

Navigating the new SEC cybersecurity disclosure requirements

Four steps to help you prepare and comply



On July 26, 2023, the Securities and Exchange Commission (SEC) issued a final rule¹ requiring registrants to provide enhanced and standardized disclosures regarding cybersecurity risk management, strategy, governance, and incidents.

The final ruling addresses concerns over investor access to timely and consistent information related to cybersecurity as a result of the widespread use of digital technologies and artificial intelligence, the shift to hybrid work environments, the rise in the use of crypto assets, and the increase in illicit profits from ransomware and stolen data, all of which continue to escalate cybersecurity risk and its related cost to registrants and investors.

The new disclosure requirements take effect starting on or after December 15, 2023, and Deloitte is here to help your organization plan for the enhanced transparency mandated by the latest rule.

¹Securities and Exchange Commission (SEC), "SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies," press release, July 26, 2023.

Final rule background

The final rule incorporates certain key changes from the proposed rule. It can be summarized in these three distinct areas:



- Intent²**
 - + Concerns over investors' access to timely and consistent information related to cybersecurity
 - + Boost investors' confidence toward cybersecurity governance
 - + Drive reporting consistency of cybersecurity matters across registrants
- Includes³**
 - + Enhanced disclosures regarding material cybersecurity incidents
 - + Enhanced disclosures for assessing, identifying, and managing material cybersecurity risks
 - + Disclosures regarding their role in assessing and managing cybersecurity risk
 - + Disclosures regarding the board of directors (board) role for oversight of cybersecurity risk
- Impacts⁴**
 - + Public, emerging growth, and smaller reporting companies subject to the reporting requirements of the Securities Exchange Act of 1934
 - + Foreign private issuers (FPIs)
 - + All companies with relevant disclosure obligations on Forms 10-K, 10-Q, 20-F, 8-K, 6-K, or proxy statements

²Deloitte, "SEC issues new requirements for cybersecurity disclosures," Heads Up 30, no. 13 (July 30, 2023) ³SEC, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," July 26, 2023. ⁴Deloitte, "SEC issues new requirements for cybersecurity disclosures."

Overview of final rules

The final rules focus on improving and standardizing disclosures related to cybersecurity incidents,⁵ as well as reporting on cybersecurity risk management, strategy, and governance for public companies.

<p>1 Disclosure of cybersecurity incidents</p> <ul style="list-style-type: none"> + Report "material" cybersecurity incidents within four business days, based on materiality determination, without "unreasonable delay" + Describe the incident's material impact or reasonably likely material impact + Disclose if one or more of the above required items is not determined or is unavailable at the time of the filing <p><small>Periodic Form 8-K Item 1.05</small></p>	<p>2 Disclosure of cybersecurity risk, management, & strategy</p> <ul style="list-style-type: none"> + Disclose processes for assessing, identifying, and managing material risks from cybersecurity threats + Describe how processes have been integrated into an overall risk management system or processes + Describe risks, including those resulting from previous incidents, that have materially affected or are reasonably likely to materially affect business strategy, results of operations, or financial condition + Disclose whether cybersecurity program engages consultants, auditors, or other third parties, as well as the processes to identify and manage risk from third parties <p><small>Annually 10-K, Regulation S-K Item 106(b)</small></p>	<p>3 Disclosure of cybersecurity governance</p> <ul style="list-style-type: none"> + Describe the board's oversight of risks from cybersecurity threats, and identify the committee or subcommittee responsible for oversight and the process for informing such committees + Describe management committees or positions responsible for, and experience with, assessing and managing cyber risks + Disclose whether and how management reports cybersecurity information to the board or a committee or subcommittee of the board <p><small>Annually 10-K, Regulation S-K Item 106(c)</small></p>
--	---	---

⁵As per SEC, materiality of an incident is based on company's evaluation of the incident. The content on this slide is based on Deloitte's "SEC issues new requirements for cybersecurity disclosures"

Taking action to prepare and comply

Here are four practical steps you can take to prepare for and comply with SEC cybersecurity rules for public companies.

- 1 Conduct an SEC readiness assessment**

Safeguard the organization's reputation and protect against cyber risks while complying with SEC rules:

 - + Develop a foundation to evolve response capabilities as threats evolve
 - + Identify potential risks and address issues promptly
 - + Provide evidence that you are taking steps to comply
 - + Understand maturity of incident response, escalation, and reporting processes
- 2 Evolve cyber incident response and reporting capabilities**

Protect the organization's interests, maintain trust, and strengthen overall cyber resilience

 - + Define materiality criteria and embed in incident processes
 - + Continue to meet disclosure obligations as incidents evolve
 - + Learn from past incidents and improve resilience
 - + Maintain investor confidence and protect shareholder value
- 3 Apply stakeholder coordination and orchestration processes**

Develop broad disclosure capabilities that are interconnected

 - + Facilitate timely and appropriate disclosures
 - + Combine legal guidance with cybersecurity experience
 - + Develop accountability for compliance and disclosure
 - + Provide consistent disclosures with transparency
- 4 Enhance the cybersecurity governance framework**

Provide shareholders with confidence that cyber is a top organizational priority

 - + Strengthen governance by educating the board and management
 - + Foster a culture of responsibility and accountability
 - + Implement operating models for risk management
 - + Identify board committee or subcommittee responsible for cybersecurity oversight

Effective cybersecurity capabilities that are essential for compliance and form the basis of a strong cybersecurity program include, but are not limited to:⁶ continuous logging and monitoring, enhanced policies and procedures, incident response, and effective governance capabilities.

⁶The above list is not an exhaustive compilation of all the actions that should be taken or capabilities deployed. Additional cybersecurity measures and leading practices may also be required to determine protection and compliance with SEC requirements for cybersecurity disclosures.

Contact us

Learn more about how Deloitte is helping clients navigate understanding and complying with the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure ruling for public companies.

<p>Emily Mossburg Advisory Principal Deloitte & Touche LLP +1 571 766 7048 emossburg@deloitte.com</p>	<p>Adnan Amjad Advisory Partner Deloitte & Touche LLP +1 713 982 4825 aamjad@deloitte.com</p>	<p>Gaurav Kumar Advisory Principal Deloitte & Touche LLP +1 212 436 2745 gukumar@deloitte.com</p>
<p>Naj Adib Advisory Principal Deloitte & Touche LLP +1 212 436 5750 nadib@deloitte.com</p>	<p>Sandra Herrygers Advisory Partner Deloitte & Touche LLP +1 313 396 3475 sherrygers@deloitte.com</p>	<p>Christine Mazor Audit & Assurance Partner Deloitte & Touche LLP +1 212 436 6462 cmazor@deloitte.com</p>

Visit us at [deloitte.com/us/MoveForwardFast](https://www.deloitte.com/us/MoveForwardFast)

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

The services described herein are illustrative in nature and are intended to demonstrate our experience and capabilities in these areas; however due to independence restrictions that may apply to audit clients (including affiliates) of Deloitte & Touche LLP, we may be unable to provide certain services based on individual facts and circumstances.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2023 Deloitte Development LLC. All rights reserved.