

Augusta University

Policy Library

Cybersecurity Risk Management Policy

Policy Manager: Chief Information Security Officer

POLICY STATEMENT

It is the policy of Augusta University (AU) to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, availability of its electronic protected health information (ePHI), protected cardholder data, financial nonpublic personal information (NPI), and student education records (and other confidential and proprietary electronic information) and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization's Cybersecurity program.

AFFECTED STAKEHOLDERS

Indicate all entities and persons within the Enterprise that are affected by this policy:

- Alumni Faculty Graduate Students Health Professional Students
 Staff Undergraduate Students Vendors/Contractors Visitors
 Other:

DEFINITIONS

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Cybersecurity Governance, Risk Management, & Compliance (GRC) Team: Individuals who are knowledgeable about the organization's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up, technical security controls, and who are responsible for the Cybersecurity risk management process and procedures outlined below. This team manages responsibilities for Cybersecurity risk management processes and procedures with the following offices: Cybersecurity, Public Safety, Enterprise Privacy, Legal, HR, Communications, Compliance and Enterprise Risk Management, Internal audit, Information Technology Services, and Security/Technology subject matter experts.

Cybersecurity Risk Management: Within this policy, it refers to two major process components: risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

NPI (nonpublic personal information): (1) provided by a consumer to a financial institution, (2) resulting from any transaction with the consumer or any service performed for the consumer, or (3) otherwise obtained by the financial institution.

Office of Legal Affairs Use Only

Executive Sponsor: VP for Information Technology

Next Review: 6/2024

Payment Card Industry Data Security Standard (PCI DSS): Data collected by organizations that accept, store, transmit, or process cardholder data must comply with the PCI DSS and is administered by the PCI SSC (Payment Card Industry Security Standards Council) to decrease payment card fraud across the internet and increase payment card data security. This includes sensitive data that is presented on a card or stored on a card - and personal identification numbers entered by the cardholder.

RAARe – Triage: This form is to be completed by the department. Is a security questionnaire/ form used to collect information on technology in use or planned to be used in a department.

RAARe – Full: This form is to be completed by the vendor. The intention of this questionnaire/ form is to collect information about the security controls built into the technology in use or planned to be used by the department/ institution.

Risk: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, financial NPI, protected cardholder data, and student education records (and other confidential or proprietary electronic information, and other system assets).

Risk Assessment: (Referred to as Risk Analysis in the HIPAA Security Rule); the process:

Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place; Prioritizes risks; and Results in recommended possible actions/controls that could reduce or offset the determined risk.

Risk Mitigation: Referred to as Risk Management in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

Threat: The potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:

- Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
- Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
- Natural – fires, floods, electrical storms, tornados, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc.
- and environmental threats, such as power outages, hazardous material spills.
- Other – explosions, medical emergencies, misuse or resources, etc.

Threat Source – Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental, which can impact the

organization's ability to protect ePHI, financial NPI, protected cardholder data, and student education records.

Threat Action – The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

RESPONSIBILITIES

Chief Information Security Officer (CISO)

- Manage the Cybersecurity Risk Management program and coordinate the development and maintenance of Cybersecurity Risk Management policies, procedures, and standards.
- Ownership of risk register.

Executive Senior Leadership

- Participate in the Cybersecurity Risk Management program, including identification of assets and services, allocation of resources, risk prioritization, risk acceptance, and implementation of risk treatment plan.
- Consider and jointly accept residual risk and Cybersecurity policy exceptions with AU Chief Information Officer where assessed risk level is medium or high.

Administrative and Faculty and Staff

- Collaborate with the CISO to complete Cybersecurity risk assessments.
- Develop and implement a risk treatment plan.
- Report updates on the risk treatment plan to the CISO or designate.
- Submit exceptions to the Cybersecurity Policy and work with University Cybersecurity through the exceptions process.

Cybersecurity Governance, Risk Management and Compliance (GRC) Team

- Schedule and prioritize Cybersecurity risk assessments.
- Request from administrative and collegiate faculty and staff information related to their collection and use of private data
- Conduct Cybersecurity risk assessments.
- Process and follow up on requested exceptions to the Cybersecurity policy.

PROCESS & PROCEDURES

This policy establishes the scope, objectives, and procedures of AU's information security risk management process. The Cybersecurity risk management process is intended to support and protect the organization and its ability to fulfill its mission. Cybersecurity risk analysis and risk management are recognized as important components of AU's compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the

HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8), the Privacy Rule (16 C.F.R. Part 313) and are in compliance with the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) as well as PCI Data Security Standard version 3.2.1 (PCI DSS).

Risk assessments are done throughout IT system life cycles:

- Before the purchase or integration of new technologies and changes are made to physical safeguards;
- While integrating technology and making physical security changes; and
- While sustaining and monitoring of appropriate security controls.

AU performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI, financial NPI, protected cardholder data, and student education records.

AU implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

- Ensure the confidentiality, integrity, and availability of all ePHI, financial NPI, protected cardholder data, and student education records the organization creates, receives, maintains, and/or transmits,
- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, financial NPI, protected cardholder data, and student education records,
- Protect against any reasonably anticipated uses or disclosures of ePHI, financial NPI, protected cardholder data, and student education records that are not permitted or required, and
- Ensure compliance by workforce.

Any risk remaining (residual) after other risk controls have been applied requires approval by Executive Senior Leadership and will be recorded by the organization's Cybersecurity GRC Team. Clinical and Information Technology Services Management will be designated as additional approvers of residual risk that is associated with their respective areas.

All Cybersecurity risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for seven years.

Responsibility: The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of AU's Information Security Officer (or other designated employee), and the Cybersecurity GRC Team.

For software and hardware security risk assessments, the entity or department who owns the technology in use are responsible for collecting and submitting information for security review.

The RAARe – Triage must be submitted by the requesting department to cybersecurity GRC to begin the vendor security review process. *Security Review of the Triage will determine any additional information that will be required.*

Risk Assessment: The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

1. System Characterization

- The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI, financial NPI, protected cardholder data, and student education records are created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media).
- *Output* – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries. Endpoints and data is discovered and inventoried.

2. Threat Identification

- In this step, potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. Consider all potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats.
- *Output* – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

3. Vulnerability Identification

- The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network.
- *Output* – A list of the vulnerabilities (observations) that could be exercised by the potential threat-sources.

4. Control Analysis

- The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat source exploiting a system vulnerability.

- Output – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.

5. Likelihood Determination

- The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
- *Output* – Quantitative ranking of likelihood.

6. Impact Analysis

- The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the organization's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.
- *Output* – Documented description of impact.

7. Risk Determination

- This step is intended to establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management must take for each risk level.
- *Output* – Quantitative ranking of Risk.

8. Control Recommendations

- The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
- *Output* – Recommendation of control(s) and alternative solutions to mitigate risk.

9. Results Documentation

- Results of the risk assessment are documented in an official report or briefing and provided to senior management to make decisions on policy, procedure, budget, and system operational and management changes.
- *Output* – The risk register is the source of record for risk management activities at AU.

Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity

and availability of ePHI, financial NPI, protected cardholder data, and student education records. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

1. Prioritize Actions

- Using results from Risk Determination of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources.
- *Output* – Actions ranked from high to low

2. Evaluate Recommended Control Options

- Although possible controls for each threat and vulnerability pair are arrived at in Control Recommendations of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a “most appropriate” control option for each threat and vulnerability pair.
- *Output* – list of feasible controls

3. Conduct Cost-Benefit Analysis

- Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.
- *Output* – Documented cost- benefit analysis of either implementing or not implementing each specific control

4. Select Control(s)

- Taking into account the information and results from previous steps, AU’s mission, and other important criteria, the Cybersecurity GRC Team, in cooperation with senior leadership to included but not limited to the Chief Information Officer, determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI, financial NPI, protected cardholder data, and student education records. These controls may consist of a mix of administrative, physical, and/or technical safeguards.
- *Output* – Selected control(s)

5. Assign Responsibility

- Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step and assign their responsibilities. Also, identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.

- *Output* – List of resources, responsible persons and their assignments

6. Develop Plan of Action and Milestone (POA&M)

- Develop an overall implementation program and individual project plans needed to implement the safeguards and controls identified. The POA&M should contain the following information as appropriate:
 - Each risk or vulnerability/threat pair and risk level
 - Prioritized actions
 - The recommended feasible control(s) for each identified risk
 - Required resources for implementation of selected controls
 - Team member responsible for implementation of each control
 - Start date for implementation
 - Target date for completion of implementation
 - Requirements.

The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to the organization's executive management/leadership team (e.g. the Board, senior management, and other key stakeholders).

Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations (often referred to as a work breakdown structure). Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates and project requirements.

- *Output* – Project Plans for selected safeguards

7. Implement Selected Controls

- As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk. Continually and consistently, communicate expectations to Cybersecurity GRC Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.

Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes. If risk reduction expectations are not met, then repeat all or a part of the Cybersecurity risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

- *Output – Residual Risk*

8. Cybersecurity Risk Management Schedule: The two principle components of the Cybersecurity risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of AU's Cybersecurity program:

Scheduled Basis – an overall risk assessment of AU's information system infrastructure will be conducted at least annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process. The Cybersecurity GRC Team must communicate and collaborate with USG's Enterprise Risk Management coordinator at least annually.

Throughout a System's Development Life Cycle – from the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.

As Needed – the Security Officer (or other designated employee) or Cybersecurity GRC Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect AU's information systems.

REFERENCES & SUPPORTING DOCUMENTS

Cybersecurity Risk Management Procedure

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

Privacy and Security regulations

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended (including the Breach Notification Rule)

PCI Data Security Standard version 3.2.1 (PCI DSS)

Privacy Rule (16 C.F.R. Part 313)

USG IT Handbook

RELATED POLICIES

Intentionally left blank.

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/2/2021

President, Augusta University Date: 6/2/2021

Deloitte.

Deloitte's Cyber Risk capabilities

Cyber Strategy, Secure, Vigilant, and Resilient

Cyber Risk



Contents

Foreword by Deloitte Cyber Risk Global Leaders 03

Deloitte's global network of Cyber Intelligence Centers (CICs)	04
Deloitte's Cyber Risk awards and recognitions	05
Deloitte's Cyber Risk portfolio	06

Cyber Strategy 07

Cyber Strategy, Transformation, and Assessments	08
Cyber Strategy Framework (CSF)	10
Cyber Risk Management and Compliance	11
Cyber Training, Education, and Awareness	13

Secure 15

Infrastructure Protection	16
Vulnerability Management	18

Application Protection	20
------------------------	----

Identity and Access Management	22
--------------------------------	----

Information Privacy and Protection	24
------------------------------------	----

Vigilant 28

Advanced Threat Readiness and Preparation	29
Cyber Risk Analytics	31
Security Operations Center (SOC)	33
Threat Intelligence and Analysis	35

Resilient 37

Cyber Incident Response	38
Cyber Wargaming	40

Contacts 42

Home

Foreword

Cyber Strategy



Secure



Vigilant



Resilient



Contacts



< > Next

Foreword

In an era of rapid digital transformation and the proliferation of ever increasing amounts of data, cyber risk is rising up the priority scale at organizations of all sizes and in all industries.

Deloitte's experience demonstrates that clients implementing cyber risk models that anticipate threats not only deal more effectively with them. They also achieve better business results, reflected in growth in their bottom lines.

Our practitioners provide capabilities across the four main domains of cyber risk—Cyber Strategy, Secure, Vigilant, and Resilient.

Deloitte's alliances with vendors globally provide access to a range of cyber risk technologies.

This enables us to collectively deliver a large number of projects every year in advisory, implementation, and managed services tailored to the precise, individual needs of each client.

Deloitte's Cyber Risk practice provides the same exceptional quality of service in all 14 capability areas showcased in this document.



Nick Galletto
Global and Americas Cyber Risk Leader



Chris Verdonck
EMEA Cyber Risk Leader



James Nunn-Price
Asia Pacific Cyber Risk Leader

[Home](#)

Foreword

Foreword

Deloitte global network of Cyber Intelligence Centers (CICs)

Deloitte Cyber awards and recognitions

Deloitte Cyber Risk portfolio
End-to-end cybersecurity

Cyber Strategy



Secure



Vigilant



Resilient



Contacts



Next

Deloitte's global network of Cyber Intelligence Centers (CICs)



Offers solutions that help its clients protect business assets and mature their security posture, while proactively detecting, responding and recovering from security events. These services are delivered through a global network of CICs, which operate around the clock, 365 days a year to provide fully customizable, industry aligned managed security solutions including advanced security event monitoring, threat analytics, cyber threat management, and incident response for businesses to meet the increasing market demand in cybersecurity services.

CYBER INTELLIGENCE center

Our solutions are supported by
Deloitte's network of CICs

[Home](#)

[Foreword](#)

Foreword

Deloitte global network of Cyber Intelligence Centers (CICs)

Deloitte Cyber awards and recognitions

Deloitte Cyber Risk portfolio
End-to-end cybersecurity

Cyber Strategy



Secure



Vigilant



Resilient



Contacts



< > Next

Deloitte's Cyber Risk awards and recognitions

Deloitte ranked #1 globally in security consulting by Gartner (fifth consecutive year)

Gartner, a technology research company, has once again ranked Deloitte #1 globally in Security Consulting, based on revenue, in its market share analysis entitled Market Share: Security Consulting Services, Worldwide, 2016. This is the fifth consecutive year that Deloitte has been ranked #1.

Source: Gartner, Market Share Analysis: Security Consulting Services, Worldwide, 2016.
Elizabeth Kim. 27 June 2017.

Deloitte named a global leader in cybersecurity consulting by ALM Intelligence

ALM Intelligence named Deloitte a leader in Cybersecurity Consulting in its report entitled *Cybersecurity Consulting 2015*. The report notes: "The firm's notable depth across the breadth of the cybersecurity consulting portfolio coupled with its ability to effectively communicate and work with the span of a client organization (boardroom down to IT operations) solidifies its position in the vanguard."

Source: ALM Intelligence, Cybersecurity Consulting 2015; © 2015 ALM Media Properties, LLC.
Reproduced under license.

Deloitte named a global leader in security operations consulting by ALM Intelligence (2016)

ALM Intelligence (a research firm, formerly known as Kennedy) notes, "The firm's emphasis on aligning SOC initiatives to what matters to the business—including legal and regulatory requirements and education on threat actors—makes Deloitte an elite firm among its peers when it comes to building a case for investment that resonates with business-side stakeholders."

Source: ALM Intelligence; Security Operations Center Consulting 2015; ALM Intelligence estimates © 2016 ALM Media Properties, LLC.
Reproduced under license.

Deloitte qualified professionals

Our consultant of all grades hold key professional and industry certifications, such as CISSP, CISM, ISO27001, COBIT, ITIL, CDPP, CEH, and many others. We have won many awards, including the Global CyberLympics for five years in a row.



Home

Foreword

Foreword

Deloitte global network of Cyber Intelligence Centers (CICs)

Deloitte Cyber awards and recognitions

Deloitte Cyber Risk portfolio
End-to-end cybersecurity

Cyber Strategy



Secure



Vigilant



Resilient



Contacts

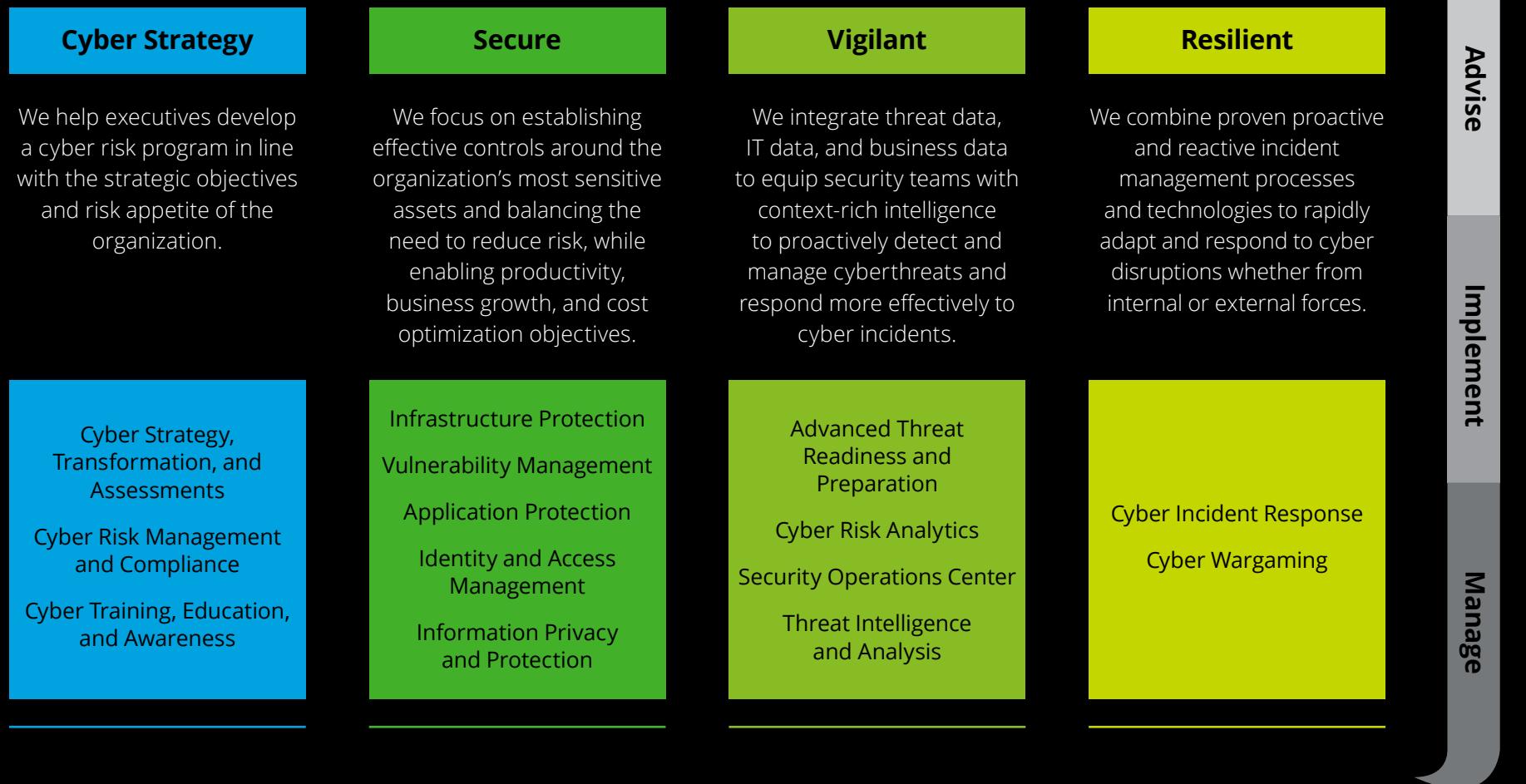


< > Next

Deloitte's Cyber Risk portfolio

End-to-end cyber risk services

More than 10,000 cyber risk professionals globally



Home

Foreword

Foreword

Deloitte global network of Cyber Intelligence Centers (CICs)

Deloitte Cyber awards and recognitions

Deloitte Cyber Risk portfolio
End-to-end cyber risk services

Cyber Strategy



Secure



Vigilant



Resilient



Contacts



Next

Cyber Strategy

We help executives develop a cyber risk program in line with the strategic objectives and risk appetite of the organization.

