servicenow | KPMG

SEC doubles down on cyber risk management accountability

Four ways to avoid gambling with cyber risk disclosure

kpmg.com

A secure cyber environment is critical to modern business success. For too long, many leaders have viewed cybersecurity risks like reminders from the doctor to eat right and exercise—wise to do if you don't want to gamble with your health. Much like a caution for better diet and exercise, cyber risk rarely becomes real until someone has a heart attack.

Investors have been feeling chest pains over cyber risk, which is why the US Securities and Exchange Commission (SEC) has "clarified" regulations with sweeping new rules, forcing companies to better manage cyber risk and require specific actions regarding timeliness, consistency, and quality of incident response.

Recent headlines highlight cyber incidents that are costing companies millions beyond that of information loss. Loss in reputation and supply chain interruption certainly hit heavy as well. For example, of the many incidents that have led the SEC to update these rules, one in particular drove a company's stock price down more than 22 percent.[1]

The SEC now seeks to add protection that can help average investors know which of their business investments take cyber risk seriously. Before the new ruling, financial evaluation driven by actual loss and stock value impact determined materiality. Now, even if a company does not lose a dollar, an incident can be material. The more public an incident becomes, the more material it is. Companies, therefore, must assess cyber risks using ***qualitative and quantitative*** factors to determine the material impact on the company's operations, customers, shareholders, and reputation.[2]

Highlights of the recent US SEC mandate

Registrations must:

Disclose any cybersecurity incident they determine to be material within four business days (with few exceptions)

Form 8-K

Describe processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material or the likely material effects or risks from cybersecurity threats and previous cybersecurity incidents

- **Includes the board of directors' oversight of risks from cybersecurity threats**

Form 10-K

Furnish FPI information with newly-qualified material details

Form 6-K 20-F

Companies that rely on old processes are gambling with cyber risk. A broad range of stakeholders, from CISO organizations and board members to finance, general counsel, enterprise risk, and investor relations groups, all now need to understand how public companies manage their cyber risk. KPMG LLP and ServiceNow offer insight to help managing the qualitative and quantitative perils buried in regulation details.

KPMG and ServiceNow bring a distinct approach to this topic as a collective that understands cybersecurity as both a technology problem and a business priority. ServiceNow brings a technology perspective with a cybersecurity and enterprise-risk management platform that includes purpose-built cyber risk, incident response, and reporting workflows. Combine that with the strategic implementation experience of KPMG, and you have here tangible and actionable advice to get you through this unprecedented time.

1 Source: Rob Sloan, *Wall Street Journal*, "What The Board Needs to Know: Cyber Attack Costs," October 9, 2023.

2 Ibid.

The ante is in: Signals to act now

We believe the SEC does not view these laws as new. The requirements read like clarifications to existing company responsibilities (i.e., to tell their shareholders about cyber risks, how the company manages them, and notification requirements when cyber incidents occur).

The new guidance also hints toward more personal accountability (read: fines) for company executives.[3] Most CFOs and general counsel do not share the same skill sets with CISOs, which could be a reason behind some of these changes, ensuring the two worlds coordinate better. **Cyber risk management is now an equal partner to enterprise risk management rather than a line item**, so the two sets of processes now must be integrated.

New regulations require companies to:

1. Report how they manage cyber risk
2. Have a process to measure whether a cyber incident can impact materiality
3. Promptly report material incidents
4. Be transparent

... in their *very next* SEC annual reporting.

Types* of cyber incidents that could trigger a materiality review:

personally identifiable information or protected health information losses, plant shutdown, supply chain interruption, critical IP losses, revenue losses, incidents that threaten reputation, incidents that harm vendor or customer relationships, incidents that impact competitiveness, incidents that cause litigation, regulatory investigation, and headline news coverage

**list not exhaustive*

Four tips to help build a strong hand to meet regulation basics

Before we can discuss tips and tricks, it's important to emphasize the foundation of a documented cyber risk management strategy. It is critical considering the global average cost of a data breach is estimated at $4.45 million but (now) could be significantly higher depending on an attack's impact plus SEC fines.[4]

Companies need a solid process to determine materiality and quickly fast-track what might be material to senior leaders who will determine if public notice is required.

