Regulatory compliance

CIO Dynamics security and privacy controls address a wide range of financial services regulations. The tables below describe how CIO Dynamics services can help you address these regulations.

FINRA Regulations		
Relevant section/topic	**Compliance Requirements**	**How We Can Help**
Books and records (Rule 3110)	Correspondence must be maintained in compliance with applicable FINRA rules and Securities Exchange Act of 1934 Rules 17a-3 & 17a-4. Also specifies supervisory procedures for the review of correspondence between individual representatives and the public.	• Secure, low-cost & long-term storage. • The storage platform supports and indexes relevant data types and formats. • Role-based permissions for accessing archive.

SEC Regulations		
Relevant section/topic	**Compliance Requirements**	**How We Can Help**
Rule 17a-3	Most members of a national securities exchange, as well as brokers and dealers, must keep current a variety of books and records that relate to their business.	• 24/7 offline data access and search with role-based permissions for accessing archive.
Rule 17a-4 & NASD 3010	Securities dealers must implement specific, enforceable retention procedures, which include the following: Messages must be stored in duplicate. Data must be verified automatically for quality and accuracy. Messages must be date/time-stamped and serialized. A searchable index of all data must be maintained. Messages and indexes must be easily retrievable.	• Stored data is backed up and stored on fully redundant platform with 99.999% uptime SLA. • Full-text indexing and search capability. • All stored files and corresponding file activity are time-stamped, and auditable via Audit Log and Admin File Management. • Configurable retention policies.

Investment Advisers Act of 1940	Hedge fund managers with assets in excess of $100M have to register with the SEC under the Investment Advisers Act of 1940, which includes provisions for securing electronic communication, including email and instant messages (same requirements as SEC 17a-4).	• Archive and index of all relevant file types. • Secure, permission-based sharing. • Data is encrypted in transit and at rest. • Versioning and full audit trail of all sharing and file management activity.

NASD Regulations		
Relevant section/topic	**Compliance Requirements**	**How We Can Help**
Rule 2860 (b)(17)	Members shall maintain and keep current a separate central log, index or other file for all options-related complaints, through which these complaints can easily be identified and retrieved. Background and financial information of customers shall be maintained at specific locations, including the principal supervisory office (or elsewhere, as long as the documents are "readily accessible and promptly retrievable")	• Full-text indexing & search. • Archived data access from any web browser, desktop, and mobile device.

GRAMM-LEACH-BLILEY ACT Regulations		
Relevant section/topic	**Compliance Requirements**	**How We Can Help**
The Financial Privacy Rule	Financial institutions must provide each consumer with a privacy notice, explaining where the info is shared, how it is used and how it is protected, at the time the consumer relationship is established and annually thereafter.	• World-class datacenter infrastructure with annual SOC 2 audits. • AES-256 bit encryption.
The Safeguards Rule	Financial institutions must design, implement, and maintain an information security plan to protect customer information; it also applies to credit reporting agencies, appraisers and mortgage brokers receiving info from financial institutions.	• Data encryption in transit and at rest (AES- 256 bit). • Complies with PCI-DSS standards. • Data encrypted at all times (in transit & at rest). • 100% file capture and backup.

Miscellaneous Statutes

Relevant section/topic	Compliance Requirements	How We Can Help
Consumer Finance Protection Bureau	Compliance with GLBA required for RESPA-TILA forms to protect NPI (Non-public Personal Information) by Real Estate Settlement Services- ALTA Best Practices Pillar #3..	• Supports GLBA with NPI-based email encryption and data encrypted at all times (in transit & at rest).
Federal Deposit Insurance Corporation	Provides guidance on security and management of Instant Messaging. Social Media communications need to be supervised, reviewed, and retained.	• Archive and index over 500 different file types in a central repository.
USA Patriot Act	Requires records retention for suspicious communications associated with money transfer and laundering.	Files are backed up, indexed, and searchable. Full audit trail of all sharing and file management activity.
SB 1386 (only in California)	Requires any agency, person, or business conducting business in California to disclose unauthorized access to unencrypted personal information.	• Encrypts data at all times (in transit & at rest). • Encrypted data is not subject to disclosure requirements in the event of a breach. • Data loss prevention features such as external sharing policies & remote device wipe.

SARBANES-OXLEY Regulations

Relevant section/topic	Compliance Requirements	How We Can Help
Protection of Security Technology	Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.	• Data encryption in transit and at rest (AES- 256 bit). • Secure key storage and distribution. • Role-based permissions for accessing archive
Cryptographic Key Management	Determine that policies and procedures are in place to ensure the protection of cryptographic keys against modification and unauthorized disclosure.	• Data encryption in transit and at rest (AES- 256 bit). • Annual SOC 2 audits. • Independent, company-wide audit of all 5 SOC 2 Trust Service Principles (security, availability, processing integrity, confidentiality and privacy).

Exchange of Sensitive Data	Determine that policies and procedures are in place to ensure the protection of cryptographic keys against modification and unauthorized disclosure.	• Standards-based technologies such as Public Key Infrastructure (PKI), S/MIME and X.509 certificates are used to establish confidentiality, message integrity and user authentication.
Security Requirements for Data Management	Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, organizational security policy, and regulatory requirements.	• Annual SOC 2 audits. • Independent, company-wide audit of all 5 SOC 2 Trust Service Principles (security, availability, processing integrity, confidentiality and privacy).

HIPAA Regulations

Relevant section/topic	Compliance Requirements	How We Can Help
HIPAA Security Rule (45 CFR Part 160, 164)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	• Email encryption designed to meet HIPAA standards. • Predefined encryption policies for PHI, identity and financial data.

This summary does not purport to list, nor should it be interpreted as stating that CIO Dynamics addresses, all legal requirements related to data storage and retention. Compliance with FINRA, SEC, HIPAA and other applicable laws is complex and multi-faceted and is ultimately the responsibility of each entity that is subject to those laws.