[Home](#)

[Foreword](#)

Cyber Strategy



Cyber Strategy,
Transformation, and
Assessment

Cyber Risk Management
and Compliance

Cyber Training, Education,
and Awareness

Secure



Vigilant



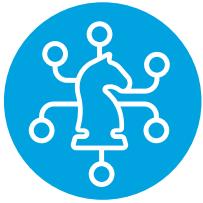
Resilient



Contacts



Next



Cyber Strategy, Transformation, and Assessment

Challenges

Organizations increasingly depend on complex technology ecosystems for several key purposes: to interact in new ways with customers and third-parties; to use data to improve decision-making; and to increase reach and profitability.

As cyberattacks become more frequent and severe, board members and executives are seeing that technology-based initiatives open doors to cyber risks.

How we can help

Our services help organizations establish their strategic direction and structures, and develop effective cyber risk reporting. They support the creation of executive-led cyber risk programs. They take account of the client's risk appetite, helping organizations identify and understand their key business risks and cyberthreat exposures.

Key solutions

Cyber Strategy, Roadmap, and Architecture

Advise | Implement

Defines cyber strategies, actionable cyber roadmaps, and reference architectures in line with the findings of a maturity assessment. Recommendations are based on a defined target state that is determined by the organization's threat exposure.

Cyber Target Operating Model

Advise | Implement

Constructs an appropriate target state for cyber risk roles, responsibilities, related processes, and governance functions. These take into account the organization's existing structure, team capabilities, resource availability, and third-party ecosystem.

Cyber Transformation

Advise | Implement | Manage

Mobilizes, manages, and delivers a structured and prioritized program of work to help

organizations transform to improved cyber governance, security, vigilance, and resilience.

Cyber Maturity Assessments

Advise | Implement | Manage

Enables organizations to identify and understand their key business risks and cyberthreat exposures. This supports measurement of their cyber maturity, either using industry-standard frameworks or Deloitte's proprietary Cyber Strategy Framework.

Cyber Risk Quantification

Advise | Implement

Provides the information needed to make security investment decisions. Deloitte uses unique methods to quantify both the client's risk and the expected risk mitigation offered by Deloitte security investments.

[Home](#)

[Foreword](#)

Cyber Strategy

Cyber Strategy, Transformation, and Assessment



Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness

Secure



Vigilant



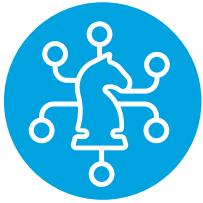
Resilient



Contacts



[Next](#)



Cyber Strategy, Transformation, and Assessment

Key differentiators

- The Deloitte Cyber Strategy framework measures cyber posture and threat exposure.
- A leading catalog of good practice standards for cyber risk, with proven success across industry sectors.

Deloitte's own Cyber Strategy Framework

(the next page contains details on the framework)



[Home](#)

[Foreword](#)

Cyber Strategy

**Cyber Strategy,
Transformation, and
Assessment**



Cyber Risk Management
and Compliance

Cyber Training, Education,
and Awareness

Secure



Vigilant



Resilient



Contacts



Next

Cyber Strategy Framework (CSF)

Home

Foreword

Managing cyber risk to grow and protect business value

The Deloitte CSF is a business-driven, threat-based approach to conducting cyber assessments based on an organization's specific business, threats, and capabilities. CSF incorporates a proven methodology to assess an organization's cyber resilience; content packs which enable us to conduct assessments against specific standards; and an intuitive online platform incorporating a range of dashboards that can be customized for an executive, managerial, and operational audience.

Three fundamental drivers that drive growth and create cyber risks:



Innovation



Information sharing



Trusting people



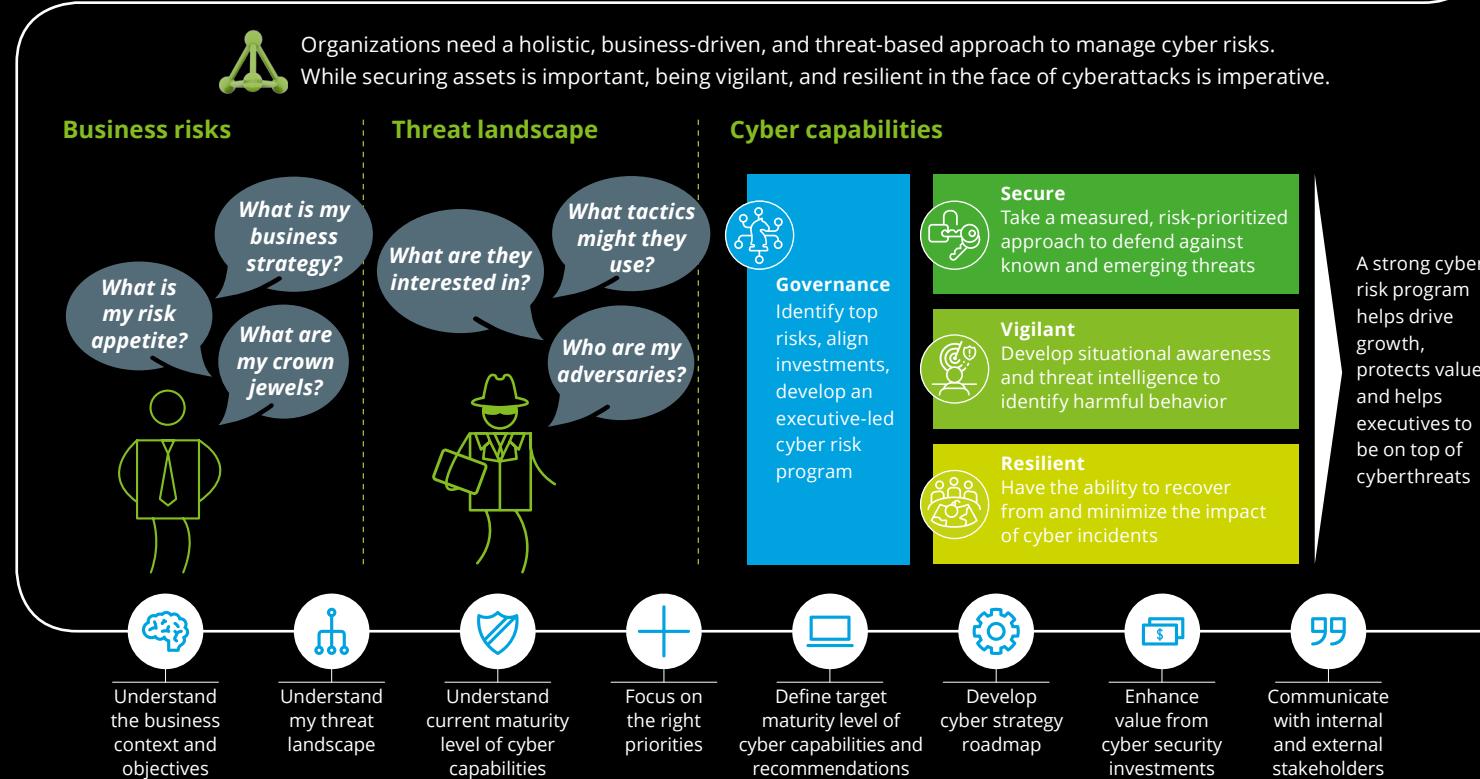
CEO:
"I read about phishing in the news. Are we exposed?"



CIO:
"Where and how much do I need to invest to optimize my cyber capabilities?"



Board:
"What is our level of resilience against these cyberattacks?"



Cyber Strategy

Cyber Strategy,
Transformation, and
Assessment



Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness

Secure



Vigilant



Resilient



Contacts



Next



Cyber Risk Management and Compliance

Challenges

Understanding the current status of an organization's security posture requires constant evaluation of evolving risks, security standards, and cyber regulations.

Today's complex and distributed IT landscape and third-party involvement means organizations must take a structured approach to understanding the road ahead.

How we can help

Deloitte's diverse experience in managing cyber risk and compliance can help organizations: define tailored cyber risk management frameworks; support risk transfer via cyber insurance; set and implement cyber-control frameworks; and ensure compliance with cybersecurity regulations.

Key differentiators

- Mature proprietary methodologies and tools, complemented by vendor alliances.
- Strong experience in integrating cyber risk into the broader enterprise risk management framework.
- Deep knowledge and experience with security control frameworks and regulations.

[Home](#)

[Foreword](#)

Cyber Strategy

Cyber Strategy, Transformation, and Assessment



Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness



Secure



Vigilant



Resilient



Contacts



[<](#) [>](#) Next



Cyber Risk Management and Compliance

Key solutions

Cyber Risk Management

Advise | Implement

Defines framework and methodologies to assess cyber risks in order for the organization to understand their magnitude and make informed decisions that align the organization's risk appetite with the risks it faces.

Cyber Risk Dashboarding

Advise | Implement | Manage

Designs and implements risk dashboard constituents, including Key Risk Indicators (KRIs) and dashboards to facilitate effective monitoring of cyber risk from the boardroom to the network.

Cyber Insurance

Advise | Implement

Evaluates coverage of existing insurance policies. Determines areas where residual cyber risk could be transferred to an insurer.

Security Control Framework

Advise | Implement

Defines tailored security-control frameworks based on best practices as guiding principles. Develops policies, procedures, and standards.

Third-Party Risk Management

Advise | Implement

Customizes services at each step of the third-party cyber risk management lifecycle. Provides end-to-end oversight of the third-party risk management program.

Security and Regulatory Compliance

Advise | Implement

Assists and prepares compliance with national and/or sectoral cybersecurity regulations.

[Home](#)

[Foreword](#)

Cyber Strategy

Cyber Strategy, Transformation, and Assessment



Cyber Risk Management and Compliance

Cyber Training, Education, and Awareness



Secure



Vigilant



Resilient



Contacts



[Next](#)



Cyber Training, Education, and Awareness

Challenges

Even with excellent people and technology in place, the organization's own employees are the weakest link when it comes to cybersecurity. The so-called insider threat is real. Building secure defenses against outside threats is not enough if data is leaked from within an organization.

How we can help

Deloitte can help to accelerate behavioral change. Organizations that adopt the right behavior make themselves more secure, vigilant, and resilient when faced with cyberthreats.

Deloitte can help organizations develop and embed a mature cyber risk culture by defining, delivering, and managing programs, both online and on-site, to improve technical skills, foster security awareness, and plan other initiatives needed to effect digital transformation successfully.

Key solutions

Insider Risk

Advise | Implement

Helps organizations identify, monitor, and manage the main sources of insider threat. We help to establish Potential Risk Indicators (PRIs) and create awareness of the main indicators of maturity in managing insider risk.

Cyber Security Awareness Program

Advise | Implement | Manage

Understands the current state of a company's awareness level, defines a strategy, and develops a recognizable awareness campaign, multimedia content package, and communication tools.

Technical Cyber Training

Advise | Implement

Delivers both introductory and highly specialized technical training in cybersecurity, either on-site or through a purpose-built online platform. Our catalog of courses covers areas such as: Hacking, Secure Development, Forensics, Reversing, Industrial Control System (ICS) security, and Incident Response.

Certification Readiness

Implement

Delivers training to prepare employees for qualifications such as Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), and Certified Information Security Manager (CISM).

[Home](#)

[Foreword](#)

Cyber Strategy

Cyber Strategy,
Transformation, and
Assessment



Cyber Risk Management
and Compliance

Cyber Training, Education, and Awareness

Secure



Vigilant



Resilient



Contacts



Next

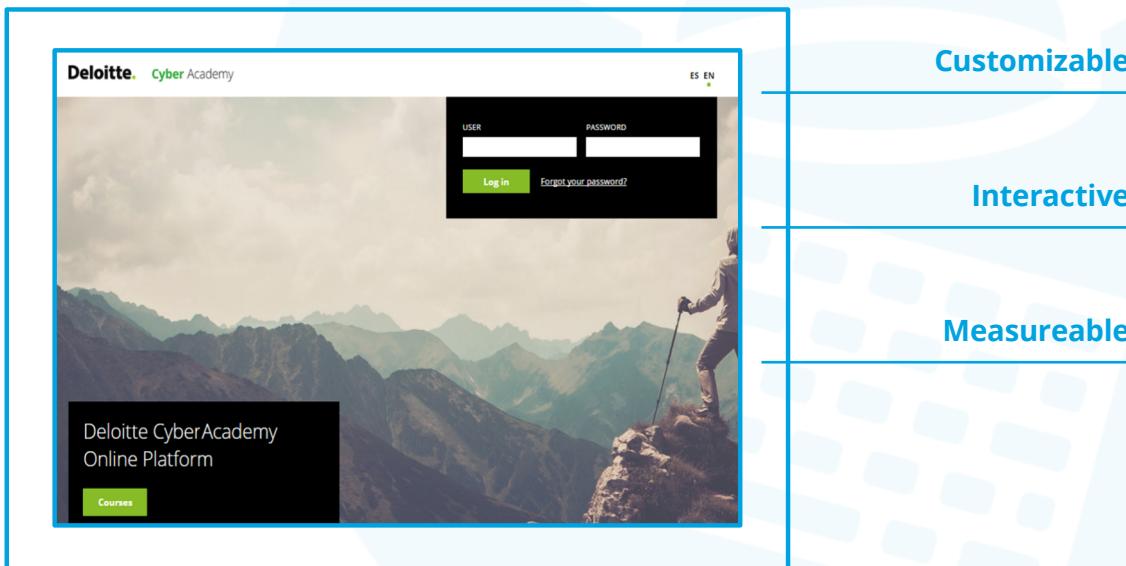


Cyber Training, Education, and Awareness

Key differentiators

- We deliver online and on-site technical training and awareness programs to clients and internal practitioners via a dedicated Cyber Academy Online Platform.
- The Academy collaborates with universities and educational institutions to create expertise and professional performance in the area of Cyber Security, with programs such as a Master's Degree in Cyber Security among our online postgraduate offering.
- We work with leadership and learning psychologists, human resources, and cyber specialists to build and deliver the most effective learning and awareness courses tailored to each audience.

Deloitte's own Cyber Academy Online Platform



Home

Foreword

Cyber Strategy

Cyber Strategy,
Transformation, and
Assessment



Cyber Risk Management
and Compliance

**Cyber Training, Education,
and Awareness**

Secure



Vigilant



Resilient



Contacts



< > Next

Secure

We focus on establishing effective controls around the organization's most sensitive assets and balancing the need to reduce risk, while enabling productivity, business growth, and cost optimization objectives.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



Secure

Infrastructure
Protection



Vulnerability Management

Application Protection

Identity and Access
Management

Information Privacy

Information Protection

Vigilant



Resilient



Contacts



< > Next



Infrastructure Protection

Challenges

Hyper-connectivity is creating a new era for cyber infrastructure. Ever more connected devices pose new cybersecurity challenges for public and private-sector organizations as the volume of threats to their infrastructure rises.

Devices connected to corporate infrastructures need to continuously acquire, store, and use large amounts of data, a significant proportion of which will be sensitive. Protecting this data against cyberattack is of paramount importance.

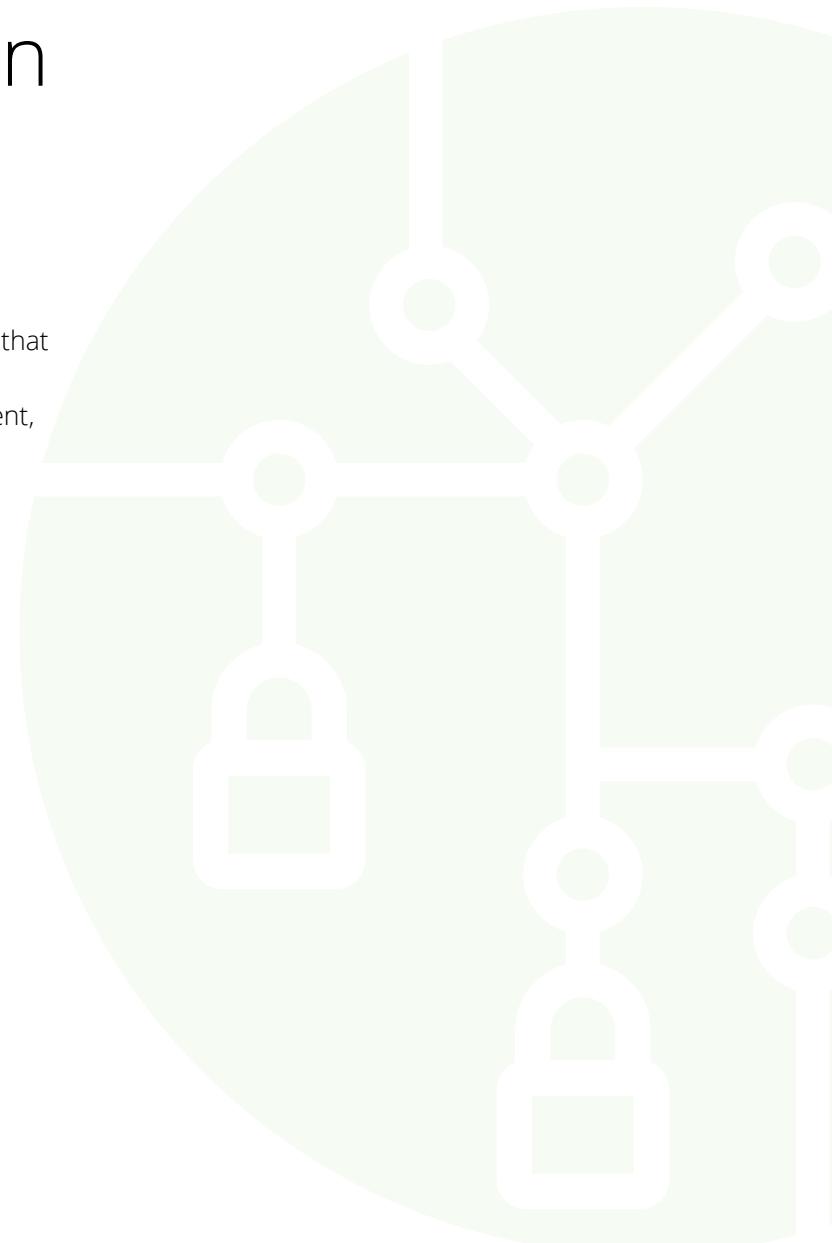
Today's smart cybersecurity protects data by using secure data platforms, clear data governance, and smart access protocols such as electronic finger printing.