The goal is to ensure that your cyber risk processes are built into your IT and asset management processes, supported with dynamic reporting around asset status, with automation for risk triggers. This connects cyber risk with enterprise risk, by providing a platform for effective incident response. It allows for scalable compliance monitoring and provides a documented basis for the 10-K.

With that emphasized, here are four tips in fortifying a solid foundation for SEC compliance.

3 Source: US Security and Exchange Commission, "Press Release: SEC Charges Chief Information Officer with Fraud," October 30, 2023.

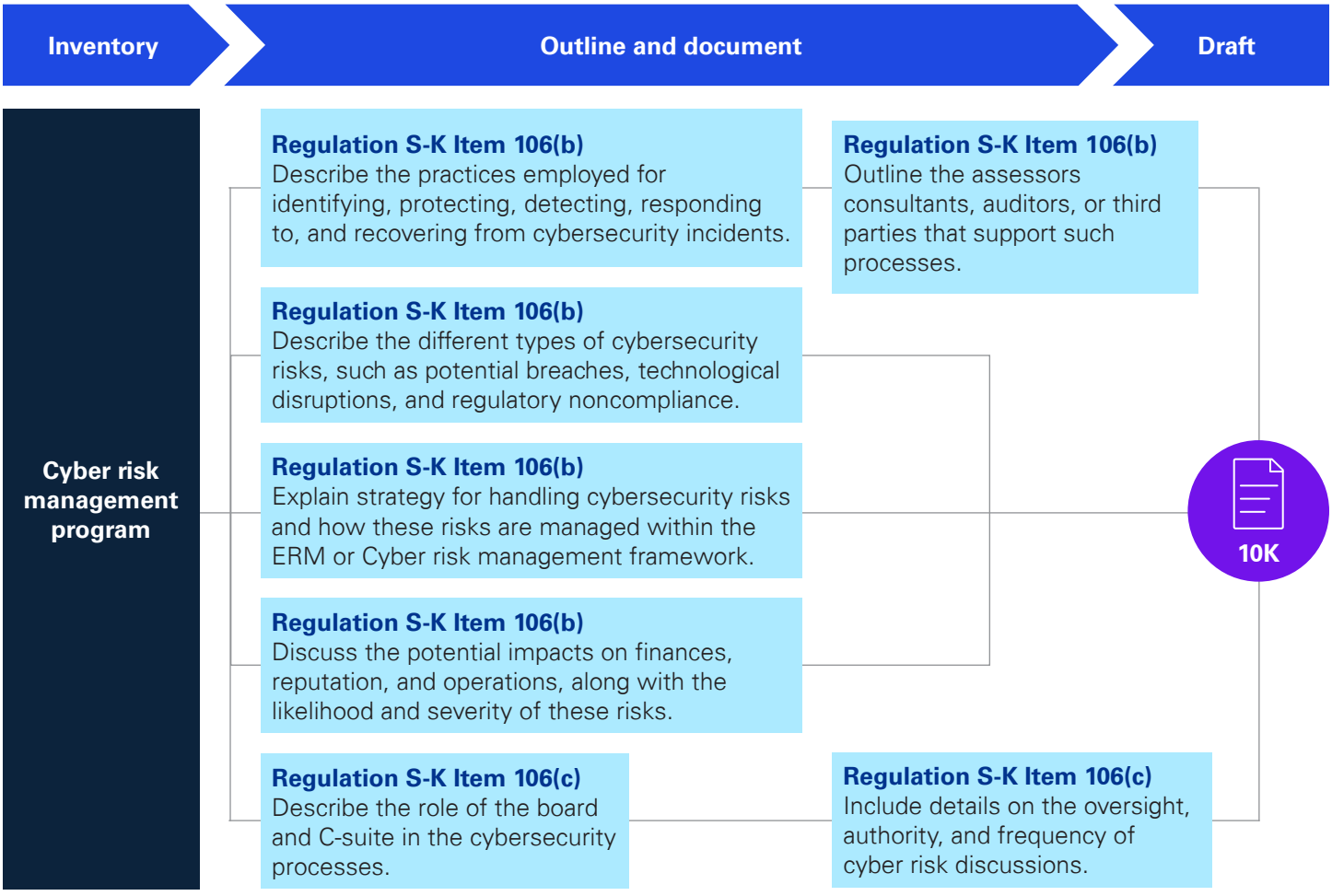
4 Source: Verizon, "Ransomware threat rises: Verizon 2022 Data Breach Investigations Report," May 24, 2022.

