2.10.2025

NAVIGATING FINRA'S 2025 THIRD-PARTY RISK UPDATES: COMPLIANCE STRATEGIES FOR FINANCIAL INSTITUTIONS

Justin P. Senior, Associate | jsenior@shumaker.com | 941.364.2792

Every year, the Financial Industry Regulatory Authority (FINRA) issues an Annual Regulatory Report in an effort to provide FINRA Member Firms with insight into findings from FINRA's regulatory operations programs. The Annual Report is intended to be an evolving resource, and FINRA just released its 2025 Annual Regulatory Oversight Report on January 28, 2025.

This year's Report addresses an entirely new category for guidance: **Third-Party Risk Landscape.**

Financial institutions increasingly rely upon third-party vendors for critical operations, creating both opportunities and compliance risks in equal measure. The Report underscores the growing risks associated with third-party vendor relationships—particularly cybersecurity threats and service outages. As regulatory expectations develop, firms must enhance their third-party risk management programs to align with FINRA's latest guidance.

Key Updates from FINRA's 2025 Guidance on Third-Party Risk

FINRA has observed increased cyberattacks and outages among third-party vendors supporting essential financial systems. Given this heightened risk, the new guidance reinforces firms' supervisory obligations under FINRA Rules 3110 (Supervision) and 4370 (Business Continuity Planning), as well as broader regulatory requirements such as Regulation S-P (Customer Information Protection).

To maintain compliance, firms must establish robust oversight mechanisms for vendor management, cybersecurity, and data protection. The Report highlights areas where firms have fallen short in examinations and offers a roadmap for improvement.

Key Compliance Considerations from FINRA

1. Strengthening Vendor Oversight
- Establishing and maintaining comprehensive third-party risk management policies.
- Conducting due diligence before engaging outside vendors—especially for cybersecurity, anti-money laundering (AML) monitoring, and IT systems.
- Validating data security controls in vendor contracts to ensure regulatory compliance.

2. Enhancing Incident Response Planning
- Involving third-party vendors in cybersecurity and incident response testing.
- Maintaining an updated inventory of third-party services, software, and infrastructure components.
- Implementing protocols to ensure secure data return or destruction when a vendor relationship ends.

3. Addressing Fourth-Party Risks
- Assessing vendors' use of subcontractors (fourth parties) and their potential impact on firm operations.
- Ensuring contractual safeguards and transparency in third-party relationships.

4. Adapting to Emerging Risks (Generative Artificial Intelligence (AI) Considerations)
- Evaluating whether vendors incorporate Generative AI (Gen AI) in their services.
- Adjusting vendor contracts to prohibit unauthorized data ingestion into open-source AI models.
- Reviewing AI-powered tools to ensure compliance with recordkeeping and supervisory requirements.

Practical Steps for Compliance Officers and Legal Teams

Firms should take proactive measures to align their third-party vendor oversight with FINRA's latest expectations. Effective strategies include:

1. Reviewing and Updating Vendor Contracts – Ensure contracts include specific cybersecurity, data protection, and termination provisions.
2. Implementing Strong Due Diligence Protocols – Conduct regular assessments of vendor security practices and operational reliability.
3. Enhancing Internal Training and Supervision – Educate staff on the risks and regulatory expectations surrounding third-party relationships.
4. Maintaining a Centralized Vendor Inventory – Catalog all third-party and fourth-party relationships for better risk monitoring.
5. Engaging with FINRA – Leverage FINRA's Risk Monitoring program to stay informed about industry trends and emerging risks.

As cyber threats and operational disruptions become more frequent, proactive third-party risk management is essential for maintaining compliance and safeguarding business continuity. FINRA's updated guidance provides a clear framework for legal and compliance teams to reassess their supervisory procedures, incident response plans, and vendor contracts.

Firms should conduct a comprehensive review of their third-party vendor policies to ensure alignment with FINRA's evolving expectations, as outlined herein. Implementing the effective practices outlined in the report will be critical for maintaining regulatory compliance in 2025 and beyond.

Please do not hesitate to reach out to Justin Senior or a member of our team for more information.