Cohasset Associates

SEC 17a-4(f), FINRA 4511(c), CFTC 1.31(c)-(d) and the MiFID II Delegated Regulation(72)(1)
Compliance Assessment

Oracle Zero Data Loss Recovery Appliance

Abstract

Oracle's Zero Data Loss Recovery Appliance (Recovery Appliance) is engineered to protect Oracle databases against catastrophic events such as business disruption and database cyber-attacks. The Recovery Appliance delivers cloud-ready scalability and may be configured to leverage the Oracle Cloud Infrastructure Object Storage service. This Assessment Report describes the compliance features and required configurations for the Recovery Appliance, designed to help meet securities industry requirements for preserving regulated electronic records.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the Recovery Appliance (see Section 1.3, *Recovery Appliance Overview and Assessment Scope*) relative to certain electronic storage requirements specified in the following regulations:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.
- Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation), Article 72(1).

It is Cohasset's opinion that the Recovery Appliance (release 21.1), when properly configured for compliance, as described in Section 2 of this Report, helps meet 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 the Recovery Appliance help meet the principles-based requirements of CFTC Rule 1.31(c)-(d) and the medium and retention of records requirements of the MiFID II Delegated Regulation(72)(1).

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

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

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

Table of Contents

1 | Introduction

Regulators, worldwide, 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 the Oracle Zero Data Loss Recovery Appliance (Recovery Appliance) 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 6.1, 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 backup* (versus *database* or *backup image*) 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 the Recovery Appliance. Additionally, refer to Section 6.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

1.1.4 The MiFID II Delegated Regulation(72)(1) Requirements

On January 3, 2018, *Directive 2014/65/EU*[3], Markets in Financial Instruments Directive II (MiFID II), became effective and established a definition of durable medium for recordkeeping to enable the client to store and access its information. As a supplement to MiFID II, the *Commission Delegated Regulation (EU) 2017/565*[4] *(the MiFID II Delegated Regulation),* Article 72(1), requires records to be *retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority* and specifies the recordkeeping conditions that must be met.

Refer to Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1),* which correlates these MiFID II requirements to the capabilities of the Recovery Appliance. Additionally, refer to Section 6.4, *Overview of the Medium* and *Retention of Records Requirements of MiFID II,* for background on these requirements.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of the Recovery Appliance for preserving regulated electronic records, Oracle engaged Cohasset Associates, Inc. (Cohasset). As a highly-respected consulting firm, Cohasset has recognized expertise and more than 50 years of experience with the legal, technical and operational issues associated with the records management practices of companies regulated by the SEC and CFTC. Additional information about Cohasset is provided in the last section of this report.

Oracle engaged Cohasset to:

- Assess the capabilities of the Recovery Appliance in comparison to the five[5] requirements of SEC Rule 17a-4(f) for the recording and non-rewriteable, non-erasable storage and retention of electronic records; see Section 2, *Assessment of Compliance with SEC Rule 17a-4(f);*

[3] *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments*.

[4] *Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive*.

[5] This assessment of the Recovery Appliance capabilities focuses on the five requirements of the Rule that Cohasset aligns with the storage subsystem; the remaining requirements pertain to compliance filings and capabilities that Cohasset asserts would reside with the source system (i.e.,the controlling application that utilizes the Oracle Recovery Appliance).

- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of the Recovery Appliance; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);*
- Associate the requirements of Article 72(1) of the MiFID II Delegated Regulation to the assessed capabilities of the Recovery Appliance; see Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1);* 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 the Recovery Appliance and its capabilities or other Oracle 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 Oracle 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 Recovery Appliance Overview and Assessment Scope

Oracle's Recovery Appliance (release 21.1) is a zero data loss, cloud-scale backup and recovery system, engineered to help protect Oracle databases against catastrophic events such as business disruption and database cyber-attacks. The Recovery Appliance continuously performs low-level management of block-level changes of the Oracle Database backup, thereby providing highly flexible database recovery options for the Oracle Database.

The Recovery Appliance, when properly configured for compliance as described in Section 2 of this Report, captures backups of protected Oracle databases and retains them on integrated storage within the Recovery Appliance and/or within Oracle Cloud Infrastructure (OCI) Object Storage buckets for long-term archival (i.e., tertiary storage). Protection Policies, along with optional Archival Backup APIs, define the rules for the immutable retention of record backups. Integrated controls are applied within the storage subsystem to retain record backups in compliance with the non-rewriteable, non-erasable storage reqirements of SEC Rule 17a-4(f).

The primary components of the Recovery Appliance environment are depicted in Figure 1 below. In addition, key terms are defined in the Oracle Zero Data Loss Recovery Appliance glossary.

- **RMAN,** a client-based utility, is embedded in each source database to be protected[6]. RMAN is responsible for sending backup data to the Recovery Appliance according to defined Protection Policies and optional Archival Backup APIs, and restores data when necessary.

[6] An Oracle database is considered to be a Protected Database when its backups are managed by a Recovery Appliance.

- The **Recovery Appliance** validates, compresses and retains content of record backups in the ***Delta Store***. Additionally, the ***Recovery Appliance Metadata Database*** retains (a) metadata associated with each record backup, (b) Protection Policies, and (c) other configuration data regarding users and protected databases.
- **Oracle Enterprise Manager,** a graphical user interface (UI), provides management access to the Recovery Appliance environment, from source database to final storage location, including tertiary storage. Additionally, a command line interface (CLI) is available for management access.
- **OCI Object Storage** is tertiary storage used for longer-term compliant retention of record backups. The Recovery Appliance leverages inherent compliance capabilities of Object Storage to immutably retain record backups in Buckets with locked *Time-bound Rention Rules*.

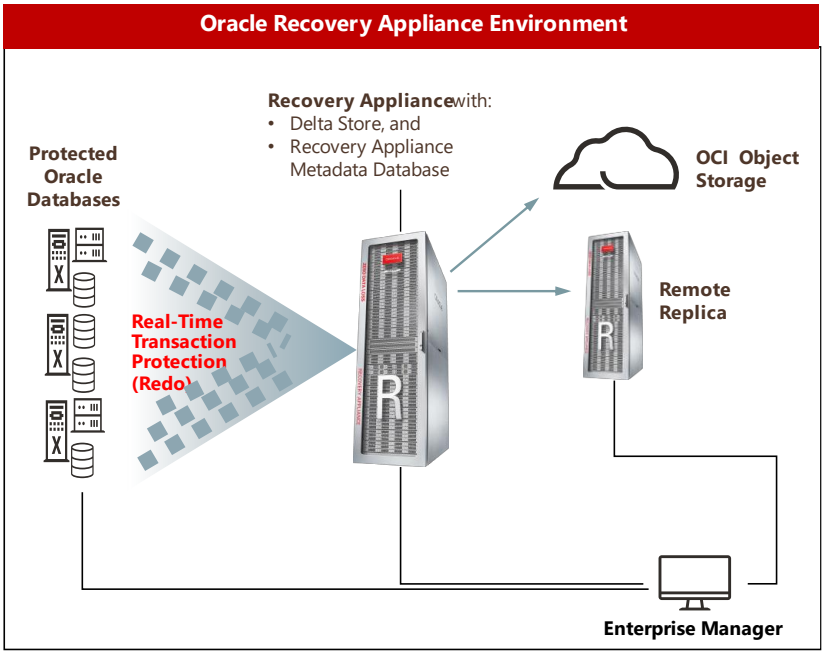


Figure 1: Storage Architecture of the Recovery Appliance Environment

The scope of this assessment is focused specifically on the compliance-related capabilities of the Oracle Recovery Appliance for preserving regulated electronic records, operating under the following conditions and configurations:

- Recovery Appliance software, version 21.1, running on any supported generation of the Recovery Appliance hardware with a minimum base rack configuration consisting of two compute servers and three storage servers, each with its own computing power. Additionally, the Recovery Appliance must be properly configured for compliance, as described in Section 2 of this Report. Oracle offers Compliance Quickstart documentation to guide how the configurations are accomplished.
- If OCI Object Storage is used for long-term archival, Object Storage Buckets must be configured within the regulated entity's Object Storage tenant, with *Time-bound Retention Rules* that are locked. The following OCI deployments are in scope:
  - OCI public cloud offering, including Commercial, Government and Dedicated Regions (i.e., localized geographic areas consisting of one or more Oracle data centers) across all storage classes.
  - On-premises, via Dedicated Region Cloud@Customer, running on Oracle hardware located in the regulated entity's data center. *Note: Cloud-at-Customer (Gen 1) is excluded from this assessment*.

Throughout this assessment, the above-described environment is being assessed. All other tertiary storage environments, such as tape or cloud storage other than OCI Object Storage, are excluded from this assessment.

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

This section presents Cohasset's assessment of the capabilities of Oracle's Recovery Appliance 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 the Recovery Appliance
- ***Recovery Appliance 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 the Recovery Appliance, as described in Section 1.3, *Recovery Appliance Overview and Assessment Scope*, relative to each of the five pertinent requirements 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 Recovery Appliance meets this SEC requirement to retain record backups in non-rewriteable, non-erasable format for time-based[7] 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 Recovery Appliance Capabilities

This section describes the capabilities of the Recovery Appliance 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*

- The Recovery Appliance captures backups of source Oracle databases (record backups) and retains them on integrated storage within the Recovery Appliance and/or in OCI Object Storage Buckets (Object Storage).
- Protection Policies applied to source Oracle databases, and optional Archival Backup APIs, provide the rules for (a) where the record backups are retained (i.e., on the Recovery Appliance and/or in Object Storage), (b) whether compliance controls are required, and (c) the retention period. *Note: The retention period may be assigned by either the Protection Policy or by an Archival Backup API.*
- When the Recovery Appliance is properly configured for compliance as described in Section 2.1.3 of this Report, and record backups are stored according to an assigned Protection Policy that requires compliant storage, integrated controls are applied which:
  - Prevent the modification or overwrite of record backups and associated metadata for the designated retention period.
  - Prohibit deletion, through any mechanism, until the assigned retention period expires and any *Compliance Holds* are removed.
  - Prohibit the *shortening* of the retention period assigned to the record backup.

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

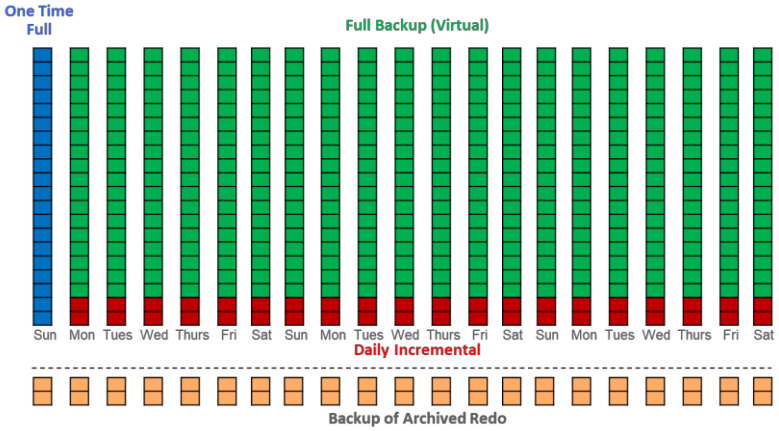
2.1.3.2 *Recovery Appliance and OCI Object Storage Configurations*

- To meet the requirements of SEC Rule 17a-4(f), the following series of configurations are required on the Recovery Appliance:
  - Create new named user accounts for (a) day-to-day Recovery Appliance management and configuration, and (b) SSH users for operating system level operations.
  - Disable root access and SSH access (for both root and Oracle accounts).
  - Disable default RASYS access and sys remote access capabilities.
  - Validate the time service utilized for storage server time clocks.

  The above steps help properly configure the Recovery Appliance for compliance, making it *capable* of applying integrated controls to protect record backups against modification, overwrite and deletion according to the requirements of the Rule. Immutability controls are *applied* once data is backed up according to rules established in a Protection Policy and/or optional Archival Backup API. (See the *Record Backups and Retention Controls* section, below, for more details on Protection Policy configurations and the use of Archival Backup APIs).
- To validate that a Recovery Appliance is properly configured to support compliance, the Recovery Appliance Administrator can perform a Run Check command, via the Recovery Appliance command line interface (RACLI).
- For longer-term immutable storage, data may be tiered to OCI Object Storage. The following configurations are required within the regulated entity's Object Storage tenant, by OCI administrators, to support compliant tiering to the cloud:
  - One or more Object Storage Buckets must be (a) created, (b) assigned a *Time-bound Retention Rule* that is equivalent to or greater than the retention period defined for a Protection Policy or optional Archival Backup API, and (c) the *Time-bound Retention Rule* must be locked.
    - *Note: Oracle recommends a one-to-one relationship between an Oracle database and Object Storage Bucket when using legal hold operations*.
    - The Recovery Appliance administrator must designate the new Object Storage Bucket as available storage for Recovery Appliance record backups.
  - A temporary metadata bucket must be created, without applied retention rules, to hold metadata markers that facilitate tracking of the copy process and recovering from any unanticipated interruptions.
  - A Lifecycle Policy may be created in the Object Storage environment to leverage archive storage capabilities (i.e., a different, more cost effective storage class).
    - *Note: Within the Object Storage Lifecycle Policy, the Delete Action attribute cannot be set or it will result in conflicts with the Recovery Appliance*.