1. Be accurate in the 10-K

With this regulation, public companies must now describe their cyber risk management practices in annual 10-K reports. Requirements include how companies evaluate, mitigate, and monitor cyber risks as well as how they allocate resources and assign responsibility for cybersecurity governance. To meet these reporting requirements, companies must map out and document current practices. **The risk is not in writing the disclosure, it's in the information accuracy required to pass an SEC audit**.

While the disclosure requirements are broader than described here, these parts of the new Item 106 in the Regulation S-K will require detailed information gathering and documentation. Working with a cybersecurity specialist to outline and document your cyber risk management program in the 10-K (as illustrated) can help improve accuracy and help close gaps.

Sample cyber risk management program



Illustrating how you are meeting between 106(b) and 106(c) will be a team effort between Cybersecurity, IT, and Risk (that then must be accepted by Compliance and the C-suite).

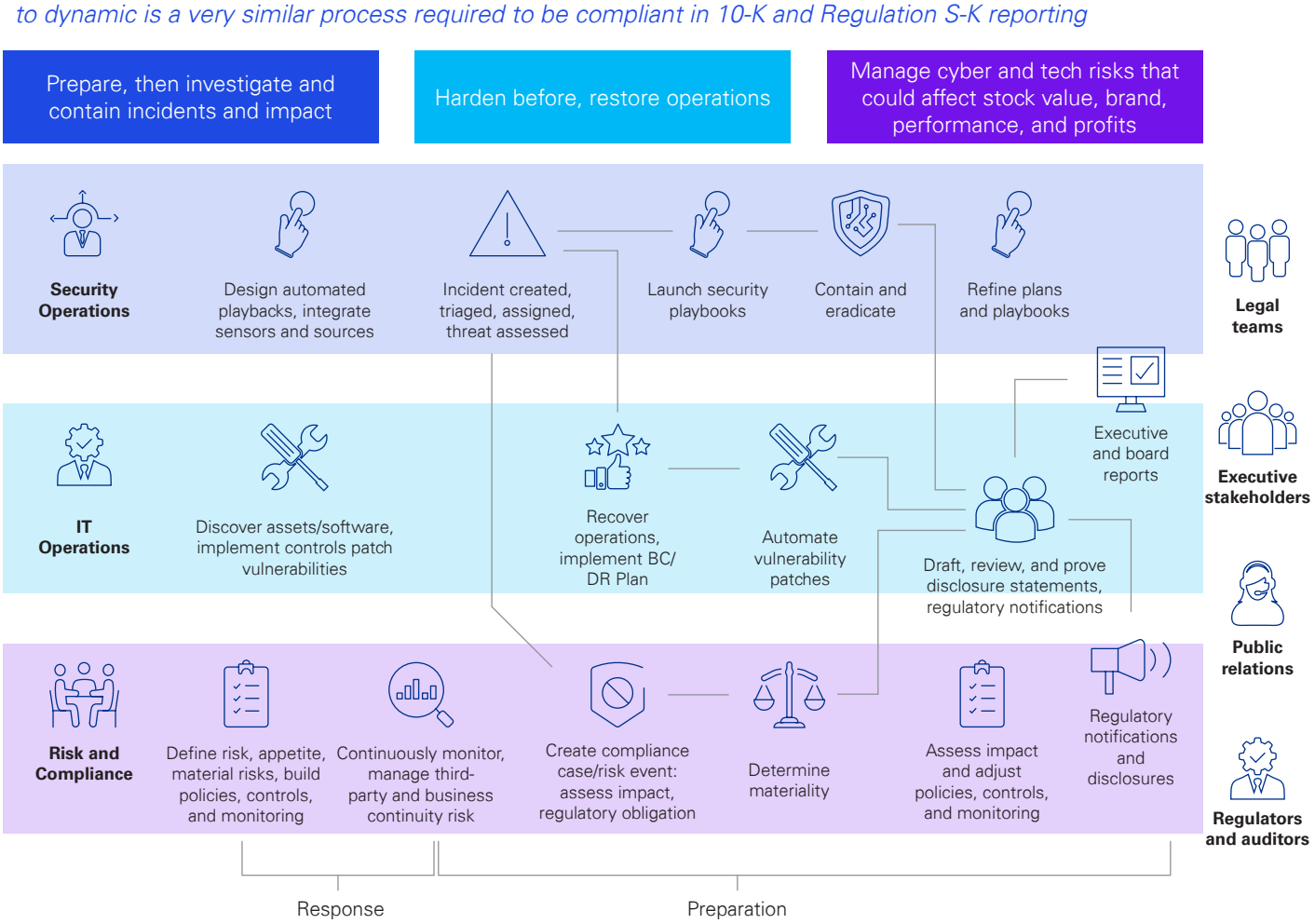
106(b) is all about documenting the practices you will employ for all the potential cybersecurity risks. 106(c) requires that you detail how involved the C-suite is and their oversight capabilities.

