



Crimson Vista, INC

# Navigating SEC Cybersecurity Disclosure Requirements: Ensuring Compliance and Building Trust

Strengthening Transparency in Cyber Risk Management and Governance

---

**By:** Maria J. Castro L., Esq.  
Founder, CastroLand Legal, PLLC

November 2024




**For Crimson Vista, BDO, Norton Rose Fulbright**

# Executive Summary

## Overview

The U.S. Securities and Exchange Commission (SEC) has implemented new cybersecurity disclosure rules to enhance transparency and accountability among public companies. These rules require timely reporting of material cybersecurity incidents, governance practices, and risk management strategies to provide investors with relevant insights. Effective December 2023, the regulations emphasize the critical role of cybersecurity in corporate governance and business strategy, requiring companies of all sizes—including smaller reporting companies (SRCs)—to adopt robust compliance measures.

## Key Findings

-  Cybersecurity risks are increasingly material to investor decision-making, driving the need for standardized disclosures
-  Many companies lack integrated processes for assessing materiality and ensuring timely incident reporting
-  Smaller reporting companies face unique challenges but are equally subject to these new requirements

**48% of public companies lack a dedicated Chief Information Security Officer (CISO) or internal cybersecurity team, exposing them to heightened risks and vulnerabilities**



48%

## Call to Action

Organizations must act swiftly to adapt to the SEC's stringent requirements by:

- Investing in robust cybersecurity infrastructure and governance frameworks.
- Aligning internal and external processes to enable rapid assessment and disclosure of material incidents.
- Collaborating across IT, legal, and compliance teams to ensure readiness.

These steps are not just about compliance—they position businesses for resilience and long-term success in an increasingly complex threat landscape.

# Introduction

The U.S. Securities and Exchange Commission (SEC) adoption of rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure for public companies is a major regulatory update designed to enhance transparency and accountability regarding cybersecurity practices. The SEC mandates that all public companies subject to the reporting requirements of the SEC Exchange Act of 1934 comply with its updated cybersecurity disclosure rules, including a) Domestic Public Companies and b) Foreign Private Issuers.

All public companies listed on U.S. exchanges, regardless of industry or size, must comply with SEC cybersecurity disclosure requirements. However, they are only obligated to disclose incidents that meet the materiality threshold—meaning those with the potential to significantly impact the company’s financial position, reputation, or operations. **As SEC Chair Gary Gensler explained, “Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors.”**

Typically, the responsibility for determining materiality lies with the company’s legal and compliance teams, who assess whether an incident warrants disclosure. At this stage, close collaboration with the cybersecurity team is crucial. The cybersecurity team provides essential insights into the incident’s scope, severity, and potential operational impact, supplying the legal and compliance teams with the technical information needed for a well-informed materiality assessment. This partnership ensures that all aspects of the incident—both technical and regulatory—are thoroughly evaluated, leading to an accurate and comprehensive disclosure decision.

**A notable aspect of the SEC’s push is the application to smaller reporting companies (SRC’s).** As noted by the commission on their report, “Smaller companies may face equal or greater cybersecurity risk than larger companies, such that cybersecurity disclosures may be particularly important for their investors.” An SRC must satisfy one of the following:

This broadened applicability really emphasizes that cybersecurity transparency is vital for all companies, regardless of their industry or size, as these rules aim to provide investors with timely, relevant insights into a company’s cybersecurity practices and risk management.

## Annual Revenue

- Less than \$100 million in annual revenue for companies with no public float, or
- a public float under \$700 million

## Public Float

- Less than \$250 million in market value of shares held by non-affiliates.

# SEC Requirements

The SEC's new cybersecurity disclosure rules for public companies, aim to provide investors with timely, relevant insights into companies' cybersecurity practices and incident management. These rules are part of a larger initiative to increase transparency at a time when cybersecurity risks have become central to a company's operations, reputation, and financial well-being.

## Objective of the Requirements

The SEC's new rules aim to provide clarity and timely information on cybersecurity risk and management practices. By standardizing the disclosure of cybersecurity incidents and governance, it seems that the SEC intends to increase investor confidence and ensure that material cybersecurity risks are made visible. Companies that fail to comply with these requirements may face enforcement actions, penalties, and reputational consequences.

