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 ZFSSA

Abstract

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

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

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

Oracle ZFS Storage Appliance (ZFSSA) is a unified storage system that allows for consolidated file, object, and snapshot storage on a single platform. ZFSSA combines flash performance with petabytes storage capacity. Oracle ZFSSA provides immutable file locking and data retention capabilities. *Retention Policies* and *Retention Rules* enable integrated controls designed to help meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the capabilities of ZFSSA (see Section 1.3, *ZFSSA 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 ZFSSA, version 8.8.45, when properly configured, helps meet the five requirements related to 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 ZFSSA 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).

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 Oracle ZFSSA 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 file and record object* (versus *data*, *file*, *object*) to consistently recognize that the content is a required record.

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

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

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

Refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, which correlates the CFTC principles-based requirements to the capabilities of ZFSSA. 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 ZFSSA. 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 ZFS Storage Appliance (ZFSSA) 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 ZFSSA files and objects storage 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);*
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) to the assessed capabilities of ZFSSA; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d);*

[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 ZFSSA 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 ZFSSA).

- Associate the requirements of Article 72(1) of the *MiFID II Delegated Regulation* to the assessed capabilities of ZFSSA; 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 ZFS Storage 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 ZFSSA Overview and Assessment Scope

Oracle ZFS Storage Appliance (ZFSSA) is a unified storage system that allows for consolidated file, object, and snapshot storage on a single platform. ZFSSA combines flash performance with petabytes storage capacity.

The ZFSSA architecture (Figure 1) consists of the following components:

- **Protocol Interfaces (Block, File, Object)** provide access to the *Shares* (standard and immutable) to store and retrieve files and to manage immutability policies.
- **Projects** are collection mechanisms that provide the ability to set storage defaults in *Policies*.
- **Shares**, configured, under Projects, as: (1) File *Share*, (2) Object *Share* (which contains Buckets), or (3) Snapshots. *Shares* inherit *Project Policies* or may be configured with their own *Policies*.
- ZFS Storage Appliances are deployed as a clustered pair with multiple attached **Drive Enclosures (DE)**, used for storing data. **DE** is a physical storage architecture consisting of numerous disk drives in a single storage enclosure.

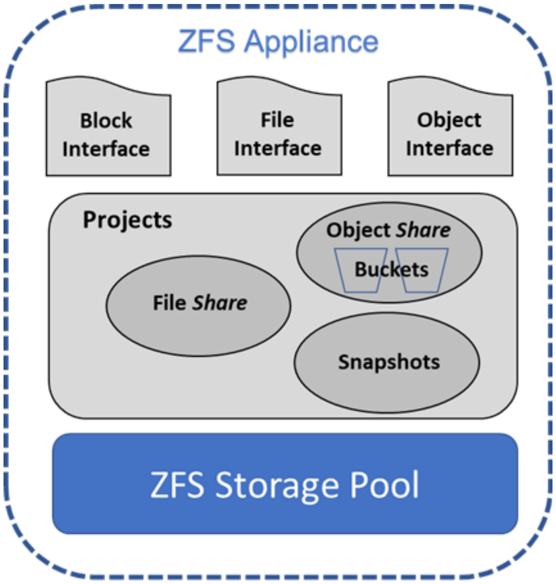

Figure 1: ZFSSA Logical View

The scope of this assessment is focused specifically on the compliance related capabilities of ZFSSA, Version 8.8.45 operating under the following conditions and configurations:

- Oracle ZFS Storage Appliance, when pre-packaged with Oracle ZFS Storage Appliance Software, Oracle Intelligent Storage Protocol, Oracle Database, and drives.
- Oracle ZFS Virtual Appliance utilizing cloud infrastructure in lieu of the physical storage hardware.
- File *Shares* and Object *Shares* for retaining immutable record objects, as well as *Manual* Snapshots of File *Shares* or the purpose of preservation in compliance with legal holds.

Note: *Scheduled* Snapshots and *Manual* Snapshots for purposes other than preservation for legal holds are outside the scope of this assessment.

The following section documents Cohasset's assessment of ZFSSA (includes both physical and virtual implementations), relative to the pertinent requirements in SEC Rule 17a-4(f). Throughout this report, the above-described acceptable operating environments of ZFSSA will be assessed.

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

This section presents Cohasset's assessment of the capabilities of Oracle ZFS Storage Appliance (ZFSSA) 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 ZFS Storage Appliance
- ***ZFSSA 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 ZFSSA, as described in Section 1.3, *ZFSSA Overview and Assessment Scope*, relative to each pertinent requirement of SEC Rule 17a-4(f).

2.1 Non-Rewriteable, Non-Erasable Record Format

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

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]."*

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

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 <u>the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules</u>.* [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 ZFSSA, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for time-based[6] retention periods and any applied legal hold, when **(1)** properly configured, as described in Section 2.1.3, which includes requirements to set *Retention Policies* to (a) *Mandatory* for File *Shares* or (b) *Locked* on the Object *Shares*, **and (2)** the considerations described in Section 2.1.4 are satisfied.