When you understand the rules in this overarching way, you can see that having a strong foundation of scalable, dynamic reporting sets you up for success because such a tool requires that you:

- Describe the key initiatives or investments taken to bolster cybersecurity
- Outline procedures for recognizing, safeguarding, identifying, responding to, and recuperating from incidents
- Detail cybersecurity risks, including potential breaches, technological disruptions, and regulatory compliance concerns
- Explain the approach to managing cybersecurity risks and how they are approached
- List the potential effects on finances, operations, and reputation—in probability and magnitude
- Describe the involvement of the board and executive leadership in these procedural decisions

SEC compliance teams up Cybersecurity, IT, and Risk

This ServiceNow implementation workflow provides illustration on how increasing reporting maturity from static to dynamic is a very similar process required to be compliant in 10-K and Regulation S-K reporting



2. Use an objective framework to evaluate materiality

Regulations now require businesses to assess cyber incident impact and communicate the information for material events to the SEC and investors **within four business days** of determining materiality (via 8-K).[5] Determining materiality could challenge many businesses, especially considering the new definition now goes beyond financial impact to include qualitative considerations such as public attention, reputation loss, and potential litigation.

Companies need a method to evaluate incidents objectively, from the view of the average investor, as well as quantitatively to assign costs to risk. KPMG uses the FAIR Institute's FAIR Materiality Assessment Model (FAIR-MAM™). It consists of 10 primary modules, such as business interruption and proprietary data loss, that companies can adapt to their cost structures and customize to estimate primary and secondary attack costs on any business asset during an incident.[6] The model enables quick probability of loss estimation from new or evolving cyber incidents. It also can create proactive assessments of top risk scenarios for materiality, by category.

FAIR-MAM (Materiality Assessment Model)