2.1.3.3 *Record Backups and Retention Controls*

- The Recovery Appliance receives backups of source Oracle databases via:
  - RMAN client: A predefined, scheduled backup (initial full illustrated in blue, incrementals illustrated in red, and the resulting virtual fulls[8] illustrated in green), which act as required "anchor points" for recovery purposes.
  - Real-time Redo Transport: A real-time, memory-to-memory buffer transfer of data blocks for each transactional change that occurs to the database (illustrated in gold). This real-time activity requires the existence of an associated anchor point (as described in #1, above).



  - Administrator actions: Stand-alone full backups, called KEEP backups, are created, as needed, by the database or Recovery Appliance administrator. Everything required for recovery is bundled together as part of a KEEP backup (i.e., no separate anchor point or redo logs are required).

- **Record backups** may be ***comprised of different backup types*** (e.g., initial full, virtual full, incremental, archived redo logs, and KEEP backups) based upon the desired backup strategy. The collection of backup types, combined, are considered to be the record backup.

- The following chart shows three **record backup strategies** and recommended storage locations:

Record Backup Strategy	Backup Types stored in the Recovery Appliance (RA)	Exemplary Retention in RA[9]	Backup Types stored in Object Storage	Exemplary Retention in Object Storage[10]	Advantage of this Record Backup Strategy	Disadvantage of this Record Backup Strategy
1. Zero Data Loss (Requires only Protection Policies)	• Initial full • Daily incremental / virtual fulls • All redo logs	Short Term (i.e., 30 days	• Initial full • **Daily** incrementals • **Weekly** fulls • All redo logs	Long Term (i.e., 6 years)	Zero data loss model allows recovery to any point in time for duration of short and long term retention periods.	Significant storage space requirement.
2. Monthly Point-in-Time (Requires both Protection	• Initial full • Daily incremental / virtual fulls • All redo logs	Short Term (i.e., 30 days)	• Initial full • **Monthly** KEEP backups	Long Term (i.e., 6 years)	Zero data loss for data retained on the Recovery Appliance.	Data created and deleted during the same month will not be captured in the

[8] Virtual full backups are created automatically by the Recovery Appliance after receipt of each new incremental backup. By continually maintaining a virtual full backup, the Recovery Appliance is able to expedite database recovery.

[9] This duration defines the retention period of the record backups, without data loss, on the Recovery Appliance.

[10] This duration defines the retention period for each backup type (e.g., Daily, Weekly, Monthly, Yearly) in Object Storage. Depending on the backup strategy employed, there may be less granular recovery points; monthly KEEP backups do not capture data that is added and deleted during the same month.

Record Backup Strategy	Backup Types stored in the Recovery Appliance (RA)	Exemplary Retention in RA[9]	Backup Types stored in Object Storage	Exemplary Retention in Object Storage[10]	Advantage of this Record Backup Strategy	Disadvantage of this Record Backup Strategy
Policies and Archival Backup APIs)					Lowest storage space requirements	monthly KEEP backups.
3. Hybrid (Requires both Protection Policies and Archival Backup APIs)	• Initial full • Daily incremental / virtual fulls • All redo logs	Short Term (i.e., 30 days)	**Most Recent 12 Months:** • Initial full • **Daily** incrementals • **Weekly** fulls • All redo logs **Prior Months**: • **Monthly** KEEP backups	Long Term (i.e., 6 years)	Zero data loss for data retained on the Recovery Appliance and for most recent 12 months in Object Storage Intermedate storage space requirements.	Beyond the most recent 12 months, data created and deleted during the same month will not be captured in the monthly KEEP backups.

- Backup types and their target storage locations are scheduled as follows:
  - Initial full backups, incremental backups and archived redo logs are Recovery Manager (RMAN) jobs, scheduled via Enterprise Manager or supported third-party scheduling tools. The target storage environment is always the Recovery Appliance, initially, with the *option* to archive record backups to a designated Object Storage bucket with a locked, *Time-Bound Retention Rule*. Copy-to-Media job templates provide the necessary instructions to ensure the correct backup types are copied to Object Storage.
  - KEEP backups of a source database are created by running an Archival Backup API on the Recovery Appliance. The target storage environment is an Object Storage bucket with a locked, *Time-Bound Retention Rule*.
- Metadata, which serves as an index of stored record backups, is automatically retained on the Recovery Appliance and, additionally, in Object Storage (if used for long-term archival storage):
  - Immutable system metadata associated with each record backup (i.e., critical attributes, including record ID, backup completion time stamp, keep until time, hash values, and storage location) are retained on the Recovery Appliance for the same retention period as the record backup, regardless of whether the record backup types exist on the Recovery Appliance and/or in Object Storage. The Recovery Appliance maintains alignment between the Recovery Appliance and the cloud.
    - *Note: For every database backup (initial full, KEEP, and incremental) RMAN synchronizes database structure and backup metadata from the control file to the Recovery Appliance catalog. The control file is also automatically included in the backup to Object Storage, which can be used independently for* any recovery operations.
  - Mutable metadata such as storage class tier, retention period, legal hold attributes are also retained in the Recovery Appliance.
- Protection Policies are assigned to Oracle source databases. Protection Policies and optional Archival Backup APIs (described in more detail, below) define the retention rules for record backups on both the Recovery Appliance and within Object Storage. A source Oracle database may only be assigned one Protection Policy.

- **Protection Policies**: When creating a Protection Policy for compliance with the Rule (*Compliance Protection Policy*[11]), the following four attributes must be set to assure the *application* of integrated compliant retention controls:

  1. Disk Recovery Window Compliance: This attribute specifies the minimum length of time (i.e., the retention period, stated in terms of days, months, or years) that a record backup is to be immutably retained on the Recovery Appliance (configured for 30 days in the table above).
     - If sufficient storage space exists, record backups may be retained on the Recovery Appliance longer than the specified Disk Recovery Window Compliance period.
     - If insufficient storage space exists to complete a scheduled new record backup, according to the Disk Recovery Window Compliance value, all backups stop until more storage space is allocated or becomes available when prior record backups are deleted at the end of their retention period.
  2. Media Manager Recovery Window Policy: This attribute specifies the length of time (i.e., the retention period, stated in terms of days, months, or years) that a record backup is to be retained in Object Storage (configured for 6 years in the table above).
  3. Keep Compliance: This attribute must be set to Yes to prevent a database administrator from using the *RMAN CHANGE* command to reduce the "keep until time" assigned to KEEP backups. This attribute can only be turned off if no record backups exist.
  4. Allow Backup Deletion: This attribute must be set to No to prevent database administrators from prematurely deleting record backups from the Recovery Appliance. Once set to No for a Protection Policy, this attribute cannot be changed while Disk Recovery Window Compliance is configured and record backups exist.

