KPMG

Enhancing the cybersecurity risk framework

Driving cyber to pre-assurance readiness

May 2022

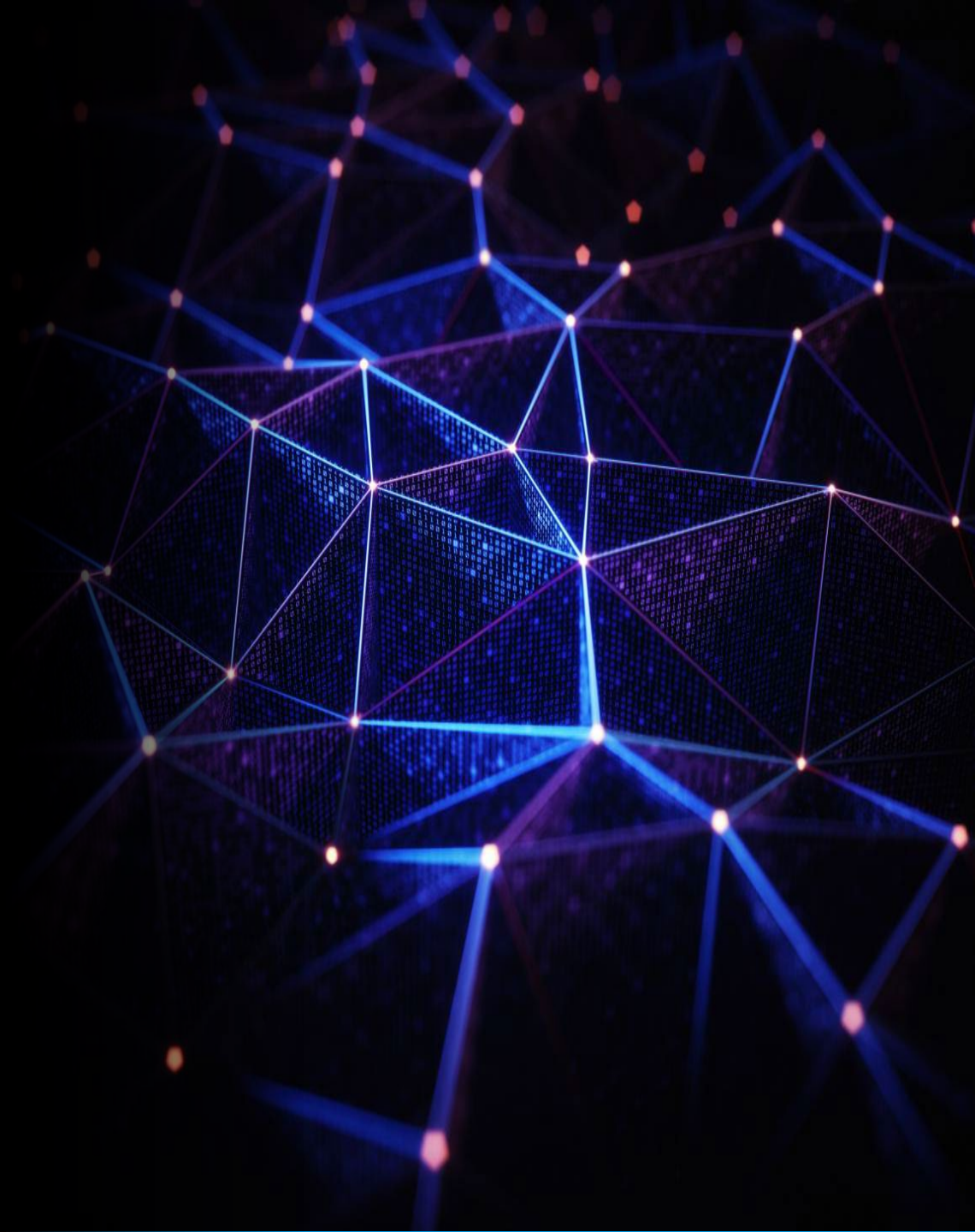


Table of Contents

Matt Miller

Principal
Cybersecurity Services
matthewpmiller@kpmg.com

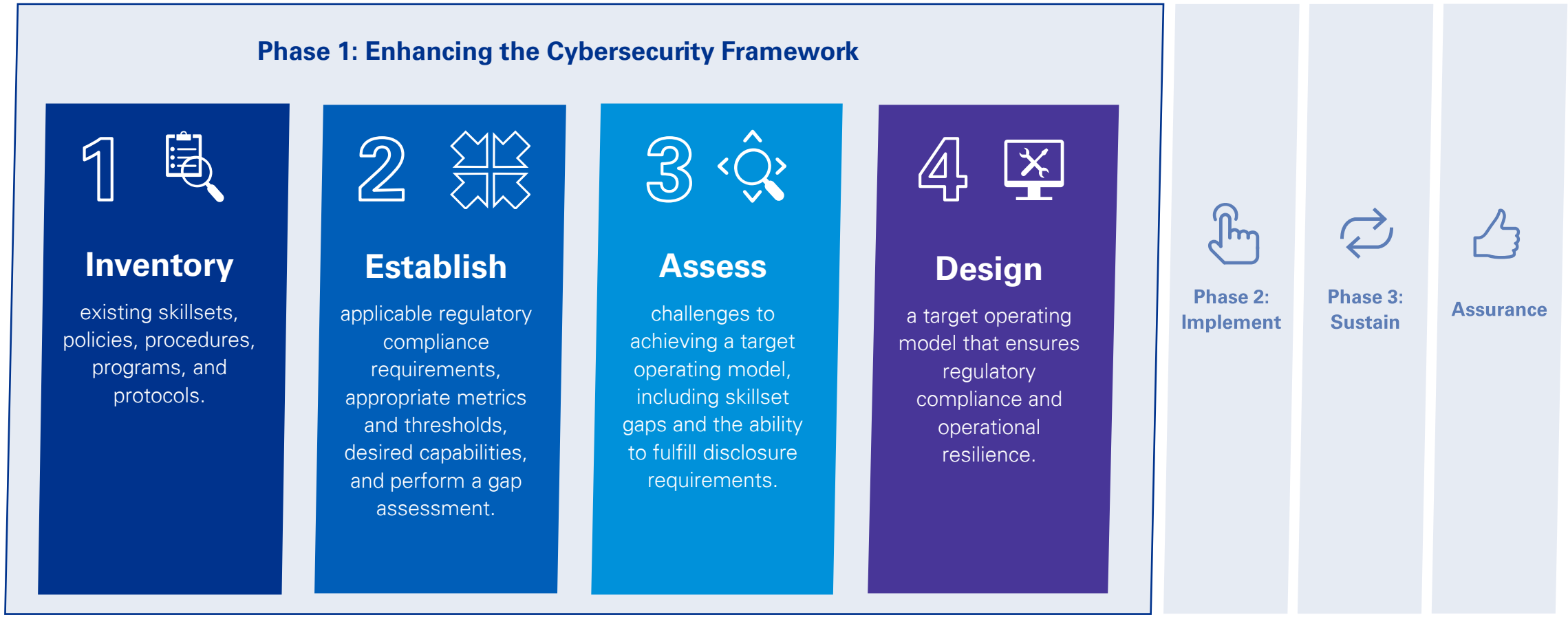
Amy Matsuo

Principal and Leader
Regulatory and ESG Insights
amatsuo@kpmg.com

KPMG

Key Actions: Enhancing the Cybersecurity Risk Framework

Recent regulatory developments around cybersecurity, such as the federal banking regulators' final rule on Cyber Incident Notification and the SEC's cybersecurity proposals, coupled with the Administration's continued alerts and directives on cyber risks are propelling companies to enhance their cybersecurity risk management frameworks across three themes: A) incident reporting and notification, B) risk management, and C) governance and oversight. Firms should look to quickly take the following four key actions prior to implementing enhancements.



