Deloitte.

# Understand SEC requirements for Cybersecurity disclosures

United States Securities and Exchange Commission (SEC) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure[1] Ruling for Public Companies

[1]SEC Final Rule Release No. 33-11216, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,

October 2023

# Table of contents



# Final rule background

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


+ 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

+ Enhanced disclosures regarding material cybersecurity incidents
+ Enhanced disclosures for assessing, identifying and managing material cybersecurity risks
+ Disclosures regarding management role in assessing and managing cybersecurity risk
+ Disclosures regarding the board of directors' (board) role for oversight of cybersecurity risk

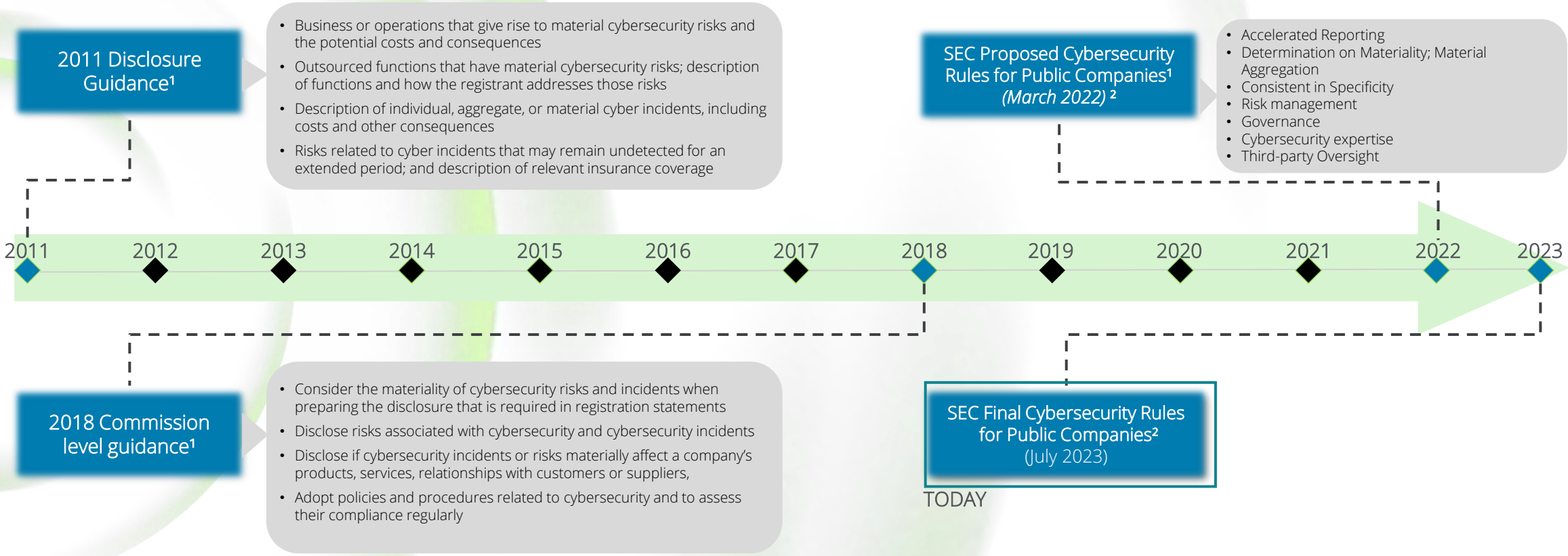
+ Public, emerging growth, and smaller reporting companies, subject to the reporting requirements of the Securities Exchange Act of 1934
+ Foreign private issuers (FPIs)
+ All companies with relevant disclosure obligations on Forms 10-K, 10-Q, 20-F, 8-K, or 6-K, and proxy statements

 | 

*[1]Heads up, Volume 30, Issue 13, Deloitte National Office, titled 'SEC Issues New Requirements for Cybersecurity Disclosures', July 30, 2023*
*[2]SEC Final Rule Release No. 33-11216, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, July 26, 2023*

# SEC cybersecurity alerts and interpretive guidance

The SEC has monitored registrants' disclosure practices as cybersecurity risk has evolved. The final cybersecurity rules can be traced through several noticeable developments over the years, including disclosure and commission level guidance provided.




On March 9, 2022, the SEC published the proposed cybersecurity rules for public companies. The final rules adopted in July 2023 incorporate specific changes, from the proposed rules, in response to over 150 comment letters received by the Commission.

