Cohasset Associates

SEC 17a-4(f) and FINRA 4511(c)
Compliance Assessment
Scality RING

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.

Scality RING is software defined native file and object storage solution for large scale on-premises storage and management of unstructured information. The Scality RING environment runs on industry standard hardware and is designed for compatibility with the Amazon Simple Storage Service (S3) protocol. The Scality RING *Object Lock* feature is designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format, when record objects are stored with the *Object Lock* mode set to *Compliance*.

In this Report, Cohasset Associates, Inc. (Cohasset) assesses the capabilities of Scality RING (see Section 1.3, *RING 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).

It is Cohasset's opinion that Scality RING, release 8.3 and Scality S3 Connector, release 7.8, when properly configured, and when *Object Lock* mode is set to *Compliance*, retains records in compliance with the recording and non-rewriteable, non-erasable storage of electronic records of SEC Rule 17a-4(f).

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-dealers 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 Scality RING 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 4.1, 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. Further, in this report *record object* pertains to each version of a record object, since Versioning must be enabled and each version has independently managed retention values.

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

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of RING, Scality 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. Additional information about Cohasset is provided in the last section of this report.

Scality engaged Cohasset to:

- Assess the capabilities of Scality RING 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);*
- 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 Scality RING and its capabilities or other Scality 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 Scality or obtained from publicly available resources.

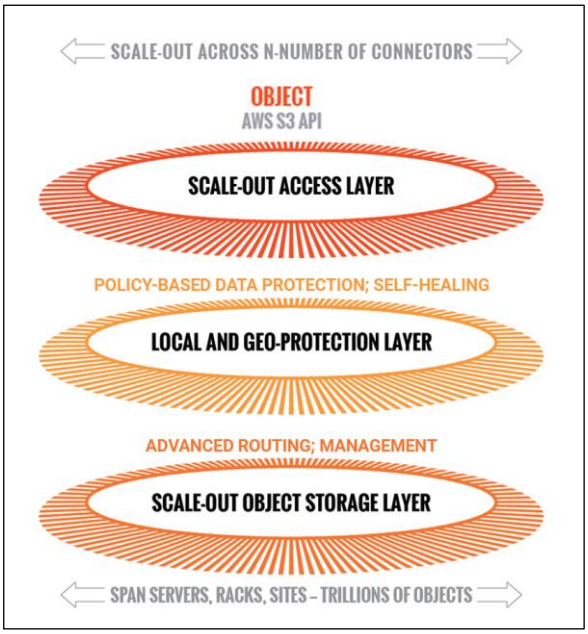
The content and conclusions of this assessment are not intended, and must not be construed, as legal advice. Relevant laws and regulations constantly evolve, and legal advice is tailored to the specific circumstances of the organization. Therefore, nothing stated herein should be substituted for the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

1.3 RING Overview and Assessment Scope

Scality RING is software defined object storage solution for large scale on-premises storage and management of unstructured information. The Scality RING environment runs on industry standard hardware and is designed for compatibility with the Amazon Simple Storage Service (S3) protocol.

The RING architecture (illustrated in the diagram) consists of the following components:

- **Connectors** natively support S3 APIs (application programming interfaces).
- ***Scale-Out Access Layer*** includes scalable access services (connectors) that provide storage protocols for applications.
- ***Local and Geo-Protection Layer*** provides a set of data protection mechanisms for data durability and integrity, self-healing processes and system management and monitoring services.
- ***Scale-Out Object Storage Layer*** is a scalable, distributed object key/value store based on second generation peer-to-peer routing protocol.



Scality designed the RING *Object Lock* feature for compliance with SEC Rule 17a-4(f) and other similar regulatory requirements. Two *Object Lock* modes are available:

1. ***Compliance* mode**: Storing records objects with the *Object Lock* feature set to *Compliance* mode, complies with the non-rewriteable and non-erasable requirements of the Rule by applying retention protections which cannot be removed from the record object.
2. ***Governance* mode**: Storing records objects with the *Object Lock* feature set to *Governance* mode, does not comply with the non-rewriteable and non-erasable requirements of the Rule, since users with appropriate permissions may remove (bypass) the applied retention protections.