These updated cybersecurity disclosure requirements underscore the increasing importance of cybersecurity as a critical component of both business strategy and corporate governance. By mandating transparency in how companies address cybersecurity risks and respond to incidents, the SEC aims to reinforce accountability at the highest levels. This ensures that boards and executives play an active role in decision-making during cybersecurity risk management and incident response, while providing investors with clearer insights into how companies are protecting sensitive data and responding to potential threats.

The SEC's new rules require (1) annual disclosures in Form 10-K regarding the company's processes, if any, for identifying, assessing and managing material risks from cybersecurity threats as well as management's and the board's roles in managing and overseeing material cybersecurity risks; and (2) that public companies disclose on Form 8-K material cybersecurity incidents within four business days of determining their materiality. . These measures aim to enhance clarity and give investors timely relevant information regarding the company's standpoint in cybersecurity and incidents.

---

Regarding the **effective date for the cybersecurity requirements**, the SEC's final rule on these disclosures went into effect on September 5, 2023, however, the **compliance dates were staggered**:

### December 15, 2023

All registrants must include cybersecurity risk management and governance disclosures in annual reports (Form 10-K or 20-F) for fiscal years ending on or after this date

### December 18, 2023

Large registrants must comply with incident disclosure requirements (Form 8-K for U.S companies and Form 6-K for foreign private issuers)

### June 15, 2024

Smaller reporting companies had until this date to comply with the incident disclosure requirements

# SEC Requirements

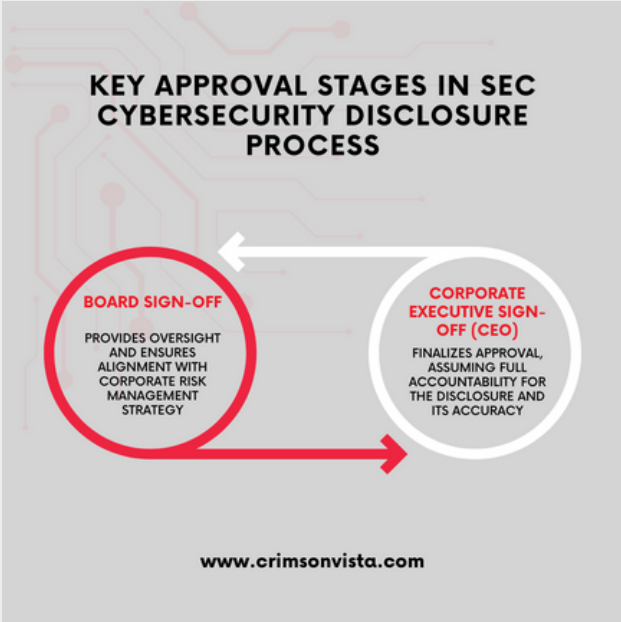
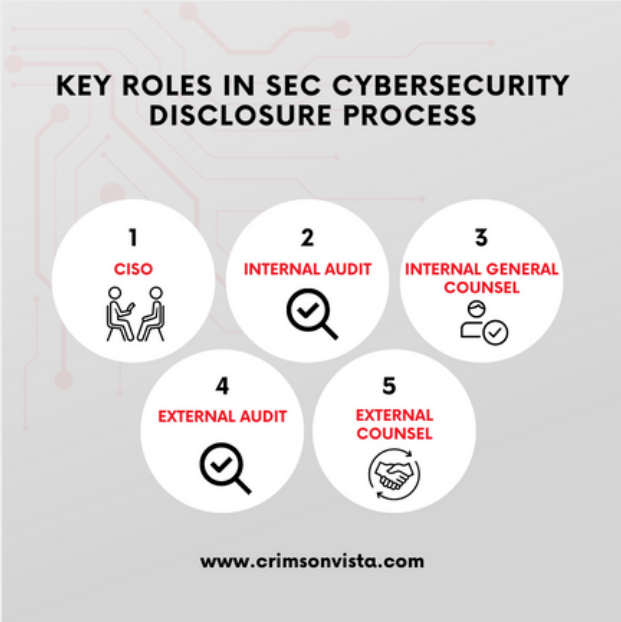
Here is a quick table review of the **latest** SEC requirements:

Disclosure Requirement	Company activities	Auditor Activities	Filing Type
<b>Cybersecurity Governance</b>	Describe board oversight of cybersecurity risks Explain management's role in assessing and managing risks Disclose relevant expertise of responsible personnel	Assess governance structure disclosures Evaluate board and management oversight processes Review expertise disclosures	Form 10-K (U.S.) Form 20-F (Foreign Private Issuers)
<b>Material Cybersecurity Incidents</b>	Determine the materiality of cybersecurity incidents Disclose within 4 business days of materiality determination Describe the material aspects of the nature, scope, and timing of the incident Disclose the material impact on financial condition and results of operations: Lawsuits (standard of care, negligence) Regulatory Investigations, Fines, Impact, Reputation	Review incident disclosure controls and procedures Assess materiality determination process Evaluate the timeliness of disclosure	Form 8-K (U.S.) Form 6-K (Foreign Private Issuers)
<b>Inline XBRL Tagging</b>	All cybersecurity-related disclosures must be tagged using <b>Inline XBRL</b> to make them machine-readable and accessible for stakeholders.		Applies to both <b>Form 10-K (U.S.)</b> and <b>Form 20-F (Foreign Private Issuers)</b> for annual disclosures, and any periodic filings containing updates to material incidents.



# Teams Involved in Cybersecurity Disclosures

In the SEC's cybersecurity disclosure process, several internal and external teams play essential roles, each contributing to different aspects of assessing, determining, and managing disclosures.



# Conclusion

In conclusion, the SEC's updated cybersecurity disclosure requirements underscore the critical role of transparency, accountability, and governance in today's business landscape. By mandating timely and detailed disclosures, the SEC ensures that investors are better informed about the cybersecurity practices and incident response strategies of public companies, as they are equally important as other financial and business decisions. This regulatory push highlights that cybersecurity is not only a technical issue but a key element of business strategy and corporate governance, with board members and executives expected to play an active role.

The structured disclosure process—starting from incident assessment by the CISO and internal audits, to materiality evaluation by legal, and validation by external auditors—ensures that each cybersecurity incident is addressed accurately and responsibly. This collaborative approach ultimately supports investor confidence and positions companies to address cybersecurity risks as integral to their resilience and reputation, reflecting the SEC's aim to protect stakeholders in an increasingly digital world.



## Need Help with SEC Compliance and Cybersecurity?

Contact us today for expert guidance on navigating SEC cybersecurity disclosure requirements and strengthening your cyber risk management strategy. **Ensure your organization leads with confidence, resilience, and security in today's dynamic regulatory environment.**

**If your organization is interested in an executive or board workshop or briefing to learn how these new regulations apply and what steps must be implemented for compliance, contact us at [info@crimsonvista.com](mailto:info@crimsonvista.com)**

# Contact

Whether you need legal guidance, risk management expertise, or advanced cybersecurity solutions, **Crimson Vista, BDO, and Norton Rose Fulbright** are here to help. Reach out today to build resilience, achieve SEC compliance, and secure your organization.

## **Crimson Vista, Inc**

Founded in 2016 by a renowned industry expert, Dr. Seth J. Nielson, **Crimson Vista** has become a trusted leader in cybersecurity consulting and compliance solutions. With nearly a decade of experience, we specialize in guiding organizations—including Fortune 100 companies—through complex regulatory landscapes, such as the SEC's cybersecurity disclosure requirements.

Recognized for our innovative approach and unparalleled expertise, Crimson Vista delivers tailored strategies that empower businesses to strengthen their cyber defenses, mitigate risks, and achieve long-term resilience.

**Website:** [www.crimsonvista.com](http://www.crimsonvista.com)

**Email:** [info@crimsonvista.com](mailto:info@crimsonvista.com)

**Phone:** (737) 240-0126

---

## **Norton Rose Fulbright**

A global law firm with over 3,000 lawyers across 50+ locations, including Houston, New York, London, and Toronto. Serving clients worldwide, the firm specializes in key industries such as financial institutions, energy, technology, healthcare, and consumer markets.

Renowned for quality and integrity, Norton Rose Fulbright provides tailored legal solutions to address complex challenges and strategic goals

**Website:** [www.nortonrosefulbright.com](http://www.nortonrosefulbright.com)



# Contact

Whether you need legal guidance, risk management expertise, or advanced cybersecurity solutions, **Crimson Vista, BDO, and Norton Rose Fulbright** are here to help. Reach out today to build resilience, achieve SEC compliance, and secure your organization.

## About BDO USA

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

**For more information, please visit:** [www.bdo.com](http://www.bdo.com)

**Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.**

© 2024 BDO USA, P.C. All rights reserved.

---