The SEC's Proposed Cyber Requirements

ACA Aponix®

On February 9, 2022, the Securities and Exchange Commission (SEC) voted to establish a formal set of cybersecurity risk management rules and requirements. Aimed at registered investment advisers and funds, these are designed to bolster investors' confidence in the advisers' and funds' operational resiliency as well as the safety of their investments. The new rule requires firms to implement cybersecurity policies and procedures while allowing them to tailor to their business size and scope.

Though the rule has not yet been finalized, the proposal outlines several requirements firms can likely expect and for which they should prepare. We have read and analyzed the proposed rule to help clarify many of these expectations. Find our breakdown below.

Twelve Expected Requirements of Rule 206(4)-9

Expected Requirement	Call to Action
Risk Assessment	Assess, prioritize, categorize, and document cybersecurity risks associated with their systems and information. The assessment should: • Occur no less often than annually and be formally documented • Identify the service providers who have access to fund information or information systems • Inform senior management of risks that can result in significant cybersecurity incidents along with remediation steps
User Security & Access	Limit the possibility of unauthorized access to fund and adviser information and systems. The controls must: • Outline acceptable behavior of individuals with access to adviser or fund information systems • Identify and validate users, such as through multifactor authentication (MFA) • Establish timetables for the distribution, replacement, and revocation of credentials • Appropriately restrict access to fund and adviser information • Secure remote access communication technologies
Information Protection	Monitor information systems and protect data from unauthorized use. Protections should: • Regularly detect anomalous behavior • Prevent unauthorized parties from interacting with data • Be periodically assessed
Vendor Management	Oversee service providers that receive, retain, or manage fund or adviser information, or have access to information systems. Firms should require through written contracts that these providers: • Implement and maintain policies and procedures to protect firm data

Expected Requirement	Call to Action
Threat & Vulnerability Management	Detect and mitigate cybersecurity threats and vulnerabilities that affect adviser or fund information or systems. This management should include: • Ongoing monitoring, scanning, patching, and tracking of vulnerabilities • Monitoring trusted government and industry sources for new vulnerability information • Role-specific threat and vulnerability response training
Cybersecurity Incident Response & Recovery	Write policies and procedures to identify, respond to, and recover from cybersecurity incidents that may lead to business disruptions. These policies must be annually tested and should facilitate: • Business operation continuity • Establishment and testing of an incident response plan • Internal and external information sharing • Incident disclosure and reporting
Annual Review & Required Written Reports	Review cyber policies and procedures annually at minimum to ensure they work as planned and that responsibilities are delegated appropriately. Firms must: • Assess the design and effectiveness of their cybersecurity policies and procedures, and determine whether they reflect changes in cybersecurity risk since the prior review • Write a formal report to describe the annual review, assessment, control tests performed and accompanying results, cybersecurity incidents, and policy changes since the last report
Fund Board Oversight	Board-authorizing funds for cybersecurity policies and procedures. Fund board oversight should not be a passive activity, meaning boards should: • Approve and review the fund's cybersecurity policies and procedures • Review written reports to understand the fund's cybersecurity risk, incidents, and material changes to the fund's policies and procedures • Ask questions and seek clarification regarding program effectiveness, available resources, and cybersecurity expertise • Determine the level of oversight of service providers based on business operations
Recordkeeping*	Maintain, create, and preserve books and records. Firms generally should maintain: • A copy of cybersecurity policies, assessments, and annual policy reviews, as well as the policies and procedures, from the last five years • A copy of any Form ADV-C/incident report filed to the SEC in the last five years (as applicable) • Records of any cybersecurity, including related response and recovery activities, from the last five years

Expected Requirement	Call to Action
Form ADV-C	Report significant cybersecurity incidents to the SEC in form ADV-C. Firms should: • Report within 48 hours of determining that a significant cybersecurity event has happened or is currently happening • Amend Form ADV-C when information becomes outdated and/or inaccurate, new information is discovered, or when an incident is resolved
Adviser Disclosures	Disclose cybersecurity risks and incidents in plain English to investors and other market participants when their advisory services are materially affected. Advisers will be required to: • Describe all cybersecurity risks (regardless of whether they have led to a disruption) that could materially impact their advisory services, as well as how they assess, prioritize, and address the risks • List cybersecurity incidents within the last two fiscal years that lead to harm of the adviser and/or its clients
Fund Disclosures	Disclose cybersecurity risks and incidents in plain English to prospective and current investors. Funds would be required to: • Describe any cybersecurity incidents in the last two fiscal years • Tag new information in a structured data language (Inline eXtensible Business Reporting Language or "Inline XBRL") • Disclose to investors in its registration statement if a cyber incident has or is currently affecting the fund or its service providers

**Actual retention periods and materials will vary amongst advisers and funds*

How ACA Can Help

Firms should not wait for the rule's ratification to become compliant. Our ACA Aponix team offers an **SEC Cybersecurity Rule Gap Analysis**, which maps out the requirements of the proposed regulation service in order to:

- Compare a firm's current state of cybersecurity policies and procedures against the proposed requirements
- Validate compliance through documented examples
- Identify gaps where a firm may be missing policies, procedures, or formal evidence of compliance

We help firms achieve compliance with the SEC's expected requirements. Learn more about our ACA Aponix cybersecurity, technology risk, and privacy solutions **here**.