  Notes:

  - *The above attribute names are utilized in the Enterprise Manager UI. A different naming convention is utilized when creating Protection Policies via PL/SQL commands, so care should be taken to ensure the correct attributes are specified.*
  - *A variety of different Protection Policies may be used within a single Recovery Appliance, based on the regulated entity's needs. However, only those Protection Policies configured to require compliant storage (Compliance Protection Policies) meet the requirements of the Rule.*

- **KEEP** backups, created via the Archival Backup API process, are associated with, or linked to, the source database's Protection Policy. A Keep Until Time attribute (i.e., current system time plus the applicable retention period) must be supplied as part of the Archival Backup API and allows for a combination of retention values to be directly assigned to record backups based on their type (i.e., retain weekly KEEP backups for a month and monthly KEEP backups for 6 years). The retention attributes of the associated

[11] Throughout this Report *Compliance Protection Policy* refers to a Protection Policy with these four attributes set.

Protection Policy are not used for these record backups. However, the associated Protection Policy ensures that the record backups are immutably stored on the Recovery Appliance for the assigned retention period.

- Record backups are first written to the Recovery Appliance, then if configured to do so, the record backup is also written to the Object Storage Bucket specified within the Protection Policy or optional Archival Backup API. *Note: The write to Object Storage can be delayed to a later, scheduled time to minimize impact on production resources.*
  - If any element(s) required for recovery is(are) missing from the record backup, alerts are issued during a background cross-check process.
- As each record backup is written to a Recovery Appliance and/or Object Storage (configured as compliant storage), according to a *Compliance Protection Policy*, integrated control codes are applied which:
  - Protect the record backup against modification or overwrite for the specified retention period.
  - Prohibit deletion, through any mechanism, until the assigned retention period expires and any *Compliance Holds* are removed. Note: The retention period may be assigned by either the Protection Policy or by the Archival Backup API.
  - Prohibit the *shortening* of the retention period assigned to the record backup.
  - Prevent deleting any Recovery Appliance tertiary Storage Libraries or Object Storage Bucket locations if any protected record backups exist in that library or location.
- Existing backups that did not have compliance attributes assigned at the time of storage (i.e., backups created prior to version 21.1.) will automatically inherit compliance attributes when a *Compliance Protection Policy* is assigned to the source Oracle database.
- Changes made to the Data Recovery Window Compliance value for a Protection Policy result in one of two behaviors:
  - If shortened, the change will only take effect for future record backups.
  - If extended, the change applies immediately to all existing and new record backups stored on the Recovery Appliance.
    - For record backups stored in tertiary storage, the *Time-bound Retention Rule* for the target Object Storage bucket must be extended separately, via Object Storage commands.
- Record backups stored in an Object Storage Bucket with an applied *Locked Retention Rule:*
  - Cannot be moved to another Bucket.
  - May be copied to another Bucket. New record backups created via a copy action are assigned a new last-modified timestamp and inherit the retention rules associated with the destination Bucket, if any. The original record backup remains unchanged, with the original retention rules applied to it.
  - May be assigned to a new storage class. Reassignment of the storage class does not impact retention or immutability controls for the record backup.

- Polling policies that allow for the temporary storage of record backups in the event the Recovery Appliance is unavailable, ***should not be used***. The Polling feature does not provide immutable protection for regulated record backups and is not compliant with the Rule.

2.1.3.4 *Legal Holds*

When litigation or a subpoena requires record backups to be placed on hold, which could entail retaining them beyond their assigned retention period, the regulated entity must ensure the subject record backups are protected for the duration of the legal hold.

- Authorized users identify databases that are subject to the hold and set a *Compliance Hold* attribute for each identified database, specifying the effective date of the hold.
  - Record backups must exist for the specified date in order for the *Compliance Hold* attribute to be set.
  - The *Compliance Hold* attribute applies to record backups that are stored on the Recovery Appliance only. Therefore, the regulated entity must set an Indefinite Retention rule on any affected Object Storage buckets, via Object Storage commands, to ensure record backups are retained for the duration of the hold.
- While subject to a *Compliance Hold*, a record backup cannot be deleted from the Recovery Appliance by any means, even if past its retention period.
  - Available storage space must be monitored closely while a *Compliance Hold* is in effect. Since record backups may be retained indefinitely, new backups will fail if storage space is insufficient.
- The *Compliance Hold* attribute can be removed when the hold is no longer required. Thereafter, immutability controls for the record backup are once again governed by the retention setting assigned to the record backup.
  - Indefinite Retention Rules applied to Object Storage buckets must be removed separately.

2.1.3.5 *Deletion*

- Record backups are automatically removed from short-term Recovery Appliance storage when (a) they reach their assigned *Recovery Window Compliance* date and (b) an automatic, background cross-check validation is performed to ensure the record backup exists in Object Storage (if Object Storage is utilized as part of the backup strategy). Long-term immutable retention of the record backup then continues in Object Storage for the duration of the assigned retention period.
- A record backup is eligible for final disposition when the following conditions are met:
  - The retention period applied to the record backup (i.e., all required elements of a record backup, including the anchor point and Redo Logs) has expired, and
  - No legal holds are applied to the record backup.
- Post-retention delete rules are configured within the Protection Policy and executed automatically by the Recovery Appliance. According to a pre-determined schedule, the Recovery Appliance attempts to delete

eligible record backups from both the Recovery Appliance and/or Object Storage. If the automatic delete action fails for any reason, the delete request is put into a queue to retry later.

- The RMAN *Delete Obsolete* command (i.e., a manual operation available to Oracle DBAs) is prohibited by the Recovery Appliance when *Compliance Protection Policies* are in effect. Only automated Recovery Appliance post-retention deletes are allowed.

- It is possible for retention values to become misaligned between the Recovery Appliance and Object Storage:
  - If the retention period in Object Storage is longer than the Recovery Appliance, the Recovery Appliance will attempt to delete the eligible record backup but will not be successful until the longer Object Storage retention period has expired. The Recovery Appliance will continue retrying the delete process until successful.
  - If the retention period in Object Storage is shorter than the Recovery Appliance, the Recovery Appliance will not attempt to delete the record backup until the retention period on the Recovery Appliance has expired. However, it is possible to delete the record backup directly from Object Storage via Object Storage commands. Note: This situation is detected during the Recovery Appliance automated cross-check validation process and an error message is issued.

