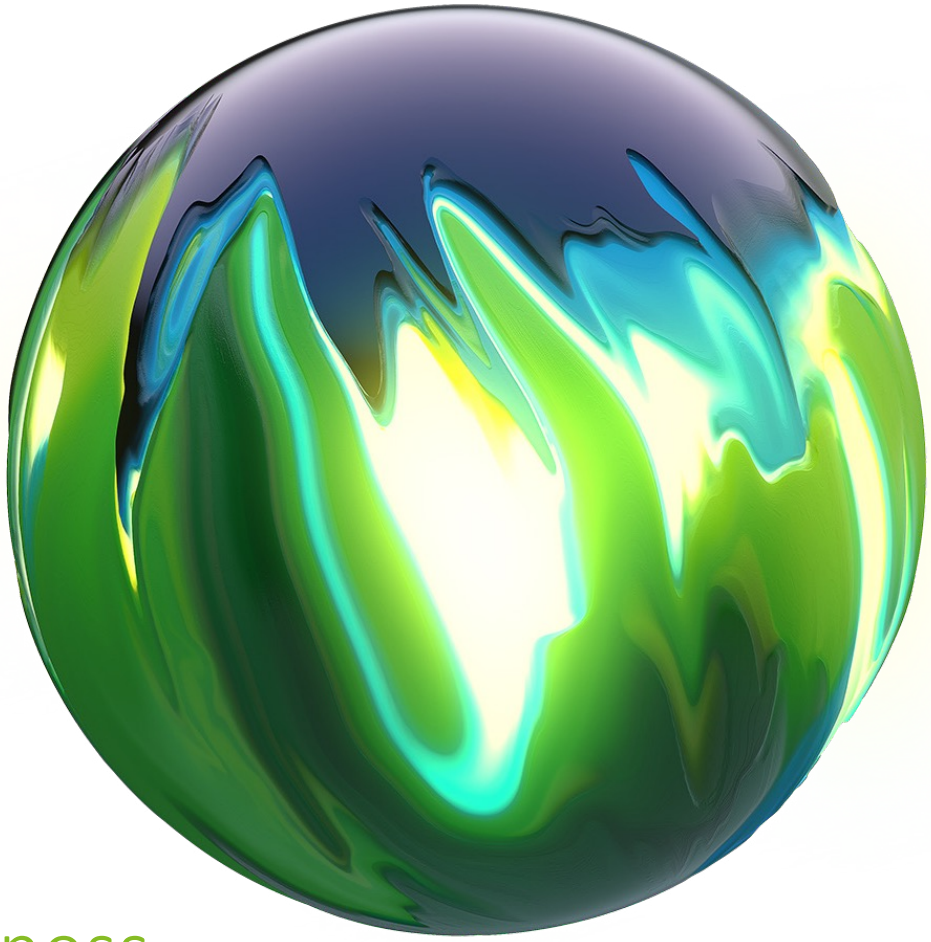
Deloitte.



Future-forward readiness

Preparing for SEC cybersecurity risk management, strategy, governance, and incident disclosure proposed ruling

MAKING AN IMPACT THAT MATTERS since 1845

What’s inside?

Market context	03
What we know about the proposed rule	03
Details of the proposed ruling	04
Drive the change with planned and strategic actions	05
What can you do?	08
The way forward: How Deloitte Cyber can help	09
Contact	09

Market context

The Securities and Exchange Commission (SEC) has proposed enhancements to disclosures regarding cybersecurity risk management, strategy and incident response in their ruling *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* issued on March 9, 2022.[1]

The ruling builds on interpretive guidance published in 2011 and 2018 and is one of the recent SEC proposed rulings[2] on cybersecurity and climate-related risks, among others, which may guide the cybersecurity priorities today and be instrumental in defining strategy for the future.

While this proposed ruling increases the compliance burden on public organizations, it comes with the opportunity to enhance response and recovery, improve cyber program governance and optimization, and implement secure intelligent operations, which could benefit the economy and investors. To realize these opportunities, business and security organization leaders should consider evolving their business models and shaping future products and services with cybersecurity and governance at the center of the initiative.

Cyberattacks can vary widely from company to company. They can include the theft of a company's (or its customers' or vendors') financial assets, intellectual property, or sensitive information; the disruption of a company's operations; or the targeting of companies that operate in industries responsible for critical infrastructure and national security, such as the energy and public utility industries. Costs and consequences of a cybersecurity incident may include remediation expenses, lost revenues, litigation, increased insurance premiums, reputational damage, and erosion of shareholder value.

Of the nearly 600 C-suite executives surveyed in Deloitte's *2021 Future of Cyber Survey*,[3] more than 72% indicated that their organizations had experienced between one and ten cyber incidents or breaches in 2020 alone.

1 Security Exchange Commission, SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, press release March 9, 2022
2 Kruti Modi et al., Deloitte, SEC Proposes New Requirements for Cybersecurity Disclosures, 2022
3 Deloitte, 2021 Future of Cyber survey, 2021. Survey includes insights from over 600 global CXOs.

What we know about the proposed rule

The proposed amendments are designed to better inform investors about material cybersecurity risks and incidents on a timely basis and an organization's assessment, governance, and management of those risks. Impacts all public organizations that are subject to the reporting requirements of the Securities Exchange Act of 1934, as well as foreign private issuers (FPIs) who are required to update Form20-F.

In summary, the amendments aim to:

Boost investor confidence in organizations' cybersecurity governance and incident disclosures, reduce mispricing of securities, and facilitate decision making by driving reporting consistency.

Enhance current reporting about material cybersecurity incidents and periodic disclosures about cybersecurity policies and procedures, management's role, and the board's expertise in implementing a cybersecurity risk program.

Who will be impacted?

All types of periodic SEC filers would be affected by the proposed rule, including domestic registrants, foreign private issuers, smaller reporting companies, and emerging growth companies.

Details of the proposed ruling

Accelerated reporting
Disclose information about a cybersecurity incident within four business days after it is determined as material

Determination on materiality
Determine incident materiality diligently and quickly. Material incidents change current information available or will be important to shareholders

Consistent in specificity
Incident reports to include discovery time, nature and scope, data and operational impact, and remediation efforts

Material aggregation
Disclose singular immaterial incidents having material aggregate impact

Risk management
Periodically disclose policies and procedures, for identifying and managing cybersecurity risks and threats

Governance
Periodically disclose governance structure, including the board of directors' and management's oversight role regarding cybersecurity risks

Cybersecurity expertise
Disclose if registrant's board of directors has cybersecurity expertise through work experience or certification in security

Third-party oversight
Disclose the selection process and cybersecurity risks associated with its use of any third-party service provider

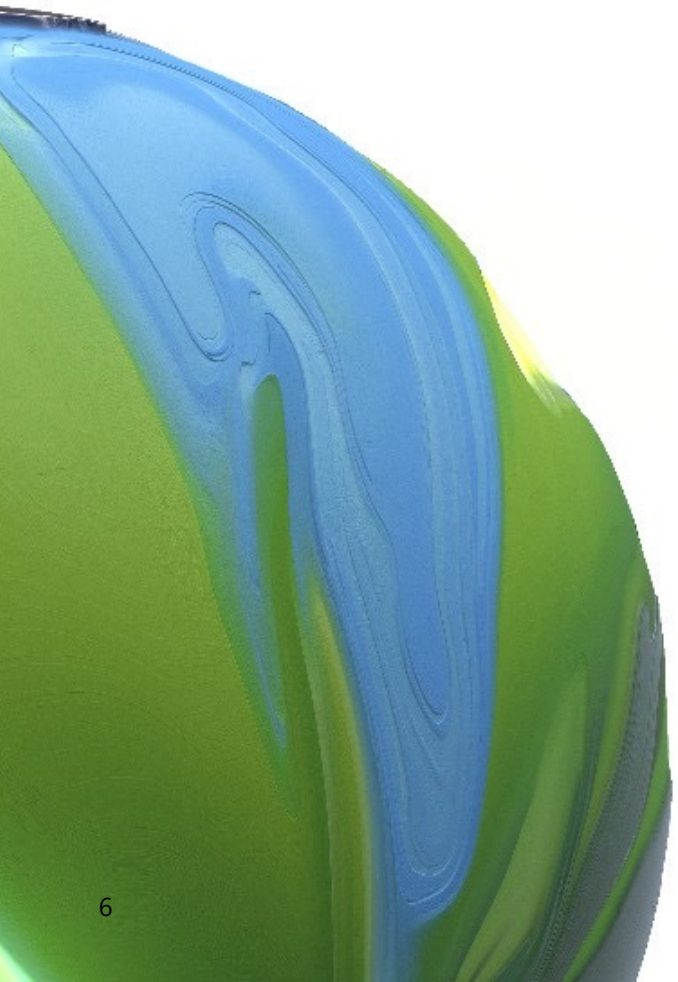
Wherever you are in your cybersecurity journey, we can help you confidently plan and execute an integrated cyber strategy empowering business growth through transformative innovation, while keeping up with the dynamic regulatory landscape.

Drive the change with planned and strategic actions

Though the proposed ruling is not final, organizations should consider the following leading practices to integrate their business and cyber strategy, improve risk management and governance, and refresh incident management processes to keep up with the evolving regulatory landscape.

Enhanced response and recovery

Prepare for the future



1. **Define and implement an incident management framework** including components of governance, strategy, technology, business operations, risk and compliance, and remediation

2. **Define, update, and maintain incident response plan** playbooks/ solutions in line with the threat landscape

3. **Establish an incident categorization and prioritization** model to identify materiality of an incident-based on quantitative and qualitative inputs

4. **Define processes to conduct impact analysis** based on the people, process, and technology capabilities affected to understand the cost and effort required for recovery

5. **Review and follow strategic risk plan** to coordinate cybersecurity incident notification and manage public relations inquiries (establish intake capability):
   - *Review agreements with vendors regarding remediation obligations and your existing cyber insurance policies*
   - *Review third-party service provider's provisions for reporting cybersecurity incidents*

6. **Conduct frequent cross functional cyber exercises** such as wargaming, table-top sessions, to improve response timelines, with involvement of senior leadership

7. **Implement continuous monitoring** through security information and event management (SIEM) solutions, intrusion monitoring systems, threat intelligence feeds from a variety of sources, including the security community and vendor-driven feeds

Cyber governance and optimization

Enhance your cyber posture

1. Establish a risk-based cybersecurity strategy that aligns with overall business and IT strategy

2. Define organization-wide cybersecurity policies, standards, and procedures that are aligned with the strategic and business goals

3. Define a governance framework and organization model to empower:

- *Full delivery of services across the cybersecurity framework*
- *Active involvement of senior management and the board in driving cybersecurity strategy risk management activities*
- *Board-level expertise in security domains to drive innovation within the cybersecurity function*

4. Establish in-house cybersecurity capabilities and engage third-party services to augment the cybersecurity capabilities wherever needed

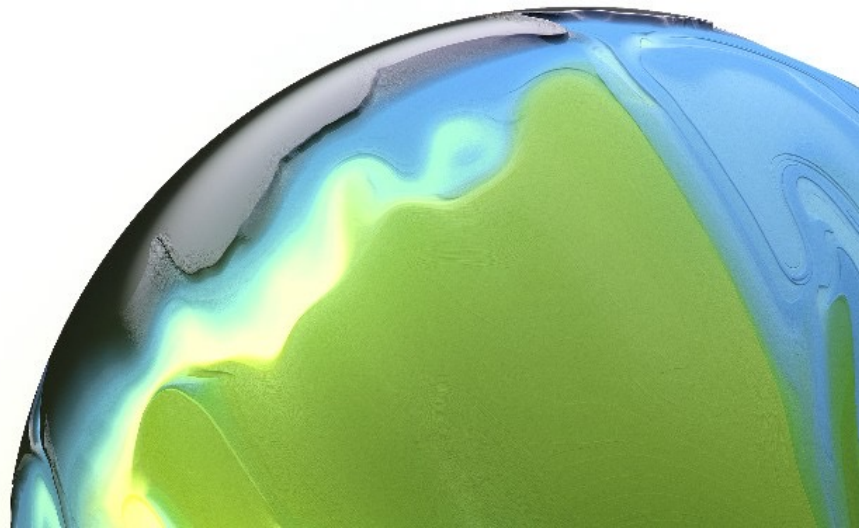
5. Define a Chief Information Security Officer (CISO) or equivalent position to be responsible for cybersecurity strategy, implementation, and monitoring within the organization

6. Establish a cyber risk management discipline:

- *Actively involve the board to review risks to critical infrastructure on a periodic basis*
- *Define and implement risk assessment methodologies to support the risk management lifecycle*
- *Gain visibility of risk emanating from extended organization (e.g., third parties, vendors, contractors) through enhanced analysis and due care of critical and high-risk third parties*
- *Define risk mitigation strategies including cyber insurance*
- *Integrate cybersecurity risk management with the enterprise risk management function*

7. Identify and adopt risk tolerances by determining the cyber risk appetite for the organization, and timely ratify with the stakeholders for streamlined response to the risks

8. Define risk metrics and reporting structure to provide periodic updates on risk management to internal and external audiences, with automated data aggregation and visualization capabilities



What can you do?

Organizations should prepare for a future of greater transparency about their cybersecurity governance program and a streamlined incident reporting approach that continues to drive trust in investors. The emphasis on maintaining technical prowess and cyber security expertise in an organization, lead by the board and the management, better positions them to strengthen relationships with investors, customers, partners, and employees, and promotes nimbleness and resilience to harness the strengths of digital revolution.

Key areas of focus

Now

Investing in the talent pipeline: Develop senior/board level expertise and acquire/invest in talent with key and emerging cybersecurity skills to lay the foundations of a strong cyber organization

Understand your state of readiness for reporting: Explore threat detection, monitoring and response programs best suited to meet your incident reporting compliance requirements to drive efficiencies within your budget

Enhance your policies and procedures framework: Rationalize your regulatory requirements to develop and maintain an integrated controls framework and policies and procedures to meet regulatory requirements and reflect experiential and situation learning and awareness

Later

Evolve from response to resilience in your extended enterprise: Develop and invest in risk intelligence tools that consolidate internal and external information on third parties to streamline management of third party risks

Adopt a continuous evaluation mindset: Integrate technical and business capabilities to drive post incident management, including analysis of incidents in aggregation, which can provide insights and opportunities for optimization

Transcend from digital risk to digital advantage: Drive a focused effort on analytics, AI, automation to accelerate threat detection, augment and expand containment and response, and enable proactive security posture

Contact

We help protect your enterprise by bringing the technology to secure your cyber estate, enabling secure, intelligent operations while providing an efficient workforce that can work for you. In doing so, we help you with business enablement, allowing you to be agile in modernization.

Amir Belkhelladi
Cyber National Leader
514-214-2336
abelkhelladi@deloitte.ca

Louis-Philippe Desjardins
Senior Manager—Cyber Risk Services
514-390-0938
lodesjardins@deloitte.ca

Vignesh Krishnamoorthy
Partner—Cyber Risk Services
416-435-5472
vigkrishnamoorthy@deloitte.ca

The way forward: How Deloitte Cyber can help

Deloitte helps clients design, build, and operate dynamic, business-aligned security programs for each stage in their cyber journey. You can be assured of being well equipped to meet the requirements, while continuing to focus on what you do best: managing your organization.

Global leadership: Deloitte has been named a global leader in Security Consulting and Cyber Incident Response. We offer differentiated domain leadership and entrenched industry experience

Ecosystems and alliances: Strong alliances with leading technology vendors, industry organizations, and research entities to provide leading insights, intelligence, information-sharing, and collaboration

Quantification of cyber risk: Through integrating data and tailored statistical models for risk quantification, we help organizations to augment their experience with technology to develop risk-intelligence responses

Smart cyber technologies: Through our established emerging technology services, we enable cyber integration through secure transitioning into next-gen technologies and environments

Deloitte Cyber

Empowering your people for the future

Our focus on personal relationships, the breadth and depth of our experience, deep technology and product innovation enable us to bring stakeholders together for increased interoperability and impact.

Whatever your organization’s strategic business priorities, we’ll ensure you improve threat awareness and visibility, and strengthen your ability to thrive in the face of cyber incidents.

No matter how complex your situation, we’ll always listen and work with you to address your questions and find the right answers for your unique needs.

Deloitte.

About Deloitte

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges.

Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our shared values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.

To learn more about Deloitte's approximately 330,000 professionals, over 12,000 of whom are part of the Canadian firm, please connect with us on LinkedIn, Twitter, Instagram, or Facebook.

Designed and produced by the Agency | Deloitte Canada. 22-6035103