The development of new technologies will drive exciting innovations in Smart Cities, Smart Factories and the Internet of Things (IoT) as communication and automation control become ubiquitous.

How we can help

Deloitte has developed a set of services that comprehensively address cybersecurity challenges in the architecture, deployment, and maintenance of traditional and new infrastructure and technologies.

Deloitte's security professionals, from diverse architecture, engineering, and operational technology backgrounds, are experts across the evolving infrastructure and product landscape.



[Home](#)

[Foreword](#)

[Cyber Strategy](#)



Secure

Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection



Vigilant



Resilient



Contacts



[Next](#)



Infrastructure Protection

Key solutions

IoT Strategy, Roadmap, and Architecture

Advise | Implement | Manage

Reviews industrial and consumer product codes and delivers secure development practices to enhance clients' capabilities in implementing next-generation connected products. We help organizations undertake readiness assessments, align their IoT security vision with their overall mission and vision statements, build IoT roadmaps and adapt traditional governance models to new IoT developments.

Cloud Security

Advise | Implement | Manage

Evaluates client requirements, assesses cloud usage, builds the business case and cloud roadmaps, and assists with cloud vendor evaluation.

Network Strategy and Optimization

Advise

Analyzes client infrastructure to identify and remedy the configuration of network components and help clients design their network architecture into secure zones.

Anti-DDoS Attacks

Advise | Manage

Analyzes organizations' readiness to defend themselves against Distributed Denial of Service (DDoS) attacks. We provide cloud-based anti-DDoS protection for infrastructures, websites, and DNS servers.

Key differentiators

- We offer secure, end-to-end solution-transformation capabilities, from vision alignment to the design of secure products.

Home

Foreword

Cyber Strategy



Secure

Infrastructure Protection

Vulnerability Management
Application Protection
Identity and Access Management
Information Privacy
Information Protection



Vigilant



Resilient



Contacts



< > Next



Vulnerability Management

Challenges

Businesses rely on a stable and secure IT environment as the foundation for driving new digital innovations, and products.

New security vulnerabilities are published on a daily basis and hackers are constantly looking for ways to gain access to systems and data.

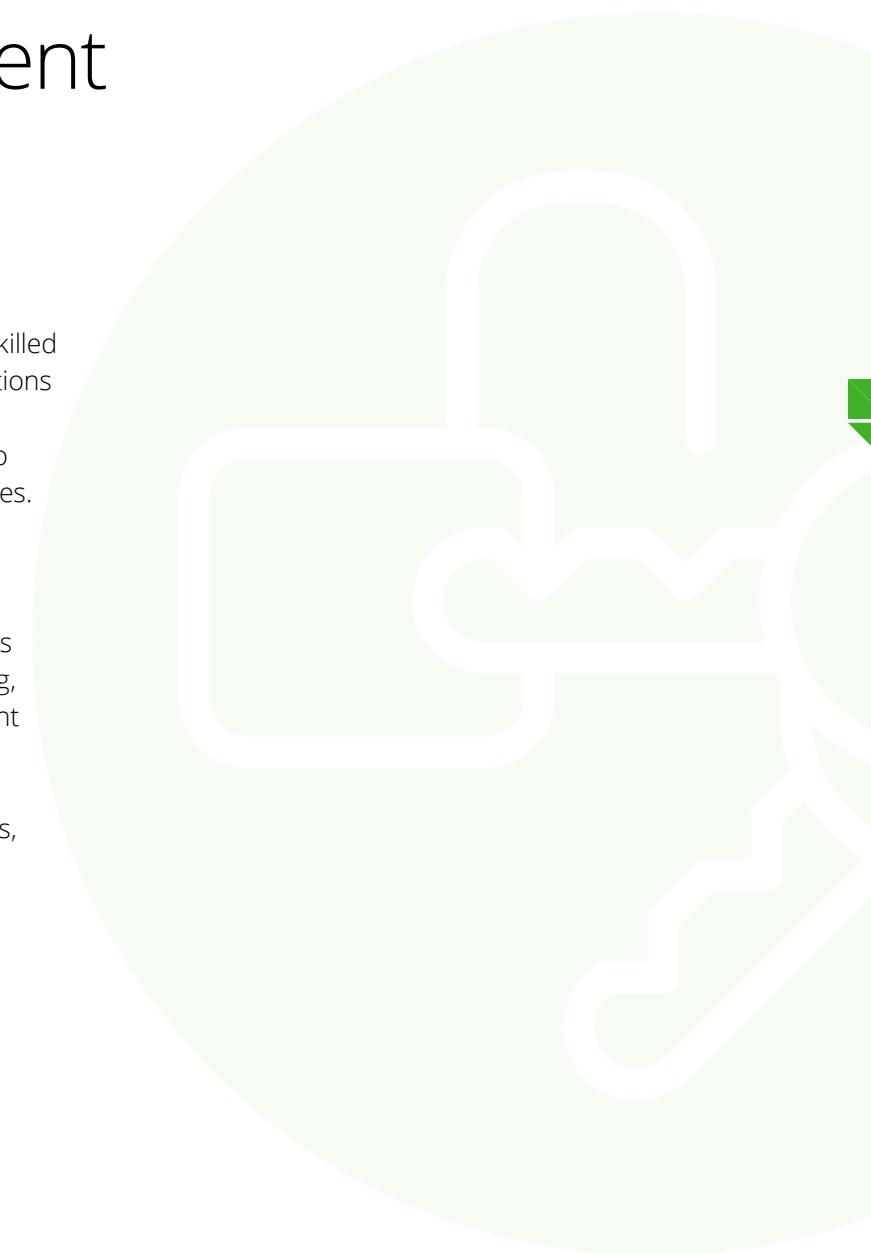
Identifying, managing, and correcting vulnerabilities in an environment that consists of multiple applications, systems, and locations is a significant management challenge.

How we can help

Deloitte offers the expertise of highly skilled security professionals to help organizations identify vulnerabilities. Deloitte's team works side by side with organizations to remedy and manage these vulnerabilities.

Our services include fully managed vulnerability assessments from Deloitte's award-winning ethical hackers and support in designing, implementing, and operating vulnerability management systems and processes.

Supported by Deloitte's network of CICs, we offer a range of managed solutions including vulnerability assessments, remediation support, and vulnerability management advisory.



[Home](#)

[Foreword](#)

[Cyber Strategy](#)



Secure

Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection



Vigilant



Resilient



Contacts



< > Next



Vulnerability Management

Key solutions

Vulnerability Assessments

Implement | Manage

Uses known hacking methods and vulnerabilities, tests the security of applications and IT systems, and achieves increased levels of security. Deloitte can undertake this work fully on behalf of organizations or complement organization's internal vulnerability assessment team.

Hacking and Phishing as a Service

Manage

Provides regular insight into an organization's potential vulnerabilities. Many organizations perform security tests only once while cyber criminals are constantly seeking to find and exploit new vulnerabilities.

Vulnerability Remediation Support

Implement | Manage

Configures and manages vulnerability management solutions providing insight into the business-relevant vulnerabilities that matter.

Vulnerability Management Capability Design

Advise

Establishes vulnerability management processes, governance, capabilities, tools, and expertise for organizations. Deloitte will enable an organization to identify, manage, and remedy issues with the various stakeholders involved in a timely way.

CYBER INTELLIGENCE center

Our solutions are supported by
Deloitte's network of CICs

Key differentiators

- Our professionals include a global pool of award-winning ethical hackers.
- We utilize proven Deloitte methods and cutting-edge vulnerability management tools.
- We offer a range of managed solutions including vulnerability assessments, remediation support, and vulnerability management advisory.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)

Infrastructure Protection

[Vulnerability Management](#)

Application Protection

Identity and Access Management

Information Privacy

Information Protection



[Vigilant](#)



[Resilient](#)



[Contacts](#)



Next



Application Protection

Challenges

Applications form a major part of every IT landscape. Ensuring they are protected requires secure design, implementation, and configuration. Testing of the protection requires robust processes, dedicated resources, and a skilled team.

Many organizations find setting up such processes and acquiring and maintaining the required skills and knowledge to be a major challenge.

How we can help

Deloitte software security specialists assist organizations to thoroughly assess the protection level of applications.

With specialized knowledge of a large number of specific applications and secure development methods, Deloitte helps secure the design, development, and configuration of applications.

Key solutions

Enterprise Application Security

Advise | Implement | Manage

Assesses the current state of an organization's applications and the security controls on the application layers for enterprise systems.

Source Code Review

Manage | Implement

Analyzes application source code to test for common mistakes. The analysis can be conducted through one-off application assessments or as an integral part of an organization's software development process.

CYBER INTELLIGENCE center

Our solutions are supported by
Deloitte's network of CICs

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)

Infrastructure Protection
Vulnerability Management

[Application Protection](#)

Identity and Access Management
Information Privacy
Information Protection



[Vigilant](#)



[Resilient](#)



[Contacts](#)



Next



Application Protection

Deloitte Application Security Platform

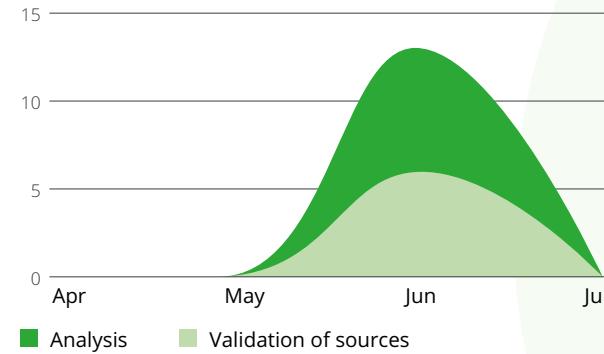
- Source code review activities centralization
- Advanced reporting capacities
- Real-time activities progress feedback
- Vulnerability lifecycle management
- Multi-vendor support
- CWE and CVSS aligned GAST taxonomy

Key differentiators

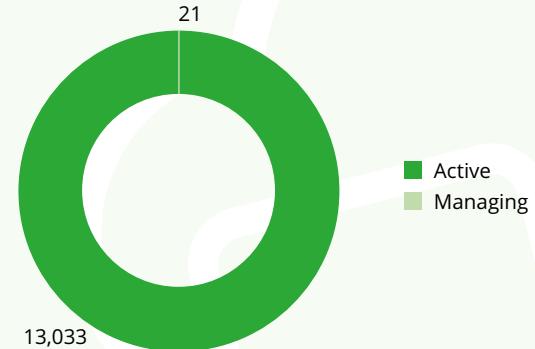
- We leverage static application security testing technology which enables the client to be one step ahead, with 40 percent portfolio coverage versus five percent portfolio coverage using the traditional approach.
- We help organizations raise their situational risk awareness and actionable remediation insights, empowering them to regulate application portfolios effectively.

Source code analysis overview

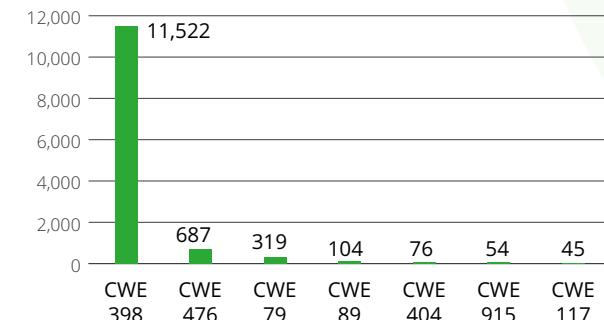
Analysis and validation of sources



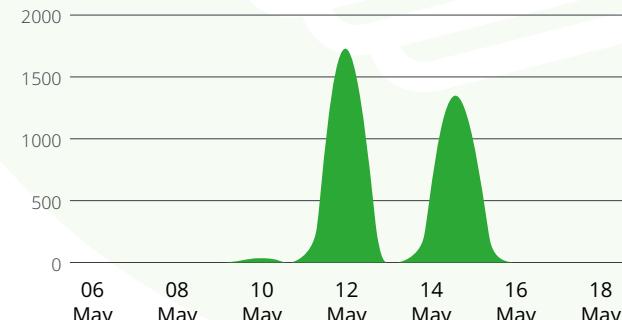
Weaknesses found



Top CWEs detected



Total analyzed lines



Home

Foreword

Cyber Strategy



Secure

Infrastructure Protection
Vulnerability Management



Application Protection

Identity and Access Management
Information Privacy
Information Protection



Vigilant



Resilient



Contacts



< > Next



Identity and Access Management

Challenges

The traditional network perimeter has faded. In response, organizations are increasingly focusing on user identity assurance and information access controls.

Identity and Access Management (IAM) provides tools, processes, and methods to enhance the security of online transactions while minimizing friction in the user experience. IAM also provides a trusted environment for omni-channel communication between users (customers, business partners, and employees) and IT platforms.

How we can help

Identity and access are two of the key elements that underpin digital commerce and automated business processes. Deloitte has established proven methodology to guide clients through the full IAM program lifecycle, from defining a clear vision and strategy for secure access to information assets, to the actual deployment and operation of IAM platforms, and integration with IT platforms.

Key solutions

IAM Drivers Identification and Selection of IAM Investment Areas

Advise

Defines the objectives for IAM, such as enabling new information exchanges (e.g. low-friction customer registration), more efficient compliance demonstration (e.g. risk-focused access reviews), and enhanced controls (e.g. monitoring of IT administrator actions).

Current State Assessments for IAM Components

Advise

Assesses the current maturity of IAM-related controls and pinpoints key improvement areas.

IAM Functionality Design and Preparation for Implementation

Advise | Implement

Formalizes requirements, designs a fitting solution landscape by selecting the most appropriate solution set, and transforms the organization and its processes to optimize returns on IAM investments.

IAM Platform Deployment

Implement

Makes the IAM vision a reality by implementing IAM solutions to support your IAM processes with Deloitte key technology partners (SailPoint, OKTA, CyberArk, and ForgeRock).

Reach of IAM Platform Extension

Manage

Integrates business applications with the IAM platform to increase the reach of automated controls.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)

Infrastructure Protection

Vulnerability Management

Application Protection

[Identity and Access Management](#)

Information Privacy

Information Protection



[Vigilant](#)



[Resilient](#)



[Contacts](#)



[Next](#)

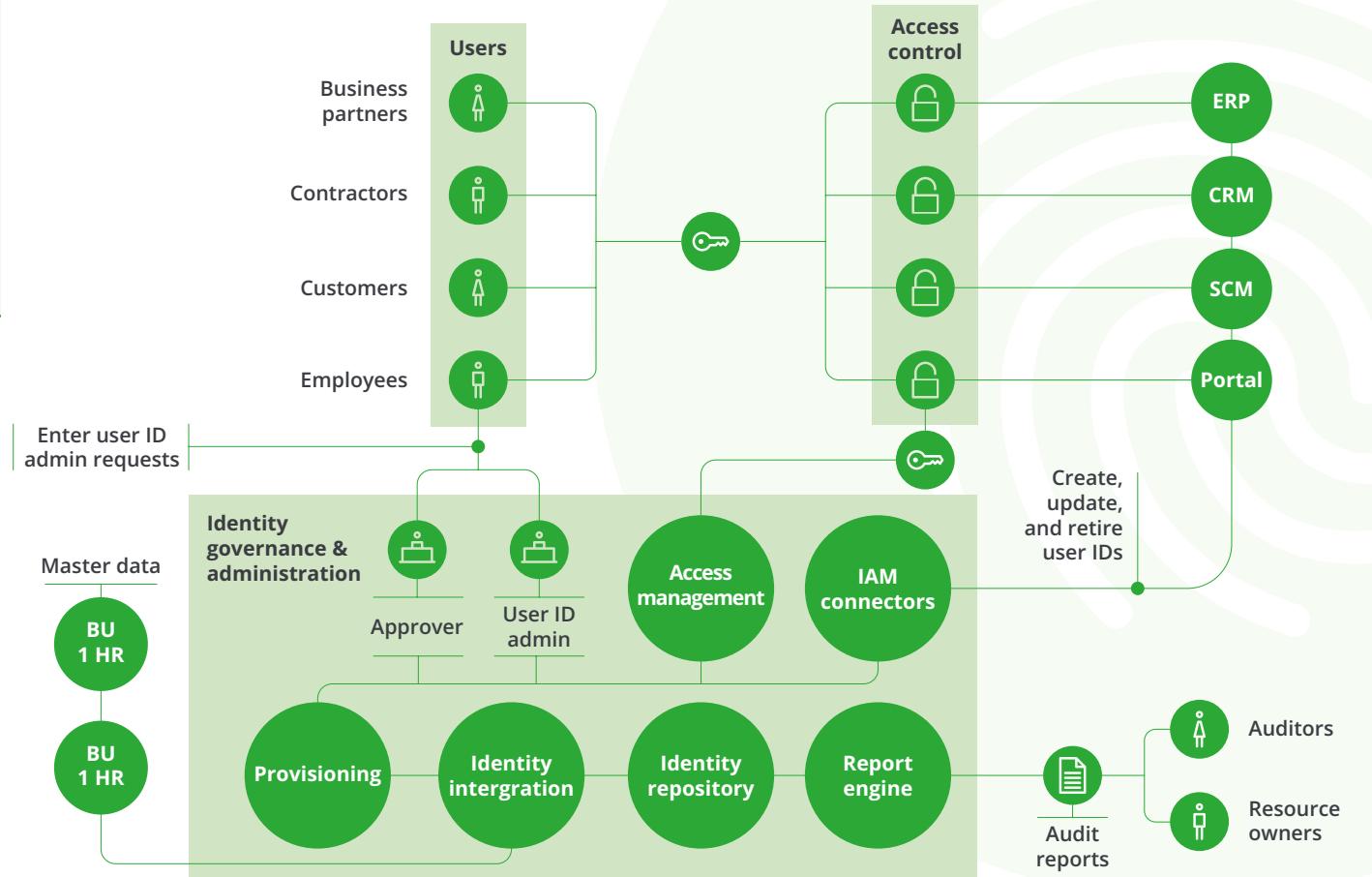


Identity and Access Management

Key differentiators

- Business and user-centric view of IAM as part of Deloitte DNA.
- Experience of global best practices and IAM solution architectures.
- Close solution partner network with major IAM capability providers.

Identity and Access Management components



Home

Foreword

Cyber Strategy



Secure

Infrastructure Protection
Vulnerability Management
Application Protection
Identity and Access Management
Information Privacy
Information Protection



Vigilant



Resilient



Contacts



Next



Information Privacy

Challenges

Organizations need to be able to use, analyze, and share their data while ensuring compliance with invasive regulatory control and customer/employee privacy expectations.

Greater reliance on effective data use, combined with increased regulation and control requirements, such as General Data Protection Regulation (GDPR), puts significant operational pressure on organizations.

This requires a holistic and integrated data privacy approach to an environment that is often highly segmented.

How we can help

With an excellent track record in turning privacy-related challenges into tested, modular, and pragmatic solutions, Deloitte is dedicated to supporting organizations in navigating privacy risk.

Key solutions

Privacy/GDPR Maturity Assessments and Roadmap

Advise | Implement

Assesses and identifies the current state of an organization's GDPR readiness. This includes a prioritized and risk-based roadmap that clearly identifies actionable mitigating measures and short-term fixes.

Privacy/GDPR Strategy and Transformation Program

Advise | Implement

Builds a holistic and tailored transformation program in close partnership with organizations. We help organizations incorporate fit for purpose privacy solutions in their DNA.

Privacy by Design/Managed Services (e.g. Data Protection Officer as a Service)

Advise | Implement | Manage

Provides hands-on, technology-enabled services and controls, using best practices,

an extensive toolkit including privacy impact assessments, GDPR/Data Protection Officer (DPO) helpdesk, GDPR stress testing, data inventory, and data mapping.

International Data Transfer Strategy and Implementation

Advise | Implement

Assesses and builds a contractual, regulatory, and operational framework for international data transfers. Includes guidance from start to finish related to, Binding Corporate Rules (BCR) applications and implementation, allowing the effective sharing of personal data across borders.

Privacy/GDPR training and Awareness

Implement

Offers tailored GDPR awareness and training, on-site or via e-learning/classroom formats, using, for example, the Deloitte Privacy Academy, and covering both GDPR compliance and its operational/technical implications.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



Secure

Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

Information Protection



Vigilant



Resilient



Contacts



[Next](#)

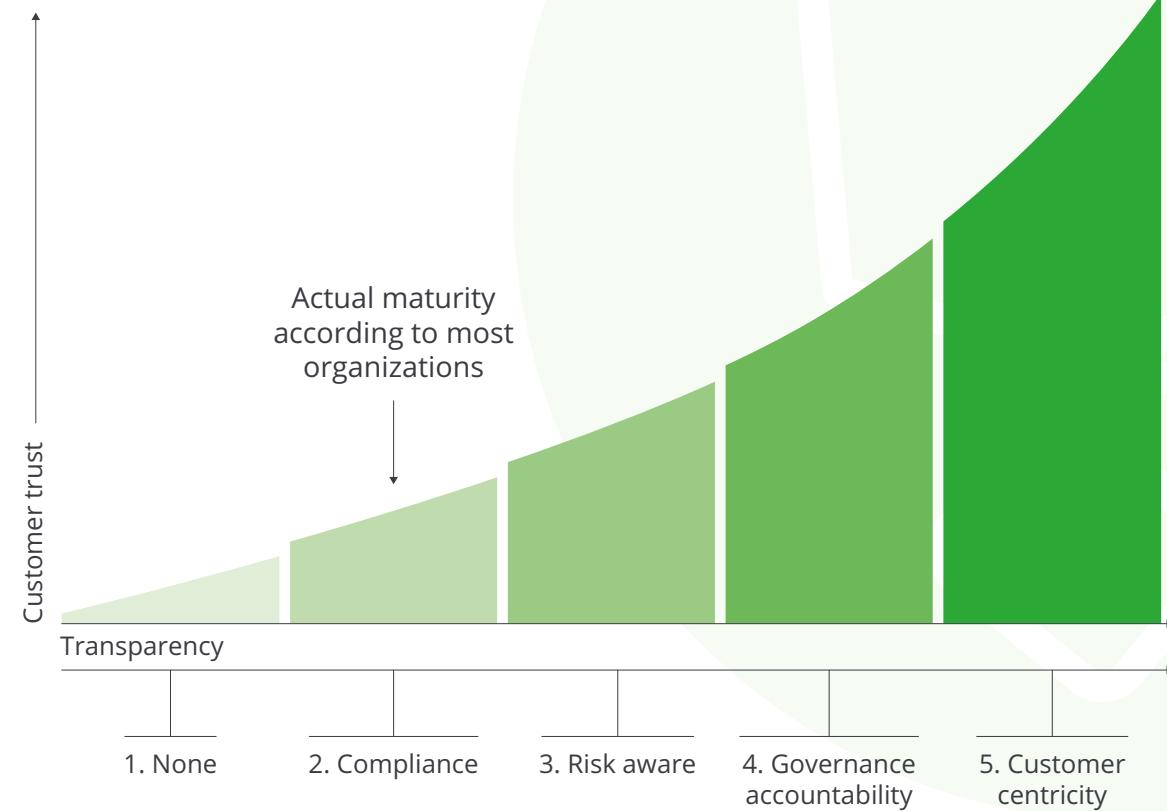


Information Privacy

Key differentiators

- Our highly integrated international team has in-depth and tested GDPR experience and ensures tailored data privacy/GDPR solutions.
- Deloitte methodology is holistic and hands-on, integrating privacy tools and in-depth data protection knowledge.

Information Privacy and Data protection maturity model



Home

Foreword

Cyber Strategy



Secure

Infrastructure Protection
Vulnerability Management
Application Protection
Identity and Access Management



Information Privacy

Information Protection

Vigilant



Resilient



Contacts



< > Next



Information Protection

Challenges

Organizations are expected to keep personal and corporate data confidential, yet data breaches still occur. These can result in financial loss, regulatory sanction, and reputation damage.

Common challenges are identifying organization's business critical information and ensuring it is adequately protected in a world where the quick exchange of information is integral to business success.

How we can help

We offer organizations access to market-leading technical, business, and operational expertise to help them make informed decisions about their data.

Deloitte solutions cover the broad challenge of information protection, including risks arising from people and processes, as well as from technology.

Key differentiators

- Team of experts who are technically certified and experienced in complex programs.

CYBER INTELLIGENCE center

Our solutions are supported by
Deloitte's network of CICs

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)

Infrastructure Protection
Vulnerability Management
Application Protection
Identity and Access Management
Information Privacy



[Information Protection](#)

[Vigilant](#)



[Resilient](#)



[Contacts](#)



Next



Information Protection

Key solutions

Data Loss Prevention (DLP)

Advise | Implement | Manage

Assists in identification, monitoring, and protection of data in motion, at rest, in use, and in the cloud.

People Risk

Advise

Enables improved security awareness and culture, and understanding of insider threats focused on protecting sensitive data.

Cryptography

Advise | Implement

Allows business integration and implementation of enterprise key management, rights management, and encryption solutions.

Data Governance

Advise | Implement

Enables monitoring of access activity and improved visibility of risks to stored data across the business.

Information Classification

Advise | Implement

Helps with integration and implementation of classification technology and programs.

Data Mapping and Data Inventories

Advise | Implement

Assists in understanding where data exists and how it is handled across the data management lifecycle through data flow diagrams and data inventories.

Privacy by Design

Advise | Implement

Enables the embedding of privacy into the design and day-to-day operation of information technologies and business practices; organizations can obtain Privacy By Design Certification from Ryerson University leveraging Deloitte's certification assessment framework.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)

Infrastructure Protection

Vulnerability Management

Application Protection

Identity and Access Management

Information Privacy

[Information Protection](#)



[Vigilant](#)



[Resilient](#)



[Contacts](#)



[Next](#)

Vigilant

We integrate threat data, IT data, and business data to equip security teams with context-rich intelligence to proactively detect and manage cyberthreats and respond more effectively to cyber incidents.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)

Advanced Threat Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence and Analysis

[Resilient](#)



[Contacts](#)



Next



Advanced Threat Readiness and Preparation

CYBER INTELLIGENCE center

Challenges

Threat techniques evolve daily in volume, intensity, and complexity as hackers seek new vulnerabilities in software to compromise key systems across organizations.

Carrying out occasional, intermittent compliance-focused technical security assessments is not enough. Much more is required to understand if organizations can become compromised.

How we can help

Deloitte helps organizations assess and prepare their IT infrastructure, software, and third-parties by combining traditional ethical hacking principles and technical security reviews with advanced services in which we adopt a similar approach to that of an attacker.

Our services allow organizations to leverage any detection or response-mechanisms already in place, augment these where necessary, and most importantly, ensure all systems work together seamlessly so that the whole is greater than the sum of its parts.

Key solutions

Advanced Threat Simulation / Red Teaming

Advise | Implement

Simulates comprehensive cyberattack that tests the organization's prevention, detection, and response mechanisms and incorporates three core elements of security: physical, cyber, and human. The red team will perform realistic attack scenarios to achieve predefined objectives, using social engineering, phishing, physical penetration testing, and network exploitation.

Purple Teaming

Advise | Implement

Combines a non-covert red team engagement with a hybrid blue team made up of Deloitte and the organization's security experts. Deloitte runs through realistic scenarios to test and verify detection and response capabilities.

Threat Readiness Advisory and Remediation

Advise | Implement | Manage

Helps most mature organizations deal with advanced threats guiding improvements of ROI on existing detection technologies. By improving interaction between systems, applying realistic use cases, and staff training.

Cyber Compromise Assessment

Advise | Manage

Examines an organization's network to identify potential compromised devices by monitoring for malicious network traffic and suspicious network activity.

EDGE: Emerging and Disruptive Technologies Evaluation

Advise

Carries out security evaluations for new technologies and paradigms, helps organizations to anticipate security risks associated with their newly-adopted technologies.

Home

Foreword

Cyber Strategy



Secure



Vigilant

Advanced Threat Readiness and Preparation



Cyber Risk Analytics

Security Operations Center

Threat Intelligence and Analysis

Resilient



Contacts



< > Next

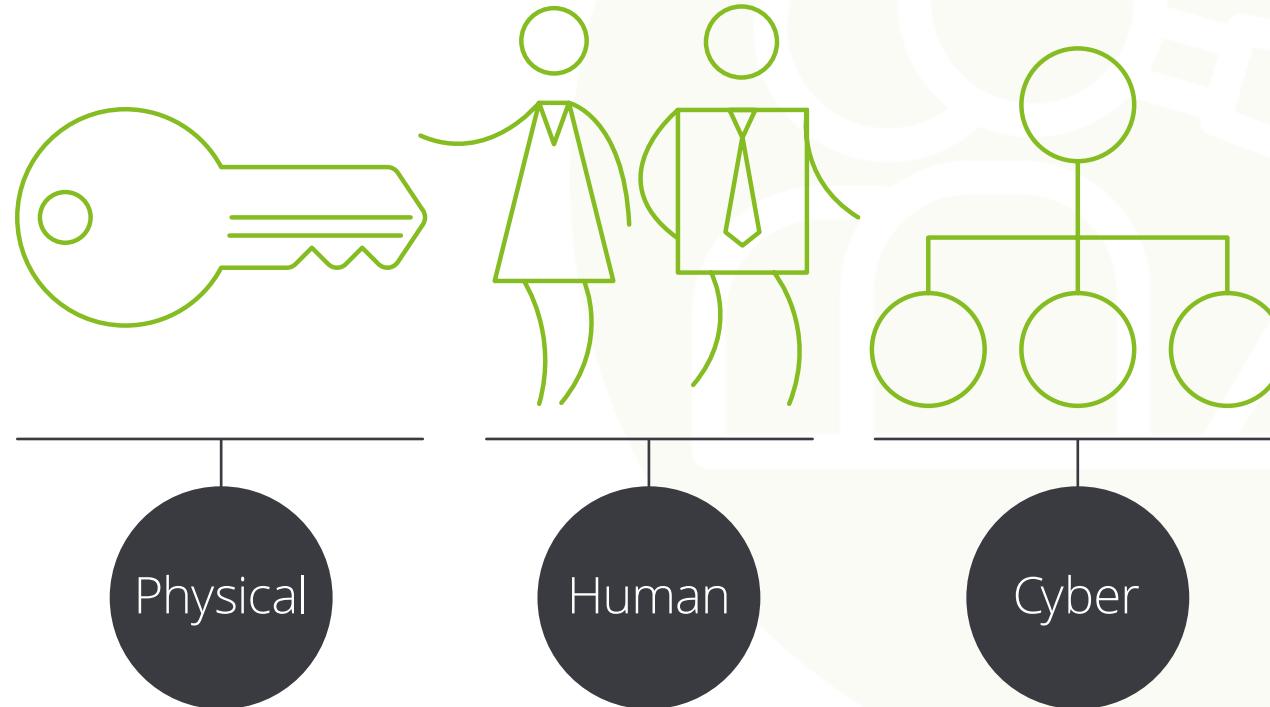


Advanced Threat Readiness and Preparation

Key differentiators

- With the Deloitte service-delivery model, organizations benefit from seamless integration with their vulnerability lifecycle management tasks.
- Our advanced services enable organizations to address emerging threats from new and disruptive technologies.
- We work with the latest open-source and commercial technologies and can work with any technology an organization might already have deployed.

Identify the weakest link with Deloitte Red, Blue, and Purple teaming



Home

Foreword

Cyber Strategy



Secure



Vigilant

Advanced Threat Readiness and Preparation

Cyber Risk Analytics

Security Operations Center

Threat Intelligence and Analysis

Resilient



Contacts



< > Next



Cyber Risk Analytics

Challenges

The greatest challenge organizations face today is the sheer abundance of threats, which makes it difficult to focus on those that pose the highest immediate risk.

How we can help

Deloitte's Cyber Risk Analytics services use advanced methods to analyze current cyberthreats and determine which are relevant and have the highest potential impact on strategic business objectives.

Our cyber risk analytics services are built around leading monitoring and correlation tools within the security information and event management (SIEM) and behavioral analytics markets. We employ various concepts, from log collection and correlation to behavioral analysis.

Armed with this information, organizations can focus resources on maintaining their desired security levels at minimum cost.

CYBER INTELLIGENCE center

Our solutions are supported by
Deloitte's network of CICs

Key solutions

Social Listening and Analytics

Advise | Implement | Manage

Empowers organizations to do more than merely react to social media. We enable them to protect themselves, leverage opportunities, and learn the risks from these sources.

Monitoring and Correlation

Implement | Manage

Enables organizations to view what is happening in cyberspace through advanced analytics. Either through monitoring and correlation of events, log collection with Deloitte Managed Security Services (MSS) platforms, or through Cyber Risk Analytics and behavior analytics tools deployed on-site. We manage all events 24/7, using the Deloitte Security Operations Centers.

SIEM Intelligence

Advise | Implement

Improves SIEM services by assessing an organization's SIEM and analytics maturity and governance. We design a SIEM evolution roadmap, and design and develop use cases, as well as assist in SIEM provisioning.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)

Advanced Threat Readiness and Preparation



[Cyber Risk Analytics](#)

Security Operations Center

Threat Intelligence and Analysis



[Resilient](#)



[Contacts](#)

[Next](#)

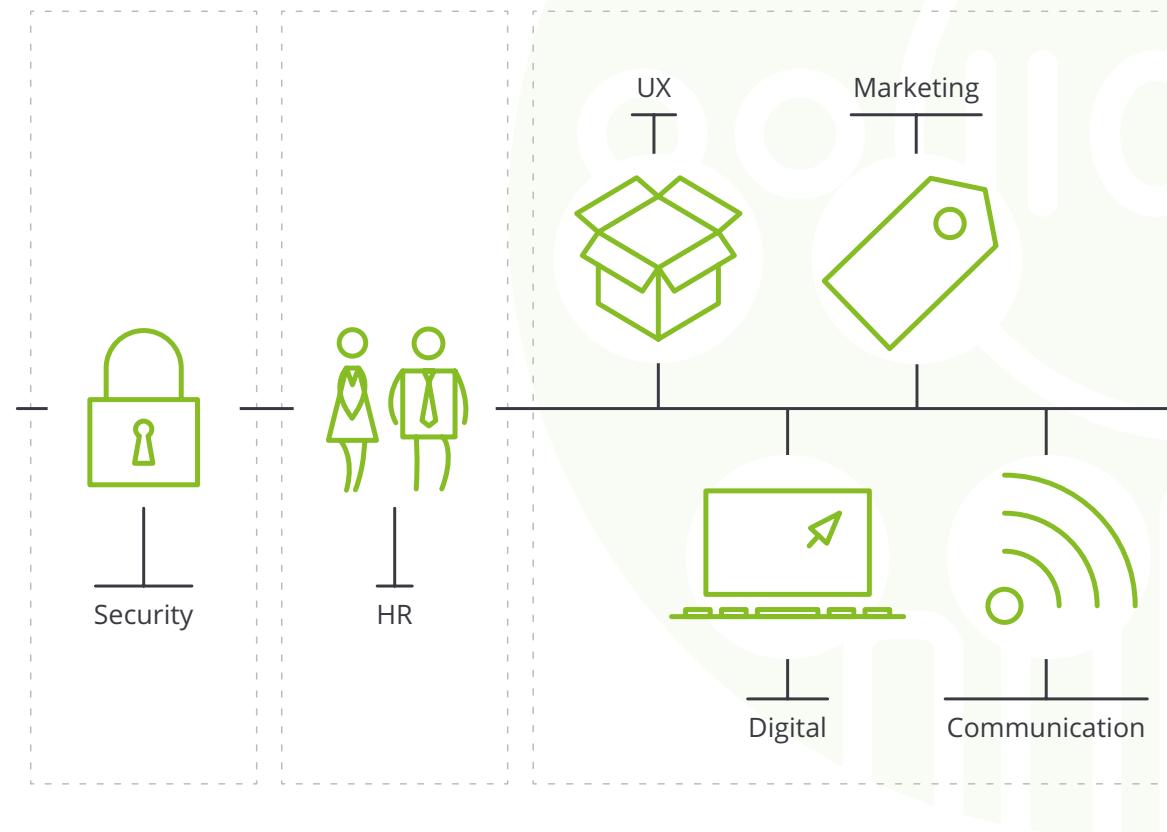


Cyber Risk Analytics

Key differentiators

- A flexible, remotely managed service as well as an on-site delivery model.
- Rapid deployment of Managed Security Services (MSS) with no setup costs.
- Broad experience with use cases and specific monitoring tools across a range of industries.

Social Listening and Analytics throughout the organization



Home

Foreword

Cyber Strategy



Secure



Vigilant

Advanced Threat Readiness and Preparation

Cyber Risk Analytics

Security Operations Center
Threat Intelligence and Analysis

Resilient



Contacts



< > Next



Security Operations Center (SOC)

Challenges

Organizations need to develop their information security capabilities, to respond faster, work more efficiently, and protect their core business. To achieve this, it is imperative that they have a mature SOC capability.

Specialist skills and technology platforms are essential. Organizations often find it difficult to build, maintain, and resource a SOC.

How we can help

We provide managed SOC services, on-site and hosted, which integrate event monitoring and correlation with threat intelligence and a business-focused output. We also advise organizations on design and deployment of their own SOC, and can help them establish and develop their capabilities.

Key solutions

24/7 Security threat monitoring

Advise | Implement | Manage

Offers a flexible and easily scalable service in which a team of certified analysts work 24/7 to detect malicious activities. Deloitte professionals operate and manage security information and event management (SIEM) platforms allowing threat-hunting capabilities.

SOC Capability Design and Deployment

Advise | Implement

Assesses the people, process, and technology aspects of an organization's SOC. Uses industry best practices to design and deploy a tailored SOC solution. This enables organizations to identify and respond to the most severe threats they face.

CYBER INTELLIGENCE center

Our solutions are supported by
Deloitte's network of CICs

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)

Advanced Threat Readiness and Preparation
Cyber Risk Analytics



[Security Operations Center](#)

Threat Intelligence and Analysis



[Resilient](#)



[Contacts](#)



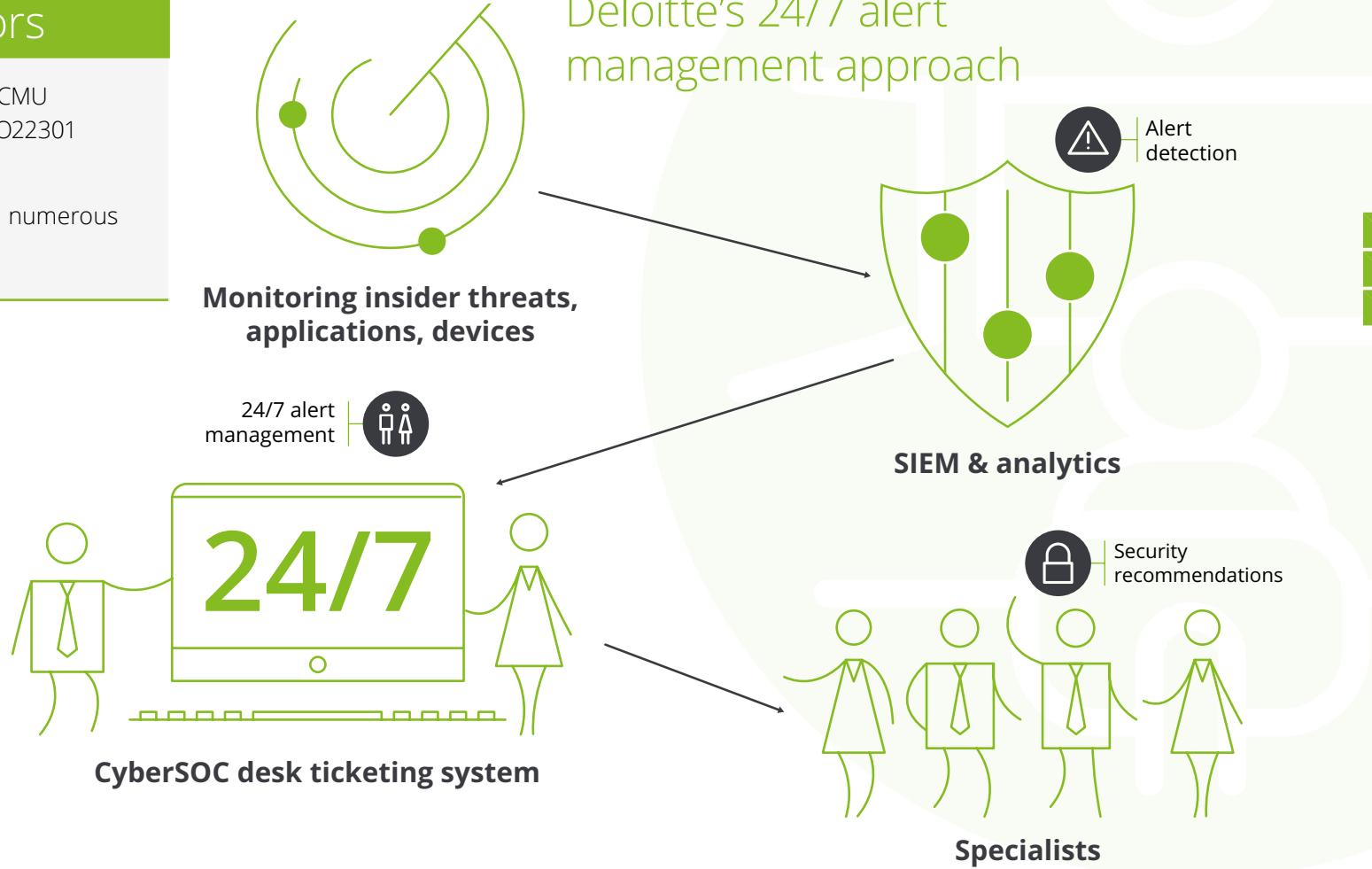
Next



Security Operations Center (SOC)

Key differentiators

- Deloitte's SOC is part of the CMU CERTNetwork, certified in ISO22301 and ISO27001.
- Deloitte's CICs benefit from numerous intelligence sources.



Home

Foreword

Cyber Strategy



Secure



Vigilant

Advanced Threat Readiness and Preparation
Cyber Risk Analytics



Security Operations Center
Threat Intelligence and Analysis

Resilient



Contacts



< > Next



Threat Intelligence and Analysis

Challenges

Understanding the cyberthreat landscape is difficult as threats are continuously evolving.

An integral approach to identifying threats requires significant resources to gather, filter, and interpret threat information from a wide variety of sources.

How we can help

Deloitte's Threat Intelligence and Analysis services offer monitoring, collection, and analysis of events that may become threats to your organization.

Deloitte's services provide actionable intelligence that supports proactive defense against potential cyberattacks and incidents.

Key solutions

Cyberthreat Intelligence

Advise | Implement | Manage

Looks for potentially threatening events taking place outside the organization's perimeter and provides custom insights in line with the organization's strategic and intelligence requirements.

Forecasting Emerging Threat

Manage

Forecasts emerging threats, enabling organizations to adapt their security methods and policies to future threats.

Intelligence Collection Grid

Manage

Collects and stores intelligence events from multiple sources around the globe and over time prevents, investigates, and forecasts threats.

CYBER INTELLIGENCE center

Our solutions are supported by Deloitte's network of CICs. Intelligence sharing among CICs allows us to be aware of threats across different regions and businesses so that Deloitte is able to provide unique, valuable, and fresh information to clients.

Threat Modeling

Advise | Implement | Manage

Identifies assets, threat actors, vulnerabilities, targets, methods, and associated countermeasures to prevent or mitigate the effects of potential threats on an organization.

Cyber Trend Report

Advise | Manage

Illustrates how threat actors work through a compilation of relevant threats across a set period of time and provides statistics, trends and a summary of the organization's cyberthreat landscape.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)

Advanced Threat Readiness and Preparation
Cyber Risk Analytics
Security Operations Center



[Threat Intelligence and Analysis](#)

[Resilient](#)



[Contacts](#)



Next

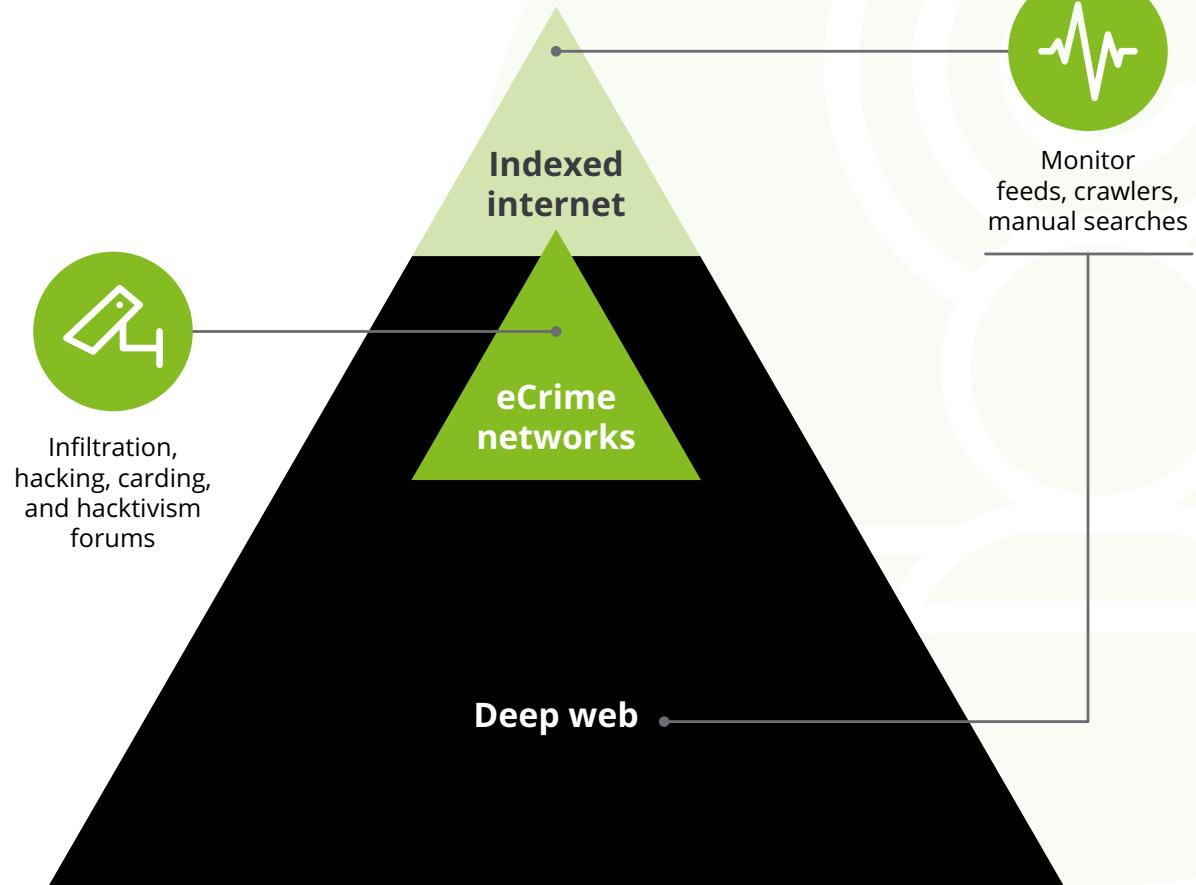


Threat Intelligence and Analysis

Key differentiators

- We provide a tailored Threat Intelligence service, not as a feed or a tool. Actionable intelligence is properly distributed to prevent or mitigate threats that target the client's business.
- Our experienced analysts undertake research, analysis, and validation of threats. They are also at the organizations disposal to attend to specific intelligence requests that can arise throughout time.

Cyberthreat Intelligence 24/7



Home

Foreword

Cyber Strategy



Secure



Cyber Vigilance

Advanced Threat Readiness and Preparation
Cyber Risk Analytics
Security Operations Center



Threat Intelligence and Analysis

Resilient



Contacts



< > Next

Resilient

We combine proven proactive and reactive incident management processes and technologies to rapidly adapt and respond to cyber disruptions whether from internal or external forces.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)



[Resilient](#)

Cyber Incident
Response

Cyber Wargaming



[Contacts](#)



Next



Cyber Incident Response

Challenges

Cyberthreats are constantly evolving and increasing in volume, intensity, and complexity. Cyber crisis management has therefore become a major focus of management and the board.

It has become more likely that an attack can penetrate an organization's defenses and security controls. When this happens organizations must respond fast, thoroughly, and decisively.

How we can help

Deloitte's services provide organizations with a set of operational and strategic cyber capabilities in a single comprehensive solution, from preparation to 24/7 real-time implementation and response.

We can help organizations to improve their cyber response capabilities, establishing a high level of readiness through effective preparation, training, and simulations. We provide real-time, on-site, and 24/7 support for a cyber incident or crisis that could harm strategic objectives, revenue, reputation, or viability.

Key solutions

Cyber Crisis Management

Advise | Implement | Manage

Assists your executive leadership to improve their strategic crisis management decision-making capabilities, helping them respond effectively to a large-scale crisis event and emerge stronger. We have one of the largest, most respected teams of crisis and continuity management professionals in the world.

Cyber Incident Response

Advise | Implement | Manage

Deploys the Deloitte Cyber Incident Response team 24/7, enabling clients to respond effectively and decisively to a cybersecurity incident. Deloitte specialists have experience dealing with a vast range of cyberthreats.

CYBER INTELLIGENCE center

Our solutions are supported by
Deloitte's network of CICs

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)



[Resilient](#)



[Cyber Incident Response](#)

[Cyber Wargaming](#)

[Contacts](#)



[Next](#)



Cyber Incident Response

Key differentiators

- Deloitte's experience in incident and crisis management minimizes the time and resources needed to resolve an emergency.
- Deloitte's understanding of business and risk allows us to respond to incidents from both a technical and a strategic perspective.

Our services are supported by the Deloitte network of CICs, providing 24/7 support with a dedicated Deloitte cyber response 'front office'. We shorten response times by leveraging Deloitte's geographic breadth and depth.

By dialing a regional Deloitte Response number, a client will immediately be connected to the integrated platform for all cyber crisis management services within Deloitte.



[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)



[Resilient](#)

[Cyber Incident Response](#)

[Cyber Wargaming](#)



[Contacts](#)



Next



Cyber Wargaming

Challenges

Organizations are not prepared to counter cyber crime unless they have been tested. An incident and crisis management response framework is not enough.

Organizations must test their defense plans regularly if they are to be confident about their ability to respond effectively to threats.

How we can help

The Deloitte Wargaming portfolio of services creates an environment for client teams to simulate incidents and crises, allowing them to develop coordinated responses and identify areas that need improvement in order to prepare for a real-world threat.

These exercises are particularly relevant for cyber threats that have the potential to turn into a major corporate crisis, requiring a coordinated response from the communications and corporate affairs functions, the board and non-executive directors.

Key solutions

Cyber Workshop

Advise

Increases awareness and supports the development of cyber crisis management plans, procedures, roles, and responsibilities. They focus on detailed discussion of an unfolding pre-prepared scenario, often split into key incident/crisis response phases. We also run more technical 'Breach Readiness Workshops' to help validate, check, and challenge existing response processes and playbooks.

Cyber Table-Top Exercise

Advise

Guides teams in reviewing plans and processes, and practice their roles and responsibilities. The exercises often focus on sharpening specific skills (such as logging, conducting risk assessments, and rehearsing decision-making processes) and identify opportunities to improve the

prevention of, response to, and recovery from a cyber incident or crisis.

Cyber Simulation Exercise

Advise | Implement

Rehearses or stress-tests existing plans and procedures against complex and multi-faceted cyber incidents or crises. Exercises are designed to take place in a realistic, real-time, and 'live' controlled environment – often involving multiple levels of an organization operating remotely on a global scale. They unfold through a variety of pre-prepared so-called 'injects' delivered by role players and experienced exercise facilitators. Participants are immersed in the pressure of a real cyber-related crisis.

