GUIDE

Cybersecurity vs. Cyber Compliance: The Complete Guide for Financial Services

Understand the differences, regulatory expectations, and risk-management requirements shaping cyber programs in financial services

smarsh

Introduction: Why cybersecurity and cyber compliance are not the same

Cybersecurity isn't new — it's been a major concern and frequent topic of discussion in the financial services industry for decades. In more recent years, a different but related area is gaining regulatory attention: cyber compliance.

Many people understandably think these are interchangeable terms and mean the same thing. However, cybersecurity and cyber compliance are distinctly different and describe different (but equally important) concepts.

To complicate matters, firms must treat cybersecurity and cyber compliance as integrated disciplines rather than different priorities with the increase of digital transformations, AI-driven attacks, and regulatory scrutiny.

In this guide, you'll learn how to:

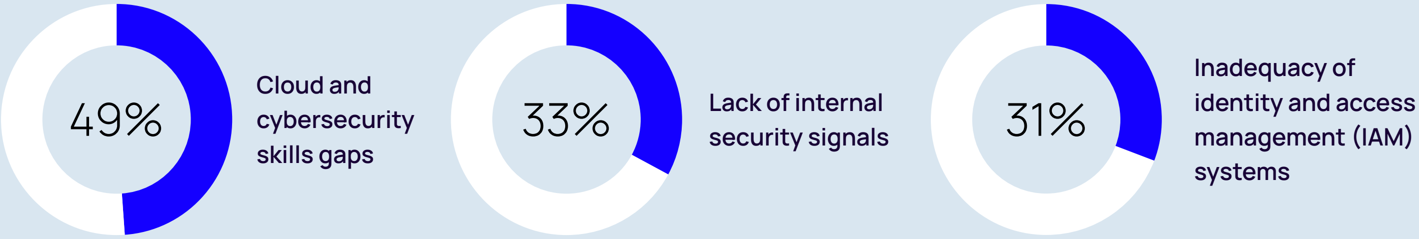
- Differentiate these terms and how they relate to your overall data management strategy
- Demonstrate to regulatory bodies that you have a proactive, continuous program in place
- Achieve and establish a robust risk posture by using automated compliance review technologies

What is cybersecurity?

Most firms understand cybersecurity as the controls that are in place to protect their IT infrastructure. This includes end-user devices, networks, cloud assets, applications and their business and customer data.

Cybersecurity has traditionally been a risk that falls under the purview of IT and encompasses the gamut of accountability from infrastructure to employee training.

The financial industry is primarily focused on internal challenges (multi-select responses), such as[1]:



[1] Cyber Resiliency in the Financial Industry Survey Report

Why cybersecurity must include third-party risk management

Establishing these cybersecurity pillars will enable firms to address changes and trends caused by the evolving technology landscape. Most firms already have cybersecurity policies in place to support hybrid and work-from-anywhere models.

However, cybersecurity isn't just about securing internal data. It's also recognizing third-party access to sensitive data. More than ever, firms are turning to partner vendors or third-party applications to maximize the value of their data. And having more access points means having more cyber risks.

Third-party risk management is an important part of a firm's larger cybersecurity strategy. It's vital to ensure that vendors that have access to your data also have a robust security posture. As firms add more vendors, they need to consider:

- How does the vendor approach cybersecurity?
- Does the vendor have risk remediation strategies?
- Does the vendor have an existing risk management process?

Firms need to have standards and systems in place to manage third-party security risks. New risks are always emerging, so it's important to regularly assess vendors to ensure they're evolving their controls over time.

What is cyber compliance?

Cyber compliance describes the aligning of cybersecurity systems to regulatory agency requirements. However, one of the biggest mistakes firms make is treating cyber compliance as a solely cybersecurity — or IT — issue.

Ensuring processes, procedures, reporting and recordkeeping are a part of your larger cybersecurity framework. While it's true that IT leads cybersecurity initiatives, firms need to recognize that regulatory agencies are making cybersecurity a priority. Recent SEC and FINRA actions emphasize risk-based programs and documented governance over prescriptive checklists, aligning cybersecurity controls with compliance accountability.

Compliance team's role in vendor oversight and cyber risk governance

A plan for collaboration between compliance and IT teams needs to be implemented for both cybersecurity and vendor risk management.

However, this doesn't just affect those who are managing processes and procedures. Reporting in plain terms to board members will be important so they can understand and make decisions based on current and future risks.

> "Operational disruption risks remain elevated due to the proliferation of cybersecurity attacks. Our focus for 2025 includes reviewing whether firms' policies and procedures, governance practices, access-controls, vendor oversight, and incident-response programs are reasonably designed to safeguard investor records and assets."
>
> SEC DIVISION OF EXAMINATIONS

How compliance teams demonstrate cyber and vendor risk readiness

Compliance teams play a critical role in demonstrating cyber and vendor risk compliance to board members and regulators. They must:

Review policies and procedures against gaps:

- Cybersecurity incident response and recovery
- Risk assessments
- User security and access
- Information protection
- Threat and vulnerability management
- Annual review and reporting
- AI systems and data model governance

Ensure recordkeeping:

- Vendor risk assessments
- Cyber incidents
- Policies
- Procedures
- Reports
- Reviews

Complete and file appropriate disclosures:

- Form ADV
- Fund Registration Statement
- Fund Prospectus
- Fund Annual Reports

Report significant incidents:

- Form ADV-C

So, what does this all mean?

With recent SEC amendments to Regulation S-P and evolving FINRA expectations, firms need to determine accountability for cyber compliance and vendor risk management — and define how to execute these processes efficiently.

Cybersecurity vs. cyber compliance: A side-by-side comparison

To recap, cybersecurity keeps threats out and cyber compliance keeps regulators satisfied. Together, they define a complete, defensible cyber-risk management posture.

	Cybersecurity	Cyber Compliance
Focus	Protect systems, networks, and data from cyber threats	Demonstrate and document adherence to regulatory expectations for safeguarding data and managing cyber risk
Managing role/teams	CIO, CISO, IT security	CCO, compliance, legal, risk
Goal	Prevent, detect, and respond to cyber incidents	Ensure policies, procedures, and managing documentation that meet SEC and FINRA requirements

How Smarsh supports cyber compliance for financial services

Regulators have made it clear that there will be no debate when it comes to data security. Firms have the fiduciary duty to apply practices that are in the best interest of their clients, including taking steps to minimize cybersecurity risks that could lead to significant business disruptions and harm to investors.

Smarsh simplifies compliance by automating review workflows (aligned to current SEC and FINRA expectations). Our software and services are purpose built to meet compliance obligations (FINRA, SEC, NIST, GDPR and more), so financial services firms have the tools they need for success.

Beyond compliance, Smarsh unifies protection across email, collaboration platforms, voice, social, and generative AI tools. By creating a single system of record, firms can better identify, manage, and mitigate risks across the full spectrum of cybersecurity, privacy, IP, and regulatory challenges.

To learn more about cyber compliance solutions purpose-built for financial services firms, visit Smarsh.com.

smarsh

Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals from the most in-demand communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions.
You must consult your attorney regarding your compliance with applicable laws and regulations.

Guide - 12/25

☎ 1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh