KPMG

SEC cybersecurity disclosure rules

Cracking the code on materiality and reporting.

Navigating materiality considerations and cybersecurity reporting

As public companies face increasing threats from malicious actors targeting their information systems and proprietary data, cybersecurity has become a key agenda item for boards[1] and audit committees[2] in 2024. Against this backdrop, the US Securities and Exchange Commission (SEC) implemented new rules, effective December 18, 2023, requiring public companies to disclose material cybersecurity incidents on Form 8-K within four business days. Additionally, detailed information regarding their cybersecurity risk management and governance must be included on Form 10-K.[3] These rules demonstrate the SEC's focus on the criticality of cybersecurity disclosures in formal financial reporting.

However, the implementation of the new rules has raised many questions specific to materiality.

The SEC defines a material incident as a matter to which "a reasonable shareholder would consider it important" in making an investment decision.[4] In other words, an incident is material if it significantly impacts a company's operations, financial position, reputation, or legal obligations.

This definition of materiality presents challenges for companies in assessing the significance of cybersecurity incidents and, in turn, supporting disclosure decisions to regulators and other interested parties. Establishing a clear process for determining the materiality of a cyber incident and ensuring proper mechanisms are in place to aid in this determination are crucial for fostering trust in the business, its cybersecurity, and the capital markets.

Identifying triggers for material cybersecurity incidents

It is up to each company to consider an array of factors surrounding a cyber incident to determine whether it meets the materiality threshold. Importantly, these factors must take into account both the actual and expected impacts of the cyber event.

One of the key difficulties that companies are encountering in assessing materiality is the need to consider qualitative factors in addition to the quantitative factors that they may be more accustomed to in financial reporting. Additionally, cybersecurity reporting requires that the information technology (IT) function play an integral role in assessing materiality—a task that is traditionally assigned to the finance or controller function.

---

[1] KPMG Board Leadership Center, On the 2024 Board Agenda, December 7, 2023.

[2] KPMG Board Leadership Center, On the 2024 Audit Committee Agenda, December 7, 2023.

[3] Matthew Johnson, Doron Rotman, and Maksim Vander, "Navigating the SEC's New Cybersecurity Disclosure Rules," News and Perspectives, September 2023.

[4] KPMG LLP, "SEC Staff Issues New C&DIs on Cybersecurity Rules," December 2023.

As a starting point for assessing the materiality of a cyber incident, consider the following factors:

Quantitative factors

Impacts on business operations:

- Duration of the cyber incident
- Number of business segments impacted
- Any loss of data or intellectual property
- Disruptions or delays in operations

Impacts on the business's earnings and financials, including:

- Stock price
- Revenue and net income
- Key ratios, such as earnings per share, return on investment, and operating margin
- Previously communicated revenue forecasts

Expenses related to the containment and resolution of the incident, such as:

- Ransom payments
- Legal fees for potential litigation and settlement
- Forensic analysis and contracting external cybersecurity experts
- Enhancements to the IT environment
- Future insurability and/or protection costs

Qualitative factors

- The type and amount of information that has been taken, reached, changed, sent out, or used for any illegitimate purpose
- Public perception and reputational damage
- Effects on intangible assets
- Impact to upstream and downstream supply chain
- Challenging situations linked to the cyber incident (e.g., incompatible interests)
- Legal disputes, inquiries, or actions by government agencies
- Motivations of the malicious actor (e.g., state-sponsored actor, criminal organization, or insider threat)
- Impact on operational efficiency if management has to change priorities and reallocate resources to address cyber issues

The following typically will not affect the materiality assessment:

- Whether the affected system was owned or operated by the impacted company or a third party
- Inability to determine the full extent of the incident, though the disclosure may need updating as additional information is uncovered
- Ongoing nature of an internal investigation
- Timing of providing information about the incident to government authorities or others

These factors are not exhaustive and may vary depending on the specific circumstances of each incident, but they provide a starting point for identifying and assessing the quantitative and qualitative impact of a breach. Importantly, these factors leave room for interpretation, necessitating further due diligence before determining materiality.

Applying new and existing materiality frameworks to cyber incident reporting

Quantitative and qualitative factors are a solid starting point for assessing materiality. However, it would be more sophisticated and prudent to leverage a combination of these factors and an established materiality framework. Most organizations already have established structures and processes for determining the severity of an operational incident. These existing frameworks, such as Enterprise Risk Management (ERM) programs, business impact assessments, Business Continuity and Disaster Recovery (BCDR) strategies, incident response strategies, and data governance and data privacy strategies, can serve as a foundation for a basic materiality framework when applied to cyber incidents.

In addition to internal frameworks, companies are starting to leverage publicly available external frameworks for assessing materiality in cyber and other accounting topics. One example is the Factor Analysis of Information Risk (FAIR) Institute Materiality Framework, based on the FAIR™ model.[5] This framework offers a detailed taxonomy of loss categories and expands the loss magnitude factor, enabling companies to quantify the impact of cyber incidents, report financial risk, and track the total cost.

Ultimately, companies should choose the framework that best suits their functions, whether it is internally developed, externally sourced, or a combination of the two. Regardless of the chosen framework, it is crucial to properly document all cyber incident materiality processes and decision points in a manner that regulators can easily interpret.

Integrating cyber response and disclosure teams

A common mistake in evaluating materiality is looking at a cyber incident solely from the perspective of the impacted company. Instead, materiality must be determined objectively and through the lens of outside stakeholders. In other words, companies must carefully determine whether an investor would consider the information related to a cyber event material to their investment decision.

In an effort to bring this multistakeholder lens to cybersecurity, many organizations are developing cross-functional disclosure committees consisting of C-suite executives, general counsel, board representatives, and finance personnel who are responsible for assessing cyber incident fact patterns and, ultimately, making the materiality determination. Integrating representatives from the existing cyber response team into the disclosure committee can facilitate a swift and comprehensive response.

The disclosure committee should be prepared to discuss various aspects of the incident and response. Consider the following questions as a starting point:

- What is the nature of the cyber incident (e.g., data breach, ransomware attack, and system compromise)?
- What is the extent of the incident's impact on our systems, data, and operations? Did the incident impact systems related to financial reporting and internal controls over financial reporting?
- Does the incident involve sensitive or regulated data (e.g., personal information and financial data)?
- Are there regulatory obligations or compliance requirements associated with the affected data?
- What strategies have we employed to contain and rectify the incident? How are we communicating with internal and external stakeholders who may have been impacted?
- How are we calculating the financial ramifications of the incident? How are we accounting for related expenses and liabilities?
- Have we evaluated the accounting considerations around software expense capitalization, particularly if the remediation efforts result in enhancements?
- Once the incident is resolved, how should we revise our risk disclosures and financial statements accordingly?
- How are we adhering to the SEC disclosure requirements and other relevant laws and regulations? Have we assessed potential legal risks and impending lawsuits?
- Have we documented our materiality considerations at the right level of detail?

[5] "An Introduction to the FAIR Materiality Assessment Model," Fair Institute, accessed February 2, 2024.

Navigating Form 8-K and Form 10-K disclosures

If a cyber incident is deemed material, then the company must disclose it on Form 8-K within four business days of making this determination.

Form 8-K Flow

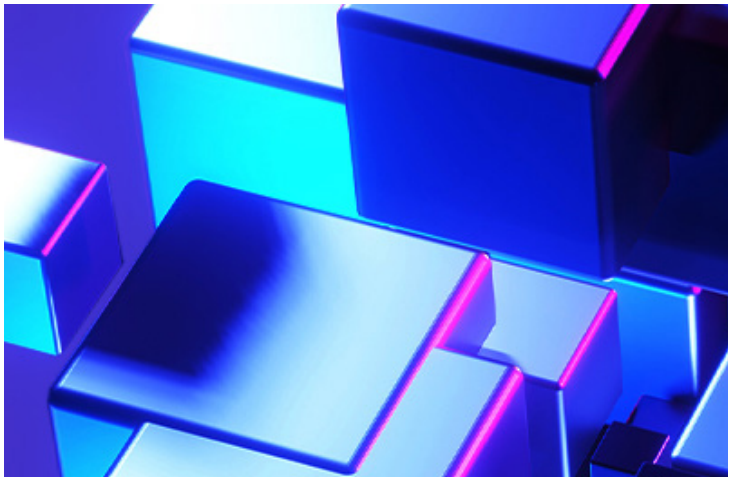
Incident → **Outline & document** → **Draft**

In the event of a breach, take necessary actions to mitigate the impact and prevent further damage. Additionally, start preparing documentation about items that will need to be disclosed in a Form 8-K to notify shareholders, regulators, and the public about the cybersecurity incident and any material consequences.

Form 8-K Item 1.05

1. **Technical Issue:** Describe the material aspects of the nature of the cybersecurity incident, such as the scope and timing of the incident and its material or reasonably likely material impact. Items not known at the time of reporting should be specified, and amendments will be needed once known within four days of gaining that understanding.
2. **Cyber Incident Description:** Clearly outline the potential impact, including financial, operational, and reputational consequences, along with any known instances of unauthorized access, data theft, or compromised systems.
3. **Responding Actions:** Detail the steps taken in response to the incident, such as deploying containment measures. This includes if the registrant has remediated or is currently remediating the incident, any changes to policies/procedures and how the incident may have informed such changes. These disclosures should not reveal specific or technical information in such detail as it would impede the registrant's response or remediation of the incident.

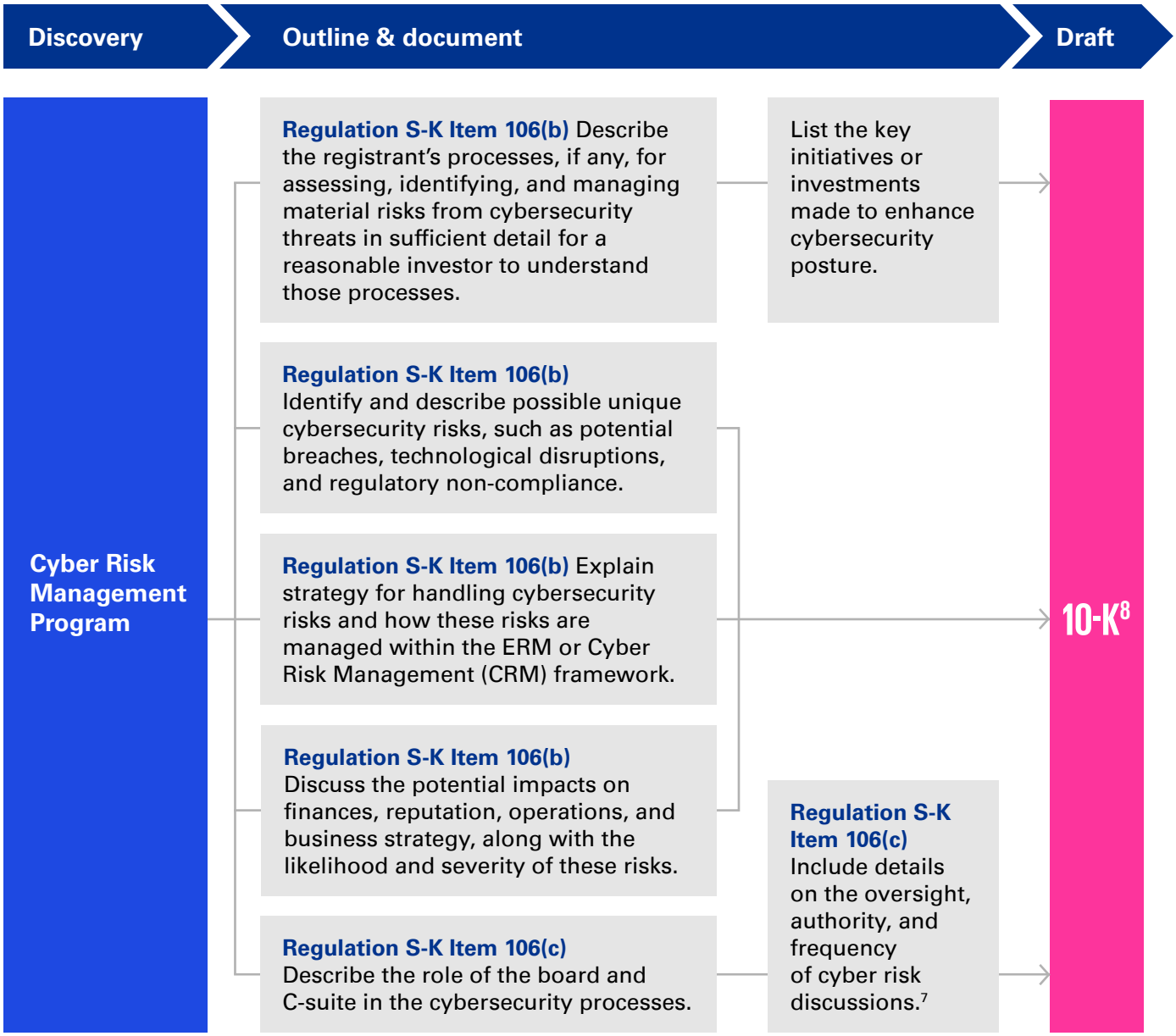
→ **8-K**[6]



On Form 10-K, in accordance with SEC guidelines, companies are required to disclose material information, and the evolving threat landscape of cybersecurity is increasingly recognized as a material factor. Therefore, companies must assess and disclose the impact of cybersecurity risks and incidents on their financial position, operations, and reputation. This disclosure should encompass the nature and scope of cyber threats faced, potential financial ramifications, management oversight, board governance, and the effectiveness of the organization's cybersecurity measures.

[6]This graphic depicts possible activities corresponding to the preparation of Form 8-K Item 1.05 and is not part of the rule.

Form 10-K Flow



Cybersecurity in the new regulatory environment

The sophistication of cyber threats is only increasing, and in turn, regulation is ramping up. To navigate this new terrain successfully, companies must reevaluate their cyber response strategies while prioritizing materiality considerations. While this may seem like a daunting task, fortunately, companies can leverage existing operational processes and frameworks related to materiality and apply them to cybersecurity scenarios. Additionally, fostering cross-functional collaboration and maintaining thorough documentation can enable companies to better address cyber risks today while remaining nimble for potential incidents in the future.

[7]The information in this graphic is not all inclusive.

[8]This graphic depicts possible activities corresponding to Regulation S-K Items 106(b) and 106(c) and is not part of the rule.

Authors

Maksim Vander
Partner, Audit
Technology Assurance
T: 212-872-7934
E: mvander@kpmg.com

Doron Rotman
Managing Director, Audit
Technology Assurance
T: 408-367-7607
E: drotman@kpmg.com

Contributors

Jonathan Fairtlough
Principal, Advisory
Cyber Security Services
T: 213-972-4000
E: jfairtlough@kpmg.com

Christopher Montone
Director, Audit
Technology Assurance
T: 267-256-7000
E: cmontone@kpmg.com

Ruixiang Wu
Director, Audit
Technology Assurance
T: 212-954-4006
E: ruixiangwu@kpmg.com

Learn about us: **kpmg.com**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.