

HP StorageWorks Reference Information Storage System— Designed to Assist Financial Services Organizations Comply with Email Retention Requirements

SEC 17a-4, NASD 3010, and NASD 3110 Regulations



| | |
|--|----|
| Target audience | 2 |
| Legal disclaimer | 2 |
| Overview..... | 2 |
| SEC Rule 17a-4..... | 3 |
| Compliance issue 1: acceptable media | 3 |
| Compliance issue 2: quality verification..... | 4 |
| Compliance issue 3: record duplication and time-dating | 4 |
| Compliance issue 4: downloadable indexes and records..... | 4 |
| Compliance issue 5: easily readable images..... | 5 |
| Compliance issue 6: facsimile enlargement | 5 |
| Compliance issue 7: separate storage of duplicate records..... | 5 |
| Compliance issue 8: organizing and indexing of records | 6 |
| Compliance issue 9: audit system | 6 |
| Compliance issue 10: documentation | 7 |
| Compliance issue 11: third-party access filing | 7 |
| NASD conduct rules 3010 and 3110 overview..... | 8 |
| RISS provisions for meeting NASD 3010 (Supervision)..... | 8 |
| Challenge 1: manual management oversight procedures | 8 |
| Challenge 2: automated pre-review and quarantining oversight procedures..... | 8 |
| Challenge 3: automated post-review management oversight procedures..... | 9 |
| RISS solutions for meeting both NASD 3010 and NASD 3110 | 9 |
| Compliance issue 1: records access | 9 |
| Compliance issue 2: downloadable records..... | 9 |
| Compliance issue 3: records review of imaged documents..... | 10 |
| Compliance issue 4: system security | 10 |
| Compliance issue 5: records access approval | 10 |
| Compliance issue 6: password protection | 11 |
| Compliance issue 7: system policies maintenance..... | 11 |
| Compliance issue 8: policies review..... | 11 |
| Summary | 11 |
| References | 12 |
| For more information..... | 12 |

Target audience

This white paper is written for professionals in financial service organizations who manage messaging and document solutions and who must ensure that their organization complies with regulations to maintain access to email for an extended period. The content is aimed specifically at those professionals in organizations who must implement processes and solutions to comply with the email retention sections of regulations and rules of the Securities and Exchange Commission (SEC) and National Association of Securities Dealers (NASD).

Legal disclaimer

The HP customer is responsible for ensuring his or her own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. HP does not provide legal advice or represent or warrant that its products or services will ensure that the customer is in compliance with any law.

Overview

Email has become the *de-facto* standard for communication for both business and government. Today, emails are no longer a few lines of text, instead they are frequently complex, business-critical documents that contain proposals, bids, contracts, legal agreements, and other vital information. The accumulated emails and, to an increasing extent, instant messages (IMs) now account for a large part of an organization's corporate memory. Email, IMs, and other types of electronic business communications must be preserved as sent and received and be readily accessible to comply with an increasing number of legal and industry regulations.

The following is a sample of regulatory requirements across multiple industries that require email to be preserved and if required produced in a verifiable unaltered state:

- Brokerage firms: SEC Rule 17a-3 and 17a-4; NASD 3010 and 3110
- Healthcare: HIPPA/HIPAA
- Defense: DOD — 5015.2 standards
- Pharmaceutical: FDA — Title 21, Part 11
- Telecommunications: FCC — Title 47, Part 2
- Banking: FDIC, OCC
- General business oversight: Sarbanes-Oxley Act

This white paper focuses on the requirements of the SEC and NASD regulations, in particular SEC Rules 17a-3 and 17a-4 and NASD Rules 3010 and 3110. Many other current message and document retention regulations for the financial services industries are based on these SEC and NASD rules. Many of the features described here are relevant to the requirements of other regulations in other industries worldwide.

The relevant SEC regulations are covered first, then the NASD regulations. For each section covered, it is described how features designed into the HP StorageWorks Reference Information Storage System (RISS) assist the storage administrator and compliance officer to meet or exceed the requirement of the regulation.

SEC Rule 17a-4

The SEC is the governing body that registers, regulates, and oversees brokerage firms, transfer agents, and clearing agencies as well as the United States' securities self-regulatory organizations. This includes the New York Stock Exchange, the American Stock Exchange, and the NASD, which operates the NASDAQ system.

The SEC has published a series of general rules and regulations that apply to the financial services industry. The SEC rule that applies to record preservation is Rule 17a-4, "Records to Be Preserved by Certain Exchange Members, Brokers and Dealers." SEC 17a-4 has become the record preservation rule on which many other record preservation regulations are based. This part of the white paper includes compliance issues found in Rule 17a-4 and the release "SEC Interpretation: Electronic Storage of Broker-Dealer Records" [Release No. 34-47806] from 2003, followed by the accompanying section of the rule, and the RISS feature or capability that facilitates meeting the SEC requirement.