2.1.3.6 *Clock Management*

- To protect against the possibility of premature deletion of record backups that could result from accelerating system time, the entire Recovery Appliance infrastructure is configured, by default, to synchronize with an external time server, e.g., a network time protocol (NTP) clock. Once configured and synchronized, the time of the system clocks are regularly checked against the external time source and automatically resynchronized as required.
  - Should a detected time drift exceed allowable thresholds, time synch error messages are issued at both the Recovery Appliance database and infrastructure levels and require manual correction.
  - Once the Recovery Appliance is configured to support compliance, system clock configurations are no longer accessible by administrators.

- Additionally, if OCI Object Storage is used as tertiary storage, clock management controls exist to protect against the possibility of premature deletion of record backups. Every Object Storage system clock within an OCI region is configured to synchronize with external time servers, e.g., network time protocol (NTP) clocks. The Object Storage system clock(s) is/are automatically checked against the external time source and resynchronized as required. This constant synchronization prevents, or immediately corrects, inadvertent or intentional administrative modifications to an Object Storage time clock that could result in the premature deletion of record backups.
  - Should Object Storage time clocks exceed set thresholds for synchronization, Object Storage stops functioning until the problem is corrected by authorized Oracle administrators.
  - The regulated entity does not have access to Object Storage system clocks at any time.

2.1.3.7 *Security*

In addition to the stringent retention protection and management controls described above, Oracle provides the following security capabilities, which support the authenticity and reliability of the record backups.

- Roles-Based Access Control (RBAC) provides for segregation of duties. For example, the Recovery Appliance Administrator assigns a Protection Policy to a database. The Oracle DBA does not have the authority to delete backups or to add, modify or remove Protection Policies from the Recovery Appliance. The Recovery Appliance administrator has no access to the protected Oracle database.
- For Recovery Appliances configured for compliance, access to the RASYS user and RA Root accounts are prohibited. *Note: Even Oracle support does not have access to these accounts*.
  - Two separately named administrators are required for management of the Recovery Appliance:
    - SSH user for Recovery Appliance patching and upgrades, health checks, etc. Actions taken by this named user are recorded in the Syslog. *Note: The SSH user is prohibited from elevating to root privileges without a quorum*.
    - Database user for application layer administration activities. Direct modification of data in Oracle tables is prohibited. Actions taken by this named user are recorded in the API history log.
  - A Recovery Appliance Monitor named user account is available to monitor user activity via the Incident Log. This account has no authority to change any Recovery Appliance settings.
  - Remote access to Root is only allowed in break-glass scenarios via a quorum. Approved access is time-bound and automatically disabled at the conclusion of the allotted time.
- At no time does the regulated entity have Root access to the Object Storage environment or to the storage layer of Object Storage.
- Encryption of record backups is available as follows:
  - Hypertext transport-layer encryption (HTTPS) is required to protect data in transit between the Recovery Appliance and Object Storage and, optionally, may be used to protect data in transit between the source database and the Recovery Appliance.
  - The regulated entity may elect to encrypt their source Oracle database (Transparent Data Encryption or TDE) prior to backing up to the Recovery Appliance, which results in the Recovery Appliance never having access to cleartext data for that record backup. The regulated entity is responsible for maintaining its encryption keys.
  - Object Storage requires data to be encrypted when stored. Each object is encrypted with its own data encryption key; the encryption key itself is then encrypted via a master encryption key assigned to the Bucket. The Oracle Key Vault holds encryption keys for all record backups that are sent from the Recovery Appliance to Object Storage.

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:

- Properly configuring the Recovery Appliances for compliance, as described in Section 2.1.3 of this Report, thereby establishing the foundation for meeting the requirements of the Rule.
- Properly configuring Object Storage Buckets, with locked *Time-bound Retention Rules* that correlate to Protection Policies, if tertiary storage is to be utilized.
- Creating and applying *Compliance Protection Policies* that require the application of compliance controls to stored record backups (i.e., set Data Recovery Window Compliance and Keep Compliance attributes).
- Using Archival Backup APIs with appropriate Keep Until Times (that exceed the retention periods defined in the associated Protection Policies) to create KEEP backups when the backup approach is either Monthly Point-in-Time or Hybrid, as explained in the table in Section 2.1.3.
- Storing record backups requiring event-based[12] retention periods in a separate compliance system, since the Recovery Appliance does not currently support event-based retention periods.
- Ensuring that Polling Policies are not utilized to store record backups on temporary Polling storage, as the Polling feature does not provide immutable protection for regulated record backups and, therefore, is not compliant with the Rule.
- Applying *Compliance Holds* to record backups that require preservation for legal matters, government investigations, external audits and other similar circumstances, and removing the *Compliance Holds* when the applicable action is completed and managing legal holds in the Object Storage environment via the application and removal of *Indefinite Retention Rules*.

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 asserts that the capabilities of the Recovery Appliance, in conjunction with the inherent capabilities of advanced magnetic storage technology, meet this requirement for accurate recording and post-recording verification.

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

2.2.3 Recovery Appliance Capabilities

The Recovery Appliance 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 record backups are written in a high-quality and accurate manner.
- During backup, RMAN calculates independent checksums at varying levels, including (a) individual data blocks, (b) headers, and (c) the entire payload. Checksums are compounding (i.e., individual block checksums must roll up to match the header checksum, etc.) to ensure integrity of the entire backup chain is maintained. Checksums are transmitted with the record backup to the Recovery Appliance.
- The Recovery Appliance calculates checksums during the write process and compares them to the supplied checksums. If checksum values match, the Recovery Appliance writes the backup to storage and records the checksums as metadata for the backup. If the checksums do not match, the Recovery Appliance issues an error message and fails the write.
- During replication to another Recovery Appliance or upload to an Object Storage bucket, the Recovery Appliance compares the checksums for all backup blocks and pieces against the original values to ensure they are valid and unaltered.

2.2.3.2 *Post-Recording Verification*

- To validate continued integrity, the Recovery Appliance regularly performs validation on all backups stored locally to ensure consistency. A cross-check validation, using checksum metadata, is also used to ensure all backups (i.e., originals and replicas) still exist on the Recovery Appliance and/or on Object Storage.
  - Checksums on the Recovery Appliance are retained at the block level.
  - Checksums in Object Storage are retained at the object level.
- In the event that checksums do not match:
  - Within the Recovery Appliance, data is repaired via self-healing mirroring capabilities.
  - Object Storage automatically initiates a repair or reconstruction of damaged objects from duplicates or erasure-coded segments.
- Notifications are issued if any elements of the record backup are determined to be missing, or are unable to be reconstructed, during the periodic validation process performed by the Recovery Appliance.

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 Recovery Appliance meets this SEC requirement to serialize the original and duplicate record backups.