The scope of this assessment is focused specifically on the compliance-related capabilities of Scality RING, operating under the following conditions and configuration:

- RING Release 8.3, on-premises
- Scality S3 Connector release 7.8 or later
- Running on Scality qualified hardware

The following section documents Cohasset's assessment of Scality RING, relative to the pertinent requirements in SEC Rule 17a-4(f). Throughout this report, the above-described operating environment of Scality RING will be assessed.

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

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

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

- ***Compliance Requirement*** – Excerpt of each electronic storage requirement in SEC Rule 17a-4(f) and Cohasset's interpretation of the requirement
- ***Compliance Assessment*** – Assessment of the relevant capabilities of RING
- ***RING 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 RING, as described in Section 1.3, *RING 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 the features of Scality RING, with *Object Lock* set to *Compliance* mode, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for time-based[3] retention periods and any applied legal holds, 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 RING Capabilities

This section describes the capabilities of Scality RING that directly pertain to this SEC requirement for preserving electronic records as non-rewriteable, non-erasable for the required retention period and any associated legal holds.

2.1.3.1 *Overview*

Scality RING, when deployed as described in Section 1.3, allows regulated entities to preserve record objects in a non-rewriteable, non-erasable format for the specified retention period and any applied legal holds. Scality RING, with the *Object Lock* feature *enabled* and *Object Lock* mode set to *Compliance*, achieves compliance with SEC Rule 17a-4(f) as follows:

- A Bucket that is intended to store regulated record objects must have the *Object Lock* feature enabled (i.e., an *Object Lock Bucket*) and, optionally, default retention settings defined (i.e., retention mode of *Compliance* and a *default retention period*, e.g., 6 years).
- For each record object stored in an *Object Lock Bucket*, (a) an appropriate *Retain Until Date* must be applied and (b) the *Object Lock* mode must be set to *Compliance*. This protects the record object from modification, overwrite, and deletion until the *Retain Until Date* has expired. The retention attributes (*Retain Until Date* and *Object Lock* mode) may be set either:
  - Explicitly by the source application, or
  - Inherited from the *Object Lock Bucket* default setting, wherein the *Retain Until Date* is calculated by adding the *default retention period* to the record object storage date.

[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.

- A legal hold may be placed on a record object to protect against modification, overwrite, and deletion until the legal hold is released. Once the legal hold is released, immutability and retention are governed by the record object's *Retain Until Date* and *Object Lock* mode setting.
- Each version of an object is an independent record object; accordingly, the *Retain Until Date*, *Object Lock* mode, and *legal hold* status, must be applied to each version, as needed for compliance.
- With the above configurations and settings, RING applies stringent integrated controls that protect record objects and associated immutable metadata as follows:
  - The record object, and its immutable metadata, cannot be modified, overwritten or deleted by any mechanism or user, including the root user, until both (a) the applied *Retain Until Date* has expired and (b) any legal hold has been released.
  - The *Object Lock* mode cannot be modified or removed from the record object.
  - The *Retain Until Date* cannot be shortened or removed, only extended, as needed.
  - The *Object Lock* feature cannot be disabled for the Bucket.

2.1.3.2 *Bucket Configuration*

- For each RING Bucket that will retain record objects required to comply with SEC Rule 17a-4(f), the *Object Lock* feature and *Versioning* must be *enabled*, when the Bucket is created. Once the *Object Lock* feature and *Versioning* are enabled on a Bucket, the configurations cannot be suspended or disabled. For existing Buckets, without *Object Lock* enabled, *Object Lock* may be enabled on the Bucket using a migration tool, available in S3utils, provided by Scality.

  IMPORTANT NOTE: Objects written to the Bucket, before *Object Lock* was *enabled,* are not protected by *Object Lock* until an explicit *Retain Until Date* and *Compliance* mode is transmitted by the source application.
- Optionally, Bucket defaults may be set for *Object Lock* mode and *default retention period*, expressed exclusively in days or in years. When configuring Bucket defaults for compliance with the Rule, the *Object Lock* mode must be set to *Compliance* and the duration (*default retention period*), must meet regulatory requirements. Once configured, when an explicit *Retain Until Date* is not transmitted with the record object, these defaults automatically apply to each stored record object and metadata.
  - The *Default retention period* is added to the storage date to calculate the record object's *Retain Until Date*. (See section *Record Object Definition and Retention Controls*, for more information.)
  - The default *Object Lock* mode may be set to either *Compliance* or *Governance*.
    - IMPORTANT NOTE: The *Object Lock* mode must be set to *Compliance*, for record objects required to comply with SEC Rule 17a-4(f), which disallows any user, including the root user, from removing *Object Lock* or shortening or removing the *Retain Until Date*.
- Optionally, *Minimum and Maximum retention periods* (Min/Max range) may be configured, using conditional operators for Identity and Access Management (IAM) roles. For example, an IAM Role is defined and

permissioned to apply retention periods between [Minimum] and [Maximum] period. The IAM Role is applied to users (e.g., source applications) permissioned to store record objects in the Bucket.

- Since the *Minimum and Maximum retention periods* are set through IAM, each permissioned user of a Bucket may be bound by a different Min/Max range.
  - Authorized users may change the Min/Max range at any time. The updated Min/Max range applies day-forward and does not apply to previously stored record objects.

- When a record object is transmitted, if the *Retain Until Date* is outside the Min/Max range for the user, the record object will be rejected, and an error will be reported. Therefore, the Bucket *Default retention period* must be set between the Min/Max range to assure that record objects using the Bucket Default are not rejected during write.

2.1.3.3 *Record Object and Retention Controls*

- Each record object is comprised of:
  - Complete content of the record object.
  - Immutable metadata, which includes, but is not limited to, unique object *Key* name, version identifier (*VersionID*), creation/storage date (last modified date), object size, and user-defined custom metadata (key-value pairs).
  - Mutable Metadata, which includes *Retain Until Date, Object Lock* mode and *Legal Hold* status. Extending the *Retain Until Date* or transitioning a record object from *Governance* to *Compliance* mode does not create a new version of the record object. Additionally, the *Legal Hold* status may be enabled (On*)* or removed (Off), as needed, without creating a new version of the record object.

- The *Object Lock* mode can be set to one of two options (*Compliance* or *Governance*) for a given record object and metadata; **only** *Compliance* mode meets the requirements of SEC Rule 17a-4(f).

  1. *Object Lock* mode set to *Compliance,* assures the following retention controls:
     - The *Retain Until Date* may be extended to a future date but cannot be shortened or cleared by any user, including the root user.
     - The *Object Lock* mode set to *Compliance* on a record object cannot be changed to *Governance* or cleared (null) by any user, including the root user.
  2. *Object Lock* mode set to *Governance,* permits shortening or clearing the *Retain Until Date,* as well as clearing the *Object Lock* mode. As a result, *Governance* is disallowed for records required to comply with the Rule.

- Further, *Object Lock* mode may be *null (blank),* which does not apply any retention protections, therefore is disallowed for records required to comply with the Rule.

- Each version of a record object is independently managed, with a separately applied *Retain Until Date*, *Object Lock* mode, and *Legal Hold* status.

