SEC Cybersecurity Rules Update

The Complete Guide

AUDITBOARD

Table of Contents

Introduction	1
What to Know Now: Dates and Basic Action Plan	3
Overview of the SEC Cybersecurity Disclosure Requirements	5
How to Prepare for Compliance With SEC Cybersecurity Rules	17
The SEC Cybersecurity Rules Demand Integrated Risk Management	19

Introduction

Every company should feel urgency about maturing cybersecurity risk management. That's the core message behind the heightened regulatory focus on cybersecurity — and with the U.S. Securities and Exchange Commission's (SEC's) final cybersecurity disclosure requirements for public companies taking effect in September 2023, it's about to get real. **The SEC cybersecurity rules will have a significant impact on your organization and role.**

Cybercriminals keep finding new ways to monetize cyberattacks, prey on geopolitical instability, evade detection, exploit or re-weaponize vulnerabilities, and use AI to conduct attacks. Cyber attacks keep growing in sophistication, relentlessness, and destructiveness, and the resulting costs and adverse consequences can be monumental.

Beyond business interruptions, lost revenues and assets, reputational damage, remediation costs, ransom payments, and liabilities to affected parties, national security and public safety are at stake.

The risk is widespread and likely underreported. Citing a recent study showing that **98% of organizations use at least one third-party vendor that has experienced a breach in the past two years**, the SEC has decreed that the time is now for enhancing and standardizing cybersecurity disclosures.

If you're a leader at a private company, you may be thinking, "But this doesn't apply to me." You're right. Officially, it doesn't. But many private companies are third parties to public companies – and thus potentially liable for any cyber incidents impacting public companies. Plus, investors and other stakeholders often hold private companies to the same standards as public companies, and the SEC's final rule is a good example of what we can expect from other cybersecurity legislation on the horizon, much of which goes beyond public companies. **Most importantly, to find a cybersecurity solution for everyone, we need to admit that cybersecurity is everyone's problem — and good cybersecurity risk management, strategy, and governance principles are universally applicable.**

Whatever your business or industry, it's time to get your head around the SEC's cybersecurity disclosure rules and similar legislation expected in 2023. Disclosure will require both accuracy and speed: accuracy to determine the materiality of cybersecurity incidents, and speed to meet the 4-business-day requirement for disclosing material cybersecurity incidents. Plus, the SEC's final rule marks a critical development in regulating cyber risk that underscores the importance of getting integrated risk management (IRM) processes in place — not just to comply with SEC cybersecurity rules, but to ensure you're doing the right things to protect, defend, and enhance your business.

You may have less time than you think. Your organization should be working now to get the processes and technologies needed to support effective cybersecurity disclosures in place by December 31 , 2023.

What to Know Now: Dates and Basic Action Plan

So, which rules apply to your business, when do they take effect, and what needs to happen to get your business on the path to compliance? The table below offers an overview, breaking the new rules down into key items, compliance dates, and recommended actions.