2.1.3 ZFSSA Capabilities and Configuration

This section describes the capabilities of ZFSSA 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

- As depicted in the figure in Section 1.3, ZFSSA provides storage services for three types of ***Shares****:* (1) File *Share*, (2) Object *Share,* and (3) *Snapshot*.
  - The capabilities, related to compliance with the Rule, vary significantly for each of type of ***Share*** and associated record type (i.e., Files, Objects and Snapshots).
  - File *Shares* and Object *Shares* are in-scope for this assessment; the specific capabilities of each of these two types of *Shares* are separately described following this <u>*Overview*</u>.
- For compliance with SEC Rule 17a-4(f), the following must be configured for the two types of in-scope ***Shares***:
  1. <u>File *Share*</u>: *Retention Policy* must be set to *Mandatory* when the File *Share* is created.
  2. <u>Object *Share*</u>: *Retention Policy* must be *Locked* on the Object *Share*.
- Once a *Retention Policy* or *Retention Rule* is configured for compliance, it cannot be changed or deleted. Retention is managed differently based on the type of ***Share*** and associated record type (i.e., File or Object):
  1. <u>File *Share*</u>: *Retention Time* attribute stores a retention expiration date and time for each record file. The *Retention Time* is either transmitted by the source application, using the last access date and time (*atime*) attribute or calculated by adding the *Default Retention Period* to the current date and time.

[6] 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. Object *Share*: *Retention Period* is assigned to the Bucket, and each record object's retention time is calculated based on the object's last modified date/time and the Bucket *Retention Period*. The calculated value is not stored in the record object's metadata.

- When the File *Share* or Object *Share* is configured for compliance with the Rule, immutability is enforced through integrated control codes that:
  - Protect the record file or record object against modification and overwrite for its lifespan.
  - Prohibit deletion, through any mechanism, until the file or object is eligible, which occurs when:
    - The assigned *Retention Time* is in the past, for File *Shares*, or
    - The calculated retention expiration date is in the past, for Object *Shares*.
  - Prohibit the shortening of the: (1) *Retention Time* assigned to the record file or (2) Bucket *Retention Rule* for record objects.
  - Prohibit deleting a *Share* containing one or more *Immutable* record files or record objects.
- Restrictions and exceptions that apply to the system administrator and root user are desirable integrated controls:
  1. File *Share*: System administrators are not able to view record files via Storage Appliance user interfaces (UI) and cannot modify the retention and immutability controls on record files with a set retention time. The underlying operating system root user is required for servicing the appliance by authorized Oracle Support. The root user has access to all configurations through a command line version of the user interface (UI), though the root user is prevented from deleting a record file by the shell/kernel. To limit access outside of the UI, ZFSSA removes the ability to log in as a root user through the SSH (Secure Shell) protocol, Browser UI (BUI) and RESTful API, when the *Mandatory* Retention policy is configured on any File *Share*.
  2. Object *Share*: Root access restrictions are not enforced. Root and system administrators, with proper authorization, can make changes to the *Retention Rules* and modify the Namespace, Bucket, and Object level permissions. Refer to Section 2.1.4 *Additional Considerations*, for recommended controls.

This Overview highlighted key configurations and controls, which are described in more detail in the following two subsections, which separately describe the capabilities associated with File *Shares and* Object *Shares*.

2.1.3.2 ***File Shares***

For **File *Shares*** the following subsections address (1) *Configuration and Controls*, (2) *Legal Holds* and (3) *Deletion Controls*.

2.1.3.2.1 Configuration and Controls

- A record file stored in a File *Share* within ZFSSA is comprised of two elements:
  - **Content:** The contents of the record file (e.g., document, image, video or database image).

- **System metadata:** Critical attributes for record file management such as:
  - *Immutable metadata*, e.g., unique identifier, transmitted file name and a cryptographic hash value. Additionally, last modified date and time (which is system managed) cannot be updated after retention controls are applied.
  - *Mutable metadata,* such as *Retention Time* which stores the retention expiration date and can be extended but cannot be shortened in File *Shares* configured with a *Mandatory Retention Policy*.

- During File *Share* creation, the *Share* may be configured with one of the following *Retention Policy* settings:
  1. *Mandatory* (File Retention Mandatory) which enforces immutability controls and ensures the retention controls applied to a record file cannot be modified or removed by any user, regardless of privileges. For a File *Share* to be compliant with the Rule, it **must** be configured with a *Mandatory Retention Policy*.
  2. *Privileged* (File Retention Privileged Override) allows retention controls to be configured and enforced on the record files, but a privileged user may remove the retention controls and subsequently delete record files. Therefore, the *Privileged* configuration is **not** compliant with the Rule.
  3. *Off* (File Retention Disabled) does not enable retention controls to be configured for record files, therefore, the *Off* configuration is **not** compliant with Rule.

