Remaining Compliant in a Changing Environment

Financial Services Compliance Whitepaper

 © 2024 by Egnyte Inc. All rights reserved.

Table of Contents

Introduction

The financial services and banking industries play an important role in the economy, and the sensitive data they manage requires the highest standards for digital storage security. Whether it's SEC oversight, FINRA compliance, or Sarbanes-Oxley reporting, maintaining control of financial data is critical.

The digital revolution and resulting explosion of unstructured data has ushered in a new era of privacy regulations like GDPR, CCPA, and NYDFS. New state and federal regulations are soon to follow. Egnyte scans reveal that sensitive data is pervasive in a typical organization, with 10 percent of files and folders containing some kind of regulated content. Consumer privacy laws apply to data that is owned by departments across the organization, from HR to finance, sales, marketing, and operations.

All financial services need a reliable way to share confidential documents such as customer activity reports and cash flow statements. In an increasingly specialized and digitized financial services ecosystem, communicating and sharing information with employees who may work in different states is becoming more common and the evolutionary pace of digital security accelerates. Traditional methods of sharing files over email, FTP, and USB drives present security problems and risk violating SEC regulations.

With Egnyte, companies get a FINRA-compliant content collaboration solution with complete end-to-end data protection. Plus, Egnyte enables full compliance under SEC 17a, 31a, 204 Recordkeeping regulations for confidential content storage, retention, digitalization, and accessibility. Egnyte's access, collaboration, and security is built for today's highly regulated and data-driven environment, with tools for seamlessly classifying known sources of sensitive data and streamlining the request process for an individual's private data. Furthermore, Egnyte has a tight integration with GSuite and Docusign, as well as Azure and Office 365, allowing companies to maximize their investments in Microsoft.

Broker-dealers and investment advisors should not have to take on the burdens required to develop and maintain independent and prudent cybersecurity solutions that protect this sensitive data as it is accessed from remote and mobile platforms. Finance professionals can seize an opportunity for increased efficiency by engaging data security experts who will ensure a secure, compliant file environment while maintaining ease of use. This allows a financial services firm to focus completely on returns in a complex market.

Secure and Compliant Collaboration

Egnyte offers companies a secure and compliance-focused platform to share files of any type and size. Egnyte enables users to create private or shared, permission-based folders, which serve as protected access points for secure client collaboration. It also provides the ability to share specific files by creating links that eliminate the need for insecure attachments and offer granular control over how the content is accessed, and by whom.

How Egnyte's solutions can work for you:

- Protect shared work with permission-based folders
- Content safeguards to prevent sensitive data leaks
- End-to-end encryption
- Two-factor authentication
- Ransomware detection
- Real-time issue alerting and scoring
- Unusual file access detection
- Suspicious login prevention
- Robust password requirements
- Remote file access with secure authentication
- Remotely wipe mobile and desktop applications
- Control and visibility for administrators
- Fully auditable
- Customer managed encryption keys (i.e. Enterprise Key Management)

This level of controlled content collaboration, combined with Egnyte's enterprise-class data security, allows financial services firms to adhere to strict business policies and government regulations.

Taking the Work Out of Data Discovery

Protect features out-of-the-box content classification configurations based on some of the largest, most complicated data usage and privacy regulations today, including FINRA, GDPR, CCPA, SEC, Fair Credit Reporting Act, Gramm-Leach, SOX, PCI-DSS, DPA, and PIPEDA. Customers choose the applicable regulations during setup, and Egnyte's scanning and classification tools will automatically detect and surface sensitive content known to be regulated under these laws.

Administrators and content owners can then ensure that access is restricted in accordance with the law, and monitor for any out-of-bounds sharing. As changes are made to regulations over time, the system automatically integrates these updates to pre-configured compliance policies and alerts you to them.

Egnyte can match to more than 400 patterns of personally identifiable information, including many specific to financial services, such as credit card numbers, US and international bank accounts, US banks and RIAs, as well as financial reporting and personal finance terms, so you can ensure access to sensitive content is appropriately limited under the law.

Policy-Based Retention

Certain kinds of information are required to be held for a set number of years to remain in compliance with the law. Egnyte's classification features not only help identify the data in your organization that is covered by these requirements, but it allows you to set and automate data retention policies while providing a seamless experience for the end user. Users can still manage their content as needed, deleting files that are no longer relevant to them, while Egnyte's automated retention system continues to store the content behind-the-scenes to maintain regulatory compliance.

Cross-Repository Classification

What if you don't want to move your data around? If your company is comfortable with your existing repository, you can still get the benefits of using Egnyte's discovery and classification. Egnyte is compatible with and can classify data in other repositories, including Microsoft File Server, SharePoint on Prem and Online, OneDrive, and CIFS. This integration allows financial services clients to customize their compliance solutions to suit an established workflow.

Handling Personal Data Requests

A key component of sweeping regulations like GDPR and CCPA (effective January 1, 2020) is the ability for users to request personal data that businesses have collected about them. Under GDPR, users may submit a Data Subject Access Request, and in the case of CCPA, a Verifiable Consumer Request. These requests can be made in any form (by email, phone, web) and include inquiries like:

- **Notification:** I would like to know the total amount and type of personal data you have about me.
- **Right to Data Portability:** I would like access to all the personal data you have about me, provided in a portable machine-readable format.
- **Right to be Forgotten:** I would like all of my personal data securely deleted.

It's easy for a person to make these requests but delivering answers has been notoriously difficult. Often, the amount of information held on a single person can be extensive, spread across many different locations, and commingled with the personal data of others. Often, responding to these inquiries requires manual analysis of terabytes of content, including archived content stored on a forgotten file server that may have not been touched in years.

A great way to simplify the process of identifying, locating, and compiling the files containing personal information is to deploy a content governance solution that "knows" what to look for. Egnyte is designed to discover and classify files containing Personally Identifiable Information (PII) and prepare them for a data subject access request. Even if data is scattered, which is often the case, Egnyte surfaces it in just a few clicks.

DSAR search and reporting features makes it easy for an organization to:

- **Collect all the personal data** about the requestor across Egnyte Protect-enabled repositories and archives.
- **Verify the data** to ensure that it is the right personal data for the right person.
- **Identify specific files** containing the data subject's personal data, so they can delete or dispatch them.

Work Remotely, Safely

Remote file access is a necessity for many financial service employees, but access beyond the firewall using traditional VPN systems can be cumbersome and unreliable. Even worse, the lack of recordkeeping or access control in many systems risks running afoul of regulation, such as the SEC requirements around safeguarding records. Egnyte solves that problem by offering secure online file access with enforced user authentication and folder permissions. No matter what location or access method (web browser, mapped drive, secure FTP, desktop sync, mobile/tablet app) employees are always authenticated using company-specific authentication policies. Every employee has a unique set of folder and sub-folder access permissions, regulated by the administrator. Employees can never view folders they aren't permitted to, ensuring privacy and compliance across all company data. With Egnyte's permissions browser, administrators can always see which users have access to regulated content—and can easily, quickly make changes if an employee has access to files they shouldn't.

Supervise and Evaluate

All data usage, file history, and user activity in Egnyte can be monitored with comprehensive audit reports designed to detect and respond to potentially harmful cybersecurity events. This way, you can be satisfied you will be in compliance with NYDFS Risk Assessment and Cybersecurity provisions requiring ongoing efforts to prevent, monitor and respond to incidents. With a continuous commitment to the financial services sector, Egnyte provides a secure scalable solution that complies with the intense needs of today's regulated environment.

Compliance Information and Notification Sheets

The following pages show how Egnyte offers redundant compliance solutions to meet SEC data use regulations for Broker Dealers and Investment Advisors. If you have questions about how Egnyte keeps you compliant for any specific sub-part for a rule, you can find your answers here. This informative section doubles as a notification in accordance with requirements to notify any examining authority—simply forward the appropriate sections to the authority.

SEC Rule 17-a: Compliance for Broker-Dealers

Preserving Records

> *Every member, broker, and dealer subject to Rule 17a-3 shall preserve for a period of not less than six years, the first two years in an easily accessible place, all records required to be made pursuant to paragraphs Rule 17a-3(a)(1), (a)(2), (a)(3), (a)(5), (a)(21), (a)(22), and analogous records created pursuant to Rule 17a-3(f).*

Documents can be stored and accessed in Egnyte for as long as needed using automated, policy-based retention and archive services. All documents and records are “easily accessible” for the duration of their existence in Egnyte. Users can easily locate records by navigating the folder hierarchy or by locating a client-centric folder through a powerful keyword, file name, or tag search.

Notifying Authorities

> *The member, broker, or dealer must notify its examining authority designated pursuant to Section 17(d) of the Act prior to employing electronic storage media. 17a-4(f)(2)(i)*

While this notification is the responsibility of the customer, Egnyte makes it easy—this compliance document can be forwarded by the customer in order to communicate Egnyte functionality.

Preserving Duplicates

> *Preserve the records exclusively in a non-rewritable, non-erasable format (Write Once Read Many (WORM) devices. 17a-4(f)(2)(ii)(A)*

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

All files are stored in a patented Egnyte Object Store (EOS) that ensures a fully redundant architecture to provide storage resiliency. A separate copy is stored offsite and fulfills backup and disaster recovery requirements. EOS has the ability to store infinite versions of a file and the ability to control the purge policy to satisfy the WORM requirement of 17a-4(f)(2)(ii)(A). Additionally, Egnyte provides an audit log of all activity.

Automatic Verification

> *Verify automatically the quality and accuracy of the storage media recording process. The intent of this rule is to provide some level of confidence that the record has actually been stored. 17a-4(f)(2)(ii)(B)*

Egnyte maintains versions of a document as it changes and also sends alerts when any file is changed.

Serializing Records

> *Serialize the original and, if applicable, duplicate units of storage media, and timestamp for the required period of retention the information placed on such electronic storage media. 17a-4(f)(2)(ii)(C)*

All files stored via EOS maintain an immutable timestamp of every Create, Read, Update and Delete operation. All file changes are kept with an audit trail and information about who changed the file and the timestamp of the change. No data is purged unless explicitly deleted by an authorized user.

Downloading Indexes and Records

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

All files are indexed in Egnyte and can be searched using keyword, partial file names, or metadata assigned to files. Files can be exported in a zipped format or copied on any magnetic media. An optional local copy of the file or all files on a direct attached storage device or network attached storage device can be provided.

Making Records Available for Examination

> *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. 17a-4(f)(3)(i)*

Customers can provide secure access to their files in Egnyte to any entity, including regulatory staff. Each such access is controlled by a specific username and password. All file access is recorded and is visible in the access history tab associated with each file.

Facsimile Enlargement

> *Be ready at all times to provide, and immediately provide, any facsimile enlargement which the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker, or dealer may request. 17a-4(f)(3)(ii)*

Egnyte provides web-based, mobile, and direct desktop access to the files. A customer can provide any or all kinds of access to the regulatory organizations, who in turn can print or fax the document from resources they have access to in their office. Egnyte also provides a viewer for most commonly used file types.

Indexing Records

> *Organize and index accurately all information maintained on both original and any duplicate storage media. 17a-4(f)(3)(iv) (A)*

All files are automatically indexed and are searchable using keywords, partial file names, or metadata associated with a file. Search function returns results based on proximity of keywords, relevancy, etc.

Making Indexes Available for Examination

> *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. 17a-4(f)(3)(iv)(A)*

All files are automatically indexed and all actions by any user against the document are recorded providing an audit trail with a date and time stamp. The Commission staff can access this information at any time using the web-based access.

Duplicating Indexes

> *Each index must be duplicated, and the duplicate copies must be stored separately from the original copy of the index. Original and duplicate indexes must be preserved for the time required for the indexed records. 17a-49f)(3)(iv)(A)*

An index, which allows the retrieval of the files, is automatically created in the Egnyte online storage. The index will exist as long as the documents are available. All documents and records are mirrored to a second datacenter, as well as remote backups of the database. Indexes and record sets are kept for as long as needed by the retention period. Egnyte uses a “High Availability” (HA) architecture for all layers of its infrastructure, ensuring redundancy and protection against losing access to the records.

SEC Rule 240: Retention Requirements

Preserving Customer Records

> *Every member, broker and dealer subject to § 240.17a-3 shall preserve for a period of not less than six years after the closing of any customer’s account any account cards or records which relate to the terms and conditions with respect to the opening and maintenance of the account.*

Each Egnyte customer can maintain records for a predetermined period of time based on universal policies, at the folder level, or based on data classification rules. Egnyte does no automatic purging unless specified by the customer’s data retention policy. Files will be archived in Egnyte as long as the customers keep their Egnyte account active.

Preserving Articles and Books

> *Every member, broker, and dealer subject to § 240.17a-3 shall preserve during the life of the enterprise and of any successor enterprise all partnership articles or, in the case of a corporation, all articles of incorporation or charter, minute books and stock certificate books (or, in the case of any other form of legal entity, all records such as articles of organization or formation, and minute books used for a purpose similar to those records required for corporations or partnerships), all Forms BD (§ 249.501 of this chapter), all Forms BDW (§ 249.501a of this chapter), all amendments to these forms, all licenses or other documentation showing the registration of the member, broker, or dealer with any securities regulatory authority.*

Egnyte enables customers to segregate and retain files by folder location, or using data classification rules. None of these are purged by the system unless explicitly deleted by the customer. The customer can therefore create specific folders to store articles of incorporation, minute books, stock certificate books, etc. If the customer deletes any of these willingly, Egnyte provides an audit log of all delete activity.

Preserving Account Records

> *Every member, broker and dealer subject to § 240.17a-3 shall maintain and preserve in an easily accessible place: All account record information required pursuant to § 240.17a-3(a)(17) until at least six years after the earlier of the date the account was closed or the date on which the information was replaced or updated.*

Egnyte allows customers to keep all their files with or without an enforced archival policy. Each customer can keep the files for six years or longer, and since data storage is redundant, data loss issues are completely prevented.Preserving Requested or Required Reports

Preserving Requested or Required Reports

> *Every member, broker, and dealer subject to § 240.17a-3 shall maintain and preserve in an easily accessible place: Each report which a securities regulatory authority has requested or required the member, broker, or dealer to make and furnish to it pursuant to an order or settlement, and each securities regulatory authority examination report until three years after the date of the report.*

Each report, which a regulatory authority has requested pursuant to an order or settlement, can be tagged with the appropriate label. Such tagged files can be maintained in the Egnyte storage system for three years or longer.

Preserving Unusual Activity Reports

> *Every member, broker, and dealer subject to § 240.17a-3 shall maintain and preserve in an easily accessible place: All reports produced to review for unusual activity in customer accounts until eighteen months after the date the report was generated*

Unusual activity reports can be tagged with the appropriate label, or discovered and retained automatically through keyword-based classification. Such tagged files can be maintained in the Egnyte storage system 18 months or longer.

Storing Written Advertisements

> *Written advertisement never released to the public must also be kept and made available to SSR. Customers must keep all compliance, supervisory, and procedures manuals, including any written procedures for reviewing communications.*

The customer can store the written advertisement files in folders with read-only access so that they are always available to SSR. They can do the same for all compliance, supervisory, and procedures manuals, including any written procedures.

SEC Rules 31a-2 and 204-2: Investment Companies and Investment Advisors

Electronic Format Recordkeeping

> *Funds and advisors may keep all of their records in an electronic format. (Amendment to Rule 31a-2 and 204-2)*

All documents including email files can be stored in the Egnyte online storage solution. Read-only folder permission on the online folders will prevent any user from deleting these files.

Safeguarding Records

> *Reasonably safeguard the records from loss, alteration, or destruction. (Rule 31a-2, 204-2, Part 270, Part 275)*

All files are stored in a patented Egnyte Object Store (EOS) that ensures a fully redundant architecture to provide storage resiliency. A separate copy is stored offsite and fulfills backup and disaster recovery requirements. Furthermore, Egnyte allows customers to create a local copy on a direct attached storage device or a network attached storage device in their office. Using Content Retention schedules, users can prevent files from being purged from the trash for a given period of time.

Egnyte also provides the ability to detect unusual file access and anomalous user behavior such as large deletions and downloads. Admins may monitor for unusual access, be alerted to suspicious activity, and quickly disable compromised accounts. Egnyte also scans and alerts admins to known ransomware signatures on the file system, blocks logins from known dangerous geographies, and prevents other suspicious login activity.

Egnyte provides two-factor authentication, end-to-end encryption, remote wipe of mobile and desktop applications, integration with SSO providers, and robust password configuration options for more secure logins.

Electronic Copies

> *Ensure that electronic copies of non-electronic originals are complete, true, and legible in the medium and format in which it is stored. (Amendment to Rule 31a-2, 204-2, Part 270, Part 275)*

Egnyte provides a viewer for many common file types. This allows users to be able to read these files despite not having the viewing application on their computer.

Limiting Record Access

> *Limit access to the records to authorized personnel, the Commission (including its examiners and other representatives), and (in the case of funds), fund directors (Rule 31a-2, 204-2, Part 270, Part 275).*

Account administrators control access rights for all documents in their Egnyte account. They can create a specific group, for example, the Commission users, and grant them the required access to the respective folders.

Using data classification rules, Egnyte admins can continuously scan the repository for data that may be improperly stored or permissioned to ensure that restrictions to appropriate personnel are enforced.

Providing Copies of Records

> *Funds and advisors may be requested by the Commission to promptly provide legible, true, and complete copies of records in the medium and format in which they are stored and printouts of such records; and means to access, view, and print the records. (31a-2, 204-2)*

Egnyte provides secure access to users within an account, including enabling the account administrator to allow secure access to other business entities like the Commission. The Commission personnel can open a file, email it, or send it to a printer or fax. Also, Egnyte allows for secure access to a single file via links.

Printouts

> *Means to access, view, and print the records in a legible, true, and complete printout. (Part270, Part 275)*

Egnyte allows secure access to users within to be able to view and print files.

Duplicating Records

> *Separately store, for the time required for preservation of the original record, a duplicate copy of the record on any medium allowed. (Part 270, Part 275)*

All files are stored in a patented Egnyte Object Store (EOS) that ensures a fully redundant architecture to provide storage resiliency. A separate copy is stored offsite and fulfills backup and disaster recovery requirements. Policy-based retention rules control when the deleted files are purged from the trash bin associated with each account. The Account Administrator manages this.

Preserving Records

> *Funds and advisors to retain records electronically for over fifteen years and easily accessible for two years.*

Documents can be stored and accessible in Egnyte online storage with no expiration. The customer can keep them for two years or 15 years. Egnyte now offers automated data retention based on policies. For example, you can tell the system that if it finds anything that looks like financial records (e.g., bank accounts) in a piece of content, to save that content for the required period. Once the initial two-year period is complete, content can be automatically moved to low-cost archive storage for the remaining period.

Format Consistency

> *Funds and advisors who choose to convert records into an electronic format must do so in the same fashion as they already keep electronically created or received records.*

Egnyte allows the funds and advisors to store the documents in the original file type and format, and automatically provides a viewer for most commonly used file types.

Flexible Standards

> *The standards are flexible and permit funds and advisors to modify their electronic record retention practices to take advantage of advances in electronic storage technology.*

Egnyte customers have secure access to their documents from anywhere and at any time. Egnyte ensures that their files are always available by keeping more than one copy across two data centers to prevent any kind of data loss.

Combining Storage Protocols

> *Funds and Advisors are free to adopt any combination of technological and manual protocols that meet the requirements of the rules.*

Egnyte provides a comprehensive Secure Content Platform at a fraction of the cost to doing it in-house. It is a more secure and robust solution than what most companies can deploy and manage with their own IT staff.

Compliance is easier with Egnyte

Start a free trial online, or contact our sales team today

15-DAY FREE TRIAL

US: 1.877.734.6983 | UK: +44 (0) 845.528.0588