Audience	Details	Date	Recommended Actions
ITEM: Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure			
All registrants.	Effective date of final rule, per publication in the Federal Register.	9/5/2023	**Perform gap assessment.** Identify the gaps between the new SEC cybersecurity rules and current practices. Assign accountability for remediation.
ITEM: Cybersecurity Risk Management, Strategy, and Governance Disclosure *(Regulation S-K Item 106)*			
All registrants.	Compliance required beginning with annual reports for fiscal years ending on or after December 15, 2023.	12/15/2023	**Integrate disclosure processes.** Many companies will be able to leverage existing disclosure processes and expertise (e.g., SOX) in building out their risk management programs; others will start from scratch. But don't make the mistake of creating a separate process that will be burdensome and costly to maintain. Instead, identify how your cybersecurity program will integrate with your current disclosure process. Determine who will be involved and how. Include legal. **Prepare to disclose cybersecurity and ITRM practices.** Final rules require disclosing specific details of cybersecurity and ITRM programs/practices throughout the year. Consider ITRM solutions that enable you to develop, standardize, and report on your program, strategy, and maturity. Such solutions can streamline reporting (e.g., board, investors, auditors, regulators) while providing processes for issue management, evidence collection, maturity and workflow assessments, and risk mitigation. **Engage board of directors early.** Help the board understand the requirements. Work together to determine governance changes needed.
ITEM: Material Cybersecurity Incident Disclosure *(Form 8-K Item 1.05)*			
All registrants.	Compliance required.	12/18/2023	**Develop capabilities and update incident management process to reduce time to complete and accurate disclosures.** Determine how you'll modify your process to consider materiality and ongoing reporting/monitoring. Consistency is crucial in determining materiality and disclosing issues, so that the same methodology, process, and controls apply for cybersecurity as for operational or financial statement issues. Meeting the 4-business-day requirement will require developing capabilities in: • **Cross-functional collaboration.** Audit, risk, compliance, and ITRM teams must work together to set thresholds and make decisions on materiality. Build streamlined workflows that enable swift identification and analysis of material cyber incidents, including identifying root causes, controls that worked or failed, and remediation needed. • **Risk quantification.** Measuring potential impact on performance requires quantifying financial impact based on an integrated view on risk that understands how cybersecurity ties in with operational and enterprise risk, linking technology assets, operational processes, and business outcomes. Consider implementing an IRM platform that connects risks and controls across the enterprise and enables teams to share data in a single system of record.] • **Leverage technology.** Get the right technology in place to integrate risk management and communication and streamline disclosures across the organization — either a single integrated solution or individual solutions tied together.
Smaller reporting companies.	Compliance required.	6/15/2024	

What to Do Now

Now that you're clear on applicability, dates, and recommended actions, make sure you're clear on what they mean for your organization in the short term. In particular:

- **Annual report considerations** — Organizations will need to issue disclosures in 2024. For calendar fiscal year issuers, disclosures will include the cybersecurity risk management and governance they have in place on ***December 31, 2023*** — including the processes and methodologies used to determine materiality.
- **Continuous monitoring considerations —** Organizations need to begin monitoring for cyber incidents and materiality on ***December 18, 2023***, so they're ready to comply with immediate reporting requirements for material cybersecurity incidents.

In other words, ***you may have less time than you think.*** **Your organization should be working NOW to get the processes and technologies needed to support effective cybersecurity disclosures in place by December 31.** For most organizations, that includes assessing gaps, establishing and integrating disclosure processes, developing capabilities, and updating risk quantification and incident management processes (including setting thresholds and building workflows to assess materiality), engaging the board, and more.

Overview of the SEC Cybersecurity Disclosure Requirements

The overview table and detailed breakdowns below simplify the how, when, and what of the final rules. By adopting these final rules, the SEC aims to provide greater transparency into how companies are managing their cybersecurity risk; accordingly, mandatory disclosures will be made via Form 8-K, 8-K/A, and 10-K filings (20-F, 6-K, and 6-K/A filings for foreign private issuers), meaning that ***all information becomes public record***. There are no requirements for the SEC to keep any information non-public. That means investors and other stakeholders can use it in their decision-making — and regulators and attorneys can use it for their purposes.

The SEC Cybersecurity Rules Update At a Glance

The SEC received more than 150 comment letters in response to its proposing release. The final rule details many of the comment letters' concerns and recommendations, explaining whether (and how) final rules were modified in response. While this is helpful in understanding the SEC's process and reasoning, the resulting 186-page PDF release of the final rule doesn't exactly make for light reading.

With that in mind, I've gone through the complete release with a fine-toothed comb to create a **summary table that tells you everything you really need to know.** For the sake of simplicity, our summary focuses on the requirements for US companies. Following the overview table, you'll also find a more detailed discussion of each disclosure requirement highlighting key considerations and differences between the draft and final regulations. All page numbers refer to the **SEC's final rule PDF** (which has been conformed to the Federal Register version).

Note that the SEC has divided the requirements into two reporting categories: "current," which includes material incident disclosures made in 8-K filings, and "periodic," which includes required disclosures on cybersecurity risk management, strategy, and governance provided via 10-K filings.

