Define and Document SEC and Cyber Risk Compliance

Define and document cyber risk management with a consistent, collaborative compliance solution.

On July 26, 2023, the U.S. Securities and Exchange Commission (SEC) adopted new rules requiring SEC registrants, including publicly traded retail and healthcare organizations, to disclose cybersecurity risks and incidents that may be material to investors.

Registrants must also provide an annual report disclosing their approach to risk management and governance of cybersecurity events.

The SEC is only one of several regulatory bodies, however, that now require the retail industry, which runs the gambit from healthcare to consumer packaged goods and fashion, to thoroughly document and report on cyber events—as well as on company-wide processes and procedures designed to mitigate risk.

Why Documentation is Critical for Risk Mitigation

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 documentation**.

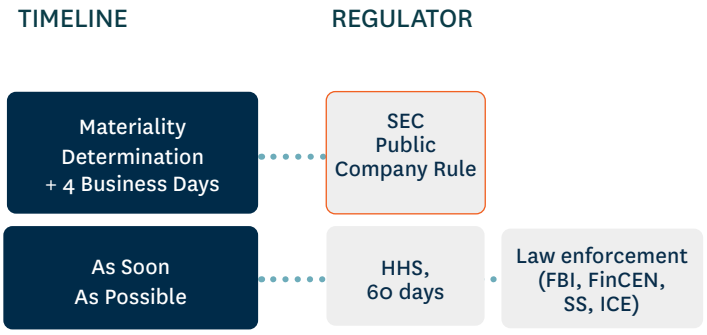
The controls process, i.e. consistency, is crucial whether an organization experiences a single incident a year, or multiple. A single incident can be costly, both to stakeholder trust, as well as to a company's bottom line.

The SEC'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 reporting 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, as evidenced by these cyber incident regulatory notification timelines mandated by a broad spectrum of potential regulators.

Cyber Event Notification Timelines For Public Healthcare Companies



Automate SEC and Cyber Risk Requirements in Radar® Compliance

✅ Event Reporting

Cybersecurity incidents deemed to be material, for instance, to investors according to SEC regulations, must be disclosed. **Radar® Compliance** streamlines the reporting process to verify reporting requirements against the organization's own predetermined risk matrix.

✅ Meeting Disclosure Timelines

Publicly traded retail and healthcare organizations can have as little as 4 business days to disclose a cybersecurity event once a determination of materiality has been made. **Radar® Compliance** supports speedy disclosures by surfacing regulator-specific disclosure timelines.

✅ Accidental vs. Malicious Events

Many regulators, including the SEC, require events to be disclosed if malicious, as well as if they were deemed to be accidental or due to unauthorized but nonmalicious access. When all events are assessed and documented within **Radar® Compliance**, organizations can easily report on all events, whether malicious or accidental.

✅ Annual Reporing Requirements

Retail and healthcare companies that are publicly traded must provide an annual report disclosing their cybersecurity risk management, strategy, and governance, regardless of whether they experienced a reportable cyber incident. **Radar® Compliance** ensures organizations have a predetermined and demonstrable controls process that can easily be shared with regulators to meet annual report requirements.

SEC and Cyber Risk Obligations Made Easy with Radar® Compliance

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 report a cybersecurity event to all critical stakeholders and regulators.

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, but also, critically, **meet the regulatory requirement for defensible and consistent documentation and annual reporting** of cybersecurity risk management, strategy, and governance.

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.