- Configuring an active ILM policy to ensure that two duplicate copies or one erasure-encoded copy is created for each record object, in order for the system-wide S3 Object Lock setting to be enabled on a StorageGRID system.
- Enabling the system-wide S3 Object Lock setting, thereby allowing the use of the *S3 Object Lock* feature.
- Creating *S3 Object Lock Buckets* to be used for compliant storage of record objects.
- Ensuring all record objects that are required to be retained for compliance with the SEC Rule are uploaded to a properly configured *S3 Object Lock Bucket* with (a) the *S3 Object Lock* retention mode set to *Compliance* and (b) an appropriate *Retain Until Date*. Cohasset recommends that record objects be protected within twenty-four hours of creation.
- Applying legal holds to record objects that require preservation for legal matters, government investigation, external audits and other similar circumstances, and removing legal holds when preservation is no longer required.
- Limiting the creation and management of delete markers. Specifically, Cohasset recommends always specifying the version identifier in delete requests.
- Establishing appropriate security policies and procedures.

- Storing record objects requiring event-based[6] retention periods in a separate compliance system, since StorageGRID does _not_ currently support event-based retention periods.

When StorageGRID, with S3 Object Lock settings enabled, is configured as a software-only deployment under the operational control of VMWare/VSphere or a NetApp-qualified third-party, open-source operating system, it is Cohasset's opinion that the logical storage controls and physical storage units must be configured such that they are exclusive to and accessible only through StorageGRID. No third party or external source should be able to access, administer, delete, overwrite or modify record object content and metadata, or in any way compromise the StorageGRID compliance protection and retention management settings.

2.2 Accurate Recording Process

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

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.

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

2.2.2 Compliance Assessment

Cohasset affirms that the capabilities of StorageGRID, 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 StorageGRID Capabilities

The recording and the post-recording verification processes of StorageGRID are described below.

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 records are written in a high-quality and accurate manner.
- The StorageGRID integrated appliance deployment provides inherent technology that validates data during each recording step from the storage controller to physical disk storage.
- StorageGRID calculates a hash digest of the record object and stores it in the metadata for use in post recording verification. The hash digest is returned to the client application for optional verification of recording accuracy.

[6] Event-based or event-time-based retention periods require the record object to be retained indefinitely until a specified event occurs (e.g., a contract expires or an employee terminates), after which the record object must be retained for a fixed final retention period.

2.2.3.2 *Post-Recording Verification Process*

- During read-back of the record object, methods inherent in advanced magnetic disk technology perform error detection and automatically correct most in-error data. Should an uncorrectable error occur at the magnetic storage level, the record object is automatically recovered from the duplicate copy or, in the case of an erasure-coded copy, from the erasure-coded segments that are not in error.
- The hash digest calculated and stored for each record object in the StorageGRID metadata is utilized for post-recording verification during read-back.
- StorageGRID also continuously checks all storage nodes to determine if there are corrupt copies of replicated and erasure coded object data. If problems are found, the StorageGRID system automatically attempts to replace the corrupt object data through erasure coding recovery processes or from copies stored elsewhere in the system.

2.2.4 Additional Considerations

As a means of verifying accuracy of the recording process, Cohasset recommends that the regulated entity calculate a hash digest prior to sending a record object to StorageGRID and compare it to the hash digest calculated and returned by StorageGRID, after a successful write operation.

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 StorageGRID meets this SEC requirement to serialize the original and duplicate records.

2.3.3 StorageGRID Capabilities

- Each record object is serialized in Buckets using a combination of: (a) a unique Object Name (which includes Bucket name and S3 Object Key) and (b) a version identifier. These attributes are immutable.
  - The Bucket name must be unique within the StorageGRID system.

  - The object name (S3 Object Key) must be unique within the Bucket.
  - The unique version identifier is generated automatically.
- The creation/storage timestamp (i.e., the ingest timestamp) is system-defined, immutable, and stored with each record object.
- This combination of Object Name, version identifier, and creation/storage timestamp serializes each record object in both space and time.

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 StorageGRID meet 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 StorageGRID Capabilities

The StorageGRID capabilities that support the capacity to locate and download record objects and metadata include:

- Authorized users can list all or a subset of record objects contained in a Bucket via the following S3 APIs:
  - ListObject - returns a list of the record objects, by S3 Object Key; if the top-level version is a delete marker the record object is not returned in the list.
  - ListObjectVersions - returns a list of record objects by S3 Object Key, along with all versions associated with each, even when a delete marker is the top-level version.
  - GetObject – returns the record object:
    - When the request includes the version identifier, the specific record object version is returned.
    - When no version identifier is specified, the top-level version is returned, unless the top-level version is a delete marker, in which case an error code is returned.

- Utilizing version-specific or purpose-specific S3 GET APIs, *S3 Object Lock* attributes such as *S3 Object Lock* retention mode, *Retain Until Date*, and legal hold status, can be retrieved for individual record objects.
- Using S3 APIs or the command line interface (CLI), selected record objects and the associated metadata (index) attributes may be downloaded to a designated storage location. Then, using local capabilities, the listed record objects can be selected and transferred to a medium acceptable under the Rule.
- When multiple versions of a record are stored, the top-level version is returned, by default. The specific version identifier must be specified in the search and download requests.