- Scality offers the two methods of applying a *Retain Until Date* and *Object Lock* mode of *Compliance* to the record object, required to comply with the regulation:
  1. The source application may transmit an explicit *Retain Until Date* (within any applicable Min/Max range) and *Object Lock* mode of *Compliance* with a record object, or
  2. Bucket defaults may be set with an *Object Lock* mode of *Compliance* and a *Default retention period*, which are applied to record objects that are transmitted without explicit retention values.
     - Cohasset recommends setting the Bucket *Default retention period* and default *Object Lock* mode of *Compliance* for Buckets used to store records required to comply with the Rule. This assures that retention controls are applied to all record objects stored in the Bucket. Otherwise, when Bucket defaults are not configured, a record object transmitted *without* explicit retention values will be stored without retention controls. Accordingly, these objects are not protected for compliance with the Rule.
- For record objects previously stored with its *Object Lock* mode set to *Compliance,* the *Retain Until Date* may be extended to a future date but cannot be shortened or cleared*,* by any user, including the root user.
- A record object may be copied between Buckets, resulting in the creation of a new copy with its own unique metadata. The copy does not retain the original record object's *Retain Until Date*, *Object Lock* mode or *Legal Hold* status, therefore the attributes need to be set via Bucket defaults or explicitly. The original record object and metadata will remain, unaltered, in the original Bucket.
- A record object cannot be moved between Buckets unless the record object is eligible for deletion. If the record object is eligible for deletion, the move results in deleting the record object version from the existing Bucket and creating a new record object in the new Bucket, with new metadata, including new *Key* name, version identifier, and creation/storage date.
- The following Scality RING features prevent modification, overwrite and deletion, until eligible.
  - The fundamental capabilities of *Object Lock* when enabled and set to *Compliance mode* immutably store record objects and key metadata.
  - The *Versioning* feature ensures record objects are not overwritten and a new version is created.
  - Each record object is protected from deletion, by users (including source applications), when either:
    - The *Retain Until Date* of the record object is a future date, or
    - The *Legal Hold* status of the record object is set (On).
- If the user attempts any of the following actions, the action is rejected:
  - Assign either (a) *Retain Until Date* or (b) *Object Lock* mode. These attributes are a pair (i.e. both must be specified, or both must be blank (null)).
  - Shorten or remove a record object's *Retain Until Date* when the *Object Lock* mode is set to *Compliance*.
  - Change the *Object Lock* mode from *Compliance* to *Governance* or from *Compliance* to blank (null).
  - Delete a record object, by *VersionID*, before the *Retain Until Date* has passed (expired).

2.1.3.4 *Legal Holds (Temporary Holds)*

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 legal hold.

- The *Legal Hold* status (On/Off) may be applied to any record object stored in a Bucket with the *Object Lock* feature *enabled* (On).
  - Each version of a record object includes a separate *Legal Hold* status attribute; therefore, the Legal Hold status must be set for each version, as needed for compliance.
  - The *Legal Hold* status is independent of the record object's *Retain Until Date* and *Object Lock* mode; therefore, a *Legal Hold* status may be applied to any record object in a Bucket with the *Object Lock* feature enabled (On), including record objects without a *Retain Until Date* and *Object Lock* mode.
  - When the *Legal Hold* status is enabled (*On)*, it prohibits deleting the record object until the *Legal Hold* status is cleared (Off). Accordingly, this feature may be used to preserve a record object for subpoena, litigation, regulatory investigation and other special circumstances.
  - When the *Legal Hold* status is cleared (Off), this attribute no longer mandates preservation of the record object; however other retention controls continue to apply to the record object.
- The *Legal Hold* status for a record object may be validated, with the S3 API, by issuing 'get-object-legal hold' command.

2.1.3.5 *Deletion Controls*

- The *Retain Until Date* and *Legal Hold* status determine if the record object version is eligible for deletion (eligibility for deletion does not cause automatic deletion). For a record object version to be eligible for deletion: (a) The *Legal Hold* status must be clear (Off) and (b) The *Retain Until Date* must have expired (must have passed).
  - When deleting a record object by version identifier, Compliance Lock protections apply, and only eligible versions are deleted. An error is logged, and the action is rejected if the user does not have the required permissions or the user attempts to delete a record object version when (a) the *Retain Until Date* has not passed or (b) the *Legal Hold* status is set (On).
  - When deleting a record object without also specifying the version identifier, a delete marker is added as the most recent version. The delete marker does not affect the stored versions of the record object. 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.
- The Scality Bucket cannot be closed or deleted, until the Bucket is empty.

2.1.3.6 *Clock Management*

- To meet the requirements of the Rule, Cohasset asserts that every system clock must synchronize to an external time server, e.g., a network time protocol (NTP) clock. During initial configuration, all RING servers are synced with NTP and all users and system administrators, except the root user, are restricted from modifying system time once the sync has occurred. These controls prevent or correct inadvertent administrative modifications of the system clock, which could allow for premature deletion of record objects.

2.1.3.7 *Security*

Scality provides the following security capabilities, in addition to the stringent retention protection and management controls described above, which support the authenticity and reliability of the record objects.

- Scality RING may be configured to protect data in-transit (data traveling to and from RING) using Hypertext transport-layer encryption (HTTPS) and Secure Sockets Layer (SSL).
- Scality offers Advanced Encryption Standard (AES-256) to encrypt objects and metadata while at rest.
- Role-Based Access Control (RBAC) provides the means to limit access to functionality for both administrators and users.