Key Action | Inventory

Phase 1: Steps to Enhancing the Cybersecurity Framework

1

2

3

4

Inventory…

existing skillsets, policies, procedures, programs, and protocols.

— **Incident Reporting**: Existing cyber incident reporting detection and reporting procedures and practices within and across systems.

— **Risk Management**: Existing cyber risk management program (risk assessments, policies/procedures, skills, monitoring & testing).

— **Governance**: Existing cyber governance protocols and documented adherence within businesses and at corporate levels.

Phase 2: Implement

Phase 3: Sustain

Assurance

Key Action | Establish

Phase 1: Steps to Enhancing the Cybersecurity Framework

Establish…

applicable regulatory compliance requirements, appropriate metrics and thresholds, desired capabilities, and perform a gap assessment.

- **Regulatory/Stakeholder**: Document all applicable regulatory and key stakeholder requirements/expectations.
- **Metrics**: Agree on desired metrics/thresholds (inclusive of definition for material, internal/external timeframes for escalation and reporting, etc.).
- **Capabilities:** Determine desired system(s), risk management, governance reporting and disclosures capabilities/skills/talent.

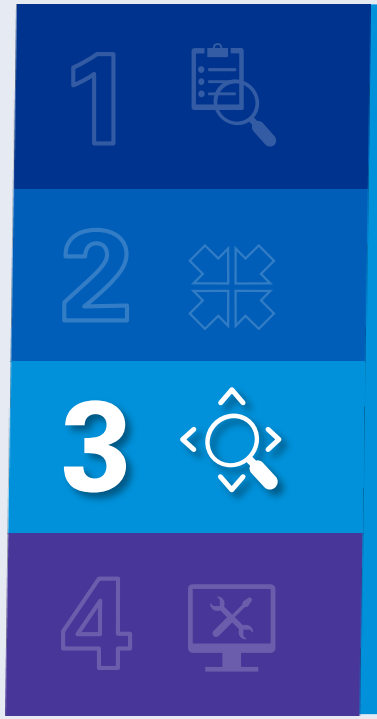
Phase 2: Implement

Phase 3: Sustain

Assurance

Key Action | Assess

Phase 1: Steps to Enhancing the Cybersecurity Framework



Assess…

challenges to achieving a target operating model including skillset gaps and the ability to fulfill disclosure requirements.

— **Control Assessment**: Assess cyber datasets & disclosure(s), including: a) any existing controls mitigating the risk of inaccurate or untimely datasets & disclosures, b) applicable internal control framework evaluating the noted controls, c) mapping to datasets & disclosure(s), and d) discover control gaps in coverage.

— **Gaps & Plan**: Evaluate the identified gaps and develop a remediation plan with considerations for level of effort required, and ability of closing identified gaps.

Phase 2: Implement

Phase 3: Sustain

Assurance

Key Action | Design

Phase 1: Steps to Enhancing the Cybersecurity Framework

Design…

a target operating model that ensures regulatory compliance and operational resilience with appropriate policies, procedures, and programs based on the analyses and gap assessments.

— **Target Design**: Development of cybersecurity reporting and disclosure programs and target operating model, including processes, controls, technology, and organizational structure based on results of the assessment and gap analysis.

— **Prioritized Implementation**: Determine schedule for remaining prioritized systems, reports & disclosures as well as potential expansion of program based on risk-based prioritization.

Phase 2: Implement

Phase 3: Sustain

Assurance

Cybersecurity: Regulatory Expectations

An Executive Order issued in 2021 directed federal agencies to undertake a "whole-of-government" approach to strengthening national cybersecurity defenses, including in areas related to cybersecurity standards, supply chain security, and incident response. Multiple agencies are looking to similarly strengthen the cybersecurity defenses of their supervised entities.

