

Amazon Web Services (AWS) Backup COMPLIANCE ASSESSMENT

SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c) and CFTC 1.31(c)-(d)

Abstract

Amazon Web Services® (AWS®) is a secure cloud services platform hosted by Amazon to provide modular cloud-based products and services. AWS Backup is an AWS service that provides a fully managed data protection service for AWS products and services.

In this report, Cohasset Associates, Inc. (Cohasset) assesses the functionality of AWS Backup (see Section 1.3, *AWS Backup Overview and Assessment Scope*) relative to the electronic records requirements, specified by multiple regulatory bodies, as follows:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)(2);
- SEC in 17 CFR § 240.18a-6(e)(2);
- Financial Industry Regulatory Authority (FINRA) in Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f); and
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d).

It is Cohasset's opinion that AWS Backup, when properly configured and used with the *Vault Lock* feature and other compliance capabilities, has functionality that meets the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). Additionally, the assessed functionality of AWS Backup meets the principles-based requirements of CFTC Rule 1.31(c)-(d).

COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to our practice is the delivery of records management and information governance professional consulting services, and education and training. Cohasset's expert consulting services support regulated organizations, including those in financial services. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls to their organizations' business priorities, facilitating regulatory compliance and risk mitigation, while generating quantifiable business efficiency.

Cohasset assesses a range of electronic recordkeeping systems, each designed to meet the requirements of the Securities and Exchange Commission Rules 17a-4(f)(2) and 18a-6(e)(2) for record audit trail and non-rewriteable, non-erasable record formats, considering the SEC 2001, 2003 and 2019 interpretations. For the non-rewriteable, non-erasable record, these interpretations authorize the use of erasable storage, conditioned on integrated software or hardware control codes, to prevent overwriting, erasing, or otherwise altering the records, during the applied retention period.

Table of Contents

Abstract 1

Table of Contents 2

1 • Introduction 3

 1.1 Overview of the Regulatory Requirements 3

 1.2 Purpose and Approach 4

 1.3 AWS Backup Overview and Assessment Scope 5

2 • Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e) 7

 2.1 Record and Audit Trail 7

 2.2 Non-Rewriteable, Non-Erasable Record Format 8

 2.3 Record Storage Verification 16

 2.4 Capacity to Download and Transfer Records and Location Information 17

 2.5 Record Redundancy 19

 2.6 Audit System 20

3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d) 22

4 • Conclusions 25

Appendix A • Overview of Relevant Electronic Records Requirements 27

 A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) *Electronic Recordkeeping System* Requirements 27

 A.2 Overview of FINRA Rule 4511(c) *Electronic Recordkeeping System* Requirements 29

 A.3 Overview of CFTC Rule 1.31(c)-(d) *Electronic Regulatory Records* Requirements 30

Appendix B • Cloud Provider Undertaking 31

 B.1 Compliance Requirement 31

 B.2 Amazon Undertaking Process 32

 B.3 Additional Considerations 32

About Cohasset Associates, Inc. 33

1 • Introduction

Regulators, worldwide, establish explicit requirements for certain regulated entities that elect to electronically retain books and records. Given the prevalence of electronic books and records, these requirements apply to most broker-dealers, commodity futures trading firms and similarly regulated organizations.

This Introduction summarizes the regulatory environment pertaining to this assessment and the purpose and approach for Cohasset's assessment. It also provides an overview of Amazon Web Services (AWS) Backup and the assessment scope.

1.1 Overview of the Regulatory Requirements

1.1.1 SEC Rules 17a-4(f) and 18a-6(e) Requirements

In 17 CFR § 240.17a-4 (SEC Rule 17a-4) for the securities broker-dealer industry and 17 CFR § 240.18a-6 (SEC Rule 18a-6) for nonbank SBS entities¹, the U.S. Securities Exchange Commission (SEC) stipulates recordkeeping requirements, including retention periods.

In 2022, the SEC adopted amendments to SEC Rules 17a-4 and 18a-6, establishing technology-neutral requirements for electronic storage systems.

*The Securities and Exchange Commission ("Commission") is adopting amendments to the recordkeeping rules applicable to broker-dealers, security-based swap dealers, and major security-based swap participants. The amendments modify requirements regarding the maintenance and preservation of electronic records ***² [emphasis added]*

For additional information, refer to Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, and Appendix A.1, *Overview of SEC Rules 17a-4(f) and 18a-6(e) Electronic Recordkeeping System Requirements*.

1.1.2 FINRA Rule 4511(c) Requirements

Financial Industry Regulatory Authority (FINRA) Rules regulate member brokerage firms and exchange markets. These Rules were amended to address security-based swaps (SBS).³

FINRA Rule 4511(c) explicitly defers to the requirements of SEC Rule 17a-4, for 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. [emphasis added]

¹ Throughout this report, 'nonbank SBS entity' refers to security-based swap dealers (SBSD) and major security-based swap participants (MSBSP) that are not also registered as a broker-dealer without a prudential regulator.

² Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants, Exchange Act Release No. 96034 (Oct. 12, 2022) 87 FR 66412 (Nov. 3, 2022) (2022 Electronic Recordkeeping System Requirements Adopting Release).

³ FINRA, Regulatory Notice 22-03 (January 20, 2022), FINRA Adopts Amendments to Clarify the Application of FINRA Rules to Security-Based Swaps.

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

In 17 CFR § 1.31 (CFTC Rule 1.31) for the U.S. Commodity Futures Trading Commission (CFTC) stipulates recordkeeping requirements, including retention periods.

In 2017, the CFTC adopted amendments to CFTC Rule 1.31, establishing principles-based, technology-neutral requirements for electronic regulatory records.

*The Commodity Futures Trading Commission (the "Commission") is amending the recordkeeping obligations set forth in Commission regulations *** The amendments modernize and make technology neutral the form and manner in which regulatory records must be kept ****⁴ [emphasis added]

For additional information, refer to Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*, and Appendix A.3, *Overview of CFTC Rule 1.31(c)-(d) Electronic Regulatory Records Requirements*.

1.2 Purpose and Approach

To obtain an independent and objective assessment of the compliance capabilities of AWS Backup for preserving required electronic records, Amazon Web Services (AWS) engaged Cohasset Associates, Inc. (Cohasset). As a specialized consulting firm, Cohasset has more than fifty 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.

AWS engaged Cohasset to:

- Assess the functionality of AWS Backup, in comparison to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and describe audit system features that support the regulated entity in its compliance with SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii); see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*;
- Address FINRA Rule 4511(c), given FINRA explicitly defers to the requirements of SEC Rule 17a-4; see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*;
- Associate the principles-based requirements of CFTC Rule 1.31(c)-(d) with the assessed functionality of AWS Backup; see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*; and
- Prepare this Compliance Assessment Report, enumerating the assessment results.

In addition to applying the information in this Compliance Assessment Report, regulated entities must ensure that the combination of its policies, procedures and regulatory submissions, in conjunction with the functionality of implemented electronic recordkeeping systems, 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 AWS Backup and its functionality or other AWS products or services. The information utilized by Cohasset to conduct this assessment consisted of: (a) oral discussions, (b) product demonstrations, including system setup and configuration, (c) system documentation, (d) user and system administrator guides, and (e) related materials provided by AWS or obtained from publicly available resources.

⁴ Commodity Futures Trading Commission, Amendments to Recordkeeping Requirements, 82 FR 24479 (May 30, 2017). (2017 CFTC Recordkeeping Requirements Adopting Release).

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 AWS Backup Overview and Assessment Scope

1.3.1 AWS Backup Overview

AWS Backup is a fully managed data protection service across AWS services. Using this service, regulated entities can configure backup plans and monitor activity for their AWS resources in one place. It allows regulated entities to automate and consolidate backup tasks that were previously performed service-by-service and removes the need to create custom scripts and manual processes. AWS Backup is configured to store unique timed backups (Recovery Points) of an AWS Resource. A Recovery Point⁵ is a point-in-time snapshot of the protected resource.

Recovery Points are created and managed according to a backup plan that is associated with the resource. The backup plan defines the frequency and total retention period (i.e., DeleteAfterDays) for each Recovery Point. Further, the Backup Vault can be configured with AWS Backup Vault Lock (*Vault Lock*). Enabling and properly configuring *Vault Lock* applies integrated control codes that place additional restrictions on the actions that can be performed on a Recovery Point and its associated metadata, to prevent erasure prior to the expiration of an assigned retention period.

The logical hierarchy of the AWS Backup service illustrated in Figure 1 is summarized as follows:

- ▶ **Centralized Backup Management** is (a) the capability to centrally manage backup plans and apply the plans to AWS resources across AWS accounts and Regions and (b) the capability to monitor backup activities and demonstrate compliance with controls and reports.
- ▶ **Backup Plans** define when and which AWS resources are backed up and for how long the Recovery Points are retained. For compliance with the Rule, a backup plan must be configured with an appropriate total retention period that is between the Minimum and Maximum retention periods (Min/Max range) for the Backup Vault where the Recovery Point will be stored. The backup plan, together with an applied *Vault Lock* setting, prevents deleting the Recovery Point and prevents modifying the total retention period assigned to the Recovery Point.