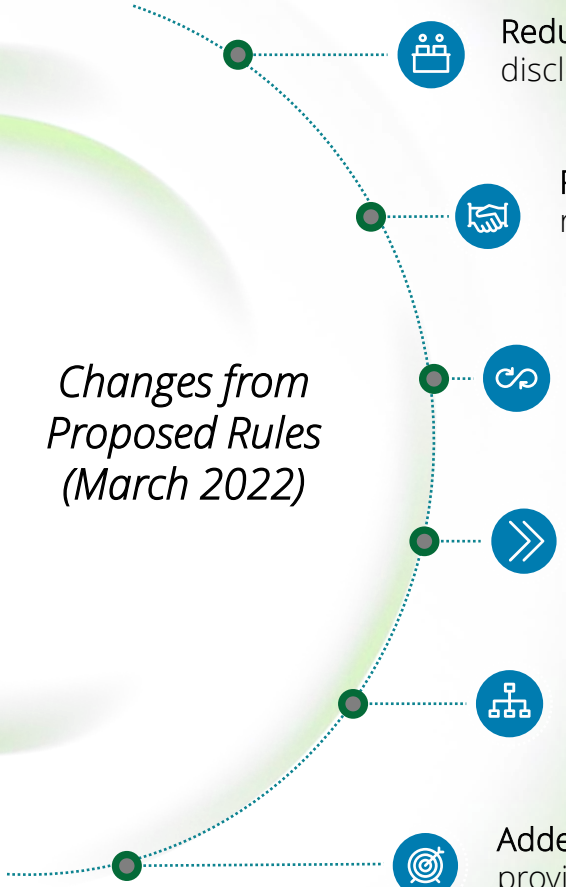
[1]Listed items are not exhaustive of disclosure or commission level guidance; they are meant to illustrate some of the requirements listed

[2]Listed items are not exhaustive of proposed or final cyber security rules; they are meant to illustrate some of the requirements listed

# Changes from the 2022 proposed rules

Compared to the March 2022 proposing release, the final rule issued incorporates certain specific changes from the proposed rules in response to the comments received.




**Reduced scope of disclosures:** Narrowing the scope of the cybersecurity incident disclosures and adding a limited delay for disclosures that may likely pose a substantial risk to national security or public safety.

**Removed requirement to disclose material changes to cybersecurity incidents on annual/quarterly reports:** Require registrants to use an amended Form 8-K instead of Forms 10-Q and 10-K to update incident disclosures.

**Removed requirement to disclose singular immaterial incidents having material aggregate impact:** Omitting the aggregation of immaterial incidents for disclosure in Forms 10-Q and 10-K; however, a series of ***related*** unauthorized occurrences may prompt a requirement to provide disclosures on Form 8-K.

**Streamlined risk management and governance disclosure requirements :** Final disclosure elements related to risk management, strategy, and governance focus on "processes" as opposed to specific policies and procedures.

**Removed requirement to identify board Cybersecurity expertise:** Removing the proposed requirement to disclose cybersecurity expertise of the board of directors.

**Added transition provisions:** Added transition provisions for disclosing material cybersecurity incidents on Form 8-K and for providing annual cybersecurity risk management, strategy, and governance disclosures.

 | 

# Final rules and forms

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

## Disclosure of Registrant's Cybersecurity Incidents on Current Reports

### Material Cybersecurity Incidents

- Disclose cybersecurity incidents within four (4) business days (based on materiality date)
- Describe the "material" aspects of incident nature, scope, and timing of the incident
- Consider whether to aggregate related cyber incidents (series of related unauthorized occurrences)
- Not exempt from disclosing incidents for third-party systems used (no safe harbor for information disclosed about third-party systems)
- Make materiality determination "without unreasonable" delay
- Describe incident's material impact or reasonably likely material impact on organization
- File amendment when incident information is determined (file an amended Form 8-K)
- 30+ day delay for disclosure if United States Attorney General (AG) determines disclosure poses a risk (national security or public safety)

*Periodic Form 8-K Item 1.05*

## Disclosure of Registrant's Cybersecurity Risk Management, Strategy and Governance

### Risk Management and Strategy

- Disclose processes to assess, identify, and manage material risks
- Disclose risks from cybersecurity threats and previous incidents, materially affected/reasonably likely to materially affect registrant
- How cybersecurity processes have been integrated into overall risk management system or processes
- Describe cybersecurity program engagement with assessors, consultants, auditors, third-parties
- Describe processes to oversee and identify material risks associated with use of third-party service providers

Annually 10-K — *Regulation S-K Item 106(b)*

### Governance

- Describe the board's oversight of risks from cybersecurity threats
  - Identify board committee or subcommittee responsible for oversight
  - Describe processes by which the board is informed
- Describe management's role in assessing and managing material risks
  - Management positions/committees responsible
  - Relevant expertise of persons/members
  - How persons/committees are informed
  - Reporting structure to the board or a committee/subcommittee of the board