Information Privacy Four subcost categories	**Proprietary Data Loss** Two subcost categories	**Business Interruption** Three subcost categories	**Cyber Extortion** One subcost category	**Network Security** Two subcost categories	**Financial Fraud** Two subcost categories	**Media Content** Two subcost categories	**Hardware Bricking** Two subcost categories	**Postbreach Security Improvements** Two subcost categories	**Reputational Damage** Six subcost categories
Sensitive PII Event Response and Management P-RC	Loss of Estimated Future Net Revenue S-CA	Direct Business Interruption P-PL	Ransom P-RC	Network Event Response and Recovery P-RC	BEC P-PC	Media Event Response P-RC	Server Replacement P-PC	Legally Mandated Improvements S-RC	Customer Retention S-RD
PCI-DSS Liability P-RC	Proprietary Data Loss Liability S-RC	Contingent Business Interruption (Supply Chain Attack Victim – 3P failure to provide IT services) P-PL		Network Security Liability (Supply Chain Attack Source) S-RC	Fund Transfer Fraud P-PC	Media Liability S-RC	Computer/ Laptop Replacement P-PC	Voluntary Improvements S-RC	Future Projects S-RD
Information Privacy Liability S-RC		Business Interruption Liability S-RC							Market Value S-RD
Regulatory Liability S-FJ									Cyber Insurance S-RD
									Cost of Capital S-RD
									Employee Churn S-RD

Legend

P – Primary Cost
S – Secondary Cost
RC – Response Cost
FJ – Fines and Judgments
CA – Competitive Advantage
PL – Productivity Loss
PC – Replacement Cost
RD – Reputational Damage

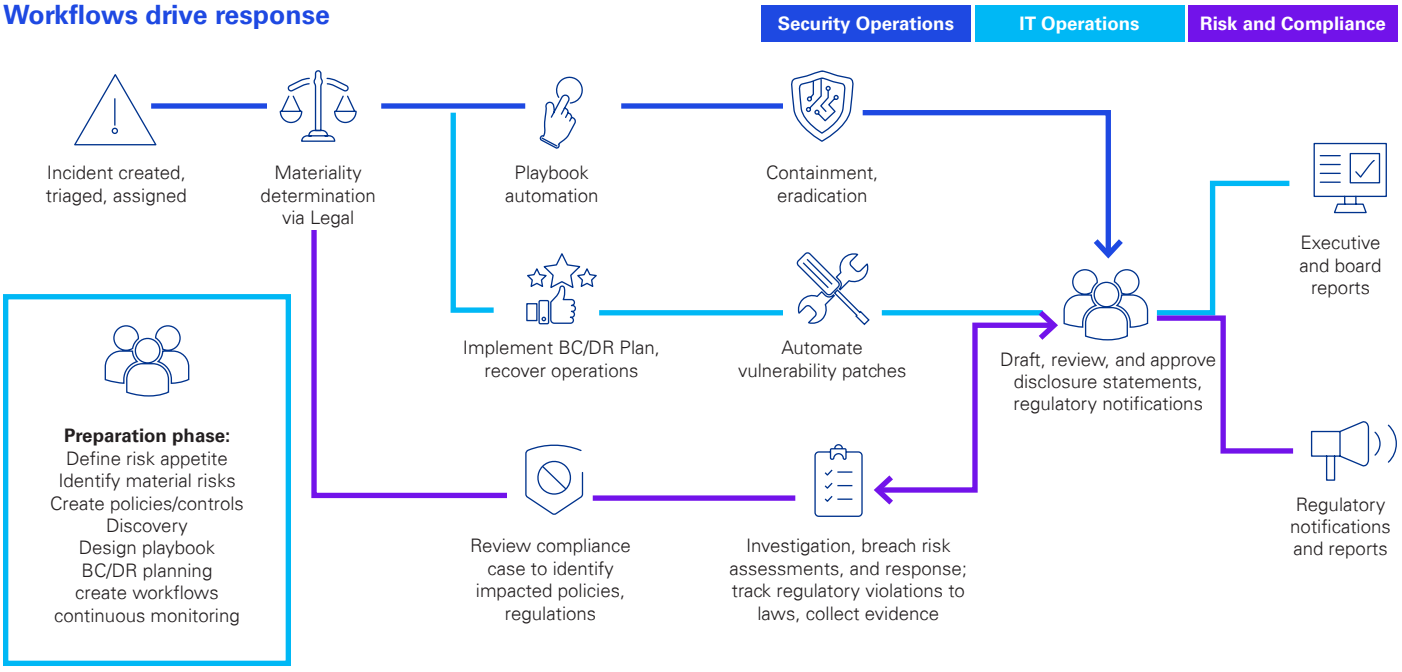
5 Source: US Security and Exchange Commission, "Press Release: SEC Adopts Rules on Cybersecurity Risk Management," July 26, 2023.