Figure 1: Logical Hierarchy of the AWS Backup Service

⁵ The SEC uses the phrase *books and records* to describe information that must be retained for regulatory compliance. In this report, Cohasset uses the term record, in addition to specific terms, e.g., *Recovery Points* (which store a *collection of records*), both terms are intended to recognize that the content may be required for regulatory compliance.

- ▶ **Backup Resources** are AWS services and third-party applications that are [supported by AWS Backup](#).
- ▶ **Backup Vaults** securely store Recovery Points separate from the Backup Resource instance. AWS Backup provides two options: (1) standard (non-air-gapped) Backup Vault owned and managed by the regulated entity and (2) logically air-gapped Backup Vault that AWS Backup owns and manages, which is outside of the regulated entity's control. For compliance with the Rule, the Backup Vault must be appropriately configured with *Vault Lock*, which may be set to:
 - *Compliance* mode, the vault's *Compliance mode start date* is met or in the past. *Compliance* mode is highly restrictive and disallows both modifications to *Vault Lock* configurations and removal of *Vault Lock*.
 - *Governance* mode, the vault's *Compliance mode start date* is not set or is in the future. *Governance* mode is less restrictive and allows both modifications to *Vault Lock* configurations and removal/deletion of *Vault Lock* from a Backup Vault, which removes the *Vault Lock* protections from associated Recovery Points.
- ▶ Each **Recovery Point** is a point-in-time snapshot of a Backup Resource, which may contain the required records. Throughout the report, Recovery Points is used to describe the snapshot of the Backup Resource and the required records contained within the snapshot.
 - The Recovery Point lifecycle specifies when it transitions to cold storage and expires.
 - The lifecycle cannot be changed for Recovery Points stored in Backup Vaults with *Vault Lock* set to either *Compliance* or *Governance* mode.

1.3.2 Assessment Scope

The scope of this assessment is focused specifically on the compliance-related capabilities of AWS Backup, using the *Vault Lock* feature in either highly restrictive *Compliance* mode or less restrictive *Governance* mode.

Note: When less restrictive *Governance* mode controls are applied, procedural controls and monitoring are required to scrutinize actions taken by administrators, who have the ability to remove/delete *Vault Lock* from the Backup Vault and then shorten or remove retention controls and prematurely delete Recovery Points, which may contain required records.

The assessment scope includes both: (1) standard (non-air-gapped) Backup Vault owned and managed by the regulated entity and (2) logically air-gapped Backup Vault that AWS Backup owns and manages, which is outside of the regulated entity's control.

NOTE:

- ▶ The scope of this assessment excludes the AWS Backup *continuous backups* feature.
- ▶ This Compliance Assessment Report excludes all AWS Services not on the list of supported [Backup Resources](#).

2 • Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)

This section presents Cohasset's assessment of the functionality of Amazon Web Services (AWS) Backup, for compliance with the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2), as well as describes how the solution supports the regulated entity in meeting the audit system requirement of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

For each compliance requirement described in this section, this assessment is organized as follows:

- **Compliance Requirement** – Excerpt of relevant regulatory requirement in SEC Rules 17a-4(f) and 18a-6(e) and Cohasset's interpretation of the specific requirement
 - ◆ Both SEC Rules 17a-4(f) and 18a-6(e) are addressed in this section, since the electronic recordkeeping system requirements (principles, controls and testable outcomes) are the same, though the Rules specify their respective regulations and regulators and include semantic differences.
- **Compliance Assessment** – Summary statement assessing compliance of AWS Backup
- **AWS Backup Capabilities** – Description of assessed functionality
- **Additional Considerations** – Additional clarification related to meeting the specific requirement

The following sections document Cohasset's assessment of the capabilities of AWS Backup, as described in Section 1.3, *AWS Backup Overview and Assessment Scope*, relative to the enumerated requirements of SEC Rules 17a-4(f) and 18a-6(e).

2.1 Record and Audit Trail

2.1.1 Compliance Requirement

This regulatory requirement, adopted with the 2022 Rule amendments, allows regulated entities to use a combination of electronic recordkeeping systems, with each system meeting either (a) the record and audit-trail requirement, as described in this section or (b) the non-rewriteable, non-erasable record format requirement, as explained in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*.

This record and audit-trail requirement is designed to allow regulated entities to use business-purpose electronic recordkeeping systems to achieve the required outcome, without specifying a particular technology.

SEC 17a-4(f)(2)(i)(A) and 18a-6(e)(2)(i)(A):

Preserve a record for the duration of its applicable retention period in a manner that maintains a complete time-stamped audit trail that includes:

- (1) All modifications to and deletions of the record or any part thereof;
- (2) The date and time of actions that create, modify, or delete the record;
- (3) If applicable, the identity of the individual creating, modifying, or deleting the record; and
- (4) Any other information needed to maintain an audit trail of the record in a way that maintains security, signatures, and data to ensure the authenticity and reliability of the record and will permit re-creation of the original record if it is modified or deleted

The SEC explains that this requirement to retain the record and its complete time-stamped audit trail promotes the authenticity and reliability of the records by requiring the electronic recordkeeping system to achieve the testable outcome of reproducing the original record, even if it is modified or deleted during the required retention period, without prescribing how the system meets this requirement.

*[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*⁶ [emphasis added]

For clarity, the record and audit-trail requirement applies only to the final records required by regulation.

*[T]he audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6.*⁷ [emphasis added]

2.1.2 Compliance Assessment

In this report, Cohasset has not assessed AWS Backup in comparison to this requirement of the SEC Rules.

For enhanced control, a business-purpose electronic recordkeeping system may store records and complete time-stamped audit trails on AWS Backup, with the features and controls described in Sections 2.2 through 2.6 of this report.

Reminder: This requirement pertains to the regulated entity's business-purpose electronic recordkeeping system, when configured to retain the record and its complete time-stamped audit trail. This requirement is an alternative to the more stringent non-rewriteable, non-erasable record format requirement (i.e., write-once, read-many or WORM requirement), which is assessed in Section 2.2.

2.2 Non-Rewriteable, Non-Erasable Record Format

2.2.1 Compliance Requirement

This regulatory requirement was first adopted in 1997. In the 2022 Rule amendments, regulated entities are allowed to use a combination of electronic recordkeeping systems, to comply with each system meeting either (a) the non-rewriteable, non-erasable record format requirement described in this section or (b) the complete time-stamped record audit-trail requirement described in Section 2.1, *Record and Audit Trail*.

The SEC further clarifies that the previously issued interpretations are extant. Therefore, records must be preserved in a non-rewriteable, non-erasable format that prevents overwriting, erasing, or otherwise altering records during the required retention period, which may be accomplished by any combination of hardware and software integrated controls.

The 2003 interpretation clarified that the WORM requirement does not mandate the use of optical disks and, therefore, a broker-dealer can use "an electronic storage system that prevents the overwriting, erasing or otherwise altering of a

SEC 17a-4(f)(2)(i)(B) and 18a-6(e)(2)(i)(B):

Preserve the records exclusively in a non-rewriteable, non-erasable format

⁶ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

⁷ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

record during its required retention period through the use of integrated hardware and software [control] codes." The 2019 interpretation further refined the 2003 interpretation. In particular, it noted that the 2003 interpretation described a process of integrated software and hardware codes and clarified that "a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule."

In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance.⁸ [emphasis added]

Moreover, records must be preserved beyond established retention periods when certain circumstances occur, such as a subpoena or legal hold:

[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.⁹ [emphasis added]

2.2.2 Compliance Assessment

It is Cohasset's opinion that the functionality of AWS Backup, when the *Vault Lock* retention controls are set to either highly restrictive *Compliance* mode or less restrictive *Governance* mode, meets this SEC requirement to retain records in non-rewriteable, non-erasable format for the applied time-based¹⁰ retention periods and legal holds, when (a) properly configured, as described in Section 2.2.3 and (b) the additional considerations described in Section 2.2.4 are satisfied.

Reminder: This non-rewriteable, non-erasable record format requirement is a more stringent alternative to the complete time-stamped audit-trail requirement, which is addressed in Section 2.1.

2.2.3 AWS Backup Capabilities

This section describes the functionality of AWS Backup that directly pertains to this SEC requirement to preserve electronic books and records in a non-rewriteable, non-erasable format, for the required retention period and any applied legal holds.

2.2.3.1 Overview

- ▶ Records, together with associated metadata, are retained in Recovery Points stored in Backup Vaults.
- ▶ To meet the non-rewriteable, non-erasable record format requirement of the Rules, the Recovery Point containing records requiring time-based retention must:
 - Be stored in a Backup Vault with *Vault Lock* feature enabled (True) and set to either *Compliance* (highly restrictive) or *Governance* (less restrictive),

⁸ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

⁹ Electronic Storage of Broker-Dealer Records, Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25283, (May 12, 2003) (2003 Interpretative Release).

¹⁰ Time-based retention periods require records to be retained for a fixed contiguous period of time from the creation or storage timestamp.