- Once a File *Share* has been configured to one of the three settings, the setting <u>cannot</u> be removed or changed, including upgrading it from a non-compliant setting (*Privileged* or *Off*) to a compliant setting (*Mandatory*).

- For *Shares* configured as *Mandatory* or *Privileged*, the administrator must set the: (1) *Default Retention Period*, (2) *Minimum Retention Period*, and (3) *Maximum Retention Period*.
  - *Default Retention Period* specifies the retention period that is used when a file is transmitted <u>without</u> an **explicit** *Retention Time* (*atime* value). ZFSSA calculates and stores the *Retention Time* by adding the *Default Retention Period* to the current (storage) date and time.
    - When setting the *Default Retention Period*, it must be between the Minimum and Maximum Retention Periods.
    - The *Default Retention Perio*d may be updated after creation, by a permissioned user. Any changes to the *Default Retention Period* <u>only</u> applies to future record files stored on the *Share* and does not modify any previously written record files.
  - *Minimum Retention Period* specifies the shortest period of time (seconds, minutes, hours, days, weeks, months, or years) that record files must be retained in an immutable state.
    - If the user or source application attempts to store a record file with a shorter retention time than the minimum, ZFSSA calculates and stores the *Retention Time* by adding the *Minimum Retention Period* to the current (storage) date and time.
  - *Maximum Retention Period* specifies the longest period (up to 100 years) of time (seconds, minutes, hours, days, weeks, months, or years) that a record file may be retained in an immutable state.

- If the user or source application transmits a record file with a longer *Retention Time* than the *Maximum Retention Period*, ZFSSA calculates and stores the *Retention Time* by adding the *Maximum Retention Period* to the current (storage) date and time.

- The user or source application uses a command line interface (CLI), graphical user interface (GUI) or REST application programming interface (API) to access ZFSSA. System administrators, including root users, cannot view the record files.

- Record files can be accessed through one of the following four protocols: (1) NFS (Network File System), (2) SMB (Server Message Block), (3) SFTP (Secure File Transfer Protocol), or (4) WebDAV (Web-based Distributed Authoring and Versioning).

- Immutability is exclusively set via the NFS or SMB protocols, by either: (1) NFS removing the record file write access or (2) SMB marking the record file as read-only.

- *Retention Time* is either transmitted, at the time of write, with the record file in the *atime* value or calculated using the *Default Retention Period*. The *Retention Time* is saved, in seconds, in the metadata of the record file.

- An *Autoretain* capability may be enabled, to automatically set immutability and the *Retention Time* (i.e., the retention expiration date) on a record file, if the record file is not modified within the specified *Autoretain* period. Upon expiration of the *Autoretain* period, the *Retention Time* is calculated by adding the *Default Retention Period* to the last modified date and time and is stored as an attribute of the record file.
  - The recommended *Autoretain* period is 24 hours or less, for compliance with the Rule.
  - Applying an explicit *Retention Time* (i.e., retention expiration date and time) to a record file is supported when *Autoretain* is used.

- File *Shares* may be **moved** between *Projects*, the retention controls continue to be enforced on the *Share* and does not affect the *Retention Time* and immutability of the record files stored on the *Share*.

2.1.3.2.2 Legal Holds

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

- For record files that must be preserved for a duration longer than the assigned *Retention Time*, the regulated entity either:
  1. Extend the existing *Retention Time*, which applies record files governed by the *Retention Policy.*
     - Using NFS or SMB commands, the administrator extends the *Retention Time* (i.e., retention expiration date and time), for select record files that are subject to the hold. If the initial extension of the *Retention Time* is not sufficient to cover the legal hold period, the *Retention Time* must continue to be extended, as required, to meet the legal hold timeframe.
  2. Take a *Manual* snapshot and initially set the retention control to *Unlocked*, which will retain the snapshot indefinitely. When the legal hold is released, change the retention control to *Off*, which will permit deletion of the snapshot.

2.1.3.2.3 *Deletion Controls*

- While deletion is not required by the Rule, record files are eligible for deletion, when the *Retention Time* applied to the record file is in the past.
- Eligible record files may be deleted by the source application or an administrator.
- Modification or overwriting of a record file is not allowed, even after its *Retention Time* has expired and it is eligible for deletion.
- Deleting a *Project* or *Share* with protected record files is prohibited.
  - A *Project* or *Share* may be deleted when the *Retention Time* of all protected record files is in the past. The ability to delete an eligible *Project* or *Share* **does not** require them to be empty.

2.1.3.3 ***Object Shares***

For **Object *Shares***[7] the following subsections address (1) *Configuration and Controls*, (2) *Legal Holds* and (3) *Deletion Controls*.

2.1.3.3.1 *Configuration and Controls*

- A record object is comprised of the following elements:
  1. **Content:** The complete content of the unstructured object, such as analytic data, large application datasets, logs, images, and videos.
  2. **Metadata:**
     - *Immutable* attributes of the record object, such as the Bucket name, ETag (i.e., unique identifier), last modified timestamp[8] (used to compute retention expiration date), key value pairs, and MD5 hash.
     - *Mutable* attributes of the record object, such as object name and user defined tags.