2.4.4 Additional Considerations

The regulated entity is responsible for authorizing user access, maintaining StorageGRID S3 Object Lock settings, and assuring that the SEC, CFTC, self-regulatory organization or designated examining authority receive downloads of the record objects and metadata (index) attributes, in the requested form 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 asserts that StorageGRID meets this SEC requirement for a persistent duplicate copy of the record objects, 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 StorageGRID Capabilities

- StorageGRID uses Information Lifecycle Management (ILM) policies to determine how many copies of data are recorded and managed. A precondition when configuring StorageGRID for managing *S3 Object Lock Buckets* is that the default rule in the active ILM policy must reflect the equivalent of storing a duplicate copy of each record object (a list of ILM rules can be requested which will indicate the compliant rules). If this precondition is not met, the attempt to configure the system to use the S3 Object Lock setting will fail. The two options for configuring the default rule in the ILM policy are:
  - Specifying that at least two copies of each record object will be stored in different, potentially geographically separate, storage nodes, or

  - Specifying that each record object will be stored as an erasure-coded copy, that is typically divided into three or more segments which are recorded across different, potentially geographically separate, storage nodes, from which a complete and accurate copy of the record object can be accurately regenerated if one or more of the segments is in error.

- Three copies of the metadata for each record object are automatically stored, managed separately from record content and protected as non-erasable and non-rewriteable, for the same retention period.

2.5.4 Additional Considerations

The regulated entity must ensure that the StorageGRID system is configured with a compliant ILM rule, as outlined above.

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 StorageGRID, as described in Section 1.3, *StorageGRID 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 StorageGRID 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 StorageGRID with the *S3 Object Lock* feature in *Compliance* mode, 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 StorageGRID, with the *S3 Object Lock* 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 StorageGRID 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 StorageGRID capabilities, utilized with the *S3 Object Lock* feature in *Compliance* mode, as described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for record objects. 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 StorageGRID, with the *S3 Object Lock* feature, retains the immutable metadata (index attributes) as an integral part of the record object. These index attributes are subject to the same retention protections as the associated record object. Immutable record object metadata includes the unique Bucket name, S3 Object Key, version identifier, creation/storage (ingest) timestamp and user-defined custom metadata. Additionally, for mutable (changeable) metadata attributes, the most recent values are retained for the same time period as the associated record object. To satisfy this requirement for other essential data related to how and when the record objects 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[7] 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 the capabilities of StorageGRID, with the *S3 Object Lock* feature, as described in Section 2.5, *Duplicate Copy of the Records Stored Separately*, 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*. Specifically, section 2.5 explains that durability of StorageGRID system is achieved by using duplicate or erasure coded copies of record objects and three copies of metadata stored separately. To satisfy this requirement for other essential data related to how and when the record objects 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*** *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

[7] 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.

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
(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 StorageGRID, with the *S3 Object Lock* feature, has features that support the regulated entity's efforts to comply with requests for inspection or production of record objects and associated system metadata (i.e., index attributes). Specifically, it is Cohasset's opinion that Section 2.4, *Capacity to Download Indexes and Records*, describes use of StorageGRID to list and download the record objects and the associated metadata retained in *S3 Object Lock Buckets*. Further, as noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the record objects and associated metadata, in the form and medium requested. If the regulator requests additional data related to how and when the record objects were created, formatted, or modified, the regulated entity will need to provide this information from appropriate client applications.	***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 | Conclusions

Cohasset assessed the capabilities of StorageGRID, version 11.5, with the *S3 Object Lock* feature, in *Compliance* mode, 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, *StorageGRID Overview and Assessment Scope*.)

Cohasset determined that StorageGRID, with the *S3 Object Lock* feature, in *Compliance* mode, has the following capabilities, which meet the regulatory requirements:

- Maintains record objects and immutable record object metadata in a non-erasable and non-rewriteable format for time-based retention periods.
- Prohibits deletion of a record object and its immutable metadata until the associated time-based retention period has expired.
- Preserves record objects and associated metadata as immutable and prohibits deletion or overwrites, while a legal hold attribute is applied.
- Verifies the accuracy and quality of the recording process by: (a) utilizing advanced storage recording technology, (b) calculating and storing a hash digest of each record object and returning the hash digest to the client application for optional verification, and (c) utilizing the hash digest as part of a continuous integrity checking process that includes, as required, recovery of in-error objects.
- Uniquely identifies and chronologically serializes each stored record object.
- Provides administrators, users and client applications the ability to list identifying metadata for all record objects stored in an *S3 Object Lock Bucket* via S3 APIs; then to select one or more record objects for copying or downloading to a storage medium compliant with the Rule or to a local storage area for viewing or reproduction.
- Automatically stores two duplicate copies or one erasure-coded copy of each record object – defined as part of a mandatory, compliant ILM policy – to ensure recovery of record objects that are found to be in error at the time of retrieval or during a continuous integrity checking process. Additionally, stores and protects three copies of each record object's metadata.

Accordingly, Cohasset concludes that StorageGRID, with the *S3 Object Lock* feature, in *Compliance* mode, when properly configured and utilized to store and 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 records and metadata (index) attributes. In addition, Cohasset asserts that 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.*[8] [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.

[8] 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 StorageGRID 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 NetApp StorageGRID 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.