- have an appropriate *DeleteAfterDays* applied to the Recovery Point, and
- ▶ Optionally, one or more Legal Holds may be set on the Recovery Point, which suspends deletion eligibility until the *Legal Hold* is released.
- ▶ The following table summarizes the integrated retention controls applied to Recovery Points (and the associated records and record metadata), when the Recovery Point is stored in a Backup Vault with *Vault Lock* configured in *Compliance* or *Governance* mode. See the subsections following this *Overview*, for information on configuring the retention features and the resulting integrated controls.

	<i>Vault Lock</i>, in highly restrictive <i>Compliance</i> mode	<i>Vault Lock</i>, in less restrictive <i>Governance</i> mode
Protecting record content and immutable metadata attributes	• A Recovery Point is a point-in-time snapshot of the Backup Resource and is inherently read-only, and therefore, immutable. • The Recovery Point <u>cannot</u> be modified or overwritten for its lifespan. • Renaming Recovery Points and the Backup Vault is <u>prohibited</u>.	
Restricting changes to applied retention controls	• The <i>Vault Lock</i> enabled (True) <u>cannot</u> be reset or removed. • <i>Compliance</i> mode and Min/Max retention period configurations <u>cannot</u> be modified or removed from the <i>Vault Lock</i>. • The total retention period (<i>DeleteAfterDays</i>) applied to Recovery Points in a <i>Locked Vault</i> <u>cannot</u> be reduced, removed, or extended. • See Section 2.2.3.3, <i>Record Definition and Controls</i>.	• Permissioned users can: ○ Remove <i>Vault Lock</i>, which sets <i>Vault Lock</i> enabled to False; this removes the <i>Vault Lock Governance</i> mode controls. ○ Change <i>Vault Lock</i> from <i>Governance</i> to <i>Compliance</i> mode. ○ Modify or remove the Min/Max retention period configurations. ○ Remove <i>Vault Lock</i>, and thereafter, modify the retention period applied to a Recovery Point. (Optionally, reinstate the <i>Vault Lock</i> configurations.) Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions taken to remove the <i>Vault Lock</i> and change retention controls. • See Section 2.2.3.3, <i>Record Definition and Controls</i>.
Applying and removing Legal Holds	• One or more Legal Holds may be applied to a Recovery Point, which prevents the overwrite or deletion until associated Legal Holds are released. • See Section 2.2.3.4, <i>Legal Holds (Temporary Holds)</i>.	
Restricting deletion of records and Backup Vault	• Deleting a Recovery Point is prohibited by users and by lifecycle actions until both the total retention period is expired and any Legal Holds are released.	Permissioned users can remove the <i>Vault Lock</i> and, thereafter, delete a Recovery Point, even if the total retention period for the Recovery Point has not expired, provided it is not subject to a Legal Hold. Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions taken to remove the <i>Vault Lock</i> and delete Recovery Points.
	• Backup Vault cannot be deleted until it is empty. Accordingly, deleting a Backup Vault to effectuate premature deletion of Recovery Points is <u>prohibited</u>. • See Section 2.2.3.5, <i>Deletion Controls</i>.	

2.2.3.2 AWS Backup Retention-related Configurations

- The following table describes AWS Backup retention-related configurations, including the *Vault Lock* feature. See Section 2.2.3.3, *Record Definition and Retention Controls*, for details on the resulting integrated controls applied to records.

	Backup Vault, IAM Policy and Lifecycle Policy Configurations related to AWS Backup Vault Lock
Backup Vault Name	The Backup Vault name must be unique within the AWS Region and account.
Configuring the Vault Lock feature	The following <i>Vault Lock</i> configurations are required for each new or existing Backup Vault intended to retain Recovery Points with required records: - The <i>Vault Lock</i> feature must be enabled (True). - The mode must be configured: - Highly restrictive <i>Compliance</i> mode is set when the <i>Compliance mode start date</i> is met or is in the past. - Before the <i>Compliance mode start date</i> is met, <i>Vault Lock</i> is in <i>Governance</i> mode. - If the Backup Vault is created as a logical air-gapped Vault, <i>Compliance</i> mode is effective <i>immediately</i>. A logical air-gapped vault is a Backup Vault in an account that AWS Backup owns and manages, which is outside of the regulated entity's control. - Less restrictive <i>Governance</i> mode is set when the <i>Compliance mode start date</i> is null or is in the future. <u>Note</u>: <i>Vault Lock</i> may be transitioned from <i>Governance</i> to <i>Compliance</i> mode by setting the <i>Compliance mode start date</i> and waiting for this date to be met. - Optionally, Minimum and Maximum retention periods (Min/Max range) may be configured for the <i>Vault Lock</i>. - When a Recovery Point is written, the total retention period must be within the configured Min/Max range; otherwise, the Recovery Point will be rejected, and an error will be reported.
SCP permissions	- Service control policies (SCPs) are organization-level permission guardrails in AWS Organizations. Rather than granting permissions, an SCP defines the maximum permissions allowed for member accounts. <u>Note</u>: SCPs do not affect the management account. - Optionally, configure an SCP to disallow any role in any member account from removing <i>Vault Lock</i>, to set additional procedural controls to manage when <i>Vault Lock</i> in <i>Governance</i> mode can be removed, after which Recovery Points may be deleted, even if the total retention period has not been met.
IAM Roles	When a Backup Vault is configured with <i>Vault Lock</i> in <i>Governance</i> mode, designated roles (users) can be granted or denied permissions to call the APIs that delete (<i>DeleteBackupVaultLockConfiguration</i>) or modify (<i>PutBackupVaultLockConfiguration</i>) the <i>Vault Lock</i> configuration, provided these actions are not restricted by Service Control Policies (SCPs).
Backup Plan Retention	- Each backup plan name must be unique within the same AWS account and Region and may include only alphanumeric characters, dashes, underscores, and periods. - A backup plan must include one or more backup rules. Each rule defines: - The backup schedule, including frequency (e.g., hourly, daily, monthly, yearly) and applicable days of the week. - The target Backup Vault where Recovery Points will be stored. - A lifecycle policy that specifies the total retention period (<i>DeleteAfterDays</i>) after which recovery points are automatically deleted. - The lifecycle policy applies only to new recovery points created in the backup vault.

2.2.3.3 Record Definition and Controls

- ▶ AWS Backup Vault contains Recovery Points, which are point-in-time snapshots of the Backup Resource and are inherently read-only and therefore immutable. Specifically, each Recovery Point is comprised of a collection of records and associated record metadata.
 - Immutable metadata applied to the Recovery Point, includes, but is not limited to: Backup Vault Name, Amazon Resource Name (ARN), backup date/time, and user-defined custom metadata (key-value pairs).
 - Mutable system metadata for the Recovery Point includes the Legal Hold indicator and tags.
- ▶ When *Vault Lock* is enabled (True), integrated controls protect the Recovery Points from certain actions. The following table describes the integrated retention controls applied to each Recovery Point stored in a Backup Vault with *Vault Lock* in *Compliance* and *Governance* modes.

	<i>Vault Lock</i>, in highly restrictive <i>Compliance</i> mode	<i>Vault Lock</i>, in less restrictive <i>Governance</i> mode
Protecting record content and immutable metadata	• A Recovery Point is a point-in-time snapshot of the resource and is inherently read-only, thus immutable. While the Recovery Point cannot be modified, certain metadata attributes (i.e., Backup Vault Name, ARN, and backup timestamp) are immutable. Other metadata attributes (i.e., tags and Legal Hold status) are mutable. • Each Recovery Point is protected from deletion, by users and by lifecycle policies, until the total retention period (<i>DeleteAfterDays</i>) for the Recovery Point has expired and any associated Legal Holds have been released.	
Modifying or removing retention controls	For a <i>Vault Lock</i> enabled (True) in <i>Compliance</i> mode: • <i>Vault Lock</i> <u>cannot</u> be reset or removed. • <i>Compliance</i> mode <u>cannot</u> be changed or removed. • The Min/Max retention period configuration <u>cannot</u> be changed or removed. • The total retention period on a Recovery Point <u>cannot</u> be changed or removed. Accordingly, <i>Compliance</i> mode is designed to ensure that <i>Vault Lock</i> and Recovery Point retention controls are not circumvented by any user or process. Important Notes: • A <u>logical air-gapped</u> Backup Vault is configured in <i>Compliance</i> mode, which is effective <u>immediately</u>. A <u>logical air-gapped</u> Backup Vault is a type of Backup Vault in an account that AWS Backup owns and manages, which is outside of the regulated entity's control. • For a <u>non-air-gapped</u> Backup Vault, while the <i>Compliance</i> mode start date is in the future, the <i>Vault Lock</i> is in <i>Governance</i> mode; see the controls described in the column for <i>Vault Lock</i>, in less restrictive <i>Governance</i> mode.	For a <i>Vault Lock</i> enabled (True) in <i>Governance</i> mode, permissioned users can: • Change the <i>Vault Lock</i> mode from <i>Governance</i> to <i>Compliance</i> mode by setting the <i>Compliance mode start date</i>, via the Application Programming Interface (API), then waiting for the date to be met. • Modify or remove the Min/Max retention period configuration. • Remove the <i>Vault Lock</i>, and thereafter, modify or remove the total retention period applied to a Recovery Point. Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions taken to remove the <i>Vault Lock</i> retention controls. For monitoring, CloudTrail logs events related to setting, modifying or removing the <i>Vault Lock</i> configuration and modifying or removing the Recovery Point total retention period.
Applying and removing Legal Holds	• One or more Legal Holds may be applied to a Recovery Point which prevents the overwrite or deletion of the Recovery Point until all associated Legal Holds are released. • If a Legal Hold attribute is applied, attempts to delete the Recovery Point are prohibited, whether <i>Vault Lock</i> is set to <i>Compliance</i> or <i>Governance</i> mode. • See Section 2.2.3.4, <i>Legal Holds (Temporary Holds)</i>.	

