Beyond Compliance: Unlocking the Benefits of Robust Cybersecurity for RIAs

Cybersecurity Policy Timeline

Industry insiders are reporting that the new SEC Cybersecurity rules may be coming as early as October 2023. Are you prepared?

We've developed a timeline to help you plan. As a world-class technology solution, IT support, cybersecurity, and hosting services provider, we're also here to help you every step of the way.

Research and Analysis

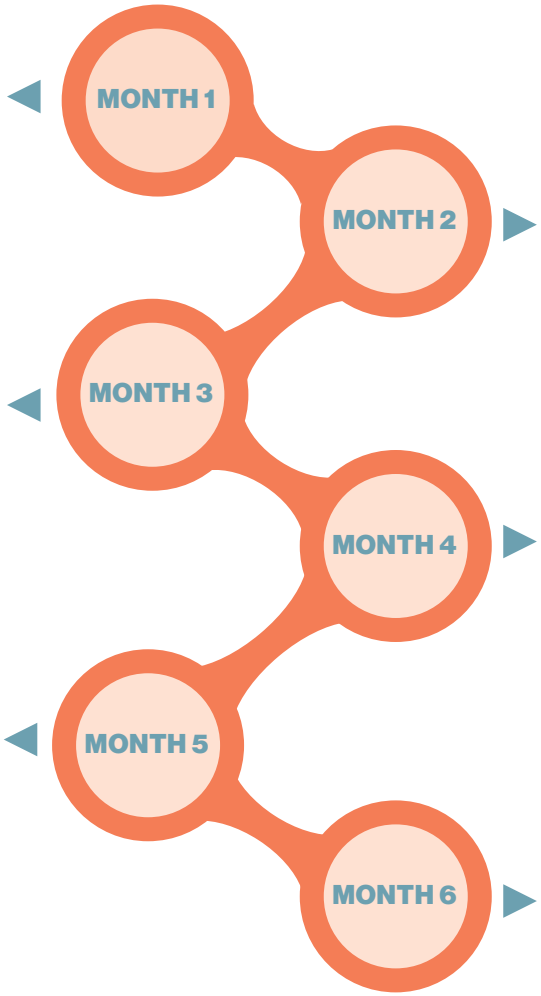
- Review the new SEC cybersecurity rules in detail.
- Understand the scope and implications of the rules for your organization.
- Identify any gaps between your current cybersecurity practices and the new requirements.

Policy and Procedure Updates

- Develop or update your cybersecurity policies and procedures to align with the new SEC rules.
- Ensure that policies cover areas such as data protection, incident response, risk assessments, and vendor management.
- Involve legal and compliance teams in reviewing and approving the policies.

Implementation, Training and Awareness

- Execute the necessary changes and improvements to your cybersecurity infrastructure.
- Enhance data protection measures, encryption practices, access controls, and monitoring systems.
- Implement processes for continuous vulnerability assessment and patch management.
- Conduct training sessions to educate employees about the updated cybersecurity policies and procedures.
- Raise awareness about the importance of cybersecurity and individual responsibilities.
- Train employees on identifying and reporting potential security incidents.



Gap Assessment

- Conduct a comprehensive assessment of your existing cybersecurity infrastructure and practices.
- Identify areas where your organization may fall short of the new SEC rules.
- Prioritize areas of improvement based on risk and potential impact.

Resource Allocation

- Assess the resources (human, financial and technological) required to implement the new cybersecurity measures.
- Allocate necessary resources and secure budget approvals, if needed.
- Identify any external vendors or consultants that may be required for specialized expertise.

Testing, Validation and Compliance Monitoring

- Perform rigorous testing of your cybersecurity controls and measures.
- Conduct vulnerability assessments, penetration testing, and security audits.
- Address any vulnerabilities or weaknesses identified during testing.
- Establish a robust monitoring program to ensure ongoing compliance with the new SEC rules.
- Regularly review and update cybersecurity policies and procedures as necessary.
- Conduct periodic internal audits to assess adherence to the rules.

Preparing for the new SEC cybersecurity rule is essential for RIAs to comply with regulatory requirements, protect client information, mitigate legal and reputational risks, and maintain operational continuity in an increasingly digital and threat-prone environment. Contact Visory https://www.visory.net to help you get started today.

Visory | www.visory.net | (913) 396-4600