2.3.3 Recovery Appliance Capabilities

- RMAN uses unique identifiers for each record backup, comprised of:
  - The Database ID, File number, Checkpoint Time, Checkpoint Change Number,
  - The backup completion date and time for each record backup, and
  - Database ID, Thread Number, Sequence Number, Low & High Checkpoint Change Number for each entry in the archived redo logs.
- The unique identifier (a) provides a serialization of each record backup in both space and time and (b) is immutably retained on the Recovery Appliance for the duration of the assigned retention period.
- Additionally, for each record backup retained in Object Storage:
  - Object Storage assigns a unique identifier (eTag) to each record backup and stores it as immutable metadata in Object Storage.
  - The last-modified timestamp (storage date and time) is captured and stored with each record backup as immutable metadata in Object Storage.

  Note: Unique Identifiers assigned by Object Storage are not retained within the Recovery Appliance, but rather, immutably retained only in Object Storage.

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

Cohasset asserts that the Recovery Appliance meets this SEC requirement to readily download record backups and indexes (metadata attributes) when the considerations described in Section 2.4.4 are addressed.

2.4.3 Recovery Appliance Capabilities

The following capabilities support the capacity to search and download record backups and indexes (metadata attributes):

- RMAN's command line interface is used to search metadata for record backups stored on both the Recovery Appliance and Object Storage:
  - A variety of available RMAN *List* commands display metadata associated with backups for a specified database or datafile (i.e., a database is comprised of multiple datafiles) and include information such as backup type (e.g., full, incremental, archived redo logs, and KEEP), backup date, number of copies, storage location, tags, etc.
  - The RMAN *Spool* command is used to direct the output of the LIST command to a specified log file for export.
- RMAN references metadata in the Recovery Appliance Catalog to determine all pieces necessary to restore a record backup to a specified point-in-time, if available, based on the implemented backup strategy. Content may exist on either the Recovery Appliance or Object Storage. Once restored to a designated location, source applications are used to view content and/or transfer to a medium acceptable under the Rule.

2.4.4 Additional Considerations

The regulated entity is responsible for (a) maintaining its account in good standing, (b) maintaining hardware and software to access the Recovery Appliance, (c) maintaining its encryption keys that have been used in addition to the Oracle encryption key, and (d) assuring that the regulator, self-regulatory organization or designated examining authority receive downloads of the record backups and 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: Based on its experience, Cohasset defines a *duplicate copy* 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, Cohasset defines a *backup copy* 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 the capabilities of the Recovery Appliance meet this SEC requirement for a persistent duplicate copy of record backups (a) when properly configured, as described in Section 2.5.3 and (b) when the considerations described in Section 2.5.4 are satisfied.

2.5.3 Recovery Appliance Capabilities

- The Recovery Appliance provides three methods for meeting the conditions of this requirement to separately store a duplicate copy:
  1. Automatically performs two-way mirroring of data across multiple storage servers during the write process, which allows for automatic self-healing of record backups should they become lost or damaged.
  2. The Recovery Appliance may be configured, as part of a Protection Policy, to copy record backups from the Recovery Appliance, according to a pre-defined schedule (i.e., every evening), to a tertiary storage location.
     - Note: The Recovery Appliance does not maintain exclusive ownership of record backups within the Object Storage environment. Therefore, if a record backup that is retained in Object Storage is copied directly via *Object Storage commands*, the Recovery Appliance will not be aware of the copy action and will not retain metadata associated with that copy.
  3. If geographically dispersed replication is needed, Backup Anywhere Replication may be utilized, which allows for two Recovery Appliances, in separate data centers, to replicate between each other.
- Record backups may be reestablished from persistent replicas/copies by restoring the necessary elements according to the recovery catalog (i.e., the closest full or incremental backup, or "anchor point", plus any archived redo logs).
- To ensure persistent duplicate copies of data in the cloud, record backups are written to Object Storage utilizing either (a) erasure coding or (b) synchronously recording three copies of each record backup across multiple fault domains (i.e., separate storage racks and/or storage servers and where available, across multiple data centers).

- The method of duplicating is dependent upon the capabilities of the OCI region hosting the data as well as the size of each record backup.

- The record backup is recoverable by either:
  - Regenerating a duplicate of the original from erasure encoded data, or
  - Automatically restoring the record backup from a duplicate located in a separate fault domain.

2.5.4 Additional Considerations

- If replication or scheduled copies are utilized to meet the requirement of a persistent duplicate copy, the Protection Policy must be configured such that the retention period for replicas/copies is set identical to that of the original record backup.
- Object Storage copy commands should not be utilized to create duplicate copies of record backups, but rather, duplicates in the cloud should be established and maintained via Protection Policies within the Recovery Appliance.

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 the Recovery Appliance, as described in Section 1.3, *Recovery Appliance 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 the Recovery Appliance 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 the Recovery Appliance when properly configured for compliance, 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 assessed capabilities of the Recovery Appliance 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 the Recovery Appliance 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 the Recovery Appliance capabilities, when properly configured for compliance, as described in Sections 2.1 through 2.4 meet CFTC requirements (c)(1) and (c)(2)(i) for record objects requiring a fixed retention period.[13] 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 the Recovery Appliance retains immutable metadata attributes (e.g., unique ID, backup completion time stamp, keep until time), for every record backup, regardless of whether the record backup resides on the Recovery Appliance or in Object Storage. The record object attributes are subject to the same retention protections as the associated record backup itself. To satisfy this requirement for other essential data related to how and when the record backups 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*

[13] The Recovery Appliance does not currently support event-based retention periods, which require records to be retained indefinitely until a specified event occurs (e.g., a contract expires or an employee terminates), after which the record is retained for a fixed final retention period. Accordingly, records requiring event-based retention periods should be stored in a separate compliance system.

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[14] 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 Recovery Appliance capabilities described Section 2.5, including options for duplicating or replicating the record backups meet the CFTC requirements (c)(2)(ii) to *ensure the availability of such regulatory records in the event of an emergency or other disruption of the records entity's electronic record retention systems*. To satisfy this requirement for other essential data that is not retained in the Recovery Appliance (such as separate indices), the regulated entity must retain this other data in a compliant manner.	***Section 2.5 Duplicate Copy of the Records Stored Separately*** *Store separately from the original, a duplicate copy of the record stored on any medium acceptable under §240.17a-4 for the time required*
(iii) The creation and maintenance of an *up-to-date inventory* that identifies and describes each system that maintains information necessary for accessing or producing electronic regulatory records.	The regulated entity is required to create and retain an *up-to-date inventory,* as required for compliance with 17 CFR § 1.31(c)(iii).	N/A
(d) Inspection and production of regulatory records. Unless specified elsewhere in the Act or Commission regulations in this chapter, a records entity, at its own expense, must *produce or make accessible for inspection* all regulatory records in accordance with the following requirements: (1) *Inspection*. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice. (2) *Production of **paper** regulatory records*. *** (3) *Production of **electronic** regulatory records*. (i) A request from a Commission representative for electronic regulatory records will specify a *reasonable form and medium* in which a records entity must produce such regulatory records. (ii) A records entity must *produce such regulatory records in the form and medium requested promptly*, upon request, unless otherwise directed by the Commission representative. *(4) Production of **original** regulatory records.* ***	It is Cohasset's opinion that the Recovery Appliance has features that support the regulated entity's efforts to comply with requests for inspection or production of record backups 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 how the Recovery Appliance is used to search for, retrieve (i.e., restore), and download the record backups and system metadata retained by the Recovery Appliance. As noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the record backups 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 source systems	***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member*

[14] 17 CFR § 1.31(a) includes indices (*Any data necessary to access, search, or display any such books and records*) in the definition of regulatory records.