	<i>Vault Lock, in highly restrictive Compliance mode</i>	<i>Vault Lock, in less restrictive Governance mode</i>
Restricting deletion of records and Backup Vaults	Each Recovery Point is protected from deletion, by users and by lifecycle policies, when the total retention period for the Recovery Point has <u>not</u> expired.	Permissioned users can remove the <i>Vault Lock</i> in <i>Governance</i> mode, and thereafter, a Recovery Point can be deleted by user action, even if the total retention period for the Recovery Point has <u>not</u> expired, provided it is not subject to a Legal Hold. Accordingly, procedural controls and monitoring are required to scrutinize privileged administrator actions taken to remove the <i>Vault Lock</i> retention controls. For monitoring, CloudTrail logs events related to setting, modifying or removing the <i>Vault Lock</i> configuration and modifying or removing the Recovery Point total retention period.
	A Backup Vault <u>cannot</u> be deleted until the Backup Vault is empty, whether <i>Vault Lock</i> is set to <i>Compliance</i> or <i>Governance</i> mode. Accordingly, deleting a Backup Vault to effectuate premature deletion of Recovery Points is <u>prohibited</u>.	
Copying records	A Recovery Point may be copied to a different Backup Vault, resulting in the creation of a new (separate) Recovery Point with its own unique metadata, including the assignment of a new <i>DeleteAfterDays</i>. The original Recovery Point and its metadata remain unaltered, in the original Backup Vault, until deletion.	
Moving records	A Recovery Point <u>cannot</u> be moved between Backup Vaults.	
Destructive Restores	A Recovery Point <u>cannot</u> be restored to the protected AWS resource; therefore, preventing an overwrite of existing data.	

2.2.3.4 Legal Holds (Temporary Holds)

When a record is subject to preservation requirements for subpoena, litigation, regulatory investigation or other special circumstances, it must be preserved immutably, (i.e., any deletion, modification or overwrite must be prohibited) until the hold is released.

	<i>Legal Hold Features for Vault Lock</i>
Creating a Legal Hold	- Legal Holds are created by selecting the Resource, Recovery Points and date range subject to the hold. - Optionally, Legal Hold tags may be applied to categorize and facilitate managing the hold. <u>Note</u>: Multiple Legal Holds may be applied to a single Recovery Point.
Removing Legal Holds	- Legal Holds are released by retrieving the Legal Hold (viewing the Hold details) and selecting and confirming the release Legal Hold option. - When a Legal Hold is released, it no longer mandates preservation of the associated Recovery Points, though other active Legal Holds may apply to the Recovery Point, mandating retention. - Additionally, any other retention controls continue to apply to the Recovery Point.
Legal Hold protections	- Once the Legal Hold is applied, it cannot be modified, it can only be released. - While an active Legal Hold is applied to a Recovery Point, overwriting and deleting the Recovery Point is prohibited, even if the associated total retention period has expired. <i>Legal Holds operate independent of Vault Lock. Compliance or Governance mode controls do not affect a Recovery Point's Legal Hold status. When a Legal Hold attribute is applied, attempts to delete the Recovery Point or Backup Vault are prohibited.</i> - The Legal Hold status can be verified in the Legal Hold user interface, which displays <i>Hold title, Status, Description, Legal Hold ID, Creation Date</i> and <i>Release Date</i>.

2.2.3.5 Deletion Controls

- ▶ A Recovery Point in a Backup Vault configured with *Vault Lock* in either highly restrictive *Compliance* mode or less restrictive *Governance* mode, together with its metadata, is eligible for deletion when (a) its *DeleteAfterDays* has expired (is in the past) and (b) any associated Legal Holds are released. However, privileged deletions may be performed when *Vault Lock* in less restrictive *Governance* mode is removed from the Backup Vault
- ▶ The following table summarizes actions taken to delete Recovery Points.

	Deletion in highly restrictive <i>Compliance</i> mode	Deletion in less restrictive <i>Governance</i> mode
Deleting Recovery Points	• The Recovery Point will be systematically deleted when the total retention period has passed (expired), if the Recovery Point is <u>not</u> subject to an active Legal Hold. • The deletion of eligible Recovery Points does <u>not</u> impact the recoverability of any Recovery Points still under retention. • If the user attempts to delete a Recovery Point with an active Legal Hold, an error is logged and the action is rejected. • If the user attempts to delete a Recovery Point, when the total retention period has <u>not</u> passed (expired), an error is logged and the action is rejected.	• Privileged delete of Recovery Points may be performed by authorized users following a multi-step process: ○ Remove <i>Vault Lock</i> in <i>Governance</i> mode. ○ Delete Recovery Points, whether or not the total retention period is in the past, as long as a Legal Hold is not applied. ○ Optionally, reinstate <i>Vault Lock</i> in <i>Governance</i> mode.
Deleting Backup Vaults	• Backup Vault cannot be deleted until the Backup Vault is empty. Accordingly, deleting a Backup Vault to effectuate premature deletion of Recovery Points is <u>prohibited</u>.	
Restricting snapshot restores	• A Recovery Point <u>cannot</u> be restored to the protected AWS resource; therefore, preventing an overwrite of existing data.	

2.2.3.6 Security

- ▶ AWS is designed to meet Enterprise security and compliance requirements.
 - Service control policies (SCPs) are organization-level permission guardrails applied across an AWS organization. SCPs define the maximum permissions allowed for member accounts. Note: SCPs does not apply to the management account.
 - IAM roles provide temporary permissions without relying on long-term credentials. The permissions (privileges) granted to a role are determined by the policies attached to it, which specify the actions the role is allowed to perform.
 - AWS data centers maintain appropriate physical security and environmental controls that are tested annually, in accordance with the SSAE 18 standard, to validate the effectiveness of protection.

- ▶ AWS protects data in transit using SSL/TLS, as well as at-rest (data stored on disks in AWS data centers) using a variety of encryption methods.
- ▶ AWS Backup supports encryption for Recovery Points and copies of the backups.
- ▶ Each logically air-gapped Backup Vault is encrypted with an AWS owned key, by default. The encryption key type information is visible through AWS Backup APIs and console.
- ▶ Access to AWS Backup requires credentials, which must have permissions to access AWS resources, such as Backup Vaults, Recovery Points, Backup Plans and Legal Holds. Moreover, Recovery Points created by AWS Backup cannot be deleted using the source service (such as Amazon EFS). Instead, deletion eligible Recovery Points can be deleted only using AWS Backup services.

2.2.3.7 Clock Management

To meet the requirements of the Rule, Cohasset asserts that every system clock must synchronize to an external time server, e.g., a network time protocol (NTP) clock.

- ▶ The AWS Backup system clocks regularly and frequently check the time of an external time source and resynchronizes. Neither end users nor system administrators have the ability to manipulate the system time. These controls prevent any inadvertent or intentional administrative modifications of the time clock, which could allow for premature deletion of Recovery Points.

2.2.4 Additional Considerations

In addition, for this non-rewriteable, non-erasable record format requirement, the regulated entity is responsible for:

- ▶ Properly configuring Backup Vaults used to store Recovery Points required to be compliant with the Rule:
 - Enabling (True) the *Vault Lock* feature and setting *Vault Lock* to highly restrictive *Compliance* mode or less restrictive *Governance* mode,
 - ◆ When configuring *Compliance* mode, for a non-air-gapped Backup Vault, configuring a *Compliance mode start time* (grace time) that expires before the Backup Vault stores Recovery Points containing required records.
 - ◆ AWS Backup provides a grace period (time between Vault Lock creation and *Compliance* mode start date), which allows organizations to validate their configuration before *Compliance* mode becomes irrevocable. AWS recommends setting a grace period that provides sufficient time for testing while ensuring *Compliance* mode is active before storing required records.
 - ◆ Cohasset suggests storing required records within 24 hours of creation in a properly configured Backup Vault where the grace period has lapsed. Therefore, during the test period (i.e., when the grace period has not yet lapsed), Cohasset recommends storing required records within 24 hours in a properly configured location that meets the requirements of the Rules.
 - Configuring the *MaxRetentionDays*, and *MinRetentionDays* to establish appropriate guardrails for the total retention period applied a Recovery Point.
- ▶ Configuring Backup Plans with the appropriate total retention period (*DeleteAfterDays*).