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:

- Appropriately assigning permissions required to manage the retention controls and properly configuring the Scality RING Buckets that will retain regulated records.
- Transmitting explicit retention controls (*Retain Until Date* and *Compliance* mode) for each record object that is required for regulatory compliance. Additionally, Cohasset recommends configuring an appropriate *Default retention period* and default *Object Lock* mode of *Compliance* for Buckets that will store record objects required for compliance with SEC Rule 17a-4(f). These defaults will assure that all record objects are stored with retention controls when explicit *Retain Until Dates* and *Object Lock* mode are not specified.
  - Optionally, the regulated entity may set *Minimum and Maximum retention periods* for a Bucket or an IAM role to validate the *Retain Until Date* applied to each record object. Note: if no explicit retention expiration date is sent with the object, the Bucket Default is used, even if it exceeds the Maximum based on the IAM role assigned to the user.
- Specifying the VersionID for all delete requests, which prevents delete markers from inhibiting searchability.
- Setting a *Legal Hold* status to On, when required, to preserve record objects for legal matters, government investigations, external audits and other similar circumstances, and setting the *Legal Hold* status to Off, when preservation is no longer required.
- Storing record objects requiring event-based retention periods in a separate compliance system, since Scality RING does not support event-based retention periods.

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 Scality RING, 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 RING Capabilities

Scality RING has a combination of recording and post-recording verification processes, which are described in the following subsections.

2.2.3.1 *Recording Process*

- A combination of checks and balances in the advanced magnetic recording technology (such as inter-component and inter-step cyclical redundancy checks (CRCs), as well as write-error detection and correction) are relied upon to assure that the records are written in a high-quality and accurate manner.
- An MD5 checksum must be transmitted with the record object. The record object will be stored only if the MD5 checksum value calculated by Scality RING matches the transmitted checksum. If the checksums do not match, an error is reported to the client, and the record object must be retransmitted.

2.2.3.2 *Post-Recording Verification Process*

- Integrity of the record object is validated during retrieval of a record object. Scality RING recalculates the hash value for the record object and compares it to the hash value stored at the time of recording.
- To validate continued data integrity, Scality RING regularly and frequently scans data at rest to verify that recalculated hash values match stored values. If a record object is corrupt, meaning the checksum value is invalid, an automatic recovery process is initiated to rebuild the chunk through erasure coding or through the restoration of the duplicate copy.

2.2.4 Additional Considerations

There are no additional considerations related to this requirement.

2.3 Serialize the Original and Duplicate Units of Storage Media

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

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

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."*

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 Scality RING meet this SEC requirement to serialize the original and duplicate records.

2.3.3 RING Capabilities

- Each record object is serialized in Scality RING Buckets using a combination of: (a) a unique object *Key* name and (b) *VersionID*. These attributes are immutable.
- The creation/storage date/time (last modified date/time) is system-defined, immutable, and stored with each record object.
- This combination of unique object *Key* name, *VersionID,* and creation/storage date 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)]

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

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.

2.4.2 Compliance Assessment

It is Cohasset's opinion that RING 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 RING Capabilities

Record objects and metadata (index) attributes may be downloaded using the S3 API. The following capabilities support the capacity to download record objects and metadata (index) attributes:

- Using the Scality RING S3 API, authorized users can:
  - List record objects in a Bucket (selection criteria may be defined to find and return a subset of the objects in a Bucket).
    - ListObject: Returns a list of the record objects, by S3 Object Key; if the most recent 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. If a delete marker is the most recent version of the record object, this criteria must be specified in the search.
  - 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 most recent version is returned, unless the most recent version is a delete marker, in which case an error code is returned.
  - Download selected record objects and the associated metadata (index) attributes to a designated storage location. 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.
- Alternatively, the RING S3 Browser may be used, by an authorized user, to filter record objects.
- For each of the above actions, based on user permissions, specific metadata will be returned, including object *Key* name, *VersionID,* creation/storage date/time, *Retain Until Date*, *Object Lock* mode, and *Legal Hold* status.