Most recently, the SEC issued two proposed rules addressing cybersecurity that would introduce new requirements for registered investment advisers and funds, and most public companies ("registrants") across three themes:

- A: Cyber incident reporting and notification
- B: Cybersecurity risk management
- C: Cybersecurity governance and oversight

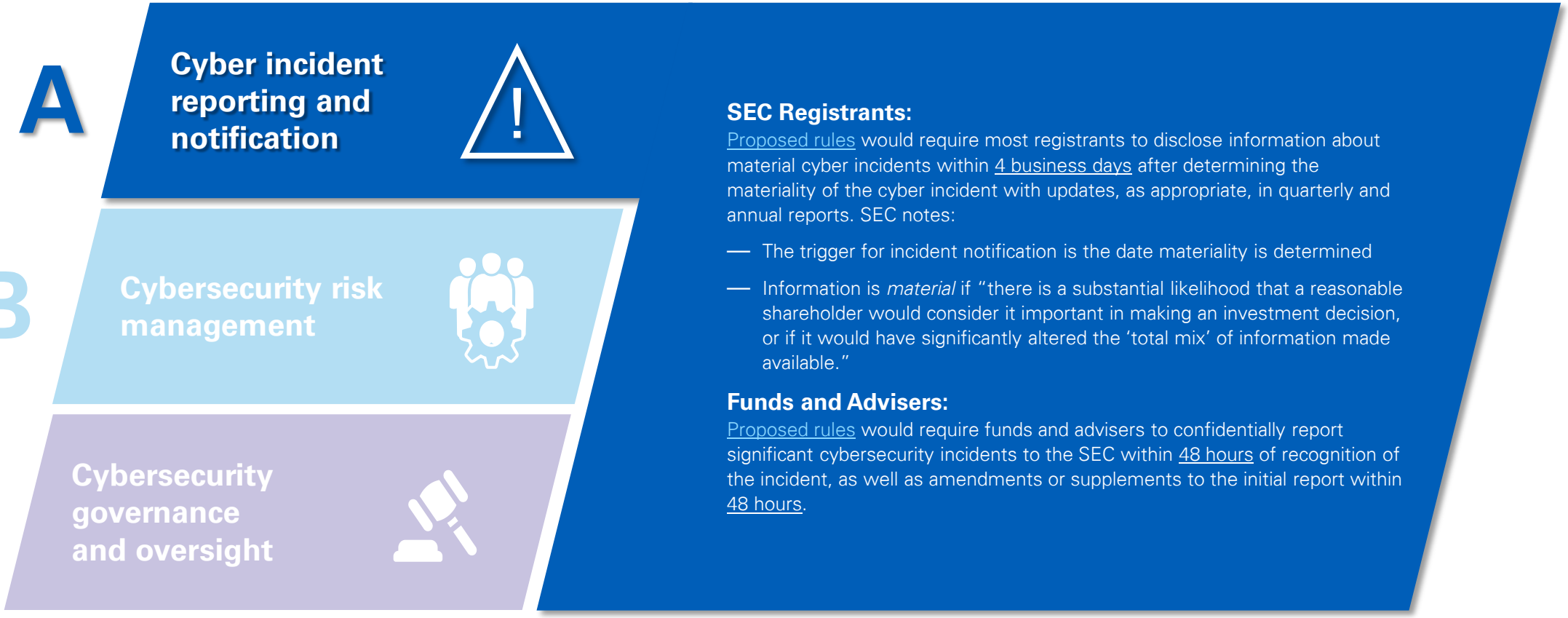
KPMG

SEC Cybersecurity proposals

SEC approved two separate proposed rules in February and March 2022 related to cybersecurity risk management and disclosure requirements for registered investment advisers and funds, and public companies, respectively. Similar measures are forthcoming for broker-dealers, and staff is considering how to address risk from service providers. (See Appendix 1 for defined terms.)

The rules introduce requirements across three themes:

A. Cyber incident reporting and notification



SEC Registrants:

Proposed rules would require most registrants to disclose information about material cyber incidents within 4 business days after determining the materiality of the cyber incident with updates, as appropriate, in quarterly and annual reports. SEC notes:

- The trigger for incident notification is the date materiality is determined
- 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."

Funds and Advisers:

Proposed rules would require funds and advisers to confidentially report significant cybersecurity incidents to the SEC within 48 hours of recognition of the incident, as well as amendments or supplements to the initial report within 48 hours.

B: Cybersecurity risk management

A **Cyber incident reporting and notification**

B **Cybersecurity risk management**

C **Cybersecurity governance and oversight**

SEC Registrants: Would be required to provide disclosures on policies and procedures around cybersecurity risk management and strategy, including:

- Cybersecurity risk assessment program and third-party engagement
- Policies and procedures to oversee and identify cybersecurity risks associated with third-party service providers
- Activities to prevent, detect, and minimize effects of cyber incidents, including business continuity, contingency, and recovery plans
- Whether the registrant's governance, policies and procedures, or technologies adapt in response to a cyber incident
- Cybersecurity-related risks and incidents effects on results of operations and financial condition

Funds and Advisers: Would be required to adopt and implement written policies and procedures designed to address cybersecurity risks, including:

- Risk assessments
- User security and access
- Information protection
- Threat and vulnerability management
- Cybersecurity incident response and recovery
- Annual Review and Written Reports
- Recordkeeping

C: Cybersecurity governance and oversight

A

Cyber incident reporting and notification

B

Cybersecurity risk management

C

Cybersecurity governance and oversight

SEC Registrants: Would be required to disclose information on:

Board's oversight of cybersecurity risk, including:

- How the board oversees cybersecurity risks
- How, and how frequently, the board is informed about cybersecurity risks
- Whether and how the board considers cybersecurity risks in business strategy, risk management, and financial oversight
- Board member expertise in cybersecurity

Management's role in assessing and managing cybersecurity-related risks, including:

- Who is responsible for measuring and managing cybersecurity risk, and their relevant expertise
- Whether a designated chief information security officer exists, to whom that individual reports, and their relevant expertise
- How responsible persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents
- How frequently management reports to the board on cybersecurity risk

Funds and Advisers: A fund's board would be required to initially approve a fund's cybersecurity risk management policies and procedures, and to review the annual written report.

Comparing Regulatory Expectations Across Themes

In March 2022, the President signed the Cyber Incident Reporting Requirements for Critical Infrastructure Act into law. It requires the owners and operators of critical infrastructure, which includes financial services, to report to the U.S. DHS Cybersecurity and Infrastructure Agency (CISA):

— Within 72 hours after a covered cyber incident is believed to have occurred

— Within 24 hours after a ransomware payment has been made

— Promptly after determining a substantial update or supplement to a previously submitted incident report is required

These reporting rules will become effective once CISA finalizes implementing rules; proposed rules are required within 24 months of enactment and final rules are required within 18 months thereafter.

The following tables compare the SEC's proposed requirements and disclosures to the expectations of select regulators and regulations across the three themes.

KPMG

A: Cyber Incident Reporting & Notification

	SEC Proposed Rules	Federal Banking Regulators	NYDFS	Privacy Regulations
Timing	**SEC Registrants:** Most registrants would be required to disclose information about material cyber incidents within 4 business days of determining materiality of the incident. **Funds and Advisers:** Would be required to report significant cybersecurity incidents within 48 hours of recognition of the incident, as well as materially amend or supplement the initial report within 48 hours of recognition of the material change	**Supervised entities.** Must notify their primary regulator as soon as possible, but within 36 hours, of determining that a "computer-security incident" that rises to the level of a "notification incident" has occurred **Bank service providers.** Must notify their bank customers as soon as possible when they determine a computer-security incident has, or could, disrupt or degrade their "covered services" for four or more hours	**Covered entities.** NYDFS-supervised entities must report to the NYDFS Superintendent within 72 hours any cybersecurity event that has a "reasonable likelihood of materially harming any normal operation of the entity" Additionally, guidance (released in 2021) directs covered entities to report any "successful deployment of ransomware" or "intrusion where hackers gain access to privileged accounts" within 72 hours	**CCPA/CPRA**. Disclosure to be made "in the most expedient time possible and without unreasonable delay" after breach is discovered **GDPR**. Notification "without undue delay" and where feasible not later than 72 hours after becoming aware of a personal data breach
Notification/ Report	**SEC Registrants:** Would require disclosure of information about the cyber incident, as well as material changes, additions, or supplements to prior reports. Similarly, disclosure would be required when a series of previously undisclosed, individually immaterial cybersecurity incidents have become material in the aggregate. **Funds and Advisers:** Upon experiencing a significant cyber incident, would be required to confidentially report the incident. Similarly, they would be required to disclose cybersecurity risks and cyber incidents, both current and over the last two fiscal years. A records retention requirement of five years would be required for cybersecurity incidents.	Notification is intended to serve as an "early alert" to the respective agencies, and may be provided via email, telephone, or similar method to an agency-designated point of contact.	**Covered entities**. Must report cybersecurity events determined to i) impact the covered entity and require notice to a government body, self-regulatory agency, or other supervisory body, or ii) have a "reasonable likelihood of materially harming any normal operation of the entity." Reporting is confidential. Covered entities must submit a written statement certifying compliance with the Cybersecurity Regulation annually. A five-year records retention requirement applies to all documents supporting the certification	**CCPA/CPRA**. Notify CA Attorney General if more than 500 CA residents impacted (notify CalPPA after January 2023). Also applies to ransomware, improper sales of data, mistaken changes to information. **GDPR**. Notification provided to supervisory authority. Explanation required for notification after 72 hours; some information may be provided in phases "without undue delay"

FinCEN *requires financial entities to file an SAR within 30 days of initial detection of facts that constitute a basis for filing. Similar instances may be filed together in one SAR. SARs related to ransomware events should be filed immediately. SARs are mandatory for cyber-related and/or ransomware events totaling $5000 or more.*

KPMG

B: Cybersecurity Risk Management

SEC Proposed Rules

SEC Registrants: Most registrants would be required to provide disclosures on their policies and procedures around cybersecurity risk management and strategy, including information regarding:

- Cybersecurity risk assessment program
- Third-party engagement in cybersecurity risk assessments
- Policies and procedures to oversee and identify cybersecurity risks associated with third-party service providers
- Activities to prevent, detect, and minimize effects of cyber incidents, including business continuity, contingency, and recovery plans
- Whether the registrant's governance, policies and procedures, or technologies adapt in response to a cyber incident
- Cybersecurity-related risks and incidents effects on results of operations and financial condition

Funds and Advisers: Would be required to adopt and implement written policies and procedures "reasonably" designed to address cybersecurity risks, including:

- Risk assessments
- User security and access
- Information protection
- Threat and vulnerability management
- Cyber incident response and recovery
- Annual Review and Written Reports
- Recordkeeping

Federal Banking Regulators

As members of the **FFIEC**, the Federal Banking Regulators follow FFIEC guidance on risk management oversight and activities related to cybersecurity (as contained in the "Architecture, Infrastructure, and Operations" (AIO) booklet, part of the IT examination handbook.) The guidance covers:

- Data governance and management
- IT asset management
- IT and business environment representations
- Change management, strategic transitioning, and operational resiliency
- Oversight of third-party service providers
- Remote access and device ownership

FFIEC guidance on identity authentication and system access also highlights cybersecurity risk management principles and practices, including:

- Risk assessments
- Identifying and verifying authorized users and necessary access controls
- Periodically evaluating the effectiveness of user access controls
- Implementing layered security to protect against unauthorized access
- Identifying and tracking unauthorized access, and monitoring, logging, and reporting of related activities

Federal banking regulators are themselves subject to cybersecurity requirements from **NIST**'s Cybersecurity Framework. This framework is voluntary for the private sector, but provides specific guidance on best practices for:

- Risk management processes and practices
- Integrating cybersecurity risk management programs with overall risk management and organization structure and strategy
- External participation of third-party service providers in risk management, identifying dependencies, and the overall cyber risk ecosystem

NYDFS

NYDFS published the first Cybersecurity Regulation in March 2017, including risk management requirements for financial services companies, requiring:

- Risk assessments
- Development of cybersecurity programs
- Designation of a CISO
- Encryption of all nonpublic information in transit and at rest
- Multifactor or risk-based authentication
- Breach notification parameters
- Data retention and disposal policies
- Third party program
- Annual reporting

2021 guidance addresses controls specific to ransomware:

- Email filtering, Anti-Phishing training
- Vulnerability/Patch Management
- Multifactor authentication
- Disabled RDP Access
- Password Management
- Privileged Access Management
- Monitoring and Response
- Tested, Segregated Backups
- Incident Response Plan

C: Cybersecurity Governance & Oversight

A B C

SEC Proposed Rules

SEC Registrants: Would be required to disclose information regarding:

Board Oversight Practices, including:

- How the board oversees cybersecurity risks
- How, and how frequently, the board is informed about cybersecurity risks
- Whether and how the board considers cybersecurity risks in business strategy, risk management, and financial oversight
- Board member expertise in cybersecurity

Management Oversight Practices, including:

- Who is responsible for assessing, measuring, and managing cybersecurity risk, and their relevant expertise
- Whether a designated CISO exists, to whom that individual reports, and their relevant expertise
- How responsible persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents
- How frequently management reports to the board on cybersecurity risk

Funds: A fund's board would be required to initially approve a fund's cybersecurity risk management policies and procedures, and to review the annual written report.

Federal Banking Regulators

The FFIEC's AIO booklet outlines regulatory expectations for boards and management..

Board Oversight Practices

- Aligning cybersecurity risk management principles and practices with the board's strategic plans and risk appetite
- Budgeting appropriate resources to support cybersecurity activities
- Ensuring board members have appropriate knowledge of risks to provide a credible challenge to management responsible for cybersecurity functions
- Enabling appropriate management training on cybersecurity to carry out its responsibilities and manage risk
- Reviewing cybersecurity operating results and performance through audit reports, testing results, and management assessments and reports

Management Oversight Practices

- Ensuring that IT architecture, integration, and testing are comprehensive, meet business and strategic plan objectives, and can assist in the identification of cybersecurity risks
- Addressing risks self-identified by management, from cybersecurity-related audits, and from other independent assessments, including the following risks:
  - Architectural risks
  - Infrastructure-related risks
  - Operational risks
- Assessing and updating management's cybersecurity strategies and plans to reflect the current business conditions and operating environment for continuous improvement
- Promoting alignment and integration between functions of cybersecurity

Board Considerations

As Boards refine their boardroom cybersecurity and data governance discussions and focus on their oversight responsibilities, they may want to consider:

01

Requesting an update from management

Requesting an update from management on the company's cybersecurity risk assessment

02

Examining supply chain & third-parties

Taking a hard look at supply chain and other third-party vulnerabilities

03

Understanding the response plan

Understanding the company's cyber-incident response plan, as well as cyber-insurance

04

Reinforcing protocols

Reinforcing the board's own cybersecurity protocols

05

Allocating responsibilities

Intentionally allocating cybersecurity and data governance oversight responsibilities between board committees.

Being intentional with oversight will ensure there is an appropriate system to manage key risks, including identifying, assessing, mitigating, and monitoring these risks.

Conclusion

The increasing regulatory and legislative focus on cybersecurity risks and impacts should compel companies to (re)assess, adapt, and formalize their cybersecurity policies and procedures. This process should utilize the framework approach outlined relative to cybersecurity incident reporting, risk management, and cybersecurity governance, and should seek to establish a target operating model that:

- Embeds operational resiliency as a key criterion across management decisions and business activities
- Addresses cybersecurity risks from third-party service providers
- Provides transparency to investors with consistent, comparable, and useful cybersecurity information

As companies utilize this framework, it is important to consider the role that board and management expertise (or acumen) in cybersecurity will play as policies and procedures are assessed and adapted. Regulators have set, or proposed, expectations for disclosures of both expertise and oversight responsibilities in general, which will be critical for companies to address to maintain compliance and achieve a target operating model. In addition, companies should continually reassess and adapt their cybersecurity risk management policies and procedures as new information, threats, and opportunities arise.

Appendices

Appendix 1: Definitions

SEC

Cybersecurity incident: An unauthorized occurrence 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: Any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein

Information systems: 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

Significant cybersecurity incident: An incident, or group of related incidents, that significantly disrupts or degrades the ability of an adviser, or a private fund client of the adviser, to maintain critical operations or leads to the unauthorized access or use of information and results in substantial harm to the adviser or client or investor in a private fund whose information was accessed.

Federal Banking Regulators

Computer-security incident: An occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits

Notification incident: A computer-security incident that a bank believes in good faith could materially disrupt, degrade, or impair:

- The ability of the bank to carry out operations, activities, or processes, or delivery of banking products and services to a material portion of its customer base
- Any business line of a bank, including associated operations, services, functions, and support, and would result in a material loss of revenue, profit, or franchise value
- Those operations of a bank, including associated services, functions, and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

Other

CISA. ***Covered cyber incident:*** A substantial cyber incident experienced by a covered entity "that [actually] jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system or an information system itself."

Covered entity: An entity in a critical infrastructure sector (defined in Presidential Policy Directive 21), such as energy, financial services, information technology, or transportation services.

NYDFS. ***Cybersecurity event:*** Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

CCPA/CPRA. ***Breach:*** Occurs when a consumer's nonencrypted or nonredacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices.

GDPR. ***Personal data breach:*** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

FinCEN. ***Cyber-Related Information:*** Information that describes technical details of electronic activity and behavior, such as IP addresses, timestamps, and Indicators of Compromise (IOCs); also includes data regarding the digital footprint of individuals and their behavior.

Cyber-Event: An attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information.

Cyber-Enabled Crime: Illegal activities (e.g., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.

Appendix 2: Relevant Thought Leadership

Through the regular publication of thought leadership papers, articles, and alerts, our professionals offer insights into the evolving regulatory landscape and what those changes might mean for participants in financial services and across industries.

If you are interested in future issues, please click to subscribe to **Regulatory Insights** or **Risk and Cyber Insights**.

Building customer trust through effective cyber security risk management

Cyber and data: Regulatory challenges

Regulatory Alerts

- *Cybersecurity: SEC Proposals for Public Company Reporting, Disclosures*
- *Cybersecurity: SEC Proposal for Adviser/Fund Risk Management*
- *Cybersecurity: SEC Reg SCI Proposal, Future Considerations*
- *Cyber incident notifications*
- *Examinations: SEC 2022 Priorities*

KPMG

Appendix 3: Acronyms

AML	Anti-money laundering
BSA	Bank Secrecy Act
CCPA	California Consumer Privacy Act
CalPPA	California Privacy Protection Agency (effective January 2023)
CISA	Cybersecurity and Infrastructure Security Agency
CPRA	California Privacy Rights Act
CISO	Chief Information Security Officer
DHS	U.S. Department of Homeland Security
FDIC	Federal Deposit Insurance Corporation
Federal banking agencies	FRB, OCC, FDIC
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
FRB	Federal Reserve Board
GDPR	EU General Data Protection Regulation
NYDFS	New York Department of Financial Services
NIST	National Institute for Standards and Technology
OCC	Office of the Comptroller of the Currency
SAR	Suspicious Activity Report
SEC	Securities & Exchange Commission

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia