

SEC issues rules

Enhancing cybersecurity disclosures

July 28, 2023



SEC final rules increase disclosure of cybersecurity incidents, risk management, strategy and governance.

Source and applicability

- SEC Release No. 33-11216, [Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure](#)
- Public companies subject to the Securities Exchange Act of 1934, including foreign filers (except Canadian foreign private issuers that file Form 40-F and asset-backed securities issuers)


Fast facts, impacts, actions

The SEC has released its final rules on cybersecurity, which address cybersecurity risk management, strategy, governance and incident reporting. They are intended to provide more consistent, comparable and decision-useful information so that investors can better evaluate a registrant’s exposure to cybersecurity risks and incidents and strategies to mitigate those risks and incidents.

The final rules require several new and enhanced disclosures based on two broad categories.

Cybersecurity incidents	Risk management, strategy and governance
<p>On Form 8-K, report:</p> <ul style="list-style-type: none"> • material cybersecurity incidents, including information about material aspects of the incidents • additional information about material aspects of previously reported incidents as that information becomes available (use Form 8-K/A) 	<p>On Form 10-K, disclose:</p> <ul style="list-style-type: none"> • cybersecurity processes • management’s role in cybersecurity governance • cybersecurity oversight by the board of directors

The final rules differ from the proposed rules in some important ways, as discussed in this publication.



The final rules are effective September 5, 2023, meaning immediate action is required to ensure compliance teams are ready. Generally, compliance with the Form 8-K filing requirements begins on December 18, 2023 at the earliest, and governance disclosures in Form 10-K are required for fiscal years ending on or after December 15, 2023. See [Effective dates](#).

Background

Before the final rules, no existing disclosure requirements explicitly referred to cybersecurity risks or incidents in the securities laws. To address concerns in this area, the SEC staff issued guidance in 2011 and 2018 that focused on how general SEC disclosure requirements applied to cybersecurity risks and incidents. See KPMG Defining Issues, [SEC issues guidance on cybersecurity disclosures](#).

The final rules reflect the SEC's belief that, despite the 2011 and 2018 guidance, disclosure practices have been inconsistent and lack sufficient information for investors' purposes. To promote the timeliness and consistency of disclosures concerning both cybersecurity incidents and governance surrounding cybersecurity, the final rules amend Regulation S-K to create specific disclosure requirements.



The 2018 guidance remains in effect after the final rules become effective. That guidance highlights where disclosure obligations about cybersecurity matters may arise in various parts of periodic filings (e.g. MD&A, risk factors), while the final rules create Item 106 in Regulation S-K that requires specific disclosures in a designated section of the Form 10-K.

Summary of new requirements

The final rules introduce several new provisions in Regulation S-K that require the following disclosures.

Cybersecurity incidents	
Reporting material cybersecurity incidents on a Form 8-K	Disclose on Form 8-K specified information about a material cybersecurity incident within four business days of determining the incident was material (not within four days of the incident occurring).
Amending the Form 8-K as material updates about reported incidents arise	Provide information that was not determined or was unavailable about a previously disclosed material incident on an amended Form 8-K.
Risk management, strategy and governance	
Disclosing cybersecurity processes	Disclose processes for assessing, identifying and managing material risks from cybersecurity threats on Form 10-K, and describe whether any such threats may have materially affected (or are reasonably likely to materially affect) the registrant's business strategy, results of operations or financial condition, and if so, how.
Disclosing management's role in cybersecurity governance	Describe management's role in assessing and managing material risks from cybersecurity threats, and the relevant expertise of such individuals on Form 10-K.
Disclosing oversight of risks from cybersecurity threats by the board of directors	Disclose the board's oversight of risks from cybersecurity threats on Form 10-K, and if applicable, identify the committee responsible for such oversight and describe the process by which the committee is informed about such risks.

Form 8-K disclosure reporting of a material cybersecurity incident

A material cybersecurity incident has to be reported on a Form 8-K. The final rules define a cybersecurity incident as “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.” Under this definition, a group of related occurrences is treated as a cybersecurity incident and if material is reported on a Form 8-K, even though each occurrence may be immaterial on its own.



The proposed rules would have required reporting of unrelated cybersecurity incidents that when aggregated are material. However, the final rules do not contain a requirement to aggregate unrelated incidents.

Content of Form 8-K disclosure

Once a registrant determines a cybersecurity incident is material (see [Materiality](#)), it must report the incident on a Form 8-K. New Item 1.05 of Form 8-K requires a registrant to “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.”



The proposed rules had listed five specific disclosure requirements, some of which may have required registrants to disclose immaterial details about a material incident. The final rules require describing only ‘material aspects’ of the incident.

Timing of filing of Form 8-K

The final rules require a Form 8-K filing within four days after a registrant determines that a cybersecurity incident is material. A registrant must make this materiality determination without unreasonable delay after discovering an incident. Once a registrant determines that an incident is material, it cannot delay reporting, unless the Commission receives authorization from the US Attorney General to delay filing due to national security or public safety concerns (see [National security and public safety provision](#)). This means filing cannot be delayed due to internal or external investigations.

If, at the time the form is due, the information required to be disclosed is not yet determined or is unavailable, the registrant includes a statement to that effect in the filing. However, it must continue to determine or obtain such information without unreasonable delay. Further, it must file an amended Form 8-K within four business days of determining or obtaining the information.



A registrant does not have to amend Form 8-K for all new information about the incident, only for information that would have initially been reported on the Form 8-K had it been known or available. However, if subsequent information indicates that any information in the prior filing(s) is untrue or misleading, a registrant may have to correct the prior filing.

Materiality

Whether a cybersecurity incident is material is based on the SEC’s traditional materiality standard, which is set out in the securities laws. Under this standard, information is material if “there is a substantial likelihood that a reasonable shareholder would consider it important” in making an investment decision, or if it would have “significantly altered the ‘total mix’ of information made available.”

The SEC has noted a materiality analysis is not a mechanical exercise that is based solely on a quantitative analysis of a cybersecurity incident. Instead, a registrant needs to thoroughly and objectively evaluate the total mix of information, considering all relevant facts and circumstances surrounding the

cybersecurity incident (including both quantitative and qualitative factors) to determine whether an incident is material.

National security and public safety provision

The final rules contain a provision permitting the deferral from filing a Form 8-K to report a material cybersecurity incident if the US Attorney General determines that disclosure would pose a substantial risk to national security or public safety. The Attorney General may authorize a deferral from reporting of up to 30 days, but may extend that for another 30 days. In extraordinary cases, the Attorney General may grant a second deferral of up to 60 days. Any further deferral would require the SEC to issue an exemptive order.



The SEC must receive written notification from the Attorney General for a delay to be authorized. SEC officials have indicated that they have established communication lines with the Department of Justice to ensure timely transmission of written notifications.

There is no filing deferral for ongoing law enforcement investigations – unless they are part of the Attorney General’s determination that national security or public safety is at risk should a cybersecurity incident be disclosed at the present time. However, in cases for which deferral is not available, the SEC does not expect the Form 8-K disclosures to include specific or technical information about planned responses to incidents or about the registrant’s cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant’s response or remediation of the incident.

Exemption and safe harbor

To be eligible to use Form S-3 to register securities, registrants are required to be current and timely in filing reports required by the Securities Exchange Act of 1934 (Exchange Act). However, the final rules amend Form S-3 to provide an exemption so that an untimely filing of Form 8-K to report a cybersecurity incident would not result in the loss of eligibility to use this form, as long as the Form 8-K reporting is current at the time the Form S-3 is filed.

The final rules also expand a limited safe harbor provision from liability under Section 10(b) or Rule 10b-5 under the Exchange Act for failing to timely file certain items on Form 8-K. The safe harbor now includes the failure to timely file a Form 8-K to report a material cybersecurity incident.

Form 10-K disclosure of cybersecurity risk management and strategy

The final rules create Item 106(b) of Regulation S-K to require disclosure about a registrant’s risk management and strategy. The first part of the disclosure requires a registrant to describe its cyber risk management system in Form 10-K by disclosing its processes for identifying, assessing and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. A non-exclusive list of items to be disclosed is as follows (not all may apply to every registrant).

Whether and how these 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 its use of any third-party service provider

The second part of the disclosure requires a registrant to describe whether any risks from cybersecurity threats (including as a result of previous cybersecurity incidents) have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations or financial condition, and if so, how.



Because registrants must describe whether the result of previous cybersecurity incidents have or are reasonably likely to have a material effect on them, registrants may want to track the nature and relationship of individual incidents – including those not deemed material – to inform them on how to adjust their processes and systems.

Form 10-K disclosure of management’s role in cybersecurity governance

The final rules create Item 106(c)(2) of Regulation S-K to require disclosure on Form 10-K of management’s role in assessing and managing the registrant’s material risks from cybersecurity threats. The required disclosures are listed below.

Whether and which management positions or committees are responsible for assessing and managing such risks and the relevant expertise of such persons

The processes by which persons or committees (described in the left column) are informed about and monitor the prevention, mitigation, detection and remediation of cybersecurity incidents

Whether such persons or committees report information about such risks to the board of directors (or committee thereof)

Form 10-K disclosure of board’s role in cybersecurity governance expertise

The final rules create Item 106(c)(1) of Regulation S-K to require disclosure about the board of directors’ oversight of cybersecurity risk. This provision requires:

- disclosure of any board committee or subcommittee responsible for such oversight; and
- a description of the processes by which the board or committee is informed about such risks.

Notably, unlike the proposed rules, the final rules do not require disclosure of any cybersecurity expertise by board members.

Miscellaneous

Foreign private issuers

The final rules align incident reporting and periodic disclosures of foreign private issuers with those of domestic public companies by:

- amending Form 6-K to include ‘material cybersecurity incident’ as a reporting trigger;
- amending Form 20-F to require the same cybersecurity risk management, strategy, governance and updated incident disclosures as proposed for domestic public companies.

Of note, the final rules do not amend Form 40-F, used by Canadian foreign private issuers, because these filers are already generally required to disclose cybersecurity risks and incidents.

Structured data requirements

The final rules require the above disclosures to be provided in Inline XBRL format; however, compliance with this requirement is delayed for one year beyond initial compliance for any issuer with the related disclosure requirements. Submission in this format is intended to make disclosures and reports more available and accessible to investors, market participants and others.

Effective dates

Compliance with the final rules will be required on the following dates.

	Smaller reporting companies	All other registrants
Form 8-K reporting	June 15, 2024	Dec 18, 2023
Form 10-K reporting – fiscal years ending on or after:	Dec 15, 2023	Dec 15, 2023

Contributing authors

Erin McCloskey, Valarie Mosier

KPMG Financial Reporting View

kpmg.com/us/frv

This newsletter is part of our Defining Issues® collection of newsletters and articles with insights and news about financial reporting and regulatory developments.

Sign up [here](#) to receive news and insights delivered to your mailbox.

kpmg.com/socialmedia



© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.