2.4.4 Additional Considerations

The regulated entity is responsible for (a) authorizing user permissions, (b) maintaining hardware and software to access Scality RING, (c) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the requested record objects and associated metadata (index) 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 current capabilities of Scality RING meet this SEC requirement for a persistent duplicate copy of the record objects, when properly configured, as described in Section 2.5.3.

2.5.3 RING Capabilities

There are three options for meeting the conditions of this requirement to separately store a duplicate copy:

Duplicate Using Erasure Coding

- Scality RING uses erasure coding (EC) to stores chunks of record objects distributed across the RING nodes, associated with its unique 160-bit key. In the event of a disk or node failure, the original record object can be regenerated from the EC chunks. The erasure coded chunks are retained for the full retention period and any applied legal holds.

Duplicate Using Geo-Replication (synchronous) or Cross Region Replication (asynchronous)

- Duplicate copies may be stored using the capabilities of Scality RING and S3 Connector to configure either geo-replication ("synchronous stretched" deployments) or asynchronous S3 Cross Region Replication (CRR).
  - Geo-replication is synchronous stretched deployments across sites within a Metro-Area Network. Geo-Replication is an active/active synchronous replication that may be deployed in either: 1) two-site stretched S3 with witness or 2) three site stretched S3.
  - S3 Cross Region Replication (CRR) asynchronously mirrors RING S3 Buckets from a primary to a secondary site.
    - When using CRR to meet this requirement of the Rule, (a) both the primary and secondary site Buckets must be configured in accordance with the Rule and (b) the retention controls (*Object Lock* mode, *Retain Until Date*, and *Legal Hold* status) must be identical for regulated record objects, across the sites. Refer to Section 2.1, *Non-Rewriteable, Non-Erasable Record Format*, for additional information.

- CRR may be configured in either of the following two levels of granularity:
  1. Site-Level (Echo), where every Bucket created on the primary site is automatically replicated to the secondary site, along with IAM accounts, and roles and policies, or
  2. Bucket-Level, where each Bucket with *Object Lock* enabled must be set-up for replication individually on both sites, and the necessary IAM accounts and policies must be created by the administrator.

2.5.4 Additional Considerations

When CRR uses the Bucket-Level configuration, the regulated entity is responsible for: (a) properly configuring the Bucket *Object Lock* and IAM policies, and (b) validating the retention controls applied to the records objects on the primary site and secondary site are identical.

3 | Conclusions

Cohasset assessed the capabilities of RING, release 8.3, and Scality S3 Connector, release 7.8, 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, *RING Overview and Assessment Scope*.)

Cohasset determined that RING, when properly configured to store record objects with *Object Lock* mode set to *Compliance*, has the following capabilities, which meet the regulatory requirements:

- Maintains record objects and immutable record object metadata in non-rewriteable, non-erasable format for time-based retention periods, when a *Retain Until Date* is applied and the *Object Lock* mode is set to *Compliance*.
- Preserves all record objects in the *Object Locked* Bucket as immutable and prohibits deletion or overwrites, while the *Legal Hold* status is applied.
- Prohibits deletion of a record object and its immutable metadata until the *Retain Until Date* for the record object has expired and the *Legal Hold* status is cleared (Off).
- Verifies the accuracy and quality of the recording process automatically utilizing (a) advanced storage recording technology and (b) an MD5 checksum that must be received from the source system. The MD5 checksum is stored as a metadata attribute and utilized for post-recording verification.
- Uniquely serializes each record object and all duplicate copies with a *Key* name, *VersionID* and creation (last modified) date/time stamp.
- Allows authorized users to list and search the record objects and metadata via the S3 API for download to a format and medium acceptable under the Rule.
- Regenerates an accurate replica of records and metadata (including index attributes) using erasure coding, should data be lost or damaged. Additionally, replication may be configured in either: (a) Geo-Replication (stretched deployment), which provides active/active synchronization of record objects and associated metadata across sites within a Metro-Area Network or (b) S3 Cross Region Replication (CRR) to asynchronously mirror RING S3 buckets from a primary site to a secondary site.

Accordingly, Cohasset concludes that RING, 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.

4 | 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.

4.1 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.*[4] [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.

[4] 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 RING related to each requirement.

4.2 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.*

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.