4 | Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1)

The objective of this section is to document Cohasset's assessment of the capabilities of the Recovery Appliance, as described in Section 1.3, *Recovery Appliance Overview and Assessment Scope*, in comparison to the following requirements of the *Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation).* Specifically, Article 72(1) defines medium and retention of records requirements:

> *1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:*
> *(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;*
> *(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;*
> *(c) it is not possible for the records otherwise to be manipulated or altered;*
> *(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and*
> *(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used.*

Paragraph (e), above, recognizes the technology evolution and defines requirements or conditions for regulated entities that retain records electronically. The approach is consistent with the SEC, which also sets forth standards that the electronic storage media must satisfy to be considered acceptable.

Additionally, the Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MiFID II) defines durable medium as follows:

> *(62) 'durable medium' means any instrument which:*
> *(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information; and*
> *(b) allows the unchanged reproduction of the information stored [emphasis added]*

While the above pertains to enabling the client to store and access its information, regulated entities often apply the MiFID II durable medium requirements to internally retained information, assuring it is immutable, retained for the appropriate time period and stored in a manner that assures unchanged reproduction. For this reason, Cohasset included this citation in its analysis for this section of the Report.

Cohasset leveraged its assessment of the capabilities of the Recovery Appliance, as described in Section 2, and correlated the assessed capabilities to the requirements for (a) *durable medium* in MiFID II and (b) the *medium* and retention of records in the *Delegated Regulation,* which supplements MiFID II. For each of the four requirements, which are highlighted in the light blue rows, the following table summarizes the results of Cohasset's analysis.

- The two left-hand columns list key requirements specified in (a) the definition of *durable medium* in MiFID II and (b) the *medium* and *retention of records* in the *Delegated Regulation*, which supplements MiFID II, respectively. The focal element for each row is underlined for clarity.
- The right-hand column provides Cohasset's compliance assessment and an analysis of capabilities of the Recovery Appliance, relative to these requirements.

Regulatory excerpts that are pertinent to each of the four specific requirements		Compliance Assessment and Analysis of the Recovery Appliance Relative to these MiFID II Requirements
***Directive 2014/65/EU* (MiFID II) Article 4(1)(62)**	***Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)***	
Requirement #1: **Store record for the required retention period**		
(62) 'durable medium' means any instrument which: *(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information* ***** [emphasis added]	*(1) The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:* ***** [emphasis added]	While this requirement pertains to the client of the regulated entity, the regulated entity itself would have a similar need to store the record for the required retention period. It is Cohasset's opinion that the Recovery Appliance has the capability to apply a fixed retention period to a record backup and its core metadata, when properly configured for compliance, as described in **Section 2.1 *Non-Rewriteable, Non-Erasable Record Format***. The associated integrated control codes: ● Prevent the modification or overwrite of record backups and associated metadata for the designated fixed retention period.[15] ● Prohibit deletion, through any mechanism, until the assigned retention period expires and any *Compliance Holds* are removed. ● Prohibit the *shortening* of the assigned retention period assigned to the record backup. Further, the Recovery Appliance assures the accurate recording (storage) of the record backup and associated metadata, as explained in **Section 2.2 *Accurate Recording Process***. The quality and accuracy of the recording process is verified during the initial recording of the record backup. Additionally, regular post-recording validations are performed on all files stored locally to ensure consistency. A cross-check validation, using checksum metadata, is also used to ensure all files (i.e., originals and replicas) still exist on the Recovery Appliance and/or on Object Storage.

[15] The Recovery Appliance does not currently support event-based retention periods, which require records to be retained indefinitely until a specified event occurs (e.g., a contract expires or an employee terminates), after which the record is retained for a fixed final retention period. Accordingly, records requiring event-based retention periods should be stored in a separate compliance system.

Regulatory excerpts that are pertinent to each of the four specific requirements		Compliance Assessment and Analysis of the Recovery Appliance Relative to these MiFID II Requirements
***Directive 2014/65/EU* (MiFID II) Article 4(1)(62)**	***Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)***	
Requirement #2: **Assure immutable record content**		
(62) 'durable medium' means any instrument which: ***** *(b) allows the unchanged reproduction of the information stored* [emphasis added]	*1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:* ***** *(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;* *(c) it is not possible for the records otherwise to be manipulated or altered;* ***** [emphasis added]	It is Cohasset's opinion that the capabilities of the Recovery Appliance, when properly configured for compliance, as described in Section 2.1.3, provides the foundation to achieve non-rewriteable, non-erasable storage and meets this requirement to assure that record content is unchangeable. See **Section 2.1 Non-Rewriteable, Non-Erasable Record Format** for additional information. Since the record content is unchangeable, any corrections or other amendments must be stored as a separate record, assuring that the changes can be ascertained. Further, the Recovery Appliance stores checksums for each record backup at varying levels, including (a) individual data blocks, (b) headers, and (c) the entire payload. Checksums are compounding (i.e., individual block checksums must roll up to match the header checksum, etc.) to ensure integrity of the entire backup chain is maintained. These checksums are subsequently used for post-recording quality and integrity checks and for automated record backup repair, as described in **Section 2.2 Accurate Recording Process.**