6 Source: The FAIR Institute, "An Introduction to the FAIR Materiality Assessment Model (FAIR-MAM™)," 2023.

3. Speed matters: Execute the process to escalate incidents fast

It may be surprising to know that 48 percent of cyberattacks are not reported to appropriate authorities and 41 percent are kept from internal leadership.[7] Since regulations now require companies report cyber incidents within a reasonable timeframe, they must have a clear process for initial alerting, whether or not the incident is material. Furthermore, companies must facilitate a way in which employees understand what qualifies as a cybersecurity risk to make it easier to report or raise concerns.

Workflows drive response



A powerful tool, such as an integrated risk management solution, can provide the baseline of cyber risk management because it collects and provides required information while building in automation (beyond simple ticketing) that escalates issues and triggers other actions.

FYI: Users can tailor ServiceNow risk management categories to the FAIR-MAM to quickly identify both material and immaterial incidents. When incidents occur, ServiceNow automates cross-functional workflow to escalate them so the company can disclose within the four-day window.

7 Source: Kevin Poireault, *Infosecurity Magazine*, "Half of Cyber-Attacks Go Unreported," September 26, 2023.

4. Recoup after a bad hand: Learn from your 8-K

Filing the 8-K is an important milestone of a cyber incident. But cyber risk management does not stop there. If done right, companies can minimize damage and strengthen the foundation to help prepare for the next cyber incident.

The first step is all about knowing. Document, with clear understanding, how the incident impacts customers, stakeholders, and clients. Know your contractual and regulatory obligations as well as the nature and type of data you store.

Communicate the state of the investigation. Accurate communication, and potential audit and disclosure activities, require a common source of truth. It is also critical to pre-train client and stakeholder relationship managers on crisis communication, so they are prepared to speak for the company. We recommend communicating in stages based on confirmed knowledge rather than speculation.

Have management processes to identify and escalate stakeholder concerns. This process should include a designated management team with people who understand stakeholder relationships to assist with communication. A pre-built escalation process made to quickly identify unhappy clients or stakeholders can address issues before they grow. It should also include implementing a known communication structure that allows stakeholders to ask questions in a controlled, informed environment.

Finally, document and track all questions along with the company's spokespeople's responses and promises. Moderating questions can help ensure they can be answered effectively in a controlled environment. A reliable tracking system that can store the questions, answers, and their status enables each of these steps.

Both KPMG and ServiceNow put a lot of energy toward educating organizations on how to leverage applications that capture and automate information enablement workflows—since it is an essential aspect of resolving and learning from the pains from cyber threats. Beyond that, such a system can be counted on for accurate information and training for general business betterment.

Don't bust: Prepare better and move faster

Every public company must up their cyber risk management game to avoid gambling with corporate and personal accountability. With experience from the data center to the boardroom, KPMG and ServiceNow teams understand cybersecurity complexities and how they impact your business. KPMG can provide assessment, strategy, program management, and implementation support. We work with you to create a thorough cyber risk management strategy that aligns your business with new SEC regulations. We enable it on ServiceNow technology for enterprise risk and compliance management and security operations so you can demonstrate to investors, customers, and regulators your commitment to robust cybersecurity practices.

KPMG can work with you to implement ServiceNow technology that will help you assess, improve, and communicate your cybersecurity posture.

Continue learning more here.

Visit these websites to learn more about other topics mentioned in this article

KPMG Cybersecurity Services

KPMG Third-Party Risk Management

KPMG AI Cybersecurity

ServiceNow Security Operations

ServiceNow Governance, Risk, and Compliance

Contacts

Jonathan Fairtlough
Principal, Cyber Security Services
KPMG LLP
jfairtlough@kpmg.com

Barbara Kay
Head of Risk and Security Product
ServiceNow
barbara.kay@servicenow.com

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

Learn about us: **kpmg.com**