

FINRA Report on Cybersecurity Practices (2015)

FINRA Cybersecurity Guidance provides regulatory expectations for broker-dealers and firms to strengthen cybersecurity and protect client assets.



What it is

FINRA Cybersecurity Guidance is a set of regulatory guidelines that assists broker-dealers and financial firms in strengthening cybersecurity controls, safeguarding sensitive data, and managing operational risks. The guidance outlines expectations for protecting client assets and maintaining the integrity of financial markets.

Issued by the Financial Industry Regulatory Authority (FINRA), this guidance is used primarily by member firms, compliance officers, and security teams within the securities industry. It addresses topics such as cybersecurity risk assessments, threat monitoring, incident response, vendor management, and regulatory compliance oversight.

At a glance

PUBLISHER

Financial Industry Regulatory Authority (FINRA)

TYPE

Guidance

VERSION

Current FINRA Cybersecurity Guidance

EFFECTIVE

July 2015

DOMAIN

Cybersecurity

FAMILY

Other

REGION

United States

INDUSTRY

Financial Services

ADOPTION MODEL

Regulatory Compliance

IMPLEMENTATION COMPLEXITY

High

Source: <http://www.finra.org/industry/cybersecurity>

Why it matters

- **Strengthen cybersecurity governance** Establish clear roles, responsibilities, and oversight for risk management and control of information security practices across the organization.
- **Enhance regulatory alignment** Support compliance with FINRA rules and related SEC cybersecurity regulations, reducing the likelihood of enforcement actions or penalties.
- **Promote operational resilience** Mitigate the impact of cyber incidents by improving preparedness, response capabilities, and recovery planning for essential business operations.
- **Improve threat detection capabilities** Enable more proactive identification and monitoring of emerging cybersecurity threats through risk assessments and continuous threat intelligence.

How SmartSuite supports FINRA Cybersecurity

Supervisory Procedures and Controls Hub Centralize cybersecurity procedures, control ownership, and evidence sources.	Risk Assessments and Governance Reporting Track cyber risk assessments, decisions, and recurring management reporting.	Third-Party Risk Management Manage vendor due diligence, monitoring, and incident preparedness expectations.
Incident Response and Escalation Workflows Run IR playbooks with timelines, communications, and post-incident actions.	Testing and Control Verification Track vulnerability management, monitoring validation, and remediation proof.	Posture and Evidence Coverage Reporting for Audits Report posture, gaps, and evidence coverage for audits and examinations.

Common framework mappings

EU DORA

GLBA Safeguards Rule (16 CFR Part 314)

ISO 27001:2022

NIST CSF 2.0

NIST 800-53 Rev.5

NYDFS 23 NYCRR 500

SOC 2

Official resources

Frequently asked questions

What is FINRA Cybersecurity Guidance used for?

FINRA Cybersecurity Guidance provides regulatory expectations for broker-dealers and financial firms to protect sensitive data, client assets, and maintain operational resilience. It helps organizations identify and manage cybersecurity risks in alignment with the requirements of the financial industry.

Is FINRA Cybersecurity Guidance mandatory for broker-dealers?

FINRA Cybersecurity Guidance is not a law or a certifiable standard, but compliance with its principles is expected for all FINRA member firms. Following the guidance demonstrates a firm's due diligence and risk management in the event of regulatory reviews or examinations.

Who does FINRA Cybersecurity Guidance apply to?

FINRA Cybersecurity Guidance primarily applies to FINRA member firms, including broker-dealers, compliance officers, and security teams in the securities industry. It is also relevant for third-party vendors who provide services to these firms.

What are the key concepts or controls required by FINRA Cybersecurity Guidance?

Key concepts include cybersecurity governance, risk assessments, layered technical controls, incident response planning, vendor risk management, and regular monitoring. The guidance outlines recommended practices for each area to help firms bolster their cybersecurity posture.

How do organizations implement FINRA Cybersecurity Guidance?

Organizations implement FINRA Cybersecurity Guidance by conducting risk assessments, developing tailored cybersecurity policies, addressing third-party risk, monitoring threats, and training staff. They routinely review and test controls as part of their ongoing compliance program.

How does FINRA Cybersecurity Guidance relate to other frameworks like NIST or SEC regulations?

FINRA Cybersecurity Guidance aligns with broader regulatory and cybersecurity frameworks, such as the NIST Cybersecurity Framework and SEC regulations. This allows financial firms to harmonize their controls and risk management practices across multiple regulatory requirements.

What are the ongoing requirements for FINRA Cybersecurity Guidance compliance?

Ongoing compliance requires regular security assessments, monitoring for new threats, testing incident response capabilities, and reviewing vendor cybersecurity practices. Firms must maintain evidence of these activities to demonstrate compliance during FINRA exams or audits.

How would SmartSuite support FINRA Cybersecurity Guidance?

SmartSuite supports FINRA Cybersecurity Guidance by providing tools for risk tracking, control management, and evidence collection across core FINRA domains. Its platform enables ongoing audit readiness, remediation tracking, and automated compliance reporting, allowing organizations to centrally manage their cybersecurity program and prepare for regulatory oversight.

License included / downloadable: Yes FINRA cybersecurity guidance is publicly available through official FINRA publications and regulatory notices.

Full framework page and mappings: smartsuite.com/frameworks/finra-cybersecurity-guidance