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)



[Resilient](#)

Cyber Incident Response



[Cyber Wargaming](#)



[Contacts](#)

[Next](#)

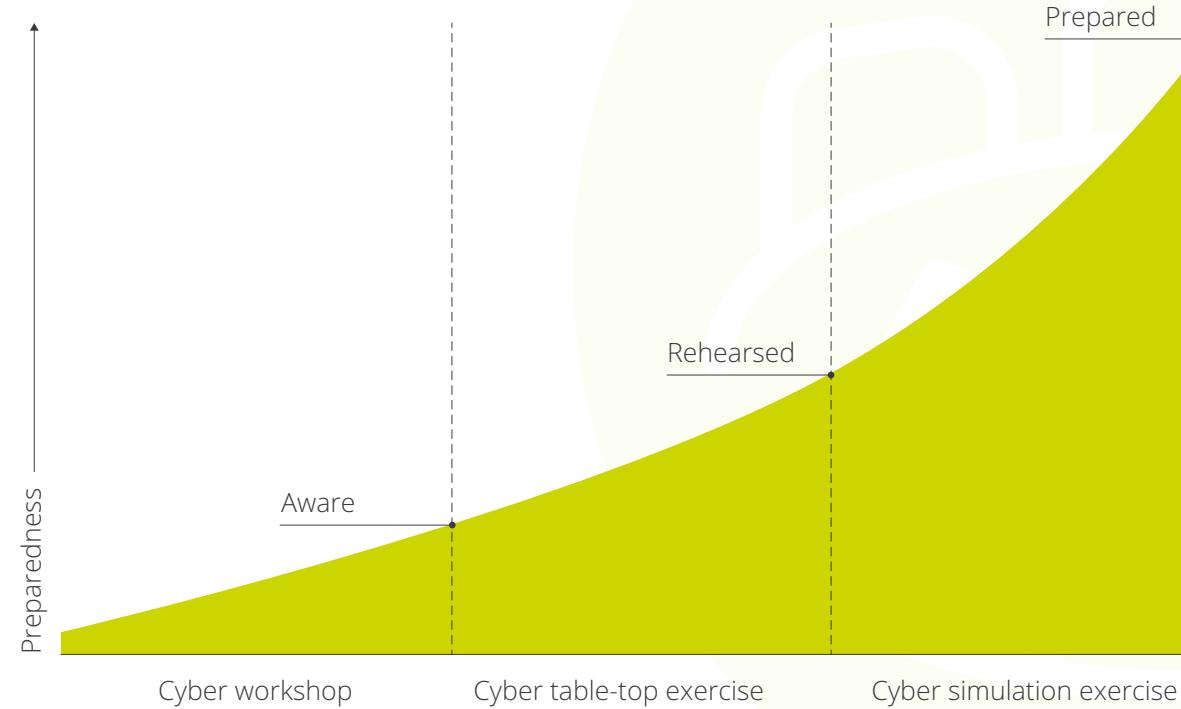


Cyber Wargaming

Key differentiators

- Deloitte's capability has been built through years of practical experience, delivering hundreds of simulations at board, executive, and operational levels.
- We use scenario-specific subject matter experts, from within the organization or Deloitte, in order to tailor highly realistic scenarios in the organization's own operating environment.
- We use innovative simulation and wargaming techniques to engage and challenge senior participants and get them thinking about 'what keeps them up at night'. This helps them to answer the questions often asked by key stakeholders, including customers and regulators:
 - Are you and your organization ready to deal with a cyber crisis?
 - Are your people clear of their roles and responsibilities during a cyber crisis?

Cyber Wargaming approach



[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)



[Resilient](#)

Cyber Incident Response



[Cyber Wargaming](#)

[Contacts](#)



[< Next](#)



Contacts

Nick Galletto

Global and Americas Cyber Risk Leader
ngalletto@deloitte.ca

Chris Verdonck

EMEA Cyber Risk Leader
cverdonck@deloitte.com

James Nunn-Price

Asia Pacific Cyber Risk Leader
jamesnunnprice@deloitte.com.au

[Home](#)

[Foreword](#)

[Cyber Strategy](#)



[Secure](#)



[Vigilant](#)



[Resilient](#)



[Contacts](#)





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit & 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 high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229, 232, 239, 240, and 249

[Release Nos. 33-11216; 34-97989; File No. S7-09-22]

RIN 3235-AM89

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

AGENCY: Securities and Exchange Commission.

ACTION: Final rule.

SUMMARY: The Securities and Exchange Commission (“Commission”) is adopting new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are adopting amendments to require current disclosure about material cybersecurity incidents. We are also adopting rules requiring periodic disclosures about a registrant’s processes to assess, identify, and manage material cybersecurity risks, management’s role in assessing and managing material cybersecurity risks, and the board of directors’ oversight of cybersecurity risks. Lastly, the final rules require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (“Inline XBRL”).

DATES: *Effective date:* The amendments are effective September 5, 2023.

Compliance dates: See Section II.I (Compliance Dates).

FOR FURTHER INFORMATION CONTACT: Nabeel Cheema, Special Counsel, at (202) 551-3430, in the Office of Rulemaking, Division of Corporation Finance; and, with respect to the application of the rules to business development companies, David Joire, Senior Special

Counsel, at (202) 551-6825 or *IMOCC@sec.gov*, Chief Counsel's Office, Division of Investment Management, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

SUPPLEMENTARY INFORMATION: We are adopting amendments to:

Commission Reference		CFR Citation (17 CFR)
Regulation S-K		§§ 229.10 through 229.1305
	Items 106 and 601	§§ 229.106 and 229.601
Regulation S-T		§§ 232.10 through 232.903
	Rule 405	§ 232.405
Securities Act of 1933 ("Securities Act") ¹	Form S-3	§ 239.13
Securities Exchange Act of 1934 ("Exchange Act") ²	Rule 13a-11	§ 240.13a-11
	Rule 15d-11	§ 240.15d-11
	Form 20-F	§ 249.220f
	Form 6-K	§ 249.306
	Form 8-K	§ 249.308
	Form 10-K	§ 249.310

¹ 15 U.S.C. 77a *et seq.*

² 15 U.S.C. 78a *et seq.*

Table of Contents

I.	Introduction and Background	5
II.	Discussion of Final Amendments	13
A.	Disclosure of Cybersecurity Incidents on Current Reports	13
1.	Proposed Amendments	13
2.	Comments	16
3.	Final Amendments	27
B.	Disclosures about Cybersecurity Incidents in Periodic Reports	46
1.	Proposed Amendments	46
2.	Comments	48
3.	Final Amendments	50
C.	Disclosure of a Registrant’s Risk Management, Strategy and Governance Regarding Cybersecurity Risks	53
1.	Risk Management and Strategy	53
a.	Proposed Amendments	53
b.	Comments	56
c.	Final Amendments	60
2.	Governance	65
a.	Proposed Amendments	65
b.	Comments	67
c.	Final Amendments	68
3.	Definitions.....	71
a.	Proposed Definitions.....	71
b.	Comments	72
c.	Final Definitions	75
D.	Disclosure Regarding the Board of Directors’ Cybersecurity Expertise	81
1.	Proposed Amendments	81
2.	Comments	82
3.	Final Amendments	85
E.	Disclosure by Foreign Private Issuers.....	85
1.	Proposed Amendments	85
2.	Comments	86
3.	Final Amendments	87
F.	Structured Data Requirements	88
1.	Proposed Amendments	88
2.	Comments	88
3.	Final Amendments	88
G.	Applicability to Certain Issuers	89
1.	Asset-Backed Issuers	89
2.	Smaller Reporting Companies	91
H.	Need for New Rules and Commission Authority	93
I.	Compliance Dates	107
III.	OTHER MATTERS.....	107
IV.	ECONOMIC ANALYSIS	108
A.	Introduction.....	108

B.	Economic Baseline.....	112
1.	Current Regulatory Framework	112
2.	Affected Parties.....	117
C.	Benefits and Costs of the Final Rules	118
1.	Benefits	119
a.	More Timely and Informative Disclosure.....	119
b.	Greater Uniformity and Comparability.....	130
2.	Costs.....	134
3.	Indirect Economic Effects.....	143
D.	Effects on Efficiency, Competition, and Capital Formation.....	145
E.	Reasonable Alternatives.....	146
1.	Website Disclosure	146
2.	Disclosure through Periodic Reports	147
3.	Exempt Smaller Reporting Companies.....	148
V.	PAPERWORK REDUCTION ACT.....	150
A.	Summary of the Collections of Information	150
B.	Summary of Comment Letters and Revisions to PRA Estimates.....	151
C.	Effects of the Amendments on the Collections of Information	152
D.	Incremental and Aggregate Burden and Cost Estimates for the Final Amendments ..	154
VI.	FINAL REGULATORY FLEXIBILITY ANALYSIS	158
A.	Need for, and Objectives of, the Final Amendments.....	158
B.	Significant Issues Raised by Public Comments.....	158
1.	Estimate of Affected Small Entities and Impact to Those Entities.....	160
2.	Consideration of Alternatives	162
C.	Small Entities Subject to the Final Amendments	165
D.	Projected Reporting, Recordkeeping, and other Compliance Requirements.....	165
E.	Agency Action to Minimize Effect on Small Entities	166
	Statutory Authority	169

I. Introduction and Background

On March 9, 2022, the Commission proposed new rules, and rule and form amendments, to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incidents by public companies that are subject to the reporting requirements of the Exchange Act.³ The proposal followed on interpretive guidance on the application of existing disclosure requirements to cybersecurity risk and incidents that the Commission and staff had issued in prior years.

In particular, in 2011, the Division of Corporation Finance issued interpretive guidance providing the Division’s views concerning operating companies’ disclosure obligations relating to cybersecurity (“2011 Staff Guidance”).⁴ In that guidance, the staff observed that “[a]lthough no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents,” and further that “material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.”⁵ The guidance pointed specifically to disclosure obligations under 17 CFR 229.503 (Regulation S-K “Item 503(c)”) (Risk factors) (since moved to 17 CFR 229.105 (Regulation S-K “Item 105”)), 17 CFR 229.303 (Regulation S-K “Item 303”) (Management’s discussion and analysis of financial condition and results of operations), 17 CFR 229.101 (Regulation S-K “Item 101”) (Description of business), 17 CFR 229.103 (Regulation S-K “Item 103”) (Legal proceedings), and 17 CFR 229.307

³ See *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release No. 33-11038 (Mar. 9, 2022) [87 FR 16590 (Mar. 23, 2022)] (“Proposing Release”).

⁴ See CF Disclosure Guidance: Topic No. 2—Cybersecurity (Oct. 13, 2011), available at <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

⁵ *Id.*

(Disclosure controls and procedures), as well as to Accounting Standards Codifications 350-40 (Internal-Use Software), 605-50 (Customer Payments and Incentives), 450-20 (Loss Contingencies), 275-10 (Risks and Uncertainties), and 855-10 (Subsequent Events).⁶

In 2018, “[i]n light of the increasing significance of cybersecurity incidents,” the Commission issued interpretive guidance to reinforce and expand upon the 2011 Staff Guidance and also address the importance of cybersecurity policies and procedures, as well as the application of insider trading prohibitions in the context of cybersecurity (“2018 Interpretive Release”).⁷ In addition to discussing the provisions previously covered in the 2011 Staff Guidance, the new guidance addressed 17 CFR 229.407 (Regulation S-K “Item 407”) (Corporate Governance), 17 CFR Part 210 (“Regulation S-X”), and 17 CFR Part 243 (“Regulation FD”).⁸ The 2018 Interpretive Release noted that companies can provide current reports on Form 8-K and Form 6-K to maintain the accuracy and completeness of effective shelf registration statements, and it also advised companies to consider whether it may be appropriate to implement restrictions on insider trading during the period following an incident and prior to disclosure.⁹

As noted in the Proposing Release, current disclosure practices are varied. For example, while some registrants do report material cybersecurity incidents, most typically on Form 10-K, review of Form 8-K, Form 10-K, and Form 20-F filings by staff in the Division of Corporation Finance has shown that companies provide different levels of specificity regarding the cause, scope, impact, and materiality of cybersecurity incidents. Likewise, staff has also observed that,

⁶ *Id.*

⁷ See *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release No. 33-10459 (Feb. 21, 2018) [83 FR 8166 (Feb. 26, 2018)], at 8167.

⁸ *Id.*

⁹ *Id.*

while the majority of registrants that are disclosing cybersecurity risks appear to be providing such disclosures in the risk factor section of their annual reports on Form 10-K, the disclosures are sometimes included with other unrelated disclosures, which makes it more difficult for investors to locate, interpret, and analyze the information provided.¹⁰

In the Proposing Release, the Commission explained that a number of trends underpinned investors' and other capital markets participants' need for more timely and reliable information related to registrants' cybersecurity than was produced following the 2011 Staff Guidance and the 2018 Interpretive Release. First, an ever-increasing share of economic activity is dependent on electronic systems, such that disruptions to those systems can have significant effects on registrants and, in the case of large-scale attacks, systemic effects on the economy as a whole.¹¹ Second, there has been a substantial rise in the prevalence of cybersecurity incidents, propelled by several factors: the increase in remote work spurred by the COVID-19 pandemic; the increasing reliance on third-party service providers for information technology services; and the rapid monetization of cyberattacks facilitated by ransomware, black markets for stolen data, and crypto-asset technology.¹² Third, the costs and adverse consequences of cybersecurity incidents to companies are increasing; such costs include business interruption, lost revenue, ransom payments, remediation costs, liabilities to affected parties, cybersecurity protection costs, lost assets, litigation risks, and reputational damage.¹³

¹⁰ See *infra* Section IV.A (noting that current cybersecurity disclosures appear in varying sections of companies' periodic and current reports and are sometimes included with other unrelated disclosures).

¹¹ Proposing Release at 16591-16592. See also U.S. FINANCIAL STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT (2021), at 168, available at <https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf> (finding that "a destabilizing cybersecurity incident could potentially threaten the stability of the U.S. financial system").

¹² Proposing Release at 16591-16592.

¹³ *Id.*

Since publication of the Proposing Release, these trends have continued apace, with significant cybersecurity incidents occurring across companies and industries. For example, threat actors repeatedly and successfully executed attacks on high-profile companies across multiple critical industries over the course of 2022 and the first quarter of 2023, causing the Department of Homeland Security’s Cyber Safety Review Board to initiate multiple reviews.¹⁴ Likewise, state actors have perpetrated multiple high-profile attacks, and recent geopolitical instability has elevated such threats.¹⁵ A recent study by two cybersecurity firms found that 98 percent of organizations use at least one third-party vendor that has experienced a breach in the last two years.¹⁶ In addition, recent developments in artificial intelligence may exacerbate cybersecurity threats, as researchers have shown that artificial intelligence systems can be leveraged to create code used in cyberattacks, including by actors not versed in programming.¹⁷ Overall, evidence suggests companies may be underreporting cybersecurity incidents.¹⁸

¹⁴ See Department of Homeland Security, *Cyber Safety Review Board to Conduct Second Review on Lapsus\$* (Dec. 2, 2022), available at <https://www.dhs.gov/news/2022/12/02/cyber-safety-review-board-conduct-second-review-lapsus>; see also Tim Starks, *The Latest Mass Ransomware Attack Has Been Unfolding For Nearly Two Months*, WASH. POST (Mar. 27, 2023), available at <https://www.washingtonpost.com/politics/2023/03/27/latest-mass-ransomware-attack-has-been-unfolding-nearly-two-months/>.

¹⁵ See, e.g., Press Release, Federal Bureau of Investigation, *FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony’s Horizon Bridge Currency Theft* (Jan. 23, 2023), available at <https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft>; Alert (AA22-257A), Cybersecurity & Infrastructure Security Agency, *Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations* (Sep. 14, 2022), available at <https://www.cisa.gov/uscert/ncas/alerts/aa22-257a>; National Security Agency et al., *Joint Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure* (Apr. 20, 2022), available at https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/joint_csa_russian_state-sponsored_and_crimeal_cyber_threats_to_critical_infrastructure_20220420.pdf.

¹⁶ SecurityScorecard, *Cyentia Institute and SecurityScorecard Research Report: Close Encounters of the Third (and Fourth) Party Kind* (Feb 1, 2023), available at <https://securityscorecard.com/research/cyentia-close-encounters-of-the-third-and-fourth-party-kind/>.

¹⁷ Check Point Research, *OPWNIAI: AI that Can Save the Day or Hack it Away* (Dec. 19, 2022), available at <https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away>.

¹⁸ Bitdefender, *Whitepaper: Bitdefender 2023 Cybersecurity Assessment* (Apr. 2023), available at <https://businessresources.bitdefender.com/bitdefender-2023-cybersecurity-assessment>.

Legislatively, we note two significant developments occurred following publication of the Proposing Release. First, the President signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCIA”)¹⁹ on March 15, 2022, as part of the Consolidated Appropriations Act of 2022.²⁰ The centerpiece of CIRCIA is the reporting obligation placed on companies in defined critical infrastructure sectors.²¹ Once rules are adopted by the Cybersecurity & Infrastructure Security Agency (“CISA”), these companies will be required to report covered cyber incidents to CISA within 72 hours of discovery, and report ransom payments within 24 hours.²² Importantly, reports made to CISA pursuant to CIRCIA will remain confidential; while the information contained therein may be shared across Federal agencies for cybersecurity, investigatory, and law enforcement purposes, the information may not be disclosed publicly, except in anonymized form.²³ We note that CIRCIA also mandated the creation of a “Cyber Incident Reporting Council . . . to coordinate, deconflict, and harmonize Federal incident reporting requirements” (the “CIRC”), of which the Commission is a member.²⁴

Second, on December 21, 2022, the President signed into law the Quantum Computing Cybersecurity Preparedness Act, which directs the Federal Government to adopt technology that is protected from decryption by quantum computing, a developing technology that may increase

¹⁹ Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, 136 Stat. 1038 (2022).

²⁰ Consolidated Appropriations Act of 2022, H.R. 2471, 117th Cong. (2022).

²¹ The sectors are defined in Presidential Policy Directive / PPD-21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), as: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; Water and Wastewater Systems. Because these sectors encompass some private companies and do not encompass all public companies, CIRCIA’s reach is both broader and narrower than the set of companies subject to the rules we are adopting.

²² 6 U.S.C. 681b(a)(1).

²³ 6 U.S.C. 681e. *See infra* Section II.A.3 for a discussion of why our final rules serve a different purpose and are not at odds with the goals of CIRCIA.

²⁴ 6 U.S.C. 681f.

computer processing capacity considerably and thereby render existing computer encryption vulnerable to decryption.²⁵

We received over 150 comment letters in response to the Proposing Release.²⁶ The majority of comments focused on the proposed incident disclosure requirement, although we also received substantial comment on the proposed risk management, strategy, governance, and board expertise requirements. In addition, the Commission's Investor Advisory Committee adopted recommendations (“IAC Recommendation”) with respect to the proposal, stating that it: supports the proposed incident disclosure requirement; supports the proposed risk management, strategy, and governance disclosure requirements; recommends the Commission reconsider the proposed board of directors' cybersecurity expertise disclosure requirement; suggests requiring companies to disclose the key factors they used to determine the materiality of a reported cybersecurity

²⁵ Quantum Computing Cybersecurity Preparedness Act, H.R. 7535, 117th Cong. (2022). More recently, the White House released a National Cybersecurity Strategy to combat the ongoing risks associated with cyberattacks. The National Cybersecurity Strategy seeks to rebalance the responsibility for defending against cyber threats toward companies instead of the general public, and looks to realign incentives to favor long-term investments in cybersecurity. *See* Press Release, White House, FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy (Mar. 2, 2023), available at <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>.

²⁶ The public comments we received are available at <https://www.sec.gov/comments/s7-09-22/s70922.htm>. On Mar. 9, 2022, the Commission published the Proposing Release on its website. The comment period for the Proposing Release was open for 60 days from issuance and publication on SEC.gov and ended on May 9, 2022. One commenter asserted that the comment period was not sufficient and asked the Commission to extend it by 30 days. *See* letter from American Chemistry Council (“ACC”). In Oct. 2022, the Commission reopened the comment period for the Proposing Release and other rulemakings because certain comments on the Proposing Release and other rulemakings were potentially affected by a technological error in the Commission’s internet comment form. *See Resubmission of Comments and Reopening of Comment Periods for Several Rulemaking Releases Due to a Technological Error in Receiving Certain Comments*, Release No. 33-11117 (Oct. 7, 2022) [87 FR 63016 (Oct. 18, 2022)] (“Reopening Release”). The Reopening Release was published on the Commission’s website on Oct. 7, 2022 and in the Federal Register on Oct. 18, 2022, and the comment period ended on Nov. 1, 2022. A few commenters asserted that the comment period for the reopened rulemakings was not sufficient and asked the Commission to extend the comment period for those rulemakings. *See, e.g.*, letters from Attorneys General of the states of Montana *et al.* (Oct. 24, 2022) and U.S. Chamber of Commerce (Nov. 1, 2022). We have considered all comments received since Mar. 9, 2022 and do not believe an additional extension of the comment period is necessary.

incident; and suggests extending the proposed 17 CFR 229.106 (Regulation S-K “Item 106”) disclosure requirements to registration statements.²⁷

We are making a number of important changes from the Proposing Release in response to comments received. With respect to incident disclosure, we are narrowing the scope of disclosure, adding a limited delay for disclosures that would pose a substantial risk to national security or public safety, requiring certain updated incident disclosure on an amended Form 8-K instead of Forms 10-Q and 10-K for domestic registrants, and on Form 6-K instead of Form 20-F for foreign private issuers (“FPIs”),²⁸ and omitting the proposed aggregation of immaterial incidents for materiality analyses. We are streamlining the proposed disclosure elements related to risk management, strategy, and governance, and we are not adopting the proposed requirement to disclose board cybersecurity expertise. The following table summarizes the requirements we are adopting, including changes from the Proposing Release, as described more fully in Section II below:²⁹

²⁷ See U.S. Securities and Exchange Commission Investor Advisory Committee, Recommendation of the Investor as Owner Subcommittee and Disclosure Subcommittee of the SEC Investor Advisory Committee Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Sept. 21, 2022), available at <https://www.sec.gov/spotlight/investor-advisory-committee-2012/20220921-cybersecurity-disclosure-recommendation.pdf>. The Investor Advisory Committee also held a panel discussion on cybersecurity at its Mar. 10, 2022 meeting. See U.S. Securities and Exchange Commission Investor Advisory Committee, Meeting Agenda (Mar. 10, 2022), available at <https://www.sec.gov/spotlight/investor-advisory-committee/iac031022-agenda.htm>.

²⁸ An FPI is any foreign issuer other than a foreign government, except for an issuer that (1) has more than 50 percent of its outstanding voting securities held of record by U.S. residents; and (2) any of the following: (i) a majority of its executive officers or directors are citizens or residents of the United States; (ii) more than 50 percent of its assets are located in the United States; or (iii) its business is principally administered in the United States. 17 CFR 230.405. See also 17 CFR 240.3b-4(c).

²⁹ The information in this table is not comprehensive and is intended only to highlight some of the more significant aspects of the final amendments. It does not reflect all of the amendments or all of the rules and forms that are affected by the final amendments, which are discussed in detail below. As such, this table should be read together with the entire release, including the regulatory text.

Item	<u>Summary Description of the Disclosure Requirement</u>³⁰
Regulation S-K Item 106(b) – <i>Risk management and strategy</i>	Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
Regulation S-K Item 106(c) – <i>Governance</i>	Registrants must: <ul style="list-style-type: none"> - Describe the board’s oversight of risks from cybersecurity threats. - Describe management’s role in assessing and managing material risks from cybersecurity threats.
Form 8-K Item 1.05 – <i>Material Cybersecurity Incidents</i>	Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its: <ul style="list-style-type: none"> - Nature, scope, and timing; and - Impact or reasonably likely impact. <p>An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General (“Attorney General”) determines immediate disclosure would pose a substantial risk to national security or public safety.</p> <p>Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.</p>
Form 20-F	FPIs must: <ul style="list-style-type: none"> - Describe the board’s oversight of risks from cybersecurity threats. - Describe management’s role in assessing and managing material risks from cybersecurity threats.
Form 6-K	FPIs must furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise

³⁰ For purposes of this release, the terms “public companies,” “companies,” and “registrants” include issuers that are business development companies as defined in section 2(a)(48) of the Investment Company Act of 1940, which are a type of closed-end investment company that is not registered under the Investment Company Act, but do not include investment companies registered under that Act.

	publicize in a foreign jurisdiction, to any stock exchange, or to security holders.
--	---

Overall, we remain persuaded that, as detailed in the Proposing Release: under-disclosure regarding cybersecurity persists despite the Commission’s prior guidance; investors need more timely and consistent cybersecurity disclosure to make informed investment decisions; and recent legislative and regulatory developments elsewhere in the Federal Government, including those developments subsequent to the issuance of the Proposing Release such as CIRCIA³¹ and the Quantum Computing Cybersecurity Preparedness Act,³² while serving related purposes, will not effectuate the level of public cybersecurity disclosure needed by investors in public companies.

II. Discussion of Final Amendments

A. Disclosure of Cybersecurity Incidents on Current Reports

1. Proposed Amendments

The Commission proposed to amend Form 8-K by adding new Item 1.05 that would require a registrant to disclose the following information regarding a material cybersecurity incident, to the extent known at the time of filing:

- When the incident was discovered and whether it is ongoing;
- A brief description of the nature and scope of the incident;
- Whether any data were stolen, altered, accessed, or used for any other unauthorized purpose;
- The effect of the incident on the registrant’s operations; and

³¹ *Supra* note 19.

³² *Supra* note 25.

- Whether the registrant has remediated or is currently remediating the incident.³³

The Commission clarified in the Proposing Release that this requirement would not extend to specific, technical information about the registrant’s planned response to the incident or its 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.³⁴

The Commission proposed to set the filing trigger for Item 1.05 as the date the registrant determines that a cybersecurity incident is material; as with all other Form 8-K items, the proposed filing deadline would be four business days after the trigger.³⁵ To protect against any inclination on the part of a registrant to delay making a materiality determination with a view toward prolonging the filing deadline, the Commission proposed adding Instruction 1 to Item 1.05 requiring that “a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident.”³⁶

The Commission affirmed in the Proposing Release that the materiality standard registrants should apply in evaluating whether a Form 8-K would be triggered under proposed Item 1.05 would be consistent with that set out in the numerous cases addressing materiality in the securities laws, including *TSC Industries, Inc. v. Northway, Inc.*,³⁷ *Basic, Inc. v. Levinson*,³⁸ and *Matrixx Initiatives, Inc. v. Siracusano*,³⁹ and likewise with that set forth in 17 CFR 230.405 (“Securities Act Rule 405”) and 17 CFR 240.12b-2 (“Exchange Act Rule 12b-2”). That is,

³³ Proposing Release at 16595.

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.* at 16596.

³⁷ *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976).

³⁸ *Basic Inc. v. Levinson*, 485 U.S. 224, 232 (1988).

³⁹ *Matrixx Initiatives v. Siracusano*, 563 U.S. 27 (2011).

information is material if “there is a substantial likelihood that a reasonable shareholder would consider it important”⁴⁰ in making an investment decision, or if it would have “significantly altered the ‘total mix’ of information made available.”⁴¹ “Doubts as to the critical nature” of the relevant information should be “resolved in favor of those the statute is designed to protect,” namely investors.⁴²

The Commission explained that the timely disclosure of the information required by proposed Item 1.05 would enable investors and other market participants to assess the possible effects of a material cybersecurity incident on the registrant, including any short- and long-term financial effects or operational effects, resulting in information useful for their investment decisions.⁴³ Aligning the deadline for Item 1.05 with that of the other Form 8-K items would, the Commission maintained, significantly improve the timeliness of cybersecurity incident disclosures as well as standardize those disclosures.⁴⁴ The Commission did not propose to provide a reporting delay in cases of ongoing internal or external investigations of cybersecurity incidents.⁴⁵ Nevertheless, the Proposing Release requested comment on whether to allow a delay in reporting where the Attorney General determines that a delay is in the interest of national security.⁴⁶

⁴⁰ *TSC Indus.*, 426 U.S. at 449.

⁴¹ *Id.*

⁴² *Id.* at 448.

⁴³ Proposing Release at 16595.

⁴⁴ *Id.*

⁴⁵ *Id.* at 16596.

⁴⁶ *Id.* at 16598.

2. Comments

Proposed Item 1.05 received a significant amount of feedback from commenters. Some commenters supported Item 1.05 as proposed,⁴⁷ saying that the current level of disclosure on cybersecurity incidents is inadequate to meet investor needs, and Item 1.05 would remedy this inadequacy by effectuating the disclosure of decision-useful information.⁴⁸ One commenter also anticipated that Item 1.05 would reduce the risk of insider trading by shortening the time between discovery of an incident and public disclosure.⁴⁹

Other commenters opposed proposed Item 1.05, for several reasons. Some commenters said that if proposed Item 1.05 were to result in disclosure while an incident is still ongoing, it would tip off the threat actor and thus make successful neutralization of the incident more difficult.⁵⁰ Commenters also expressed concern that public notice of a vulnerability could draw attacks from other threat actors who were previously unaware of the vulnerability; and such attacks could target the disclosing registrant or other companies with the same vulnerability, particularly if the vulnerability is with a third-party service provider used by multiple

⁴⁷ See letters from American Institute of CPAs (“AICPA”); Better Markets (“Better Markets”); BitSight Technologies, Inc. (“BitSight”); California Public Employees’ Retirement System (“CalPERS”); Crindata, LLC (“Crindata”); Council of Institutional Investors (“CII”); Information Technology and Innovation Foundation (“ITIF”); North American Securities Administrators Association Inc. (“NASAA”); Professor Jerry Perullo (“Prof. Perullo”); Professor Preeti Choudhary (“Prof. Choudhary”); Tessa Mishoe (“T. Mishoe”). See also IAC Recommendation.

⁴⁸ *Id.*

⁴⁹ See letter from Better Markets.

⁵⁰ See letters from ACC; American Gas Association and Interstate Natural Gas Association of America (“AGA/INGAA”); BioTechnology Innovation Organization (“BIO”); Bank Policy Institute, American Bankers Association, and Mid-Size Bank Coalition of America (“BPI et al.”); BSA / The Software Alliance (“BSA”); Business Roundtable (“Business Roundtable”); Canadian Bankers Association (“CBA”); Edison Electric Institute (“EEI”); Energy Infrastructure Council (“EIC”); Federation of American Hospitals (“FAH”); Financial Services Sector Coordinating Council (“FSSCC”); Information Technology Industry Council (“ITI”); LTSE Services, Inc. (“LTSE”); National Association of Manufacturers (“NAM”); National Defense Industrial Association (“NDIA”); Quest Diagnostics Incorporated (“Quest”); Rapid7, Inc. (“Rapid7”); Society for Corporate Governance (“SCG”); Securities Industry and Financial Markets Association (“SIFMA”); TransUnion; R Street Institute (“R Street”); U.S. Chamber of Commerce (“Chamber”).

companies.⁵¹ Some of these commenters objected specifically to the requirement in Item 1.05 to disclose whether remediation has occurred, stating that this information could assist threat actors in their targeting or invite further targeted attacks,⁵² while others more generally stated that the Item 1.05 disclosure would be overly detailed, such that it would give a road map to threat actors for planning attacks.⁵³ One commenter argued that the prospect of possibly having to file an Item 1.05 Form 8-K could chill threat information sharing within industries, because companies would fear that any cybersecurity risk information they share could later be used to question their disclosure decisions.⁵⁴

Some of the commenters that disagreed with the level of disclosure required by proposed Item 1.05 recommended that the Commission narrow the disclosure requirements of the rule. For example, one such commenter advised dropping the proposed requirement to disclose “when the incident was discovered,” arguing that this detail may cause confusion, particularly where an incident was detected some time ago but a significant aspect rendering it material surfaced only recently.⁵⁵ Another commenter opined that “whether the registrant has remediated or is currently remediating the incident” is duplicative of “whether it is ongoing,” so either of the two could be

⁵¹ See letters from ABA Committee on Federal Regulation of Securities (“ABA”); Aerospace Industries Association of America (“AIA”); Alliance for Automotive Innovation (“Auto Innovators”); AGA/INGAA; American Property Casualty Insurance Association (“APCIA”); BPI et al.; BSA; Business Roundtable; CBA; Chamber; Cellular Telecommunications and Internet Assoc. (“CTIA”); Cybersecurity Coalition; EEI; EIC; Empire State Realty Trust, Inc. (“Empire”); Enbridge Inc. (“Enbridge”); FSSCC; Internet Security Alliance; ITI; Microsoft Corporation (“Microsoft”); NDIA; PPG Industries, Inc. (“PPG”); PricewaterhouseCoopers LLP (“PWC”); Rapid7; R Street; SCG; SIFMA; U.S. Senator Rob Portman (“Sen. Portman”); Virtu Financial (“Virtu”).

⁵² See letters from ABA; AGA/INGAA; BPI et al.; Cybersecurity Coalition; Empire; Enbridge; PWC; SIFMA; SCG; Virtu.

⁵³ See letters from AGA/INGAA; BSA; EIC; ITI; PPG.

⁵⁴ See letter from Consumer Technology Association (“CTA”).

⁵⁵ See letter from Prof. Perullo.

eliminated.⁵⁶ One commenter contended that a materiality filter should be added to the details required by Item 1.05, such that companies would have to disclose only details that themselves are material, rather than immaterial details of a material incident.⁵⁷

By contrast, there were also commenters that recommended expanding the disclosure requirements in the proposed rule. In this regard, some commenters recommended requiring that registrants disclose asset losses, intellectual property losses, and the value of business lost due to the incident.⁵⁸ Other suggestions included requiring that incidents be quantified as to their severity and impact via standardized rating systems, and that registrants disclose how they became aware of the incident, as this may shed light on the effectiveness of a company's cybersecurity policies and procedures.⁵⁹ Additionally, commenters suggested banning trading by insiders during the time between the materiality determination and disclosure of the incident.⁶⁰

Commenters provided reactions to the application of Item 1.05 to incidents connected with third-party systems. A number of commenters contended that registrants should be exempt from having to disclose cybersecurity incidents in third-party systems they use because of their reduced control over such systems.⁶¹ Similarly, several commenters advocated for a safe harbor for information disclosed about third-party systems, given registrants' reduced visibility into such systems.⁶² A few commenters suggested a longer reporting timeframe for third-party

⁵⁶ See letter from ABA.

⁵⁷ See letter from ITI.

⁵⁸ See letters from Profs. Rajgopal & Sharpe; PWC.

⁵⁹ See letters from BitSight; Cloud Security Alliance ("CSA").

⁶⁰ See letter from Prof. Mitts.

⁶¹ See letters from ABA; AIA; APCIA; Business Roundtable; Cybersecurity Coalition; Chamber; EIC; FAH; ISA; ITI; NAM; NDIA; National Multifamily Housing Council and National Apartment Association ("NMHC"); Paylocity; SIFMA.

⁶² See letters from Chevron Corporation ("Chevron"); APCIA; BPI et al.; BIO; CSA; Financial Executive International's Committee on Corporate Reporting ("FEI"); ITI; ISA; NMHC; SIFMA.

incidents, because the registrant may be dependent on the third party for information (which may not be provided in a timely manner), and to avoid harm to other companies reliant on the same third party.⁶³ Commenters also recommended that Item 1.05 be phased in over a longer period of time with respect to third-party incidents, to give registrants time to develop information sharing processes with their third-party service providers.⁶⁴

Commenters also requested guidance or otherwise raised concerns where the proposed requirements might trigger disclosures by third-party service providers. A commenter requested clarity on whether an incident should be disclosed by the third-party service provider registrant that owns the affected system or the customer registrant that owns the affected information, or both.⁶⁵ And two commenters argued that third-party service providers should simply pass along information to their end customers, who would then make their own materiality determination and disclose accordingly; this should particularly be the case, a commenter said, where an attack on a third-party data center results in a data breach for an end customer but does not affect the services the data center provides.⁶⁶

The proposed timing of incident disclosure also received a significant level of public comment. For example, a few commenters said the level of detail required by Item 1.05 is impractical to produce in the allotted time.⁶⁷ Other commenters said that the proposed deadline would lead to the disclosure of tentative, unclear, or potentially inaccurate information that is not

⁶³ See letters from ABA; R Street.

