SmartSuite

Framework / Cybersecurity / Other

FINRA Cybersecurity Guidance: Report on Cybersecurity Practices (2015), Report on Selected Cybersecurity Practices (2018), Cybersecurity Effective Practices (2026) and the Annual Regulatory Oversight Report



What it is

FINRA Cybersecurity Guidance is the body of non-binding guidance the Financial Industry Regulatory Authority publishes for its member broker-dealers. It comprises the Report on Cybersecurity Practices (February 2015), the Report on Selected Cybersecurity Practices (December 2018) and the Cybersecurity Effective Practices framework of 12 principles (August 2026). It also includes the cybersecurity section of the Annual Regulatory Oversight Report, most recently the 2026 edition released on December 9, 2025. Every FINRA member firm is examined against the rules this guidance explains, chiefly SEC Regulation S-P Rule 30, Regulation S-ID and FINRA Rules 3110 and 4370.

At a glance

PUBLISHER
Financial Industry Regulatory Authority (FINRA); underlying rules adopted by the SEC

TYPE
Guidance

VERSION
Cybersecurity Effective Practices, August 2026 (12 principles); 2026 Annual Regulatory Oversight Report, December 9, 2025

EFFECTIVE
No legal effective date (guidance); Regulation S-P amendments effective August 2, 2024, compliance December 3, 2025 and June 3, 2026

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States

INDUSTRY
Financial Services

ADOPTION MODEL
Industry Requirement

IMPLEMENTATION COMPLEXITY
High

Source: finra.org/rules-guidance/key-topics/cybersecurity

Why it matters

- **One place to read FINRA's expectations** The August 2026 Cybersecurity Effective Practices framework gathers 12 principles, from Governance to Resilience and Recovery, each with practices FINRA says are scalable to firms of all sizes.
- **A direct line to the binding rules** Each document ties its practices to Regulation S-P Rule 30(a), Regulation S-ID, FINRA Rules 3110 and 4370 and the Exchange Act recordkeeping rules 17a-3 and 17a-4, so a firm can show which obligation each control serves.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports FINRA Cybersecurity

Principle-to-Rule Control Library

Load the 12 effective-practice principles as controls, tag each with the obligation it supports and assign an owner and a review date.

Regulation S-P Incident Response Workflow

Run the incident response program with the 30-day customer notice clock, the 72-hour vendor notice, decision records and the documentation Regulation S-P requires.

Rule 4370 Business Continuity Register

Keep the plan's ten required elements, the annual review by a registered principal, customer disclosure text and the two emergency contact persons in one record.

Vendor and Third-Party Oversight

Track due diligence, data access and monitoring for each service provider under Third Party Risk Management, with evidence linked to the principle it satisfies.

Annual Threat Review

Record the threats and effective practices named in each Regulatory Oversight Report, rate the firm against them and assign remediation tasks with due dates.

Examination Evidence and Reporting

Report control status, open findings and evidence coverage to leadership and produce the examination request package from the same data.

Common framework mappings

EU DORA · FFIEC IT Handbook · 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

FINRA Report on Cybersecurity Practices (February 2015)

FINRA's 2015 report on broker-dealer cybersecurity practices across governance, risk assessment, technical controls, incident response, vendor management, training, intelligence sharing and cyber insurance.

finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

FINRA Report on Selected Cybersecurity Practices (December 2018)

Effective practices observed by FINRA for branch office controls, phishing, insider threats, penetration testing and mobile devices.

finra.org/sites/default/files/Cybersecurity_Report_2018.pdf

FINRA Cybersecurity topic page

FINRA's hub for cybersecurity rules, notices, reports and small-firm resources.

finra.org/rules-guidance/key-topics/cybersecurity

FINRA 2026 Annual Regulatory Oversight Report — Cybersecurity

The cybersecurity section of FINRA's current oversight report: findings, effective practices and emerging threats.

finra.org/rules-guidance/guidance/reports/2026-finra-annual-regulatory-oversight-report/cybersecurity

Frequently asked questions

What documents make up FINRA's cybersecurity guidance?

Four main pieces: the Report on Cybersecurity Practices (February 2015), the Report on Selected Cybersecurity Practices (December 2018), the Cybersecurity Effective Practices framework of 12 principles (August 2026) and the cybersecurity section of the Annual Regulatory Oversight Report, whose 2026 edition was released on December 9, 2025. FINRA also issues Regulatory Notices and cyber alerts on specific threats.

 © 2026 SmartSuite Inc. All rights reserved.

Is FINRA's cybersecurity guidance binding?

No. Each document states that it creates no new legal or regulatory requirements. The obligations come from SEC Regulation S-P Rule 30, Regulation S-ID and FINRA Rules 3110 and 4370, and FINRA examines member firms against those rules. The guidance shows the practices FINRA expects to find behind them.

What are the 12 principles in the August 2026 framework?

Governance; Risk Management; Third-Party Risk Management; Asset Management; Access Control and Identity Management; Data Protection; Security Awareness and Training; Vulnerability and Patch Management; Security Monitoring; Threat Intelligence and Information Sharing; Incident Response and Reporting; and Resilience and Recovery. FINRA describes each practice as scalable to firms of all sizes.

How did the 2024 Regulation S-P amendments change what broker-dealers must do?

The SEC adopted the amendments on May 16, 2024 (effective August 2, 2024). Covered firms must run a written incident response program, notify affected individuals as soon as practicable and no later than 30 days after becoming aware of an incident, oversee service providers (which must notify the firm within 72 hours) and keep records. Larger entities had to comply by December 3, 2025 and smaller entities by June 3, 2026.

What does FINRA Rule 4370 require?

A written business continuity plan that addresses ten elements, including data backup and recovery, mission critical systems, financial and operational assessments, regulatory reporting and how customers will access their funds and securities. A senior management member who is a registered principal must approve the plan and review it annually, firms must disclose a summary to customers and report two emergency contact persons to FINRA.

License included / downloadable: Yes FINRA publishes its cybersecurity reports, the Cybersecurity Effective Practices framework and the Regulatory Oversight Report free of charge on finra.org; the platform links to the official documents.

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

 © 2026 SmartSuite Inc. All rights reserved.