Regulatory excerpts that are pertinent to each of the four specific requirements		Compliance Assessment and Analysis of the Recovery Appliance Relative to these MiFID II Requirements
***Directive 2014/65/EU* (MiFID II) Article 4(1)(62)**	***Commission Delegated Regulation (EU) 2017/565, (the MiFID II Delegated Regulation), Article 72(1)***	
Requirement #3: **Provide access to and reproduce the stored records**		
(62) 'durable medium' means any instrument which: *(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information* *(b) allows the unchanged reproduction of the information stored [emphasis added]*	*1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:* ***** *(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;* ***** *(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and* ***** [emphasis added]	Cohasset asserts that the Recovery Appliance provides the ability to search, via a variety of LIST commands on the CLI, for core system metadata associated with record backups that are stored on either the Recovery Appliance or Object Storage. The resulting list of record backups can be directed to a log file for export. Select record backups can be restored to a designated location, after which, local applications may be used to view content and/or transfer to an acceptable medium. See ***Section 2.4 Capacity to Download Indexes and Records*** for additional information. Further, the Recovery Appliance ensures that record backups are readily available by providing three methods for separately storing duplicate copies, including data mirroring, duplicate copies on tertiary storage, and geographically dispersed replication. See ***Section 2.5 Duplicate Copy of the Records Stored Separately*** for additional information.
Requirement #4: **Provide access to and reproduce the stored records**		
N/A	*1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:* ***** *(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used.* ***** [emphasis added]	Cohasset asserts that the Recovery Appliance provides the ability to search, via a variety of LIST commands on the CLI, for core system metadata associated with record backups that are stored on either the Recovery Appliance or Object Storage. The resulting list of record backups can be directed to a log file for export. Select record backups can be restored to a designated location, after which, local applications may be used to view content and/or transfer to an acceptable medium. See ***Section 2.4 Capacity to Download Indexes and Records*** for additional information. As may be required, the regulated entity may transfer record backups to other media or migrate record objects to new file formats, in advance of technological obsolescence.

5 | Conclusions

Cohasset assessed the capabilities of the Recovery Appliance (release 21.1), properly configured for compliance, as described in Section 2, in comparison to the five requirements related to the recording and non-rewriteable, non-erasable storage and retention of electronic records, as set forth in SEC Rule 17a-4(f) and its associated Interpretive Releases. (See Section 1.3, *Recovery Appliance Overview and Assessment Scope*.)

Cohasset determined that the Recovery Appliance, when properly configured for compliance, as described in Section 2, has the following capabilities, which meet the regulatory requirements:

- Immutably maintains record backups and associated system metadata for time-based retention periods.
- Prohibits deletion of a record backup and its immutable metadata until the retention period has expired.
- Preserves all record backups that are stored on the Recovery Appliance as immutable and prohibits deletion or overwrites, while a *Compliance Hold* attribute is applied. (Separately, Indefinite Retention Rules may be applied to effectuate holds in Object Storage buckets.)
- Verifies the accuracy and quality of the recording process through the use of checksums and Recovery Appliance post-recording validation processes.
- Uniquely serializes each record backup and all duplicate copies with a unique ID and a date/time stamp.
- Automatically mirrors each record backup across three storage servers during the write process, which allows for automatic self-healing of record backups that become lost or damaged. Additionally, supports scheduled copying of record backups to tertiary storage as well as geographically dispersed replication of record backups.
- Provides the capacity and tools to (a) search for record backups, (b) list record backups, and (c) restore record backups to a designated location, after which a local application may be used to view content and/or transfer to a medium acceptable under the Rule.

Cohasset also correlated the assessed capabilities of the Recovery Appliance to the:

- Principles-based technology requirements of CFTC Rule 1.31(c)-(d),
- *Medium* and *retention of records* requirements in Article 72(1) of the *Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II (the MiFID II Delegated Regulation).*

Accordingly, Cohasset concludes that the Recovery Appliance, when properly configured for compliance, as described in Section 2, and utilized to retain time-based records, meets the five requirements of SEC Rule 17a-4(f) and FINRA Rule 4511(c), which relate to the recording and non-rewriteable, non-erasable storage of electronic records. In addition, the assessed capabilities meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d) and the *medium* and *retention of records* requirements of the *MiFID II Delegated Regulation(72)(1)*.

6 | 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.

6.1 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.*[16] [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.

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

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

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

> *Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.* [emphasis added]

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

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

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

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

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

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

6.2 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.*

6.3 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 the Recovery Appliance in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

6.4 Overview of *the Medium* and *Retention of Records* Requirements of MiFID II

Markets in Financial Instruments Directive II (MiFID II), approved by the European Parliament as *Directive 2014/65/EU,* became effective January 3, 2018. Specifically, Article 4(1)(62) of MiFID II defines durable medium as:

(62) 'durable medium' means any instrument which:
(a) enables a client to store information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information; and
(b) allows the unchanged reproduction of the information stored [emphasis added]

While the above pertains to enabling the client to store and access its information, regulated entities often apply the MiFID II durable medium requirements to internally retained information, assuring it is immutable, retained for the appropriate time period and stored in a manner that assures the unchanged reproduction.

Further, with implementation of the revised MiFID II, investment firms must arrange for records to be kept of all services, activities and transactions. The key recordkeeping provisions are in Article 16, *Organisational requirements*, paragraphs 6 and 7:

***6.** An investment firm shall arrange for records to be kept of all services, activities and transactions undertaken by it which shall be sufficient to enable the competent authority to fulfil its supervisory tasks and to perform the enforcement actions under this Directive, Regulation (EU) No 600/2014, Directive 2014/57/EU and Regulation (EU) No 596/2014, and*

in particular to ascertain that the investment firm has complied with all obligations including those with respect to clients or potential clients and to the integrity of the market.
7. *Records shall include the recording of telephone conversations or electronic communications relating to, at least, transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission and execution of client orders.*
Such telephone conversations and electronic communications shall also include those that are intended to result in transactions concluded when dealing on own account or in the provision of client order services that relate to the reception, transmission and execution of client orders, even if those conversations or communications do not result in the conclusion of such transactions or in the provision of client order services.
For those purposes, an investment firm shall take all reasonable steps to record relevant telephone conversations and electronic communications, made with, sent from or received by equipment provided by the investment firm to an employee or contractor or the use of which by an employee or contractor has been accepted or permitted by the investment firm.
*****
Orders may be placed by clients through other channels, however such communications must be made in a durable medium such as mails, faxes, emails or documentation of client orders made at meetings. In particular, the content of relevant face-to-face conversations with a client may be recorded by using written minutes or notes. Such orders shall be considered equivalent to orders received by telephone.
*****
The records kept in accordance with this paragraph shall be provided to the client involved upon request and shall be kept for a period of five years and, where requested by the competent authority, for a period of up to seven years.
[emphasis added]

Article 16(6) allowed the Commission to make delegated legislation, resulting in the issuance of *Commission Delegated Regulation (EU) 2017/565* (*the MiFID II Delegated Regulation*).

The *MiFID II Delegated Regulation* in Section 8, *Record-keeping*, Article 72, *Retention of records*, paragraph 1, specifies:

1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:
(a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each transaction;
(b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;
(c) it is not possible for the records otherwise to be manipulated or altered;
(d) it allows IT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and
(e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used.

See Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1),* for a summary assessment of the capabilities of the Recovery Appliance in relation to requirements for (a) *durable medium* in MiFID II and (b) the *medium* and *retention of records* in the *MiFID II Delegated Regulation*.

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.