DATASHEET

Radar® Compliance

Operationalize SEC Rules in Radar ® Compliance

Simplified compliance with SEC cybersecurity requirements.

On July 26, 2023, the U.S. Securities and Exchange Commission (SEC) adopted new rules that require registrants with the SEC to disclose cybersecurity risks and incidents that may be material to investors.

Additionally, the rules require registrants to provide an annual report disclosing their approach to risk management and governance of cybersecurity events.

SEC Obligations

The U.S. Securities and Exchange Commission (SEC) is a federal agency tasked with protecting investors by ensuring a fair and transparent market.

The agency's new cybersecurity rules, which took effect in December 2023, aim to increase the consistency and comparability of cybersecurity risk reporting and event disclosure by SEC registrants to ensure that investors have the data required to make sound decisions.

Did You Know?

Due to the intent behind the new rules, the SEC is particularly concerned with registrants being able to "show their work," i.e. prove they have a controls process in place to ensure consistency in their cybersecurity event reporting procedures and documentation.

The controls process, i.e. consistency, is crucial whether an organization experiences a single incident a year, or multiple. A single incident can be costly, both to stakeholder trust, as well as to a company's bottom line.

The SEC cybersecurity rules requirements include:

- **Event Reporting:** Cybersecurity incidents deemed to be material to investors must be disclosed to the SEC.
- **Disclosure Timeline:** Registrants have four business days to disclose a cybersecurity event once a determination of materiality has been made.
- **Accidental vs. Malicious:** Events must be disclosed if malicious, as well as if they were deemed to be accidental, or due to unauthorized but nonmalicious access.
- **Annual Report:** Registrants must provide an annual report disclosing their cybersecurity risk management, strategy, and governance, regardless of whether they experienced a reportable cyber incident.

SEC Cybersecurity Use Case

Radar® Compliance addresses the need for a demonstrable controls process around cyber event notification triggers via a configurable workflow solution. This allows organizations to verify, against their own predetermined criteria and risk matrix—and in a consistent and standardized manner—whether there is a need to notify the SEC of a cybersecurity event.

While many organizations already have a clearly defined risk matrix, they often cannot consistently and transparently operationalize cyber-based event assessments against their own notification triggers.

The configurable workflow offered by Radar® Compliance operationalizes security, risk, and cyber requirements with their associated internal and external notification obligations, shortening the time spent getting to a notification decision, freeing up resources for incident investigation, and providing a transparent process to all stakeholders—including the SEC.

The result is a **streamlined, company-wide cybersecurity compliance process that enables cross-functional collaboration and risk mitigation between IT, InfoSec, cybersecurity, privacy, legal, HR, and compliance teams**.

Organizations can be confident that they not only fulfill event notification obligations to all stakeholders, from the SEC to the Board of Directors, and, critically, also meet the regulatory requirement for defensible and consistent documentation and annual reporting of cybersecurity risk management, strategy, and governance.

SEC Obligations made Easy with Radar® Compliance

The SEC's new cybersecurity rules consider that cyber events are inevitable. **They expect that registrants are prepared for the inevitable with consistent processes for documenting, assessing, and notifying** to safeguard investors and the market at large. The first time you trial a cybersecurity incident playbook should never be in the midst of a live remediation effort.

Radar® Compliance operationalizes registrants' risk matrices, ensuring that both primary requirements of the SEC's cybersecurity rules can be satisfied: consistent and timely event disclosure, and annual reporting on risk management, strategy, and governance.

Additionally, organizations that adopt Radar® Compliance meet not only the letter, but the spirit of the SEC rules, i.e. the ability to prove that your organization, from Risk to InfoSec to Compliance, all follow a predetermined, consistent, and automated process for assessing, documenting, and disclosing cybersecurity events.

Avoid costly penalties and fines—and an erosion of investor and public trust—by operationalizing your SEC risk matrix within Radar® Compliance.

INFO@RADARFIRST.COM | 1.844.737.3778

Schedule a Demo >

RadarFirst

Learn more at radarfirst.com

RadarFirst offers enterprise risk solutions to automate intelligent decisions for state, federal, international, and industry-specific regulations. Our patented assessment technology enables organizations to act quickly to determine obligations with evolving legal, contractual, and regulatory requirements. With RadarFirst, organizations can confidently navigate complex privacy and compliance reporting with consistent, documented decision-making.