

SEC Cybersecurity Disclosure Rule – Item 1.05 (Form 8-K) / Item 106 (Reg. S-K) – 2023



SEC Cybersecurity Disclosure Rule requires public companies to disclose material cyber incidents and annual cybersecurity risk management and governance.

What it is

The SEC Cybersecurity Disclosure Rule (2023) is a U.S. securities regulation that requires publicly traded companies to disclose material cybersecurity incidents and provide annual updates on their cybersecurity risk management, strategy, and governance. This rule aims to enhance transparency and ensure investors receive timely and consistent information about cybersecurity risks and events that may impact a company's financial position or operations.

Issued by the U.S. Securities and Exchange Commission (SEC), the rule applies to all domestic and foreign public companies registered with the SEC. It focuses on the disclosure of material cybersecurity incidents, board oversight, risk management processes, and the company's approach to handling data protection and cyber threats, expanding compliance obligations in line with evolving cyber risk landscapes.

At a glance

PUBLISHER U.S. Securities and Exchange Commission (SEC)	TYPE Regulation	VERSION SEC Cybersecurity Disclosure Rule (2023)
EFFECTIVE September 2023	DOMAIN Financial Services Regulation	FAMILY Other
REGION United States	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.sec.gov/securities-topics/cybersecurity>

Why it matters

- **Strengthen board oversight** Improve executive engagement by requiring the board and management to oversee cybersecurity strategy and risk management processes.
- **Enhance investor transparency** Ensure investors receive timely, consistent disclosures about cybersecurity incidents that may impact financial performance or operations.
- **Support regulatory compliance** Align information security practices with SEC requirements, reducing risks of enforcement actions and reputational harm.
- **Improve incident response accountability** Mandate formal incident response planning and reporting, which leads to more effective organizational response and recovery from cyber events.

How SmartSuite supports SEC Form 8-K Item 1.05SEC Reg S-K Item 106

Governance and Oversight Documentation Track leadership roles, board reporting, and cyber risk governance artifacts.	Materiality Decision Workflow Run a repeatable process for incident evaluation, documentation, and approvals.	Incident Timeline and Evidence Trail Capture actions, decisions, and communications in a complete incident record.
Risk Management Program Evidence Centralize risk assessments, controls, and assurance artifacts that support disclosures.	Third-Party and Concentration Risk Oversight Track key providers, monitoring, and contingency planning evidence.	Disclosure Readiness Reporting Report posture, incidents, open risks, and governance evidence for readiness.

Common framework mappings

CIS Controls v8.1

COSO IC 2013

ISO 27001:2022

NIST CSF 2.0

NIST 800-53 Rev.5

NYDFS 23 NYCRR 500

SOX

SOC 2

Official resources

SEC Cybersecurity Disclosure Rule Summary Outlines the key requirements and implications of the SEC's 2023 Cybersecurity Disclosure Rule. sec.gov/securities-topics/cybersecurity	SEC Cybersecurity Guidance Provides the SEC's official interpretative guidance on cybersecurity-related disclosures for public companies. sec.gov/rules/interp/2018/33-10459.pdf
--	--

Frequently asked questions

- What is the SEC Cybersecurity Disclosure Rule (2023) used for?**
The SEC Cybersecurity Disclosure Rule (2023) is designed to enhance transparency around cybersecurity risks and incidents affecting publicly traded companies. It requires organizations to disclose material cybersecurity incidents and provide updates on their cybersecurity risk management, governance, and strategy, ensuring investors have consistent and timely information about threats impacting a company's financial health.
- Is compliance with the SEC Cybersecurity Disclosure Rule mandatory?**
Yes, compliance with the SEC Cybersecurity Disclosure Rule is mandatory for all domestic and foreign public companies registered with the SEC. Failure to comply with the rule's disclosure requirements can result in regulatory penalties and enforcement actions.
- Who does the SEC Cybersecurity Disclosure Rule apply to?**
The rule applies to all companies—both US-based and international—that are publicly traded and subject to SEC reporting requirements. This includes any organization that files annual or periodic reports under the Securities Exchange Act of 1934.
- What key disclosures and artifacts are required under the rule?**
Organizations must disclose material cybersecurity incidents within four business days of determining materiality and provide annual updates on their cybersecurity governance, risk management processes, and strategy. Required artifacts include incident reports, descriptions of risk assessment processes, and documentation of board and management oversight.
- How do organizations implement the SEC Cybersecurity Disclosure Rule?**
Implementation involves developing incident response and evaluation procedures, updating disclosure controls, and integrating cybersecurity risk management into broader SEC reporting and corporate governance frameworks. Organizations should train relevant teams, establish clear criteria for materiality assessments, and maintain readiness to meet filing deadlines.

How does the SEC Cybersecurity Disclosure Rule relate to other cybersecurity frameworks?

While the SEC Cybersecurity Disclosure Rule is a regulatory requirement, organizations often align their cybersecurity programs with industry standards such as NIST or ISO 27001 to strengthen risk management and governance. Alignment with these frameworks can streamline compliance and support consistent reporting.

What ongoing compliance activities are required by the rule?

Ongoing compliance involves regularly assessing cybersecurity risks, ensuring timely identification and evaluation of potential incidents, maintaining updated governance documentation, and reviewing disclosure processes. Companies must monitor evolving threats and regulatory guidance to ensure disclosures remain accurate and complete.

How would SmartSuite support SEC Cybersecurity Disclosure Rule (2023)?

SmartSuite streamlines compliance by providing workflows for incident reporting, risk tracking, and governance activities. It supports control management, document retention, and evidence collection for disclosures, helping organizations demonstrate audit readiness. Reporting tools enable timely and accurate submissions to the SEC and maintain clear records to support regulatory reviews.

License included / downloadable: Yes The SEC Cybersecurity Disclosure Rule is publicly available through official U.S. Securities and Exchange Commission publications.

Full framework page and mappings: smartsuite.com/frameworks/sec-cybersecurity-disclosure-rule-2023-item-105-form-8k-item-106-reg-sk