Prevalent™

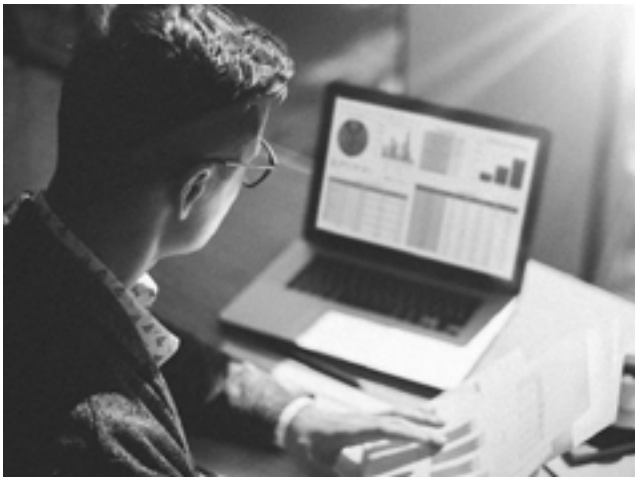
Third-Party Risk Management Compliance Checklist

U.S. Securities & Exchange Commission Cybersecurity Risk Management, Governance & Incident Disclosure Rules

Table of Contents

SEC Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure for Third Parties

In July 2023, the U.S. Securities and Exchange Commission (SEC) adopted new rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and incident reporting by public companies. The new amendments will be effective 30 days after publication in the Federal Register, and public companies are expected to begin reporting on the new requirements for fiscal years starting on or after December 18, 2023.



This paper reviews third-party considerations in the new SEC cybersecurity risk management amendments and rules, while identifying critical third-party risk management (TPRM) capabilities to address the requirements.

Summary of the SEC Cybersecurity Disclosure Rules

The SEC rules and amendments were introduced in March 2022 in response to a lack of consistency in public company cybersecurity incident reporting, which can erode investor confidence. The SEC publication notes that cybersecurity risks have recently been escalating for a variety of reasons, including companies' increasing reliance on third-party service providers for IT services and a growing number of cybersecurity incidents involving third-party service providers.

The new amendments are divided into two categories: reporting on cybersecurity incidents; and risk management, strategy and governance.

Cybersecurity Incident Reporting

New rules will require public companies to:

- Disclose information about a material cybersecurity incident within four business days after the company determines that the incident is material (using Form 8-K). The final rule clarifies the four-day disclosure requirement may be suspended for up to 30 days if the SEC receives written authorization from the US Attorney General to delay filing due to national security or public safety concerns.
- Provide updated disclosures relating to previously disclosed cybersecurity incidents when they become material overall (using Form 8-K/A).

Risk Management, Strategy and Governance

On Form 10-K, public companies must:

- Describe policies and procedures for the identification and management of risks from cybersecurity threats, and oversight of third-party service providers.
- Explain management's role in cybersecurity governance.
- Disclose cybersecurity oversight by the board of directors.

Checklist for Meeting SEC TPRM Requirements

Because 41% of organizations experienced an impactful third-party security incident in the last year, it is essential that public companies consider the SEC reporting amendments in the context of those relationships. This section identifies requirements in the SEC cybersecurity risk management amendments and maps best practices capabilities to those requirements to help security teams mitigate third-party risks and meet reporting obligations.

NOTE: This is a summary of the most relevant amendments only, and it should not be considered comprehensive, definitive guidance. For a complete list of rules, please review the complete document in detail and consult your auditor.

Table 1. Best Practices Capability Mappings to SEC Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure Amendments

Amendments	Best Practices Capabilities
Reporting of Cybersecurity Incidents on Form 8-K **Item 1.05**	
"Describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."	As part of your broader incident management strategy, ensure that your third-party incident response program enables your team to rapidly identify, respond to, report on, and mitigate the impact of third-party vendor security incidents. Look for managed services where dedicated experts centrally manage your vendors; conduct proactive event risk assessments; score identified risks; correlate against continuous cyber monitoring; and issue remediation guidance – all on your behalf. Managed services can greatly reduce the time required to identify vendors impacted by a cybersecurity incident and ensure that remediations are in place. Key capabilities in a third-party incident response service include: • Continuously updated and customizable event and incident management questionnaires • Real-time questionnaire completion progress tracking • Defined risk owners with automated chasing reminders to keep surveys on schedule • Proactive vendor reporting • Consolidated views of risk ratings, counts, scores and flagged responses for each vendor • Workflow rules to trigger automated playbooks to act on risks according to their potential impact on the business • Built-in reporting templates for internal and external stakeholders • Guidance from built-in remediation recommendations to reduce risk

Amendments	Best Practices Capabilities
	• Data and relationship mapping to identify relationships between your organization and third, fourth or Nth parties to visualize information paths and reveal at-risk data. Also, consider leveraging databases that contain data breach history for thousands of companies around the world – including types and quantities of stolen data; compliance and regulatory issues; and real-time vendor data breach notifications. Armed with these insights, your team can better understand the scope and impact of the incident; what data was involved; whether the third party's operations were impacted; and when remediations have been completed – all by leveraging experts.
Disclosure About Cybersecurity Incidents in Periodic Reports: Updates to Previously Filed Form 8-K Disclosure	
"Disclose information that would have initially been reported on the Form 8-K had it been known or available at the time of initial disclosure."	Continuously track and analyze external threats to third parties. As part of this, monitor the Internet and dark web for cyber threats and vulnerabilities, as well as public and private sources of reputational, sanctions and financial information. All monitoring data should be correlated with assessment results and centralized in a unified risk register for each vendor, streamlining risk review, reporting, remediation and response initiatives. Monitoring sources typically include: • criminal forums; thousands of onion pages; dark web special access forums; threat feeds; and paste sites for leaked credentials — as well as several security communities, code repositories, and vulnerability databases • Databases containing 10+ years of data breach history for thousands of companies around the world Be sure to incorporate third-party operational, reputational and financial data to add context to cyber findings and measure the impact of incidents over time.

Amendments	Best Practices Capabilities
Disclosure of a Registrant's Cybersecurity Risk Management and Strategy **Item 106(b) of Regulation S-K**	
"Whether and how the described cybersecurity processes in Item 106(b) have been integrated into the registrant's overall risk management system or processes;"	Build a comprehensive third-party risk management (TPRM) program in line with your broader information security and governance, risk and compliance programs. Seek out experts to collaborate with your team on defining and implementing TPRM processes and solutions; selecting risk assessment questionnaires and frameworks; and optimizing your program to address the entire third-party risk lifecycle – from sourcing and due diligence, to termination and offboarding – according to your organization's risk appetite. As part of this process, you should define: • Clear roles and responsibilities (e.g., RACI) • Third-party inventories • Risk scoring and thresholds based on your organization's risk tolerance • Assessment and monitoring methodologies based on third-party criticality • Fourth-party mapping • Sources of continuous monitoring data (cyber, operational, reputational, financial) • Key performance indicators (KPIs) and key risk indicators (KRIs) • Governing policies, standards, systems and processes to protect data • Compliance and contractual reporting requirements against service levels • Incident response requirements • Risk and internal stakeholder reporting • Risk mitigation and remediation strategies

Amendments	Best Practices Capabilities
"Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes;"	Look for solutions that feature a large library of pre-built templates for third-party risk assessments. Assessments should be conducted at the time of onboarding, contract renewal, or at any required frequency (e.g., quarterly or annually) depending on material changes. Assessments should be managed centrally and be backed by workflow, task management and automated evidence review capabilities to ensure that your team has visibility into third-party risks throughout the relationship lifecycle. Importantly, a TPRM solution should include built-in remediation recommendations based on risk assessment results to ensure that your third parties address risks in a timely and satisfactory manner, and can provide the appropriate evidence to auditors. Ensure that your TPRM solutions automatically maps information gathered from control-based assessments to ISO 27001, NIST, and other regulatory frameworks, enabling you to quickly visualize and address important compliance requirements and adjust your program accordingly – including whether or not to accept residual risks. For organizations with limited resources and expertise, leverage managed services to manage the third-party risk lifecycle on your behalf – from onboarding vendors and collecting evidence, to providing remediation guidance and reporting on contract SLAs. As a result, you reduce vendor risk and simplify compliance without burdening internal staff.
"Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider;"	Developing a good process begins with profiling and tiering third parties, which involves quantifying inherent risks for all third parties. Criteria used to calculate inherent risk for third-party classification includes: • Type of content required to validate controls • Criticality to business performance and operations • Location(s) and related legal or regulatory considerations • Level of reliance on fourth parties (to avoid concentration risk) • Exposure to operational or client-facing processes • Interaction with protected data • Financial status and health • Reputation From this inherent risk assessment, your team can automatically tier suppliers; set appropriate levels of further diligence; and determine the scope of ongoing assessments. Rule-based tiering logic enables vendor categorization using a range of data interaction, financial, regulatory and reputational considerations.

Amendments	Best Practices Capabilities
Disclosure of a Registrant's Management's Role and Board Role in Cybersecurity Governance Items 106(c)(1) and 106(c)(2) of Regulation S-K	
"The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents;" "Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors."	Measure third-party KRIs against your requirements with machine learning (ML) insights and customizable, role-based reports. The capabilities can help your team to uncover risk trends, determine third-party risk status, and identify exceptions to common behavior that could warrant further investigation. And, it makes it easier for report recipients to quickly determine risk acceptability and make confident decisions, regardless of skill level.

The Prevalent Difference

Prevalent solutions can help your organization to establish and mature your third-party cybersecurity risk management, strategy, governance and incident disclosure program. With Prevalent, you can:

- Profile and tier all third parties, gaining inherent risk scores that indicate the likelihood and impact of a cybersecurity incident and enable you to right-size ongoing due diligence activities
- Map fourth and Nth parties to identify concentration risk and reveal data flows across the extended vendor ecosystem
- Automate third-party risk assessment, risk scoring and remediation processes
- Continuously monitor third parties for cybersecurity risks and correlate risks against assessment results to validate findings
- Automate incident response processes, speeding reporting and time to resolution
- Simplify board and executive reporting to enable clear and efficient decision making
- Benchmark your program against accepted best practices with compliance reporting against several frameworks and regulations

Contact Prevalent today for a free maturity assessment to determine how your TPRM policies stack up to the SEC requirements, or schedule a demo to learn whether our solutions are a fit for you.

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors and suppliers throughout the third-party lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit www.prevalent.net.