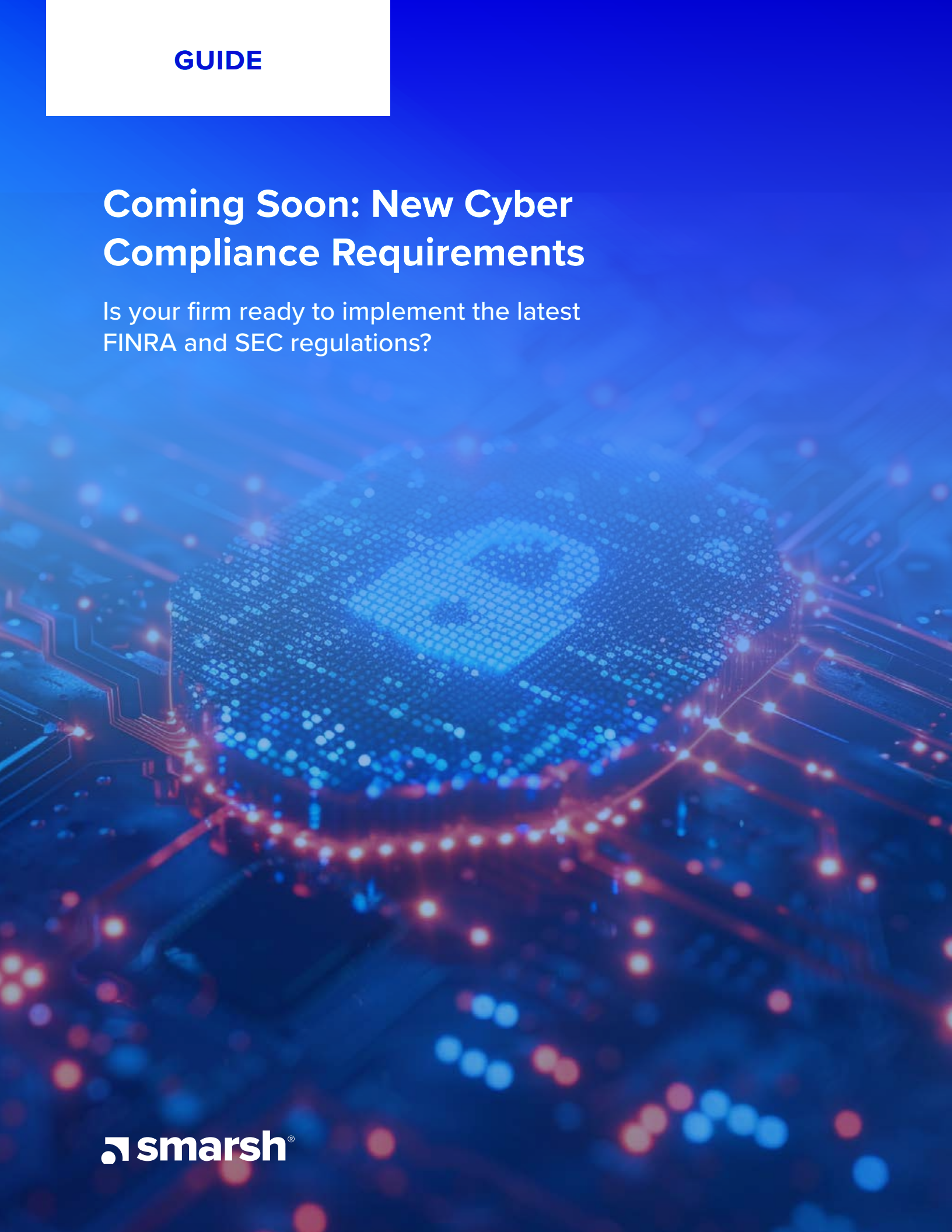
GUIDE

Coming Soon: New Cyber Compliance Requirements

Is your firm ready to implement the latest FINRA and SEC regulations?



smarsh®

The financial services sector is undergoing a cyber compliance evolution. This means firms are receiving increasingly precise guidance from FINRA and the SEC, and new amendments and rules mean new compliance requirements are to follow.

With the constant threat of cyber-attacks or data mismanagement, firms must ensure their cyber compliance governance is in good standing. Data breaches can ruin a firm's reputation and cost hundreds of thousands of dollars in damages from litigation and regulatory fines.

This guide provides an overview of the latest FINRA and SEC amendments that will soon be enforced.

Understanding the new cyber compliance expectations

Financial and investment firms must stay constantly vigilant to detect and investigate potential data breaches. FINRA amendments have recently been added for consideration to SEC rules with some added requirements to ensure:

- Secure maintenance and operational controls over the firm's data and communications *(SEC Rule 10)*
- Minimized user-related risks and unauthorized access from hackers and cyber-attacks *(SEC Rule 30)*
- Documented plans are in place to detect, mitigate, and remediate all cybersecurity threats and vulnerabilities in writing *(FINRA Rule 3120)*
- Quick response to, reporting on and recovery from any cyber compliance breaches *(FINRA Rule 4370)*
- Annual reviews and assessments of the design and effectiveness of the firm's cyber compliance policies and procedures are performed annually *(FINRA Rule 3110.8)*
- Assessments reflect any changes made to cyber compliance or said governance risk over the period covered by the review *(FINRA Rule 4370)*
- Periodical assessment of risk plans to ensure cyber compliance governance is up to date *(FINRA Rule 3110.8)*

> “We know that cybercriminals are always one step ahead…adopting strong and robust policies and procedures is arguably the most important rule you should have in place at your firm.”
>
> *Steve Trigili, CCO of Garden State Securities and Garden State Investment Advisory Services*

The FINRA Annual Regulatory Oversight Report provides detailed information and about the latest updates and amendments in conjunction with the SEC.

Read the Complete FINRA Report

Several new amendments call for more active business continuity and disaster recovery planning related to cyber compliance governance and communications technology. Others call for more robust measures to protect data and archive data records.

This latest release of requirements builds upon existing regulations by strengthening transparency and incident reporting. It requires firms to ensure these four key elements are activated.

1. Implement written cybersecurity policies and procedures that promptly address cybersecurity risks and incidents.

2. Promptly share written recordkeeping policies with advisers and funds.

3. Confidentially report to the SEC if the adviser (or a fund they advise) is subject to specific cybersecurity incidents.

4. If specific cybersecurity incidents occur, disclose them in writing on brochures and registration statements for registered funds.

The importance of implementing cyber compliance requirements

The SEC and FINRA explained their reasoning for making new cyber compliance requirements into rules: to provide added assurance and reduce the risks posed by significant data breaches and other incidents.

As data grows in volume and complexity, so do the threats through cyber intrusion, denial of service attacks, manipulation, misuse by insiders, and other cyber misconduct. The new rules and amendments are designed to enhance cyber compliance preparedness beyond the obvious reasons and improve investor confidence in the resiliency of advisers and funds against cybersecurity threats.

> “Realistically, many of these compliance regulations should already be in place.”
>
> *Wiley Asher, cybersecurity compliance subject matter expert at Smarsh*

The good news is that FINRA and the SEC will allow a long runway for when these new requirements need to be implemented. The timeline for new compliance regulations to be put in place is 24 months for large enterprises and 18 months for small to mid-sized businesses. The clock start time is still in the air, depending on when these new regulations are signed into books, but the expectation is that these new requirements will need to be implemented in 2025.

There are too many details to keep track of manually, and using a variety of software tools can get confusing. The SEC recommends assigning at least one team member dedicated to ongoing cyber compliance governance and planning. Smarsh solutions can help you achieve cyber compliance with proactive support to manage it all for your firm.

> “If you have lax procedures and you’re not able to hold compliance in place, your firm is vulnerable to hefty fines and a tarnished brand reputation, or worse case; may be forced to close your doors,” said Trigili.

Why cyber compliance timing matters

If your firm has not already evaluated its electronic communications compliance policies, procedures, and internal controls, it should do so sooner rather than later.

Unfortunately, cyber incidents happen often, and the risk landscape is still treacherous. Cyber compliance technology and governance failures can lead to substantial financial, operational, legal, and reputational harm for advisers and funds, and even more importantly, they can lead to investor harm.

Key takeaways

- New regulations require financial services firms to provide specific reporting measures to stay resilient against cyber threats and operational disruptions
- Implementing effective compliance solutions streamlines operational integrity and reduces the risk of threats and disruptions
- Compliance is essential for avoiding further regulatory scrutiny, fines, and a negative reputation
- Save time and resources and ensure the cyber compliance technology governance follows any new or changing regulations

> "What are you doing to protect your network, endpoints, and internal communications documentation? Do you have your technology audit plan in place? ... It comes down to firms creating their own plan and then following their own policy," said Asher.

Proactively manage cyber compliance requirements

Financial services firms must always be prepared for potential cyber risks and threats. The Smarsh Cyber Compliance platform empowers firms to meet regulatory requirements with simple-to-use monitoring, remediation, and reporting automation. Streamline risk assessment processes with proactive solutions that help you stay ahead of compliance requirement deadlines.

The FINRA and SEC requirements can seem complicated, but Smarsh simplifies cyber compliance with our single-pane-of-glass solution. All firms — no matter their size — need a robust operational cyber compliance governance framework that can withstand regulatory scrutiny and foster long-term trust, integrity, and growth.

smarsh®

Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals from the most in-demand communications channels. Regulated agencies 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. federal, state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com

---

Guide - 10/24

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