     Note: *Attributes associated with Retention Rules are properties of the Bucket, not the record object.*
- During the configuration the *Share* must be set to Object Cloud Infrastructure (OCI) "enabled" for object storage. Once the *Share* (i.e., Object *Share*) is enabled for OCI, it cannot be used with any other protocol (i.e., NFS or SMB).
- An Object *Share* may be configured with one of the following *Retention Policy* settings:
  1. *Locked:* Enforces immutability controls on the *Retention Policy*, which is assigned to the Object *Share*.
     - The *Lock* feature is applied to the *Retention Policy*. For an Object *Share* to be compliant with the Rule, the applied *Retention Policy* **must** be configured as *Locked*.
     - The *Locked Retention Policy* cannot be modified or removed from the Object *Share* by any user, regardless of privileges.

[7] An Object *Share* contains Buckets, which house objects.

[8] When retention controls are applied to a record object, it is immutable (actions that would change the record object are blocked), accordingly, the last modified timestamp is immutable metadata for an object contained within a locked retention-controlled bucket.

- Since the *Retention Policy* applies to all Buckets in the Object *Share* and associated Retention Rules, after the *Retention Policy* is locked, the retention and immutability controls **cannot** be removed from any Bucket

2. *Unlocked*: The *Retention Policy* can be modified (retention time of the associated Retention Rules can be shortened or lengthened) or removed by a privileged user. As a result, retention and immutability controls may be removed and objects may be deleted. An *Unlocked Retention Policy* is **not** compliant with the Rule.

- Within an Object *Share*, record objects are stored in logical containers, called Buckets.

- Retention time periods are defined at the Bucket level, via *Retention Rules* which apply to all record objects contained within the Bucket. There are two types of Bucket-level *Retention Rules*:

  1. *Time-bound* Bucket-level *Retention Rules* retain record objects for a specified duration of time. Retention duration is specified in terms of years and days only and is added to each record object's last-modified timestamp to determine its retention expiration date. *Note: Retention expiration dates are calculated for each record object during requests for overwrites or deletion; no retention expiration date attribute is stored with the record object.*

     - A Bucket-level *Retention Rule* is active immediately, however, there is a default waiting period of 14 days (i.e., scheduled lock wait time) before the lock takes effect, during which time the *Retention Rule* can be modified and/or deleted from a Bucket. The scheduled lock wait time can be changed, prior to the lock taking effect, from the default value to any future date. Therefore, any record objects stored in the Bucket prior to the lock taking effect are **not** compliant with the Rule.

     - Once the lock takes effect:

       - The *Locked Retention rule* cannot be removed from the Bucket, by any means.
       - The assigned *Retention Period* cannot be shortened, only extended.
       - The Bucket cannot be deleted unless it is empty.

       Note: Time-bound Retention Rules that are not Locked are not compliant with SEC Rule 17a-4(f), since authorized users may modify and/or remove an unlocked Retention Rule from a Bucket at any time.

  2. *Indefinite* Bucket-level *Retention Rules* retain record objects indefinitely, or until the *Indefinite Retention Rule* is removed from the Bucket. *Indefinite Retention Rules* cannot be locked and therefore, are used for legal holds or other temporary suspensions of deletion eligibility. *Indefinite Retention Rules* **cannot** be used as a substitute for a properly configured *Locked Retention Rule* for compliance with the Rule.

- *Retention Rules* may be applied to both new and existing Buckets.

  - *Time-bound Retention Rules* and *Indefinite Retention Rules* can apply to a single Bucket. *Indefinite Retention Rules* always take precedence, followed by the longest retention period of the applied *Time-bound Retention Rules*.

  - The maximum retention duration that is applied to the Bucket is considered the protection period for all record objects contained within the Bucket.

    - When the retention duration of a *Time-bound Retention Rule* is extended, the new duration applies to all existing and new record objects stored in the Bucket.

- Record objects are uploaded to and managed on an object *Share* using one of the following interfaces: (1) OCI (Oracle Cloud Infrastructure) CLI (Command Line Interface), (2) Amazon S3 Compatible APIs (Application Programming Interface), and (3) SWIFT APIs.
- Record objects stored in a Bucket with a *Locked Retention Rule*:
    - Cannot be **moved** to another Bucket.
    - May be **copied** to another Bucket. New record objects created via a copy action are assigned a new last-modified timestamp and will inherit any *Retention Rules* associated with the destination Bucket. The original record object remains unchanged, with the original *Retention Rules* applied to it.
- Object *Shares* and associated Buckets may be **moved** between *Projects*, and all Bucket retention controls are moved and continue to apply.