SEC Cybersecurity Final Rules Update At a Glance

Topic	#	Current Reporting (Form 8-K)	Periodic Reporting (Form 10-K)
1. Material Cybersecurity Incident Disclosure — Form 8-K Item 1.05	1	***Timing of Disclosure:*** Material incidents must be disclosed within **4 business days** of determining an incident was material. Materiality must be determined "without unreasonable delay" after discovery, considering factors like impact on key systems, unauthorized access to large quantities of important data, financial impact, harm to reputation, customer/vendor relationships, or competitiveness.	
	2	***Scope of Disclosure:*** Includes material aspects of the **nature, scope, timing,** and **material impact or reasonably likely material impact** on the registrant, including its financial condition and results of operations. Companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident.	
	3	***Broad Definition of "Cybersecurity Incident":*** An unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the **confidentiality, integrity, or availability** of a registrant's information systems or any information residing therein. Includes incidents on third-party systems.	
	4	***Newly Discovered Incident Information:*** Companies must provide an **amended Form 8-K** for any information that was not determined or was unavailable at the time of the initial Form 8-K filing. This may include any corrections of prior disclosures that were untrue or omitted a material fact.	
2. Exceptions Permitting Limited Delay of Material Incident Disclosure	1	***National Security or Public Safety:*** Written notification from the U.S. Attorney General can delay disclosures due to substantial risk to national security or public safety (up to 120 days from the original disclosure obligation in extraordinary circumstances).	
	2	***Compliance with FCC's CPNI Rules:*** Entities subject to the FCC's customer proprietary network information (CPNI) rule can delay an 8-K filing up to 7 business days following notification to the U.S. Secret Service and FBI with written notification to the SEC.	

Topic	#	Current Reporting (Form 8-K)	Periodic Reporting (Form 10-K)
3. Cybersecurity Risk Management, Strategy, and Governance Disclosure — Regulation S-K Items 106(b) and 106(c)	1		***Required Disclosures — General Cyber Risk Management and Strategy:*** Description of processes for assessing, identifying, and managing material risks from cybersecurity threats (including third-party involvement), and description of whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition. Includes the following: • Whether and how the described processes have been integrated into the registrant's overall risk management system or processes. • Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with such processes. • Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with using third-party service providers. • Any additional information deemed necessary, based on the registrant's facts and circumstances, for a reasonable investor to understand the registrant's processes.
	2		***Required Disclosures — Corporate Governance:*** Description of the board's oversight of risks from cybersecurity threats, and management's role in assessing and managing material risks from cybersecurity threats, including specific positions or committees responsible and reporting to the board. Includes the following: • Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise. • 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.
4. Compliance Dates	1	***All Registrants:*** The disclosure rules are effective **September 5, 2023.**	
	2	***All Registrants Other Than Smaller Public Companies:*** Incident disclosures (Form 8-K Item 1.05) effective **December 18, 2023.**	***All Registrants:*** General cyber risk management, strategy, and governance disclosures (Regulation S-K Items 106 (b) and (c)) beginning with annual reports for fiscal years ending on or after **December 15, 2023.**
	3	***Smaller Public Companies:*** Extension until **June 15, 2024.**	
5. Safe Harbors	1	***Future Security Registration and Anti-fraud:*** If a company is late in reporting a significant cybersecurity incident, it won't lose the ability to use a simplified process for registering securities (Form S-3 eligibility), nor will it be considered to have broken specific anti-fraud laws (Section 10(b) and Exchange Act Rule 10b-5). For full understanding, legal counsel may be required.	

Disclosure Requirements for Material Cybersecurity Incidents

To keep it simple, the SEC's current reporting requirements (Form 8-K Item 1.05) are about being able to:

1. **Identify material cybersecurity incidents.**
2. **Quantify their impact.**

There will be a lot to pull together in a very short time frame, from the material incident determination to 8-K filing. For most organizations, this will require much more timely investigation and quantification around cybersecurity risk than is being done today.

The final rule includes **several noteworthy changes from the original proposal**, including:

- **No specific materiality definition**. The SEC declined to adopt a cybersecurity-specific materiality definition, stipulating, "we expect that registrants will apply materiality considerations as would be applied regarding any other risk or event that a registrant faces." *(See p. 80.)*
- **Limited delays permitted:**
    - **In verified matters of national security or public safety.** Companies may delay disclosure if the U.S. Attorney General (AG) "determines immediate disclosure would pose a substantial risk to national security or public safety." In these circumstances, written notification from the AG to the SEC is required. *(See pp. 34-35.)*
    - **For entities subject to the Federal Communications Commission's (FCC's) customer proprietary network information (CPNI) rule.** The SEC permitted this exception given concerns about a potential conflict with existing FCC rules. *(See pp. 41-42.)*
- **No required disclosures regarding remediation status.** The final rule did not adopt the proposal to require disclosure regarding the incident's remediation status, whether it is ongoing, and whether data were compromised. The SEC considers that registrants will determine as part of materiality analyses whether such disclosures are necessitated. *(See p. 30.)*
- **No required disclosure of immaterial cybersecurity incidents in aggregate.** The proposal to require disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate was not adopted. *(See pp. 52 and 140.)*
- **No aggregation requirement for related incidents.** The proposed aggregation requirement to capture the material impacts of related incidents was not adopted. *(See p. 52.)* That

said, the SEC's adopted definition of "cybersecurity incident" does extend to "a series of related unauthorized occurrences."

- **Rejection of periodic reporting only.** The suggestion to replace Item 1.05 with periodic reporting of material cybersecurity incidents on Forms 10-Q and 10-K was not adopted, since such an approach may result in significant variance as to when investors learn of material cybersecurity incidents. *(See p. 36.)* Instead, updates to prior incidents reported via 8-K filings will be made in an 8-K amendment rather than in a 10-Q or 10-K. **In other words, all cybersecurity incident information will be disclosed in current rather than periodic reports.**

Material Cybersecurity Incident Disclosure — Form 8-K Item 1.05

Form	8-K filing
Timing	Within 4 business days of determining an incident was material.
Information	Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its: • Nature, scope, and timing. • Impact or reasonably likely impact.
Required Amendments	Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.

Disclosure Requirements for Cybersecurity Risk Management and Strategy

The cybersecurity risk management and strategy disclosure requirements (Regulation S-K Item 106(b)) aim to provide a consistent, comparable view of cybersecurity risk management programs that offers insight into program capabilities, strategy, and effectiveness. To this end, companies will be required to affirm whether they have a cybersecurity risk assessment program, how it works, how it fits into overall risk management, and whether it uses third parties. Notably, this will include disclosing a description of "whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition."

The final rule includes a few **noteworthy changes from the original proposal**, including:

- **Streamlining of required disclosure elements**. Commenters expressed concerns that disclosing specific policies, procedures, and technologies could undermine cybersecurity and increase vulnerability to cyberattacks. Others worried that elements were overly prescriptive, such that companies would feel pressured to model policies on the final rule's disclosure elements rather than what was best-suited to each company's unique circumstances. In response to these concerns and others, the SEC eliminated several elements to support "disclosure of information material

to the investment decision of investors... while steering clear of security sensitive details," including:

- **Substituting the word "process" for "policies and procedures,"** to avoid disclosing details (or the lack thereof) that could be weaponized. *(See p. 60.)*
- **Removing proposed disclosures** of "prevention and detection activities," "continuity and recovery plans," and "previous incidents" and r**equiring only high-level disclosures** regarding third party-service providers. *(See p. 62.)*
- **Clarifying that elements listed are non-exclusive**, such that registrants should also "disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes." *(See p. 63.)*

Risk Management and Strategy Disclosures — Regulation S-K Item 106(b)

Form	10-K filing
Timing	Annually
Information	Description of processes for assessing, identifying, and managing material risks from cybersecurity threats (including third-party involvement), and description of whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition. Includes the following: • Whether and how the described processes have been integrated into the registrant's overall risk management system or processes. • Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with such processes. • Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with using third-party service providers. • Any additional information deemed necessary, based on the registrant's facts and circumstances, for a reasonable investor to understand the registrant's processes.

Disclosure Requirements for Cybersecurity Governance

Finally, the cybersecurity governance disclosure requirements (Regulation S-K Item 106(c)) ask companies to account for how material cybersecurity risks are overseen at the board level, assessed and managed at the management level, and communicated to the board. **This approach encourages a fresh look at how cybersecurity risk management connects with strategy and integrates with overall risk management.**

The final rule includes a couple of **noteworthy changes from the original proposal** to require "less granular" disclosures, including:

- **No required disclosure regarding the board's cybersecurity expertise.** The proposed requirement to disclose the cybersecurity expertise of a registrant's board members was not adopted. *(See p. 140.)*
- **Limiting required disclosures** to those the SEC believes "balances investors' needs to understand a registrant's governance of risks from cybersecurity threats in sufficient detail to inform an investment or voting decision with concerns that the proposal could inadvertently pressure registrants to adopt specific or inflexible cybersecurity-risk governance practices or organizational structures." *(See pp. 70-71.)*

It's important to appreciate that, if the SEC had mandated the disclosure of board cybersecurity expertise, it may have offered investors a deceptive comfort. Board members' fundamental role is to oversee risk, not directly handle it. Their expertise should be reflected in their ability to guide, not operate. That said, even without a concrete mandate to disclose cybersecurity proficiency within the board, the need for it remains implicit in the final rules.

Governance Disclosures — Regulation S-K Item 106(c)

Form	10-K filing
Timing	Annually
Information	Description of the board's oversight of risks from cybersecurity threats, and management's role in assessing and managing material risks from cybersecurity threats, including specific positions or committees responsible and reporting to the board. Includes the following: • Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise. • 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.

How to Prepare for Compliance With the SEC Cybersecurity Rules

The best way to organize your to-do list is to start at the end and work backwards: Make sure you understand the final rules, and let that guide your analysis of what needs to be done. Look beyond disclosure preparation to ensure you have the needed infrastructure in place. Use the recommended action plan provided above to get started.

Again, to ensure the speed and accuracy needed for identifying incidents, assessing materiality, and preparing disclosures within the 4-business-day requirement, **an IRM approach will be critical.** IRM and IRM technologies can help you connect and streamline processes, controls, and teams to enable effective cross-functional collaboration and risk and impact quantification. The graphic below illustrates the interplay between the new rules and the bigger picture of IRM and IRM technologies, including the four universal IRM objectives of better performance, stronger resilience, greater assurance, and more cost-effective compliance.

How Tech Enables IRM and Compliance With SEC Cybersecurity Rules

Most companies have work to do in connecting technology and teams. AuditBoard's *2023 Digital Risk Report* found that only 30% of organizations currently use cloud-based risk management software to manage digital risk. Another 18% use on-premises risk management software, 44% still rely on manual technologies (e.g., spreadsheets, email, shared drives, and SharePoint), and 8% do not manage digital risk at all.

The SEC Cybersecurity Rules Demand Integrated Risk Management

With their final rules, **the SEC has elevated IT risk and cybersecurity as true business risks.** This is an important step in helping organizations to understand and manage their entire spectrum of strategic, operational, financial, and digital risks, helping them to make more informed, timely, and strategic decisions. But companies face significant challenges in maturing risk management and determining materiality. According to the SEC's 1999 Staff Accounting Bulletin No. 99 and a March 2022 statement from Acting Chief Accountant Paul Munter, **determining materiality is both qualitative and quantitative. It cannot be calculated using a formulaic method.** As I told *InformationWeek*, "Determining materiality for cybersecurity will, in my opinion, require an integrated view of risk — tying cybersecurity to critical areas of the business operations. Without this view, the impact on a reasonable investor cannot be determined."

An IRM approach is crucial for linking cybersecurity, operational, and enterprise risk to determine materiality. Audit, risk, compliance, and ITRM professionals will be forced to work together to come up with solutions, engendering a clearer understanding of cybersecurity's impact on the business — and better alignment of technologies, processes, and business outcomes.

Every organization should recognize that **the SEC cybersecurity rules are part of a larger trend toward integrated reporting and risk management.** Just like standalone financial reports don't give the full picture of how a business is doing, disconnected technologies aren't effective in meeting today's risk management challenges. Integrated technology solutions bring together different data and perspectives into a common risk framework — creating an integrated view of risk that connects people, increases understanding, enables prioritization, and supports performance, resilience, assurance, and compliance. If your organization is still dragging its feet on integrating risk management, 2023 is the time to get moving.

To learn how AuditBoard can help *streamline your compliance efforts*, request a *tailored demo here*.

About the Author

John A. Wheeler is the Senior Advisor, Risk and Technology for AuditBoard, and the founder and CEO of Wheelhouse Advisors. He is a former Gartner analyst and senior risk management executive with companies including Truist Financial (formerly SunTrust), Turner Broadcasting, Emory Healthcare, EY, and Accenture.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, IT security, and ESG management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fourth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.