Annually 10-K — *Regulation S-K Item 106(c)*

## Disclosure by Foreign Private Issuers (FPIs)

- Amends Forms 20-F and 6-K to require FPIs to provide disclosures that are generally consistent with those discussed herein for domestic registrants. Specifically, FPIs should disclose in their annual Form 20-F the board's oversight of risks from cybersecurity threats and management's role in assessing and managing material risks from cybersecurity threats.
- Requires FPIs to furnish on Form 6-K information on material cybersecurity incidents that they disclose or publicize in a foreign jurisdiction to any stock exchange or security holders

Disclose Material Cybersecurity Incidents (Form 8-K, Item 1.05): all registrants the later of 90 days after the date of publication in the Federal Register or December 18, 2023. For smaller reporting companies, the later of 270 days from the effective date of the rules or June 15, 2024.

Disclose Cybersecurity Risk Management, Strategy and Governance (Regulation S-K, Item 106 (in Form 10-K, Item 1C,): Beginning with annual reports for fiscal years ending on or after December 15, 2023.

# Select guidance

During discussions with cybersecurity, legal, business, and IT leaders about the final rules, several requirements were raised that required immediate clarity or further guidance.

## What constitutes incident materiality?

Work to formally codify what constitutes materiality, including qualitative and quantitative factors:

- Probability of adverse outcomes, such as a significant disruption or degradation of the ability to maintain critical operations
- Potential significance of the loss nature and extent of harm to the organization such as theft of intellectual property or theft of data, and importance of information compromised
- Nature and extent of harm to individuals, customers, vendor relationships
- Nature and extent of harm to registrant's reputation, brand, or competitiveness

*Note: A lack of quantifiable harm does not necessarily mean an incident is not material.

## What type of incident information should be disclosed?

It is important to disclose required information regarding material aspects of the nature, scope, and timing of the incident, including:

- Nature: type or category, including data breach, ransomware, supply chain
- Scope: extent to which the incident has affected operations, systems, data, or customers
- Timing: timeline of the incident, indicating occurrence, discovery

*Note: It is important to disclose the material impact of the incident, or the reasonably likely material impact – meaning that there is a realistic possibility of a material impact, even if the full extent of the incident's consequences is not yet known.

## How do I address cyber incident disclosure for TPSPs[1]?

Incident disclosure for Third Party Services Providers (TPSP) may be required by both the service provider, the organization, or by one but not the other, or by neither:

- Review information provided by TPSP, compare information received to materiality definition
- Determine if there is any other publicly available information; determine the need to engage TPSP
- Develop a decision matrix for TPSP reported incidents; categorize by type of information
- Provide integration of TPSP reported incidents into existing incident reporting framework
- No requirement to conduct additional inquiries outside of regular channels of communication

## How do I identify and manage cyber risk?

Develop risk management and assessment mechanisms, including:

- Understand business environment or increased awareness of high-risk processes, areas
- Define methods to identify untreated or natural levels of risk in processes or activities
- Determine what controls or protocols can be applied to manage identified cyber risk
- Define criteria for determining inherent risk
- Develop protocols for risk treatment (e.g., mitigate, accept, share)
- Define processes to elevate cyber incidents to those tasked with assessing incidents for disclosure

[1] *TPSPs: Third Party Service Providers*

*Note: Some content on this slide is based on Deloitte publication, Heads up, Volume 30, Issue 13, titled 'SEC Issues New Requirements for Cybersecurity Disclosures'*

# Act now to prepare and comply

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

## Conduct a SEC readiness assessment

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

- Design disclosure controls and procedures to elevate cyber incidents to the appropriate individuals to determine incident materiality in a timely manner
- Confirm that those making the disclosures have controls that allow for complete and accurate disclosure of all material information
- Validate operational preparedness across select cyber capabilities (e.g., Incident Response, Risk Management, Governance, Reporting)

## Evolve cyber incident response and reporting capabilities

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

- Define a process for assessing materiality criteria and embed in incident response process
- Continue to meet disclosure obligations as incidents evolve
- Clearly communicate the threat and impact implications through defined reporting channels
- Learn from past incidents and improve resilience

## Apply stakeholder coordination and orchestration processes

Develop broad disclosure capabilities that are inter-connected

- Engage with legal counsel prior to disclosure
- Develop accountability for compliance and disclosure
- Provide consistent disclosures with transparency
- Policies should be specific and not generic or boiler plate
- Educate employees on how to apply them / respond to red flags

## 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
- Consider how and how often the board will be updated on cybersecurity risks

Underpinned by effective cybersecurity capabilities and activities that are essential for compliance and that form the basis of a strong cybersecurity program[1], including continuous logging and monitoring, cyber incident response, risk assessments, and governance mechanisms.

[1]The 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.

# Appendix

# Definitions - Terms

The Commission has defined three terms to delineate the scope of the amendments: “cybersecurity incident”, “cybersecurity threat”, and “information systems”. Below are the definitions:

***Cybersecurity incident***
means 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

***Cybersecurity threat***
means any potential unauthorized occurrence on or conducted through a registrant’s information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant’s information systems or any information residing therein

***Information systems***
means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant’s information to maintain or support the registrant’s operations

*Content on this slide is referred from SEC Final Rule Release No. 33-11216: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*

# Overview of disclosure requirements

The final rule requires that registrants provide enhanced and standardizing disclosures related to cybersecurity incidents as well as reporting on cybersecurity risk management, strategy, and governance. It retains a broad definition of a cyber security incident and applies to systems owned AND used by the registrant.

## Form 8-K Incidents

- Report “material” cybersecurity incidents within four business days of when an incident is determined to be material
- Describe nature and scope of incident, timing and material impacts (i.e., financial condition and results of operations)
- If required information is not determined or is not available at the time of the initial, disclose that fact and provide via an amendment

## Form 10-K Risk, Management, Strategy

- Disclose processes for assessing, identifying, and managing material risks from cybersecurity threats
- Describe whether risks, including those resulting from previous incidents, have materially affected or are reasonably likely to materially affect business strategy, results of operations or financial condition

## Form 10-K Governance

- Describe board’s oversight of risks from cybersecurity threats
- Describe management's role in assessing and managing material risks from cybersecurity threats

*Note: As per SEC, materiality of an incident is based on company’s evaluation of the incident.*

# Overview of SEC final rule: material cybersecurity incident

## Item 1.05 Form 8-K Reporting Requirements (Material Cybersecurity Incidents)

### 01 Disclosure Timeline

- Item 1.05 Form 8-K must be filed within four (4) business days of determining a cybersecurity incident was material
- Registrant may delay filing if US Attorney General determines immediate disclosure would pose substantial risk to national security or public safety pursuant to Item 1.05(c)

### 02 Disclosure Requirements

- Registrants must include "material" aspects of the event's:
  - Nature, scope, and timing
  - Material impact or reasonably likely material impact on the registrant (including its financial condition and results of operations)
    - Qualitative and quantitative aspects should be considered in assessing the material impact
  - Registrants are not exempt from providing disclosures regarding cybersecurity incidents on third-party systems or information disclosed about third-party systems
  - To the extent information is not determined or it is unavailable at the time the initial Form 8-K is filed, the registrant can include a statement to the effect in the filing, and would then file an amendment to the form 8-K within four (4) business days after information is determined or becomes available

# Overview of SEC final rule: material cybersecurity incident

## Materiality considerations

The guidance emphasizes that companies should  make materiality determinations without “unreasonable delay”.


### Nature, extent, and potential magnitude

The magnitude of cybersecurity risks or incidents depends on, among other things, their nature, extent, and potential magnitude.

### Importance of Compromised Information

The impact to the company’s “crown jewels”, most critical data and assets should be evaluated.

### Business and scope of operations

Consider the impact of the cybersecurity risks and incidents related to a company’s business and scope of operations.  It does not depend on whether the registrant owns the impacted system.

### Range of harm and probability of an adverse outcome

The materiality of cybersecurity risks and incidents depends on the range of harm that such incidents could cause and the probability an adverse outcome will occur.

### Financial, legal, and reputational consequences

The possibility of litigation or regulatory investigations may also impact materiality assessments.

*****Consistent with the standard of materiality articulated by the Supreme Court, the final rule holds that a fact is material if there is a substantial likelihood a reasonable shareholder would consider it important in an investment decision or disclosure would significantly alter the total mix of information available.

# Overview of SEC final rule: material cybersecurity incident

## Materiality considerations[1]

- Costs of business disruption
- Impact to reputation and competitiveness
- Implications to relationship with customers and vendors
- Loss of intellectual property
- Costs of litigation, investigation, and remediation
- Regulatory requirements and compliance costs

**Quantitative and qualitative factors to consider**

**A lack of quantifiable harm does not necessarily mean that an incident is not material.**

[1]The above list is not an exhaustive compilation of all materiality considerations.

Deloitte.

# Thank you.