2.1.3.3.2 Legal Holds

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

- To protect record objects for a hold, an authorized user assigns an *Indefinite Retention Rule* to Buckets which contain record objects subject to the hold. The *Indefinite Retention Rule* applies to all record objects in the Bucket and takes precedence over other *Time-bound Retention Rules* that are applied to the Bucket.
- While the Bucket is subject to an *Indefinite Retention Rule,* the stored record objects cannot be modified, overwritten, or deleted by any means, even if past their retention period.
- The *Indefinite Retention Rule* can be removed from the Bucket by an authorized user when the hold is no longer required. Thereafter, immutability controls for the record object are governed by the *Time-bound Retention Rules* applied to the Bucket.

2.1.3.3.3 Deletion Controls

- While deletion is not required by the SEC Rule, record objects eligible for deletion remain immutable, but may be deleted, when the following conditions are met:
    - The retention period applied to the record object (as calculated by adding the Bucket's longest, time-bound *Retention Duration* to the last-modified timestamp for the record object) is in the past, and
    - No *Indefinite Retention Rules* are applied to the record object's Bucket.
- Eligible record objects may be deleted using the OCI CLI.
- Deleting a Bucket with protected record objects is prohibited.
    - A *Locked Retention Rule* applied to a Bucket cannot be removed, which means all record objects in the Bucket must be eligible for deletion and deleted before the Bucket can be deleted.

2.1.3.4 ***Clock Management***

- To protect against the possibility of premature deletion of record files or record objects that could result from accelerating the system time clock, the ZFS system clock is configured to synchronize with one or more network time protocol (NTP) clocks. The ZFS 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 the ZFS system clock that could result in the premature deletion of record objects.
- There are no system administrator permissions that allow disabling of the NTP service via the ZFSSA UI or RESTful interface. If the NTP service were to fail due to a software defect it would automatically restart.

2.1.3.5 ***Security***

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

- Administration is conducted over an HTTPS browser session or SSH connection. Administrators can configure the ZFSSA with an appropriate signed certificate by a trusted certificate authority or use the default self-signed certificate that is uniquely generated for each Oracle ZFS Storage Appliance system at initial installation time.
- Administrative access is limited to the root user Local administrators defined with the relevant privileges, and those authorized through identity servers such as Lightweight Directory Access Protocol (LDAP) and Network Information Service (NIS).
- ZFS file system provides file access control through access control lists (ACLs).
- ZFSSA supports Transport Layer Security (TLS) v1.1 and v1.2 and their associated ciphers for data transfer.
- ZFSSA supports data encryption using the built-in local keystore and the ability to connect to the Oracle Key Manager (OKM) system.
  - ZFSSA supports RESTful access authentication tokens, over the HTTPS transport, which eliminates the need for user passwords.
  - ZFSSA supports SSH public key authentication which can be used in lieu of a password. SSH keys can be uploaded to the ZFSSA or retrieved from LDAP. When using SSH keys, password based SSH authentication should be disabled.
  - ZFSSA supports OASIS Key Management Interoperability Protocol (KMIP) 1.4 capable remote key manager.
  - ZFSSA support multiple network access protocols, “Allow Administration" should be disabled on network interfaces used for data protocol access from clients to segregate administrative activities.

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:

2.1.4.1 Record Files

- Configuring the File *Share Retention* policy as Mandatory and setting the *Default, Minimum and Maximum* retention periods, to be in compliance with the Rule.
- Transmitting an explicit retention time (atime) for record files that require a specific retention time to applied.
- Configuring the *Autoretain* setting, if applicable, to process record files within 24 hours of the last modified date/time.
- Extending the *Retention Time* of record files subject to preservation for legal matters, government investigations, external audits and other similar circumstances, and periodically reviewing the holds to determine if the *Retention Time* must be extended further to meet on-going holds.

2.1.4.2 Record Objects

- Configuring the Object *Share* as *OCI enabled*.
- Applying a *Locked Retention rule* with appropriate retention duration, to each Bucket intended to retain regulated record objects. Objects required for compliance with the Rule should be stored in the Bucket only after the Bucket waiting period, e.g., 14 day scheduled lock wait time, has lapsed. Care should be taken to ensure that the assigned retention duration for a Bucket reflects the longest retention requirement of all record objects in that Bucket.
- Applying an *Indefinite Retention rule* to Buckets that contain record objects subject to preservation for legal matters, government investigations, external audits and other similar circumstances, and removing the *Indefinite Retention rule* when the applicable action is completed. Note: An *Indefinite Retention rule* is not a substitute for a properly configured Locked Retention policy.

2.1.4.3 Overall Requirements

- Ensuring all record files and record objects required to be retained for compliance with the SEC Rule are stored with appropriate settings within 24 hours of creation.
- Storing record objects requiring event-based[9] retention periods in a separate compliance system, since ZFSSA does not currently support event-based retention periods.
- Cohasset recommends procedural controls be established to limit root and system administrator access.
- Configuring an NTP clock synchronization.
- When using SSH public key authentication, disable password based SSH authentication.

[9] 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 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 current capabilities of ZFSSA, in conjunction with the inherent capabilities of advanced magnetic storage technology, meet this SEC requirement for accurate recording and post-recording verification, when the considerations described in Section 2.2.4 are satisfied.

2.2.3 ZFSSA Capabilities

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

2.2.3.1 Recording Process

- A combination of checks and balances in the advanced magnetic recording technology (such as inter-component and inter-step cyclical redundancy checks (CRCs), as well as write-error detection and correction) are relied upon to assure that the records are written in a high-quality and accurate manner.
- During the write process, ZFSSA calculates and stores a checksum with each block or object and subsequently uses the checksum for post-recording quality and integrity checks.

2.2.3.2 Post-Recording Verification

- ZFSSA performs the following verifications, using the previously stored checksum:
  - When the record is read back from the disk, the system verifies the checksum to ensure that the record has not been altered since it was written.
  - Automated scrubbing is “on” by default and may be scheduled to run in increments of 15 days (15, 30, 45, 60 or 90) time periods. If the system identifies a block where the stored checksum and current checksum do not match it perform an automated repairs from the redundant copy.

2.2.4 Additional Considerations

There are no additional considerations related to this requirement.

2.3 Serialize the Original and Duplicate Units of Storage Media

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

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

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

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

2.3.2 Compliance Assessment

It is Cohasset's opinion that ZFSSA meets this SEC requirement to serialize the original and duplicate records.

2.3.3 ZFSSA Capabilities

2.3.3.1 ***File Share***

- ZFSSA assigns a unique identifier (Object Number and Generation Number) for each record file and the date and time (timestamp) of the write is recorded.
- The combination of the unique identifier and the timestamp represent a serialization of the record file in both space and time.

2.3.3.2 ***Object Share***

- Object *Shares* assign a unique identifier (ETag) to each record object and stores it as immutable metadata.
- The last-modified timestamp (storage date and time) is captured and stored with each record object as immutable metadata.
- The combination of the ETag and the last-modified timestamp provide a serialization of each record object in both space and time.

2.3.4 Additional Considerations

There are no additional considerations related to this requirement.

2.4 Capacity to Download Indexes and Records

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

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

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

2.4.2 Compliance Assessment

It is Cohasset's opinion that ZFS meets this SEC requirement to readily download records and indexes (metadata attributes) when the considerations described in Section 2.4.4 are addressed.

2.4.3 ZFSSA Capabilities

2.4.3.1 File Shares

- The directory of a ZFS file system, including record file name, date stored, and other directory attributes (indexes or metadata) can be viewed by the client application through the standard NAS protocols (NFS and SMB). The appropriate record files can then be identified, retrieved, and downloaded, whereupon they can be transferred using local capabilities to any medium acceptable under the Rule.

2.4.3.2 Object Shares

- The Object Storage console (OCI CLI) provides the ability to list Buckets that exist within a given *Share*. When an individual Bucket is selected, a list of the objects it contains is displayed in alphabetical order by record object name, along with any user-specified metadata, as key value pairs.
- Alternatively, using CLI commands, authorized users can (a) list all Buckets or filter the list based on Bucket attributes, (b) list all record objects within a Bucket, or filter the list of objects within a Bucket based on prefixes and/or timestamps, if utilized as part of the record object naming convention, (c) download the list of record objects and associated indexes (metadata attributes), (d) download selected objects for viewing and/or further filtering by client-side tools, and (e) produce the record objects and indexes (metadata attributes).

2.4.4 Additional Considerations

The regulated entity is responsible for (a) assuring that hardware and software capacity allows for ready access to the record files and metadata (index) attributes, (b) maintaining its encryption keys, and (c) assuring that the regulator, self-regulatory organization, or designated examining authority receive downloads of the record files 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: A *duplicate copy* is defined as a persistent copy that allows the complete and accurate record to be reestablished from data stored on a compliant storage system or medium. Whereas, a *backup copy* is defined as a non-persistent copy that is overwritten as it is *rotated* on a periodic basis, resulting in a much shorter retention period than the original.

2.5.2 Compliance Assessment

Cohasset asserts that ZFSSA, meets this SEC requirement for a persistent duplicate copy of the record objects, when (a) properly configured, as described in Section 2.5.3, and (b) the considerations described in Section 2.5.4 are satisfied.

2.5.3 ZFSSA Capabilities

- ZFSSA provides the ability for continuous or scheduled replication of the record files or record objects and associated metadata to another similarly configured ZFS Storage Appliance.
  - Replication is recommended to be performed at the *Project* level.
  - For Object *Shares*, mirrored/raid configuration is required.
- All compliance-required attributes are replicated with the duplicate copy of the record files or record objects.
- The duplicate copies are retained for the full retention period of the record.
- The duplicate copy can be utilized when the primary source is not accessible, to either: (a) restore the primary source or (b) retrieve record files or record objects.

2.5.4 Additional Considerations

When using ZFSSA replication capabilities, the source and destination storage appliance must remain connected and must not be disassociated to ensure a duplicate copy is maintained. When using scheduled replication, it is recommended that the replication should be scheduled for at least once every 24 hours.

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 ZFSSA, as described in Section 1.3, *ZFSSA 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 ZFSSA 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 ZFSSA when (a) *Retention Policies* are set to *Mandatory* for File *Shares* or (b) *Retention Rules* are set to *Locked* on the Bucket for Object *Shares*, which is a highly restrictive configuration that assures the storage solution applies controls to (a) protect immutability of the record content and certain system metadata and (b) prevent deletion over the applied retention period.

In the following table, Cohasset correlates the capabilities of ZFSSA when (a) *Retention Policies* are set to *Mandatory* for File *Shares* or (b) *Retention Rules* are set to *Locked* on the Bucket for Object *Shares*, to the *principles-based* CFTC requirements related to the *form and manner of retention* and the *inspection and production of regulatory records*. In addition, Cohasset contends that ZFSSA with *File Retention Privileged Override* for File *Share* or *Unlocked* for Object *Share*, meets these *principles-based* CFTC requirements, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be modified or deleted prior to expiration of the retention period. This less restrictive *File Retention Privileged Override* for File *Share* or *Unlocked* for Object *Share* provides flexibility to remove or shorten retention periods, which may be beneficial for compliance with privacy and data protection requirements.

The left-hand column lists the *principles-based* CFTC requirements. The middle column provides Cohasset's analysis and opinion regarding the ability of ZFSSA 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 ZFSSA capabilities, utilized when (a) *Retention Policies* are set to *Mandatory* for File *Shares* or (b) *Retention Rules* are set to *Locked* on the Bucket for Object *Shares*, 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[10]. 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 ZFSSA retains immutable metadata attributes (e.g., Unique Identifier, create date and time and Retention Interval), as an integral part of the record file or record object. The record file or record object attributes are subject to the same retention protections as the associated record file or record object. To satisfy this requirement for other essential data related to how and when the record files or record objects were created, formatted, or modified, the regulated entity must retain this data in a compliant manner.	**Section 2.1 *Non-Rewriteable, Non-Erasable Record Format*** *Preserve the records exclusively in a non-rewriteable, non-erasable format* **Section 2.2 *Accurate Recording Process*** *Verify automatically the quality and accuracy of the storage media recording process* **Section 2.3 *Serialize the Original and Duplicate Units of Storage Media*** *Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media* ***Section 2.4 Capacity to Download Indexes and Records*** *Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member*

[10] Oracle ZFSSA 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[11] 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 ZFSSA capabilities described Section 2.5, including options for duplicating or replicating the record objects 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 ZFSSA (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 ZFSSA has features that support the regulated entity's efforts to comply with requests for inspection or production of record files or record objects and associated system metadata (i.e., index attributes). ● Specifically, it is Cohasset's opinion that Section 2.4, *Capacity to Download Indexes and Records*, describes use of ZFSSA to retrieve and download the record files or record objects and the system metadata retained by ZFSSA. As noted in the *Additional Considerations* in Section 2.4.4, the regulated entity is obligated to produce the record files or record objects and associated metadata, in the form and medium requested. ● If the regulator requests additional data related to how and when the record files or 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*

[11] 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 ZFSSA, as described in Section 1.3, *ZFSSA 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) '<u>durable medium</u>' means any instrument which:*
> *(a) enables a client to <u>store information</u> addressed personally to that client in a way <u>accessible for future reference and for a period of time adequate for the purposes of the information</u>; and*
> *(b) allows the <u>unchanged reproduction of the information stored</u> [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.

While the focus of this assessment pertains to ZFSSA, with *File Retention Mandatory* for File *Share* or *Locked* for Object *Share*, Cohasset contends that ZFSSA configured to utilize *File Retention Privileged Override* for File *Share* or *Unlocked* for Object *Share* retention features meet the *medium* and *retention of records* requirements of the MiFID II Delegated Regulation, when the regulated entity applies appropriate procedural controls to oversee operations that may allow content to be changed or deleted prior to expiration of the retention period.

Cohasset leveraged its assessment of the capabilities of the ZFSSA, 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 ZFSSA, relative to these requirements.

Regulatory excerpts that are pertinent to each of the four specific requirements		**Compliance Assessment and Analysis of the ZFSSA 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 ZFSSA, when configured in File Retention *Mandatory* for File *Share* or *Locked* for Object *Share* has features that apply a fixed retention period to a record object and its core metadata, as described in **Section 2.1 *Non-Rewriteable, Non-Erasable Record Format***. The associated integrated control codes: ● Disable all write permissions for the content of the file or object, thus protecting it against modification or overwrite for the specified fixed retention period[12]. ● Prohibit deletion, through any mechanism, until the assigned retention period expires and any Legal Holds are removed. ● Prohibit the shortening of the retention period assigned to the record files or record objects. ● Prohibit the deletion or renaming of a directory containing one or more record files or record objects. Further, ZFSSA assures the accurate recording (storage) of the record content and associated metadata, as explained in **Section 2.2 *Accurate Recording Process***. The quality and accuracy of the recording process is verified: (a) during the initial recording of the file or object record; (b) using post-recording verification during read-back, and (c) by conducting periodic consistency and integrity checking.