- ▶ Creating and applying Legal Holds, as appropriate to preserve Recovery Points needed for legal matters, government investigations, external audits and other similar circumstances. Releasing Legal Holds, when appropriate.
- ▶ Ensuring that Recovery Points required to comply with the Rule are stored in the properly configured Backup Vault after the grace time has expired, which establishes a *Vault Lock* in *Compliance* mode that cannot be changed or removed. Alternatively, when using *Governance* mode, ensuring procedural controls and monitoring are required to scrutinize privileged administrator actions taken to modify or remove *Vault Lock* retention controls.
- ▶ Storing records requiring event-based¹¹ retention periods in a separate compliant system or otherwise planning for event-based retention, since AWS Backup does not currently support event-based retention periods.
- ▶ Granting only the minimum necessary permissions (via IAM roles and, if needed, organization-level SCP guardrails) to users who must update or remove *Governance* mode Vault Lock, (e.g., limit permissions to *PutBackupVaultLockConfiguration* or *DeleteBackupVaultLockConfiguration*). Removing the permissions immediately after the changes are complete.
- ▶ Generating and storing Recovery Points containing required records within 24 hours to help ensure accurate and complete records are captured. Subsequent Recovery Points may include prior day's records; however, the longer timespan from record creation to Recovery Point capture may result in the Recovery Point containing records that have been changed or missing records that have been deleted.

Additionally, the regulated entity is responsible for (a) maintaining its account in good standing and paying for appropriate services to allow records to be retained until the applied total retention periods and holds have expired or until the records have been transferred to another compliant storage system, (b) authorizing user privileges, and (c) maintaining appropriate technology, encryption keys, and other information and services needed to retain the records.

2.3 Record Storage Verification

2.3.1 Compliance Requirement

The electronic recordkeeping system must automatically verify the completeness and accuracy of the processes for storing and retaining records electronically, to ensure that records read from the system are precisely the same as those that were captured.

This requirement includes both quality verification of the recording processes for storing records and post-recording verification processes for retaining complete and accurate records.

SEC 17a-4(f)(2)(ii) and 18a-6(e)(2)(ii):

Verify automatically the completeness and accuracy of the processes for storing and retaining records electronically

¹¹ Event-based retention periods require records to be retained indefinitely until a specified condition is met (e.g., a contract expires or an employee terminates), after which the record is retained for a fixed final retention period.

2.3.2 Compliance Assessment

Cohasset affirms that the functionality of AWS Backup meets this SEC requirement for complete and accurate recording of records and post-recording verification processes, when properly configured as described in Section 2.3.3 and the additional considerations identified in Section 2.3.4 are satisfied.

2.3.3 AWS Backup Capabilities

The recording and post-recording verification processes of AWS Backup are described below.

2.3.3.1 Recording Process

- ▶ AWS Backup uses a combination of integrity checks, including inter-component and inter-step cyclic redundancy checks (CRCs) along with write-error detection and correction mechanisms, are designed to ensure Recovery Points are written accurately and with high quality across supported storage technologies.
- ▶ Upon backup completion, the integrity of the Recovery Point data is validated by comparing a SHA256 summary checksum of the full primary resource against AWS Backup's representation of the resource.

2.3.3.2 Post-Recording Verification Process

- ▶ AWS Backup is designed to use the AWS global infrastructure to replicate Recovery Points across multiple Availability Zones for durability of 99.999999999% (11 nines) in any given year.
- ▶ AWS Backup Audit Manager provides evidence of AWS Backup activities via automatically generated reports and configurable compliance controls.
- ▶ AWS regularly verifies the integrity of data stored using checksums. If AWS detects data corruption, it is repaired using redundant data.
- ▶ AWS computes checksums on data transmitted over the network to detect any corruption during restore operations.

2.3.4 Additional Considerations

The source system is responsible for storing the complete contents of the required records and AWS Backup validates the accuracy of the recording process for the snapshot of the source system.

2.4 Capacity to Download and Transfer Records and Location Information

2.4.1 Compliance Requirement

This requirement calls for an adequate capacity to readily download records and information needed to locate the record in both a:

- Human readable format that can be naturally read by an individual, and

SEC 17a-4(f)(2)(iv) and 18a-6(e)(2)(iv):

Have the capacity to readily download and transfer copies of a record and its audit trail (if applicable) in both a human readable format and in a reasonably usable electronic format and to readily download and transfer the information needed to locate the electronic record, as required by the staffs of the Commission, [and other pertinent regulators] having jurisdiction over the [regulated entity]

- Reasonably usable electronic format that is compatible with commonly used systems for accessing and reading electronic records.

The downloaded records and information needed to locate the records (e.g., unique identifier, index, or properties) must be transferred to the regulator, in an acceptable format.

Further, this requirement to download and transfer the complete time-stamped audit trail applies only when this alternative is utilized; see Section 2.1, *Record and Audit Trail*.

2.4.2 Compliance Assessment

Cohasset asserts that the functionality of AWS Backup meets this SEC requirement to maintain capacity to readily download and transfer the records and information used to locate the records, when the additional considerations described in Section 2.4.4 are satisfied.

2.4.3 AWS Backup Capabilities

The following capabilities relate to the capacity to readily search, access, download, and transfer records and the information needed to locate the records.

- ▶ Recovery Points and metadata (index) attributes may be listed using the AWS Backup console. The Recovery Points may be viewed, either: (1) for a particular AWS resource or (2) all Recovery Points in a single Backup Vault.
- ▶ To facilitate findability, AWS Backup serializes each Recovery Point through a combination of: Backup Vault Name, Amazon Resource Name (ARN), and backup date/time. These attributes are immutable for the lifespan of the snapshot.
- ▶ Recovery Points may be restored using specific parameters dependent on the resource type. For each restore, a job is created with a unique job ID. Once the Recovery Point is restored, the applicable records can be extracted using local resources and provided to the examining authority.
- ▶ AWS Backup stores all Recovery Points with availability equivalent to standard Amazon S3. Access to backed-up data is performed exclusively through AWS Backup, which provides 99.95% availability. AWS Backup is designed to provide sufficient hardware and software capacity to support timely access to records and their associated metadata. In addition, AWS Backup uses redundant storage media, networking, and power to reduce the risk of data unavailability due to infrastructure outages

2.4.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing, (b) authorizing user privileges, (c) maintaining appropriate technology and resource capacity, encryption keys, and other information and services needed to use AWS Backup to readily access, download, and transfer the records and the information needed to locate the records, and (d) providing requested information to the regulator, in the requested format.

2.5 Record Redundancy

2.5.1 Compliance Requirement

The intent of this requirement is to retain a persistent alternate source to reestablish an accessible, complete and accurate record, should the original electronic recordkeeping system be temporarily or permanently inaccessible.

The 2022 final Rule amendments adopted two redundancy options, paragraphs (A) or (B).

- ▶ The intent of paragraph (A) is:

*[B]ackup electronic recordkeeping system must serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible because, for example, it is impacted by a natural disaster or a power outage.*¹² [emphasis added]

- ▶ The intent of paragraph (B) is:

*[R]edundancy capabilities that are designed to ensure access to Broker-Dealer Regulatory Records or the SBS Entity Regulatory Records must have a level of redundancy that is at least equal to the level that is achieved through using a backup recordkeeping system.*¹³ [emphasis added]

Note: The alternate source must meet “*the other requirements of this paragraph [(f)(2) or (e)(2)]*”, thereby disallowing non-persistent copies that are overwritten on a periodic basis, resulting in a much shorter retention period than the original.

2.5.2 Compliance Assessment

Cohasset upholds that the functionality of AWS Backup meets both paragraphs (A) and (B) of this SEC requirement by retaining a persistent duplicate copy of the records or alternate source to reestablish the records, when (a) properly configured as described in Section 2.5.3 and (b) the additional considerations described in Section 2.5.4 are satisfied.

2.5.3 AWS Backup Capabilities

The two options for meeting the record redundancy requirement are described in the following subsections.

2.5.3.1 Redundant Set of Records

- ▶ Optionally, the regulated entity can configure:
 - AWS Backup to automatically copy Recovery Points across AWS accounts within an organization or to multiple AWS Regions as part of a defined backup plan, ensuring controlled redundancy and geographic separation.

SEC 17a-4(f)(2)(v) and 18a-6(e)(2)(v):

(A) Include a backup electronic recordkeeping system that meets the other requirements of this paragraph [(f) or (e)] and that retains the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and in accordance with this section in a manner that will serve as a redundant set of records if the original electronic recordkeeping system is temporarily or permanently inaccessible; or

(B) Have other redundancy capabilities that are designed to ensure access to the records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and this section

¹² 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

¹³ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66421.

- AWS Backup with a logically air-gapped Backup Vault, a premium vault type owned and managed by AWS that provides additional access restrictions and enhanced security controls. Each logically air-gapped Backup vault is encrypted using an AWS-owned KMS (Key Management Service) key by default and is automatically configured with AWS Backup *Vault Lock* in compliance mode.
- Backup status and plan compliance can be continuously monitored through the AWS Backup console to verify that all Recovery Points remain protected.

2.5.3.2 Other Redundancy Capabilities

- Data is sharded and redundantly stored across multiple Availability Zones within an AWS Region. All writes are synchronously replicated across these geographically separated facilities.
- The underlying multi-AZ storage system is designed to provide 99.999% availability, even in the event of an Availability Zone disruption.
- Over the lifespan of the Recovery Point, AWS Backup continuously monitors integrity and automatically regenerates accurate replicas if any shard becomes lost or corrupted.

2.5.4 Additional Considerations

In addition, for this requirement, the regulated entity is responsible for: (a) maintaining its account in good standing and (b) maintaining the technology, storage capacity, encryption keys, and other information and services needed to use AWS Backup and permit access to the redundant records.

2.6 Audit System

2.6.1 Compliance Requirement

For electronic recordkeeping systems that comply with the non-rewriteable, non-erasable format requirement, as stipulated in Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, the Rules require the regulated entity to maintain an audit system for accountability (e.g., when and what action was taken) for both (a) inputting each record and (b) tracking changes made to every original and duplicate record. Additionally, the regulated entity must ensure the audit system results are available for examination for the required retention time period stipulated for the record.

The audit results may be retained in any combination of audit systems utilized by the regulated entity.

2.6.2 Compliance Assessment

Cohasset asserts that AWS Backup, in conjunction with the AWS CloudTrail, when enabled, supports the regulated entity's efforts to meet this SEC requirement for an audit system.

SEC 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii):

For a [regulated entity] operating pursuant to paragraph [(f)(2)(i)(B) or (e)(2)(i)(B)] of this section, the [regulated entity] must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to [§ 240.17a-3 or § 240.18a-5] and this section to the electronic recordkeeping system and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

(A) At all times, a [regulated entity] must be able to have the results of such audit system available for examination by the staffs of the Commission [and other pertinent regulators].

(B) The audit results must be preserved for the time required for the audited records

2.6.3 AWS Backup Capabilities

The regulated entity is responsible for an audit system, and compliance is supported by AWS Backup.

- ▶ For each Recovery Point, AWS Backup stores the (a) Backup Vault Name, Amazon Resource Name (ARN), and backup date/time. These attributes (a) are immutable, (b) uniquely identify each Recovery Point, (c) chronologically account for each Recovery Point, and (d) are retained for the same time period as the Recovery Point.
- ▶ Each Recovery Point is inherently immutable, meaning changes are disallowed.
- ▶ AWS Backup also provides AWS CloudTrail which is a highly configurable service that monitors and records API calls and user activity within an AWS account.
 - By default, management events within a given AWS Region are captured and immutably retained for 90 days. CloudTrail management events include operations such as creating or deleting Backup Vaults, enabling Vault Lock, and attempting to modify or remove Vault Lock settings.
 - ◆ Management event history is viewable with limited search and filter options via the CloudTrail console or via API (Application Programming Interface) and CLI (Command-Line Interface) commands.
- ▶ To retain CloudTrail data for longer than the default 90 days, AWS offers the following options:
 - *CloudTrail Lake event data stores* (i.e., managed data lakes, optimized for fast retrieval and analysis) can be configured to retain both management and data events, in addition to other types of data logs, from the current AWS Region or from all AWS Regions within an AWS account. Events stored in the data store may be retained for up to ten years, during which time the data is available for advanced queries. Query results can be saved to an S3 Bucket or downloaded to a CSV file for export to an external security information event management (SIEM) tool.
 - *CloudTrail "trails"* may be configured to capture management and data events and deliver them directly to an: (i) S3 Bucket, where they may be viewed and/or downloaded or (ii) external SIEM tool. Trails may be configured for a single AWS Region, multiple AWS Regions, or for an entire AWS Organization

2.6.4 Additional Considerations

The regulated entity is responsible for maintaining an audit system for inputting records and changes made to the records. In addition to relying on the immutable metadata, the regulated entity may utilize the AWS CloudTrail service. When relying on the AWS CloudTrail service, Cohasset recommends using either (a) the CloudTrail Lake event data store service which provides long-term, immutable retention of event data or (b) the CloudTrail trails service which allows for the export of audit events to a secure S3 Bucket or an external SIEM tool.

3 • Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)

This section contains a summary assessment of the functionality of AWS Backup, as described in Section 1.3, *AWS Backup Overview and Assessment Scope*, in comparison to CFTC electronic regulatory record requirements. Specifically, this section associates the features described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, with the principles-based requirements of CFTC Rule 1.31(c)-(d).

In the May 30, 2017, adopting release, the CFTC amended its recordkeeping obligations to *"modernize and make technology neutral the form and manner in which regulatory records must be kept"*. The CFTC amendments replaced previous requirements to retain records in a non-rewriteable, non-erasable record format (a.k.a., WORM) with a less-prescriptive, principles-based approach to recordkeeping.

*Consistent with the Commission's emphasis on a less-prescriptive, principles-based approach, [the final rule] 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.*¹⁴ [emphasis added]

In the October 12, 2022, adopting release, the SEC recognizes the CFTC principles-based requirements and asserts a shared objective of ensuring the authenticity and reliability of regulatory records. Moreover, the SEC contends that its two compliance alternatives for electronic recordkeeping, i.e., (i) record and complete time-stamped audit trail and (ii) non-rewriteable, non-erasable record format, a.k.a. WORM, are more likely to achieve this objective because each alternative requires the specific and testable outcome of accessing and producing modified or deleted records, in their original form, for the required retention period.

*The proposed amendments to Rules 17a-4 and 18a-6 and the [CFTC] principles-based approach recommended by the commenters share an objective: ensuring the authenticity and reliability of regulatory records. However, the audit-trail requirement is more likely to achieve this objective because, like the existing WORM requirement, it sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.*¹⁵ [emphasis added]

Cohasset's assessment, enumerated in Section 2, pertains to the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2), including requirements for non-rewriteable, non-erasable record format. Specifically, Cohasset assesses AWS Backup with the *Vault Lock* feature enabled and used with either:

- *Locked* mode, a highly restrictive option that applies integrated controls to protect against overwrites and modifications and enforces strict retention controls, or
- *Unlocked* mode, a less restrictive option that protects against overwrites and modifications but requires administrative procedures and monitoring to ensure compliant retention, since administrators are allowed to shorten or remove retention controls.

¹⁴ 2017 CFTC Recordkeeping Requirements Adopting Release, 82 FR 24482.

¹⁵ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

See Section 2.2, *Non-Rewriteable, Non-Erasable Record Format*, for information on the *Vault Lock* controls.

In the following table, Cohasset correlates the specific *principles-based* CFTC requirements for electronic records with the functionality of AWS Backup when the *Vault Lock* feature is properly configured and applied to meet SEC requirements. The first column enumerates requirements of the CFTC regulation. The second column provides Cohasset's analysis and opinion regarding the capabilities of AWS Backup, relative to these requirements.

CFTC 1.31(c)-(d) Regulation [emphasis added]	Compliance Assessment Relative to CFTC 1.31(c)-(d)
<i>(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:</i> <i>(1) Generally. Each records entity shall retain regulatory records in a form and manner that ensures the <u>authenticity and reliability</u> of such regulatory records in accordance with the Act and Commission regulations in this chapter.</i> <i>(2) Electronic regulatory records. Each records entity maintaining electronic regulatory records shall establish appropriate systems and controls that ensure the <u>authenticity and reliability</u> of electronic regulatory records, including, without limitation:</i> <i>(i) Systems that maintain the security, signature, and data as necessary to ensure the <u>authenticity</u> of the information contained in electronic regulatory records and to monitor compliance with the Act and Commission regulations in this chapter;</i>	It is Cohasset's opinion that the CFTC requirements in (c)(1) and (c)(2)(i), for records¹⁶ with time-based retention periods, are met by the functionality of AWS Backup, with the <i>Vault Lock</i> feature applied in either <i>Compliance</i> or <i>Governance</i> mode. The functionality that supports retention, authenticity and reliability of electronic records is described in the following sections of this report: • Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i> • Section 2.3, <i>Record Storage Verification</i> • Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i> • Section 2.6, <i>Audit System</i> Further, for <u>records stored electronically</u>, the CFTC definition of <u>regulatory records</u> in 17 CFR § 1.31(a) includes information to access, search and display records, as well as data on records creation, formatting and modification: <u>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:</u> <u>(i) Any data necessary to access, search, or display any such books and records; and</u> <u>(ii) All data produced and stored electronically describing how and when such books and records were created, formatted, or modified.</u> [emphasis added] AWS Backup retains immutable metadata (e.g., Backup Vault Name, Amazon Resource Name (ARN), and backup timestamp) as an integral component of the Recovery Points, and, therefore, these attributes are subject to the same retention controls as the associated Recovery Point. These immutable attributes support both (a) access, search and display of the Recovery Point and associated records and (b) audit system and accountability for inputting the Recovery Point. Further, mutable metadata stored for Recovery Points include retention controls and legal hold attributes. The most recent values of mutable metadata are retained for the same time period as the associated Recovery Points. Further, AWS Backup in conjunction with the CloudTrail service, tracks management and data audit events and provides storage options for retaining this additional audit system information for the same time

¹⁶ The regulated entity is responsible for retaining and managing any additional required information, such as information to augment search and data on how and when the records were created, formatted, or modified, in a compliant manner.

COMPLIANCE ASSESSMENT REPORT

AWS Backup: SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c) and CFTC 1.31(c)-(d)

CFTC 1.31(c)-(d) Regulation [emphasis added]	Compliance Assessment Relative to CFTC 1.31(c)-(d)
	period as the Recovery Point. For additional information, see Section 2.6, <i>Audit System</i> .
<i>(ii) Systems that ensure the records entity is able to produce electronic regulatory records 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;</i>	It is Cohasset's opinion that AWS Backup capabilities described in Section 2.5, <i>Record Redundancy</i> , including methods for a persistent duplicate copy or alternate source to reestablish the records and associated system metadata, meet the CFTC requirements (c)(2)(ii) and are designed to <u>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</u> .
<i>(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.</i>	The regulated entity is required to create and retain an <i>up-to-date inventory</i> , as required for compliance with 17 CFR § 1.31(c)(iii).
<i>(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:</i> <i>(1) Inspection. All regulatory records shall be open to inspection by any representative of the Commission or the United States Department of Justice.</i> <i>(2) Production of paper regulatory records. ***</i> <i>(3) Production of electronic regulatory records.</i> <i>(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.</i> <i>(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.</i> <i>(4) Production of original regulatory records. ***</i>	It is Cohasset's opinion that AWS Backup has features that support the regulated entity's efforts to comply with requests for inspection and production of records, as described in. ● Section 2.2, <i>Non-Rewriteable, Non-Erasable Record Format</i> ● Section 2.4, <i>Capacity to Download and Transfer Records and Location Information</i> ● Section 2.6, <i>Audit System</i>

4 • Conclusions

Cohasset assessed the functionality of AWS Backup¹⁷ in comparison to the electronic recordkeeping system requirements set forth in SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and described audit system features that support the regulated entity as it meets the requirements of SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii).

Cohasset determined that AWS Backup, when properly configured, has the following functionality, which meets the regulatory requirements:

- ▶ Maintains Recovery Points, comprised of a collection of records and associated record metadata, and Recovery Point metadata in a non-erasable and non-rewriteable format for time-based retention periods, when the total retention period (*DeleteAfterDays*) is applied and the *Vault Lock* mode is set to either *Compliance* or *Governance* mode.
- ▶ Allows one or more Legal Holds to be applied to Recovery Points subject to preservation requirements, which retains (preserves) the Recovery Point as immutable and prohibits deletion or overwrites until the Legal Hold is released.
- ▶ Prohibits deletion of Recovery Points until the total retention period (*DeleteAfterDays*) has expired and any applied Legal Hold has been released.
 - Compliance mode: Prohibits deletion of Recovery Points by any user or process until the total retention period has expired and any Legal Hold has been released.
 - Governance mode: Prohibits deletion under normal operations; however, users with sufficient IAM permissions can remove the Vault Lock and thereafter delete Recovery Points even if the retention period has not expired (provided no Legal Hold is active). Procedural controls and monitoring are required to scrutinize such privileged actions.
- ▶ Encrypts Recovery Points at rest by default and supports encryption of data in-transit using SSL (Secure Sockets Layer).
- ▶ Verifies the accuracy and quality of the recording process through cryptographic hash values and AWS validation processes, in addition to the inherent capabilities of advanced magnetic storage technology.
- ▶ Provides the capacity and tools to: (a) list and view Recovery Points and (b) restore a Recovery Point for download of the associated records and associated metadata attributes.
- ▶ Maintains Recovery Point redundancy to either retrieve an accurate replica or regenerate an accurate replica of the Recovery Point from data shards should an error occur or an availability problem be encountered.

¹⁷ See Section 1.3, *AWS Backup Overview and Assessment Scope*, for an overview of the solution and the scope of deployments included in the assessment.

Accordingly, Cohasset concludes that AWS Backup provides the functionality necessary to meet the electronic recordkeeping system requirements of SEC Rules 17a-4(f)(2) and 18a-6(e)(2) and FINRA Rule 4511(c), as well as supports the regulated entity in its compliance with the audit system requirements in SEC Rules 17a-4(f)(3)(iii) and 18a-6(e)(3)(iii). However, meeting these requirements depends on the regulated entity properly configuring its Backup Vaults with Vault Lock (in either Compliance or Governance mode), applying appropriate retention periods, and satisfying the additional considerations described in this report. Once properly configured, the assessed capabilities of AWS Backup meet the principles-based electronic records requirements of CFTC Rule 1.31(c)-(d).

Appendix A • Overview of Relevant Electronic Records 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 electronic records retained on compliant electronic recordkeeping systems.

A.1 Overview of SEC Rules 17a-4(f) and 18a-6(e) Electronic Recordkeeping System Requirements

In 17 CFR § 240.17a-4 (SEC Rule 17a-4) for the securities broker-dealer industry and 17 CFR § 240.18a-6 (SEC Rule 18a-6) for nonbank SBS entities, the U.S. Securities and Exchange Commission (SEC) stipulates recordkeeping requirements, including retention periods.

In 2022, the SEC adopted amendments to SEC Rules 17a-4 and 18a-6, which define technology-neutral requirements for electronic recordkeeping systems. These 2022 amendments became effective on January 3, 2023, with compliance dates of May 3, 2023, for 17 CFR § 240.17a-4, and November 3, 2023, for 17 CFR § 240.18a-6.

*The objective is to prescribe rules that remain workable as record maintenance and preservation technologies evolve over time but also to set forth requirements designed to ensure that broker-dealers and SBS Entities maintain and preserve records in a manner that promotes their integrity, authenticity, and accessibility.*¹⁸ [emphasis added]

These amendments allow regulated entities to use electronic recordkeeping systems that either (a) retain the records together with complete time-stamped audit trails or (b) retain records in a non-rewriteable, non-erasable (i.e., WORM or write-once, read-many) format.

*Under the final amendments, broker-dealers and nonbank SBS Entities have the flexibility to preserve all of their electronic Broker-Dealer Regulatory Records or SBS Entity Regulatory Records either by: (1) using an electronic recordkeeping system that meets either the audit-trail requirement or the WORM requirement; or (2) preserving some electronic records using an electronic recordkeeping system that meets the audit-trail requirement and preserving other electronic records using an electronic recordkeeping system that meets the WORM requirement.*¹⁹ [emphasis added]

The following sections separately address (a) the record and audit trail and (b) the non-rewriteable, non-erasable record format alternatives for compliant electronic recordkeeping systems. Also see Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, for each SEC electronic recordkeeping system requirement and a description of the functionality of AWS Backup related to each requirement.

¹⁸ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66428.

¹⁹ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

A.1.1 Record and Audit-Trail Alternative

The objective of this requirement is to allow regulated entities to keep required records and complete time-stamped audit trails in business-purpose electronic recordkeeping systems.

[T]o preserve Broker-Dealer Regulatory Records and SBS Regulatory Records, respectively, on the same electronic recordkeeping system they use for business purposes, but also to require that the system have the capacity to recreate an original record if it is modified or deleted. This requirement was designed to provide the same level of protection as the WORM requirement, which prevents records from being altered, over-written, or erased.²⁰ [emphasis added]

The complete time-stamped audit trail must (a) establish appropriate systems and controls that ensure the authenticity and reliability of required records and (b) achieve the testable outcome of enabling access to and reproduction of the original record, if it is modified or deleted during the required retention period, without prescribing how the system meets this requirement.

[L]ike the existing WORM requirement, [the audit-trail requirement] sets forth a specific and testable outcome that the electronic recordkeeping system must achieve: the ability to access and produce modified or deleted records in their original form.²¹ [emphasis added]

Further, the audit-trail requirement applies only to required records: *"the audit-trail requirement applies to the final records required pursuant to the rules, rather than to drafts or iterations of records that would not otherwise be required to be maintained and preserved under Rules 17a-3 and 17a-4 or Rules 18a-5 and 18a-6."*²² [emphasis added]

A.1.2 Non-Rewriteable, Non-Erasable Record Format Alternative

With regard to the option of retaining records in a non-rewriteable, non-erasable format, the adopting release clarifies that the previously released interpretations of SEC Rules 17a-4(f) and 18a-6(e) continue to apply.

The Commission confirms that a broker-dealer or nonbank SBS Entity can rely on the 2003 and 2019 interpretations with respect to meeting the WORM requirement of Rule 17a-4(f) or 18a-6(e), as amended.

*In 2001, the Commission issued guidance that Rule 17a-4(f) was consistent with the ESIGN Act. The final amendments to Rule 17a-4(f) do not alter the rule in a way that would change this guidance. Moreover, because Rule 18a-6(e) is closely modelled on Rule 17a-4(f), it also is consistent with the ESIGN Act ***²³ [emphasis added]*

In addition to the Rules, the following interpretations are extant and apply to both SEC Rules 17a-4(f) and 18a-6(e).

- *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), Exchange Act Release No. 44238 (May 1, 2001), 66 FR 22916 (May 7, 2001) (2001 Interpretative Release).*
- *Electronic Storage of Broker-Dealer Records, Exchange Act Release No. 47806 (May 7, 2003), 68 FR 25281, (May 12, 2003) (2003 Interpretative Release).*

²⁰ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

²¹ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66417.

²² 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66418.

²³ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66419.

- *Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68568 (Dec. 16, 2019) (2019 SBSD/MSBSP Recordkeeping Adopting Release).*

The 2003 Interpretive Release allows rewriteable and erasable media to meet the non-rewriteable, non-erasable requirement, if the system delivers the prescribed functionality, using appropriate integrated control codes.

A broker-dealer would not violate the requirement in paragraph [(f)(2)(i)(B) (refreshed citation number)] 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.²⁴ [emphasis added]

Further, the 2019 interpretation clarifies that solutions using only software control codes also meet the requirements of the Rules:

The Commission is clarifying that a software solution that prevents the overwriting, erasing, or otherwise altering of a record during its required retention period would meet the requirements of the rule.²⁵ [emphasis added]

The term *integrated* means that the method used to achieve non-rewriteable, non-erasable preservation must be an integral part of the system. The term *control codes* indicates the acceptability of using attribute codes (metadata), which are integral to software or hardware controls, or both, which protect preserved records from overwriting, modification or erasure.

The 2003 Interpretive Release is explicit that merely mitigating (rather than preventing) the risk of overwrite or erasure, such as relying solely on passwords or other extrinsic security controls, will not satisfy the requirements.

Further, the 2003 Interpretive Release requires the capability to retain a record beyond the SEC-established retention period, when required by a subpoena, legal hold or similar circumstances.

[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.²⁶ [emphasis added]

A.2 Overview of FINRA Rule 4511(c) Electronic Recordkeeping System Requirements

Financial Industry Regulatory Authority (FINRA) Rules regulate member brokerage firms and exchange markets. Additionally, FINRA adopted amendments clarifying the application of FINRA Rules to security-based swaps (SBS).²⁷

FINRA Rule 4511(c) explicitly defers to the requirements of SEC Rule 17a-4, for 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.

²⁴ 2003 Interpretive Release, 68 FR 25282.

²⁵ Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security- Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68568 (Dec. 16, 2019) (2019 SBSD/MSBSP Recordkeeping Adopting Release).

²⁶ 2003 Interpretive Release, 68 FR 25283.

²⁷ FINRA, Regulatory Notice 22-03 (January 20, 2022), FINRA Adopts Amendments to Clarify the Application of FINRA Rules to Security-Based Swaps.

A.3 Overview of CFTC Rule 1.31(c)-(d) *Electronic Regulatory Records Requirements*

In 17 CFR § 1.31 (CFTC Rule 1.31) for the Commodity Futures Trading Commission (CFTC) stipulates recordkeeping requirements, including retention periods.

In 2017, the CFTC adopted amendments to CFTC Rule 1.31 to modernize and make technology-neutral the form and manner in which regulatory records must be kept. This resulted in less-prescriptive, principles-based requirements, which became effective on August 28, 2017.

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.²⁸ [emphasis added]

The following definitions in 17 CFR § 1.31(a) confirm that recordkeeping obligations apply to all *records entities* and 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.

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 retention time periods for required records include both time-based and event-based retention periods. Specifically, 17 CFR § 1.31(b) 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.

(4) A records entity shall keep regulatory records exclusively created and maintained on paper readily accessible for no less than two years. A records entity shall keep electronic regulatory records readily accessible for the duration of the required record keeping period. [emphasis added]

For a list of the CFTC principles-based requirements and a summary assessment of AWS Backup in relation to each requirement, see Section 3, *Summary Assessment of Compliance with CFTC Rule 1.31(c)-(d)*.

²⁸ 2017 CFTC Recordkeeping Requirements Adopting Release, 82 FR 24482.

Appendix B • Cloud Provider Undertaking

B.1 Compliance Requirement

Separate from the electronic recordkeeping system requirements described in Section 2, *Assessment of Compliance with SEC Rules 17a-4(f) and 18a-6(e)*, the SEC requires submission of an undertaking when records are stored on systems owned or operated by a party other than the regulated entity.

The purpose of the undertaking is to ensure the records are accessible and can be examined by the regulator.

SEC Rules 17a-4(i)(1)(ii) and 18a-6(f)(1)(ii) explain an 'Alternative Undertaking,' which applies to cloud service providers if the regulated entity has 'independent access' to records, which allows it to (a) regularly access the records without relying on the cloud service provider to take an intervening step to make the records available, (b) allow regulators to examine the records, during business hours, and (c) promptly furnish the regulator with true, correct, complete and current hard copy of the records.

This undertaking requires the cloud service provider (a) facilitate the process, (b) not block access, and (c) not impede or prevent the regulated entity or the regulator itself from accessing, downloading, or transferring the records for examination.

These undertakings are designed to address the fact that, while the broker-dealer or SBS Entity has independent access to the records, the third party owns and/or operates the servers or other storage devices on which the records are stored. Therefore, the third party can block records access. In the Alternative Undertaking, the third party will need to agree not to take such an action. Further, the third party will need to agree to facilitate within its ability records access.

This does not mean that the third party must produce a hard copy of the records or take the other actions that are agreed to in the Traditional Undertaking. Rather, it means that the third party undertakes to provide to the Commission

SEC 17a-4(i)(1)(ii) and 18a-6(f)(1)(ii):

(A) If the records required to be maintained and preserved pursuant to the provisions of [§ 240.17a-3 or § 240.18a-5] and this section are maintained and preserved by means of an electronic recordkeeping system as defined in paragraph [(f) or (e)] of this section utilizing servers or other storage devices that are owned or operated by an outside entity (including an affiliate) and the [regulated entity] has independent access to the records as defined in paragraph [(i)(1)(ii)(B) or (f)(1)(ii)(B)] of this section, the outside entity may file with the Commission the following undertaking signed by a duly authorized person in lieu of the undertaking required under paragraph [(i)(1)(i) or (f)(1)(i)] of this section:

The undersigned hereby acknowledges that the records of [regulated entity] are the property of [regulated entity] and [regulated entity] has represented: one, that it is subject to rules of the Securities and Exchange Commission governing the maintenance and preservation of certain records, two, that it has independent access to the records maintained by [name of outside entity], and, three, that it consents to [name of outside entity or third party] fulfilling the obligations set forth in this undertaking. The undersigned undertakes that [name of outside entity or third party] will facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the records by a representative or designee of the Securities and Exchange Commission as permitted under the law. *****

(B) A [regulated entity] utilizing servers or other storage devices that are owned or operated by an [outside entity or third party] has independent access to records with respect to such [outside entity or third party] if it can regularly access the records without the need of any intervention of the [outside entity or third party] and through such access:

(1) Permit examination of the records at any time or from time to time during business hours by representatives or designees of the Commission; and

(2) Promptly furnish to the Commission or its designee a true, correct, complete and current hard copy of any or all or any part of such records [emphasis added]

*representative or designee or SIPA trustee the same type of technical support with respect to records access that it would provide to the broker-dealer or SBS Entity in the normal course.*²⁹ [emphasis added]

B.2 Amazon Undertaking Process

The regulated entity and Amazon collaborate to reach agreement on the scope, terms and conditions of the undertaking.

- ▶ The undertaking requires actions taken by both parties:

1. The regulated entity affirms, in writing, it:

- ◆ Is subject to SEC Rules 17a-3, 17a-4, 18a-5 or 18a-6 governing the maintenance and preservation of certain records,
- ◆ Has independent access to the records maintained on AWS Backup, and
- ◆ Consents to Amazon fulfilling the obligations set forth in this undertaking.

2. Amazon:

- ◆ Acknowledges that the records are the property of the regulated entity,
- ◆ For the duration of the undertaking, agrees to facilitate within its ability, and not impede or prevent, the examination, access, download, or transfer of the records by a regulatory or trustee, as permitted under the law, and
- ◆ Prepares the undertaking, utilizing the explicit language in the Rule, then submits, via email, the undertaking to the SEC.

- ▶ Important Note: While Amazon provides this undertaking to the SEC on behalf of the regulated entity, the regulated entity is not relieved from its responsibility to prepare and maintain required records.

B.3 Additional Considerations

The regulated entity is responsible for (a) initiating the undertaking, (b) reaching agreement with Amazon on the scope, terms, and conditions of the undertaking, (c) maintaining its account in good standing, (d) implementing and configuring the cloud services to ensure its records are maintained and preserved as required by applicable laws and regulations, (e) maintaining technology, encryption keys and privileges to access AWS Backup, and (f) assuring that the regulator has (when needed) access privileges, encryption keys, and other information and services to permit records to be accessed, downloaded, and transferred.

²⁹ 2022 Electronic Recordkeeping System Requirements Adopting Release, 87 FR 66429.

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com) is a professional consulting firm, specializing in records management and information governance. Drawing on more than fifty 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, designing and supporting implementations that promote interdisciplinary information governance, achieve business objectives, optimize information value, improve compliance, and mitigate information-related risk.

Cohasset is 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.

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.

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 supports the implementation of information lifecycle practices that mitigate the cost and risk associated with over-retention*
- *Defines strategy and design for information governance in collaboration tools, such as M365*
- *Defines technical and functional requirements and assists with the deployment of enterprise content management and collaboration tools*