Compliance issue 1: acceptable media

Rule 17a-4(f)(2)(ii) The electronic storage media must:

A. Preserve the records exclusively in a non-rewriteable, non-erasable format;¹

The SEC interpretive release states: "A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes."²

RISS solution—This requirement is fulfilled by the following options based on the requirements and the customer's compliance strategy. The actual option chosen is the decision of the customer based on the customer's legal interpretation of the rules.

- Requirement—Data stored to the HP StorageWorks Reference Information Storage System (email, files, documents, and so on) is not modifiable in the RISS environment nor is remote access possible for editing, modification, or deletion. This makes the RISS a combination software-hardware write-once read-many (WORM) device.

Note: The SEC 17a-4 requirements and the clarification require broker-dealers to capture records on non-erasable, non-rewriteable media. Before the clarification, most firms interpreted the requirement to be WORM technology, typically based on optical or magneto-optical technology. The clarification now allows a tamper-proof combined software-hardware solution based on rewriteable magnetic disk as long as that solution prevents data manipulation and access into the system internals. The HP StorageWorks Reference Information Storage System solution meets these requirements.

Compliance issue 2: quality verification

Rule 17a-4(f)(2)(ii) B. Verify automatically the quality and accuracy of the storage media recording process;"¹

RISS solution—The following capabilities of the HP StorageWorks Reference Information Storage System fulfill this requirement:

- Writes are verified by confirming that the data is identical on both the primary and secondary storage smart cell (storage media).
- The HP StorageWorks Reference Information Storage System digital signature contains a hash and timestamp of the information stream and archived object. The integrity of the stored information is verified for each read operation using the digital signature.
- The HP StorageWorks Reference Information Storage System provides a WORM digital signature validation capability. This provides a complete validation of the accuracy of the recording process and guarantees the integrity of the message/object.

Compliance issue 3: record duplication and time-dating

Rule 17a-4(f)(2)(ii) C. Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media;"¹

RISS solution—The following capabilities of the HP StorageWorks Reference Information System fulfill this requirement:

- Serializes all objects stored inside the RISS and on duplicate media or replicated systems.
- Supports data replication.
- Can provide a completely duplicated remote system by provisioning the storage mirror at a remote site.

Compliance issue 4: downloadable indexes and records

Rule 17a-4(f)(2)(ii) D. Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member."¹

RISS solution—Fully supported. The HP StorageWorks Reference Information Storage System provides secure access to data and query results. These results can be stored in a secure RISS database or copied to media such as CD, paper, or magnetic media in industry-standard formats.

Compliance issue 5: easily readable images

Rule 17a-4(f)(3). If a member, broker, or dealer uses micrographic media or electronic storage media, it shall:

- i) At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images.”¹

RISS solution—Fully supported. The HP StorageWorks Reference Information Storage System can recover documents immediately and the recovered documents are readable through a wide range of options, including web browser, email client, printed hard copy, and optical or magnetic media.

Compliance issue 6: facsimile enlargement

Rule 17a-4(f)(3)(ii) Be ready at all times to provide, and immediately provide, any facsimile enlargement which the Commission or its representatives may request.”¹

RISS solution—Fully supported.

Compliance issue 7: separate storage of duplicate records

Rule 17a-4(f)(3)(iii) Store separately from the original, a duplicate copy of the record stored on any medium acceptable under Rule 17a-4 for the time required.”¹

RISS solution—The following capabilities of the HP StorageWorks Reference Information Storage System fulfill this requirement:

- Supports data replication to duplicate media.
- Can also provide complete system duplication by replicating all data to another HP StorageWorks Reference Information Storage System located at a remote site.

Compliance issue 8: organizing and indexing of records

From Rule 17a-4(f)(3)(iv):

- “
- Organize and index accurately all information maintained on both original and any duplicate storage media.
 - At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.
 - Each index must be duplicated and the duplicate copies must be stored separately from the original copy of each index.
 - Original and duplicate indexes must be preserved for the time required for the indexed records.”¹
-

RISS solution—The following capabilities of the HP StorageWorks Reference Information Storage System fulfill this requirement:

- All documents stored in the HP StorageWorks Reference Information Storage System can be fully indexed on both the original and duplicate storage media.
- Document indexes can be replicated on a separate system.
- Document indexes can be stored on both original and duplicate media for any period of time.

Compliance issue 9: audit system

Rule 17a-4(f)(3)(v) The member, broker, or dealer must have in place an audit system providing for accountability regarding inputting of records required to be maintained and preserved pursuant to Rule 17a-3 and Rule 17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

- A) At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.
- B) The audit results must be preserved for the time required for the audited records.”¹
-

The SEC interpretive release states: “The audit procedures for a storage system using integrated software and hardware codes to comply with paragraph (f) would need to provide accountability regarding the length of time records are stored in a non-rewriteable and non-erasable manner.”²

RISS solution—The following capabilities of the HP StorageWorks Reference Information Storage System fulfill this requirement:

- RISS provides an audit capability that records the inputting (storage) of and changes to records performed on the HP StorageWorks Reference Information Storage System.
- Audit records can be maintained for any period of time as required by the customer.
- Audit records can be stored on compliant media.

Compliance issue 10: documentation

Rule 17a-4(f)(3)(vi) The member, broker, or dealer must maintain, keep current, and provide promptly upon request by the staffs of the Commission or the self-regulatory organizations of which the member, broker, or broker-dealer is a member all information necessary to access records and indexes stored on the electronic storage media; or place in escrow and keep current a copy of the physical and logical file format of the electronic storage media, the field format of all different information types written on the electronic storage media and the source code, together with the appropriate documentation and information necessary to access records and indexes.*¹

RISS solution—Fully supported. The HP StorageWorks Reference Information Storage System can provide current data formats and data to the customer. There are several ways to do this; for email, the simplest being an administrator with compliance officer privileges uses the web interface to output records to a .PST file.

Compliance issue 11: third-party access filing

Rule 17a-4(f)(3)(vii) For every member, broker, or dealer exclusively using electronic storage media for some or all of its record preservation under this section, at least one third party ('the undersigned'), who has access to and the ability to download information from the member's, broker's, or dealer's electronic storage media to any acceptable medium under this section, shall file with the designated examining authority for the member, broker, or dealer the following undertakings with respect to such records: *¹

*The following information was omitted because it pertains specifically to the responsibilities of the third parties.

RISS solution—Fully supported. The HP StorageWorks Reference Information Storage System can provide current data formats and data to a third-party record download provider.

NASD conduct rules 3010 and 3110 overview

The review and archiving of email is a regulatory requirement for firms in the financial services industry, and, for many of these firms, all communications with the public are subject to compliance with the NASD Conduct Rules. NASD Conduct Rule 3010 (Supervision) requires member firms to supervise the activities of each registered representative. The supervisory responsibility of the member firm covers the use of email, group email, bulletin boards, chat rooms, and websites when it relates to the firm's business. NASD Conduct Rule 3110 addresses the document storage and accessibility (Books and Records) requirements for NASD registered representatives, and is largely based on the SEC 17a-4 rules in regards to electronic document storage.

Note: This section provides potential options that a RISS customer may use to comply with NASD compliance rules. The actual method chosen and deployed is the decision of the customer's legal counsel and compliance officers.

RISS provisions for meeting NASD 3010 (Supervision)

While NASD makes it quite clear what type of information is required in the supervisory procedures, it leaves substantial flexibility in how compliance with the rule is implemented. Financial institutions often design and implement specific pre- and post-review capabilities (one or both) to satisfy their interpretation of NASD Supervision rules. Following are the challenges of these options and the RISS solution for each.

Challenge 1: manual management oversight procedures

Some financial institutions implement manual management supervision procedures to fulfill their NASD supervisory requirements. While in smaller environments, manual post-review surveillance of email may be adequate; in larger financial institutions it becomes impractical.

RISS solution—The HP StorageWorks Reference Information Storage System supports both pre-review and post-review email surveillance capabilities, offering organizations a wide range of surveillance options to meet their business requirements.

Challenge 2: automated pre-review and quarantining oversight procedures

Compliance workflow applications can identify and flag email content that could raise legal and compliance issues. Workflow applications typically run on the email server and review incoming and outgoing messages and attachments, retain a permanent record of the results, and track all associated events. Due to the processing overhead involved with compliance workflow applications, they are often only enabled for specific projects or in sensitive financial transactions.

RISS solution—The HP StorageWorks Reference Information Storage System provides a major component of a NASD compliance solution for **pre-review** oversight and surveillance. When combined with a compliance workflow application, the solution can review incoming and outgoing messages and attachments, flag and/or quarantine specific messages that could raise legal or compliance concerns, retain a permanent audit record of the results, and track all associated events.

Of course, all post-review capabilities specified would be fully supported also.

While HP does not partner with or endorse any specific compliance workflow application for RISS, there are several available in the marketplace that can be integrated with RISS software solutions to provide an overall pre-review surveillance solution.

Challenge 3: automated post-review management oversight procedures

Automated post-review supervision uses automated query and archival systems to identify and flag email content that could raise legal and compliance issues. Note that post-review solutions identify issues after the fact; they are not part of the actual real-time workflow.

RISS solution—The HP StorageWorks Reference Information Storage System provides NASD compliance solution for **post-review** oversight and surveillance:

- Email and documents are archived, indexed, and replicated remotely per SEC 17a-4 and NASD 3110 requirements.
- Documents can be rapidly queried and retrieved and are readable through a wide range of options, including web browser, email client, printed hard copy, and magnetic media.
- Post-review supervision policies and criteria can be manually or automatically initiated.

RISS solutions for meeting both NASD 3010 and NASD 3110

This section includes brief summaries of the compliance requirements of NASD 3010 (Supervision) and 3110 (Books and Records), followed by the feature or capability of the HP StorageWorks Reference Information Storage System that supports the NASD requirement.

Compliance issue 1: records access

Summary—The system must allow NASD examining staff immediate access to required records and documents.

RISS solution—Fully supported. The HP StorageWorks Reference Information Storage System can recover documents near-instantaneously and make them readable through a wide range of options, including web browser, email client, hard copy, and magnetic media.

Compliance issue 2: downloadable records

Summary—The system must allow NASD examining staff to download and print hard copies of required records and documents.

RISS solution—Fully supported. The HP StorageWorks Reference Information Storage System can recover documents near-instantaneously and are readable or downloadable through a wide range of options, including web browser, email client, hard copy, and magnetic media.

Compliance issue 3: records review of imaged documents

Summary—The system must allow NASD examining staff to review copies of all relevant imaged documents and will provide an audit trail of principals who reviewed the customer accounts and orders.

RISS solution

- The HP StorageWorks Reference Information Storage System can recover relevant imaged documents near-instantaneously and are readable or downloadable through a wide range of options, including web browser, email client, hard copy, and magnetic media.
- Audit records can be maintained for any period of time as required by the customer.

Compliance issue 4: system security

Summary—The system must store all required records and documents on a secured server, which will operate in a redundant, multi-server environment to ensure the integrity of the data.

RISS solution—The HP StorageWorks Reference Information Storage System:

- Supports remote backup capabilities or offsite backup media support to meet SEC and NASD offsite copy requirements.
- Can provide a completely duplicated remote system by provisioning the storage mirror at a remote site.
- Incorporates a wide range of security capabilities, including (but not limited to) firewalls, encryption, and password protection to protect against external and internal security threats.

Compliance issue 5: records access approval

Summary—The system and operational/organizational policies and procedures must allow the system to be used only by those individuals who have been approved and only at the level of access for which those individuals have been approved.

RISS solution—Fully supported. The HP StorageWorks Reference Information Storage System provides access control list (ACL) security to every repository, which enables organizations to restrict access to approved individuals.

Compliance issue 6: password protection

Summary—If Web-based, the system can only be viewed through a password-protected and encrypted web browser and the system must instruct users to change their passwords frequently.

RISS solution—Fully supported. If the browser interface is used, the HP StorageWorks Reference Information Storage System supports password time limits and HTTPS (secure http) access including 128-bit encryption.

Compliance issue 7: system policies maintenance

Summary—The regulated organization must maintain current written policies and procedures at each branch office that utilizes and accurately describes the system, its safeguards, and its operating procedures.

RISS solution—This requirement is procedural and administrative in nature. However, the HP StorageWorks Reference Information Storage System provides manuals and documentation that accurately describe the system as well as its safeguards and operating procedures.

Compliance issue 8: policies review

Summary—The regulated organization must periodically review the policies, procedures, and operations to ensure conformance with changes and enhancements in policies and procedures.

RISS solution—The HP StorageWorks Reference Information Storage System assists the customer with system and enhancement documentation and training to help the customer comply with this requirement.

Summary

With the HP StorageWorks Reference Information Storage System, storage and retrieval of reference data has never been easier. This self-contained, self-managing, and fault-tolerant system transforms unstructured reference data into exploitable information. Now you can manage storage costs and comply with data retention regulations with one solution. Now you can deploy a single, highly scalable, cost-effective solution to manage excessive reference information.

References

1. Excerpt from the *General Rules and Regulations promulgated under the Securities Exchange Act of 1934*, SEC Rule 17a-4, "Records to Be Preserved by Certain Exchange Members, Brokers and Dealers."
2. Excerpt from the *Securities and Exchange Commission Interpretation*, 17 CFR Part 241 [Release No. 34-47806], "Electronic Storage of Broker-Dealer Records."
3. NASD Conduct Rule 3010, *Supervision*, in NASD Conduct Rules.
4. NASD Conduct Rule 3110, *Books and Records*, in NASD Conduct Rules.

For more information

Consult your HP representative or look on the HP website at www.hp.com/go/ILM.

© 2004 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

5982-4299EN, Rev. 1, 11/2004