[12] Oracle ZFSSA 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 ZFSSA 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 features of ZFSSA in File Retention *Mandatory* for File *Share* or *Locked* for Object *Share* to achieve non-rewriteable, non-erasable storage meet this requirement to assure that record content is unchangeable. See **Section 2.1 *Non-Rewriteable, Non-Erasable Record Format*** for additional information. If the regulated entity corrects or amends a record, it must store each rendition as a separate record. The features for assuring a non-rewriteable, non-erasable format assure that the original record is not modified. Further, ZFSSA stores a cryptographic hash value for each record files or record objects during the recording process and subsequently uses it for post-recording quality and integrity checks and for automated record object repair, as described in **Section 2.2 *Accurate Recording Process*.**
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 ZFSSA provides the following methods of retrieving records, based on record type: 1. File: NAS protocols (NFS and SMB). 2. Object: Object Storage console (OCI CLI). The selected records may be downloaded and local capabilities may be used to view or print the records. See ***Section 2.4 Capacity to Download Indexes and Records*** for additional information. Further, ZFSSA ensures that records are readily available by storing a duplicate copy of each record by configuring replication to a second, equivalently configured ZFSSA system. See ***Section 2.5 Duplicate Copy of the Records Stored Separately*** for additional information.

Regulatory excerpts that are pertinent to each of the four specific 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)***	**Compliance Assessment and Analysis of the ZFSSA Relative to these MiFID II Requirements**
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 ZFSSA provides the following methods of retrieving and then exporting record files or record objects: 1. File: Industry Standard Protocols (NFS and SMB) may be used to export selected records. 2. Object: Object Storage console (OCI CLI) can be used to export a list of record objects. The selected records may be exported and local capabilities may be used to view, reproduce or transfer the record objects to another medium. See ***Section 2.4 Capacity to Download Indexes and Records*** for additional information. As may be required, the regulated entity may transfer records to other media or migrate record objects to new file formats, in advance of technological obsolescence.

5 | Conclusions

Cohasset assessed the capabilities of ZFS Storage Appliance (ZFSSA), version 8.8.45, when (a) *Retention Policies* are set to *Mandatory* for File *Shares* or (b) *Retention Rules* are set to *Locked* on the Bucket for Object *Shares*, 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, *ZFSSA Overview and Assessment Scope*.)

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

- Maintains record files or record objects and immutable metadata in non-rewriteable, non-erasable format for time-based retention periods.
- Holds records beyond their assigned retention period, as immutable and prohibits deletion or overwrites for: (a) Record Files by manually extending the retention period or taking *Manual* Snapshots of the File *Share* and applying an *Unlocked* Retention Policy, and (b) Record Objects by applying an Indefinite Retention policy.
- Prohibits deletion of a record file or record object and its immutable metadata until the retention period for the record file or object has expired.
- Verifies the accuracy and quality of the recording process through cryptographic hash values and ZFSSA validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- Uniquely serializes each record file or record object and all duplicate copies with a unique identifier and a date/time stamp.
- Provides the ability for continuous or scheduled replication of the record files or record objects and associated metadata to a second similarly configured ZFS Storage Appliance.
- Provides the capacity and tools to (a) search for records, (b) list the names, and (c) download the records and associated metadata attributes for a browser or other local tool to render as a human-readable image.

Cohasset also correlated the assessed capabilities of ZFSSA, when (a) *Retention Policies* are set to *Mandatory* for File *Shares* or (b) *Retention Rules* are set to *Locked* on the Bucket for Object *Shares*, 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 ZFSSA, 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.*[13] [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.

[13] 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[14], 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.

[14] 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 ZFSSA 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 ZFSSA 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.*** *<u>Records shall include the recording of telephone conversations or electronic communications</u> 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 <u>such communications must be made in a durable medium</u> 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 <u>medium that allows the storage of information in a way accessible for future reference by the competent authority</u>, and in such a form and manner that the following conditions are met:*
> *(a) the competent authority is able to <u>access them readily</u> and to reconstitute each key stage of the processing of each transaction;*
> *(b) it is possible for any <u>corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained</u>;*
> *(c) it is <u>not possible for the records otherwise to be manipulated or altered</u>;*
> *(d) it <u>allows IT or any other efficient exploitation</u> 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 <u>comply with the record keeping requirements irrespective of the technology used</u>.*

See Section 4, *Summary Assessment of Compliance with the MiFID II Delegated Regulation(72)(1)*, for a summary assessment of the capabilities of ZFSSA 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.