⁶⁴ See letters from Business Roundtable; Deloitte & Touche LLP (“Deloitte”).

⁶⁵ See letter from Business Roundtable.

⁶⁶ See letters from BSA; ITI.

⁶⁷ See letters from ABA; NMHC; Quest.

decision-useful to investors,⁶⁸ resulting in the market mispricing the underlying securities.⁶⁹

Commenters also argued that Item 1.05 is qualitatively different from all other Form 8-K items in that the trigger for Item 1.05 is largely outside the company’s control.⁷⁰ Some commenters worried the proposed deadline would lead to disclosure of “false positives,” that is, incidents that appear material at first but later on with the emergence of more information turn out not to be material.⁷¹

Commenters suggested a range of alternative reporting deadlines for Item 1.05. A common suggestion was to modify the measurement date from the determination of materiality to another point in the lifecycle of the incident when the incident is no longer a threat to the registrant—commenters variously termed this as “containment,” “remediation,” “mitigation,” and comparable terms.⁷² One commenter recommended conditioning a reporting delay on the registrant being actively engaged in containing the incident and reasonably believing that containment can be completed in a timely manner.⁷³ Similarly, several commenters recommended that the rule allow for a delay in providing Item 1.05 disclosure based on a registrant’s assessment of the potential negative consequences of public disclosure, using a

⁶⁸ See letters from ABA; ACC; AIA; Auto Innovators; American Investment Council (“AIC”); BIO; Business Roundtable; CBA; Chamber; Confidentiality Coalition; CTIA; Davis Polk & Wardwell LLP (“Davis Polk”); Debevoise & Plimpton (“Debevoise”); Federated Hermes; FSSCC; Microsoft; NAM; Nasdaq Stock Market, LLC (“Nasdaq”); NDIA; Quest; SCG; TransUnion; Wilson Sonsini Goodrich & Rosati (“Wilson Sonsini”); Virtu.

⁶⁹ See letters from ABA; ACC; AIA; AIC; BIO; BPI et al.; Business Roundtable; Confidentiality Coalition; Davis Polk; ISA; Nasdaq; PPG; Quest; Rapid7; SCG; Sen. Portman; SIFMA; Virtu.

⁷⁰ See letters from CTIA; Debevoise; EIC; LTSE; New York City Bar Association (“NYC Bar”); Quest.

⁷¹ See letters from LTSE; PPG; SCG.

⁷² See letters from American Council of Life Insurers (“ACLI”); BCE Inc., Rogers Communications Inc., TELUS Corporation (“BCE”); BPI et al.; Business Roundtable; Chamber; CTA; Cybersecurity Coalition; Empire; FAH; Federated Hermes; FSSCC; ISA; ITI; NAM; Nasdaq; NDIA; NMHC; NYSE Group (“NYSE”); Quest; Rapid7; Sen. Portman; SCG; SIFMA; SM4RT Secure LLC (“SM4RT Secure”); TransUnion.

⁷³ See letter from Rapid7.

variety of measures they suggested.⁷⁴ Another suggestion was to replace the proposed deadline with an instruction to disclose material incidents “without unreasonable delay.”⁷⁵

Some commenters recommended instead increasing the number of days between the reporting trigger and the reporting deadline. A few commenters recommended adding one business day to make the deadline five business days;⁷⁶ one noted this would result in every registrant having at least a full calendar week to gather information and prepare the Form 8-K.⁷⁷ Another commenter recommended a deadline of 15 business days, along with a cure period to allow registrants a defined period of time to fix potential reporting mistakes.⁷⁸ A few commenters recommended a 30-day deadline,⁷⁹ with their choice of 30 days tending to be a proxy for some other factor, such as containment or remediation,⁸⁰ or state notification requirements.⁸¹

⁷⁴ See letters from BSA (suggesting a “tailored, balancing test”); EEI (advocating delay “to the extent... the registrant in good faith concludes that its disclosure will expose it or others to ongoing or additional risks of a cybersecurity incident”); EIC; Microsoft (requesting that companies be allowed to “manage the timing” of disclosure “when compelling conditions exist such that premature disclosure would result in greater harm to the company, its investors, or the national digital ecosystem”); Nareit and The Real Estate Roundtable (“Nareit”) (stating delay should be permitted where disclosure “would exacerbate injury to the company and/or its shareholders”); SIFMA (advocating a “‘responsible disclosure’ exception” that applies “where disclosure of a cyber incident or vulnerability could have a more damaging effect than delayed disclosure”); Wilson Sonsini (stating “the Commission should allow board members to decide to delay reporting if doing so could cause material harm to the company”).

⁷⁵ See letters from CTIA; National Restaurant Association (“NRA”).

⁷⁶ See letters from AIC; Debevoise; NYC Bar.

⁷⁷ See letter from AIC.

⁷⁸ See letter from R Street.

⁷⁹ See letters from APCIA; Hunton Andrews Kurth, LLP (“Hunton”); Rapid7.

⁸⁰ See letters from APCIA (“[w]e believe that permitting a registrant to delay the filing for a short period of time strikes an appropriate balance between timely disclosure to shareholders and an opportunity for a registrant to achieve the best resolution for itself and its shareholders”); Rapid7 (“[i]n Rapid7’s experience, the vast majority of incidents can be contained and mitigated within that time frame [30 days]”).

⁸¹ See letters from APCIA (“[a]llowing up to 30 days for disclosure would also bring the SEC’s proposal in line with data breach disclosure requirements at the state level”); Hunton (“[w]hile state data breach notification laws vary from state to state, 30 days from the cybersecurity incident is the earliest date any state requires that notification to affected persons be made”).

Several commenters recommended addressing the timing concerns by replacing current reporting on Form 8-K with periodic reporting on Forms 10-Q and 10-K, to allow additional time to assess an incident’s impact before reporting to markets.⁸² In this vein, one commenter likened cybersecurity incident disclosure to the disclosure of legal proceedings under Regulation S-K Item 103.⁸³

A few commenters recommended instead that the materiality trigger be replaced with a quantifiable trigger; for example, an incident implicating a specified percentage of revenue, or the costs of an incident exceeding a specified benchmark, could trigger disclosure.⁸⁴ Other commenters advocated for the disclosure trigger to be tied to any legal obligation that forces a registrant to notify persons outside the company.⁸⁵

Commenters also recommended a number of exceptions to the filing deadline. The most common recommendation was to include a provision allowing for delayed filing where there is an active law enforcement investigation or the disclosure otherwise implicates national security or public safety.⁸⁶ A representative comment in this vein advanced a provision whereby registrants may “delay reporting of a cybersecurity incident that is the subject of a *bona fide*

⁸² See letters from ABA; Davis Polk; Debevoise; LTSE; NYC Bar; Quest; SCG.

⁸³ See letter from Quest.

⁸⁴ See letters from BIO; Bitsight; EIC; Paylocity.

⁸⁵ See letters from ABA; Business Roundtable.

⁸⁶ See letters from ABA; ACC; ACLI; AGA/INGAA; AIA; AICPA; APCIA; Auto Innovators; Rep. Banks; BPI et al.; BIO; BSA; Business Roundtable; CBA; Chamber; Chevron; CII; CSA; CTA; CTIA; Cybersecurity Coalition; Debevoise; EEI; EIC; Empire; Enbridge; FAH; FedEx Corporation (“FedEx”); FEI; FSSCC; Global Privacy Alliance (“GPA”); Hunton; ISA; ITI; ITIF; Microsoft; NAM; Nareit; NASAA; NDIA; NMHC; NRA; NYC Bar; Prof. Perullo; Sen. Portman; PPG; PWC; Quest; R Street; Profs. Rajgopal & Sharpe; Rapid7; SCG; SIFMA; TransUnion; Virtu; USTelecom – The Broadband Association (“USTelecom”); U.S. Chamber of Commerce & various associations (“Chamber et al.”).

investigation by law enforcement,” because such “delay in reporting may not only facilitate such an investigation, it may be critical to its success.”⁸⁷

In calling for a law enforcement delay, associations for industries in critical sectors emphasized the national security implications of public cybersecurity incident disclosure. For example, one association explained that disclosure “may alert malicious actors that we have uncovered their illegal activities in circumstances where our defense and intelligence agencies wish to keep that information secret.”⁸⁸ Likewise, another association pointed out that, in its industry, companies “are likely to possess some of the nation’s most critical confidential information, including cybersecurity threat information furnished by government entities, such as the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the National Security Agency (NSA),” and therefore, disclosure may not be possible.⁸⁹

Commenters largely advocated for “a broad law enforcement exception that applies not only in the interest of national security but also when law enforcement believes disclosure will hinder their efforts to identify or capture the threat actor.”⁹⁰ Many commenters that responded to the Commission’s request for comment regarding a provision whereby the Attorney General determines that a delay is in the interest of national security indicated that such a provision should be more expansive and extend to other law enforcement authorities.⁹¹ One of these commenters questioned whether the Attorney General would opine on matters “that are under the ambit of other Federal agencies, such as the Department of Homeland Security, Department of

⁸⁷ See letter from Debevoise.

⁸⁸ See letter from AIA.

⁸⁹ See letter from EEI.

⁹⁰ See letter from ABA.

⁹¹ See letters from BPI et al.; CBA; CSA; Hunton; ITIF; SCG; Wilson Sonsini.

State and the Department of Defense.”⁹² Another commenter pointed out that “the Department of Justice is not the primary, or even the lead, organization in the Federal Government for cybersecurity response, rather the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency is often the first call that companies make,” while “[f]or defense contractors, the Department of Defense is likely to have the highest interest in the timing of an announcement.”⁹³ For the financial industry specifically, one suggestion was to permit a delay if the Federal Reserve, Federal Deposit Insurance Corporation, or Office of the Comptroller of the Currency finds that disclosure would compromise the safety or soundness of the financial institution or of the financial system as a whole.⁹⁴

Some commenters specifically urged that state law enforcement be included within any delay provision,⁹⁵ and one commenter appeared to contemplate inclusion of foreign law enforcement.⁹⁶ A few commenters advocated for a confidential reporting system, whereby a registrant would initially file a nonpublic report with the Commission while a law enforcement investigation is ongoing, and then unseal the report upon the investigation’s completion.⁹⁷

A number of commenters provided feedback regarding proposed Instruction 1, which would have directed registrants to make their materiality determination regarding an incident “as

⁹² See letter from Hunton. This commenter also questioned whether law enforcement would be inclined to provide a written determination, particularly within four business days, because in its experience with State data breach laws, “the relevant state and federal law enforcement agencies seldom (if ever) provide written instructions when the relevant exception comes into play.”

⁹³ See letter from Wilson Sonsini.

⁹⁴ See letter from BPI et al. Cf. letter from FSSCC.

⁹⁵ See, e.g., letter from ITIF.

⁹⁶ See letter from CBA (stating “the scope of the contemplated exemption is indefensibly narrow, particularly for registrants with operations outside of the United States . . . there should be an exemption to permit delayed disclosure upon the request of any competent national, state or local law enforcement authority”).

⁹⁷ See letters from CSA; Hunton; SCG. See also letter from LTSE (positing the Regulation SCI disclosure framework as a model for Item 1.05).

soon as reasonably practicable after discovery of the incident.” Several commenters recommended removing the instruction altogether as, in their view, it would place unnecessary pressure on companies to make premature determinations before they have sufficient information.⁹⁸ Other commenters stated that the instruction is too ambiguous for registrants to ascertain whether they have complied with it.⁹⁹ Conversely, one commenter advised the Commission not to provide further guidance on the meaning of “as soon as reasonably practicable,” explaining that doing so would interfere with each registrant’s individual assessment of what is practicable given its specific context, resulting in pressure to move more quickly than may be appropriate.¹⁰⁰ Another commenter likewise found that “as soon as reasonably practicable” is a “reasonable approach” that “provides public companies with the appropriate degree of flexibility to conduct a thorough assessment while ensuring that the markets get timely and relevant information.”¹⁰¹ One commenter recommended a safe harbor for actions and determinations made in good faith to satisfy Instruction 1 that later turn out to be mistaken.¹⁰²

In response to a request for comment in the Proposing Release, several commenters recommended registrants be permitted to furnish rather than file an Item 1.05 Form 8-K, so that filers of an Item 1.05 Form 8-K would not be subject to liability under Section 18 of the Exchange Act.¹⁰³ A significant number of commenters also endorsed the proposal to amend 17

⁹⁸ See letters from ABA; AGA/INGAA; Federated Hermes; ISA; Paylocity; Quest; SCG.

⁹⁹ See letter from Center for Audit Quality (“CAQ”); CSA; Institute of Internal Auditors (“IIA”); LTSE; NYC Bar.

¹⁰⁰ See letter from Cybersecurity Coalition.

¹⁰¹ See letter from NASAA.

¹⁰² See letter from Nasdaq.

¹⁰³ See letters from BPI et al.; Business Roundtable; Chevron; CSA; EEI; LTSE; NAM; SCG.

CFR 240.13a-11(c) (“Rule 13a-11(c)”) and 17 CFR 240.15d-11(c) (“Rule 15d-11(c)”) under the Exchange Act to include Item 1.05 in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) or 17 CFR 240.10b-5 (“Rule 10b-5”) under the Exchange Act.¹⁰⁴ Likewise, the proposal to amend General Instruction I.A.3.(b) of Form S-3 and General Instruction I.A.2 of Form SF-3 to provide that an untimely filing on Form 8-K regarding new Item 1.05 would not result in loss of Form S-3 or Form SF-3 eligibility received much support.¹⁰⁵

Finally, a number of commenters averred that Item 1.05 would conflict with other Federal and state cybersecurity reporting or other regulatory regimes. For example, one commenter stated Item 1.05 would counteract the goals of CIRCIA by requiring public disclosure of information the act would keep confidential, and went on to assert that CIRCIA was intended as the primary means for reporting incidents to the Federal Government.¹⁰⁶ Also related to CIRCIA, a number of commenters urged harmonization of the Commission’s proposal with forthcoming regulations expected from CISA pursuant to CIRCIA.¹⁰⁷ Several commenters alleged Item 1.05 would conflict with rules the Department of Health and Human Services (“HHS”) has adopted pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”) regarding the reporting of private health information breaches.¹⁰⁸ A few commenters likewise said Item 1.05 would conflict with the reporting regime set forth in Federal Communications Commission (“FCC”) regulations for breaches of customer proprietary network

¹⁰⁴ See letters from ABA; APCIA; BIO; Business Roundtable; Chevron; CTIA; Cybersecurity Coalition; Debevoise; EEI; LTSE; NYC Bar; PWC; SCG.

¹⁰⁵ See letters from ABA; APCIA; BIO; Business Roundtable; Chevron; CTIA; Cybersecurity Coalition; Debevoise; EEI; LTSE; NYC Bar; PWC; SCG.

¹⁰⁶ See letter from Sen. Portman.

¹⁰⁷ See letters from ACC; ACLI; APCIA; BPI et al.; BIO; Confidentiality Coalition; Chamber; CTA; CTIA; Cybersecurity Coalition; EIC; FEI; FSSCC; Insurance Coalition (“IC”); ISA; ITI; ITIF; Nareit; NAM; NRA; R Street; SCG; SIFMA; USTelecom.

¹⁰⁸ See letters from Chamber; Confidentiality Coalition; FAH; R Street.

information.¹⁰⁹ Conflicts were also alleged with regulations and programs of the Department of Defense (“DOD”),¹¹⁰ Department of Energy (“DOE”),¹¹¹ and Department of Homeland Security (“DHS”).¹¹² Commenters called for harmonization of Item 1.05 with regulations issued by Federal banking regulators,¹¹³ as well as with regulations of the Federal Trade Commission (“FTC”).¹¹⁴ Some commenters noted the potential interaction between the proposed rules and state laws.¹¹⁵ One commenter noted the McCarran-Ferguson Act, which provides that a state law preempts a Federal statute if the state law was enacted for the purpose of regulating the business of insurance and the Federal statute does not specifically relate to the business of insurance.¹¹⁶

3. Final Amendments

Having considered the comments, we remain convinced that investors need timely, standardized disclosure regarding cybersecurity incidents materially affecting registrants’ businesses, and that the existing regulatory landscape is not yielding consistent and informative disclosure of cybersecurity incidents from registrants.¹¹⁷ However, we are revising the proposal

¹⁰⁹ See letters from Chamber; CTIA; USTelecom.

¹¹⁰ See letter from Chamber et al.

¹¹¹ See letter from EEI.

¹¹² See letter from ACC. This letter additionally alleged conflicts with regulations of the Department of Energy, Transportation Security Agency, Department of Defense, and Environmental Protection Agency, but did not explain specifically where those conflicts lie.

¹¹³ See letters from FSSCC; Structured Finance Association (“SFA”); SIFMA.

¹¹⁴ See letters from BIO; CTIA.

¹¹⁵ See letters from IC (noting “[a]n important issue will be to ensure harmonized regulation between the federal government and the several states with proposed or preexisting cybersecurity regulations”); R Street (noting that state privacy laws “mandate reporting of incidents across very different timelines”); SIFMA (noting that “many state financial services and/or insurance regulators already require regulated entities certify cybersecurity compliance”).

¹¹⁶ See letter from IC.

¹¹⁷ As the Commission has previously stated, markets rely on timely dissemination of information to accurately and quickly value securities. *Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date*, Release No. 33-8400 (Mar. 16, 2004) [69 FR 15593 (Mar. 25, 2004)] (“Additional Form 8-K Disclosure Release”). Congress recognized that the ongoing dissemination of accurate information by issuers about

in two important respects in response to concerns raised by commenters. First, we are narrowing the amount of information required to be disclosed, to better balance investors' needs and registrants' cybersecurity posture. And second, we are providing for a delay for disclosures that would pose a substantial risk to national security or public safety, contingent on a written notification by the Attorney General, who may take into consideration other Federal or other law enforcement agencies' findings.

As described above, commenters' criticisms of Item 1.05 generally arose from two aspects of the proposal: (1) the scope of disclosure; and (2) the timing of disclosure. With respect to disclosure scope, we note in particular commenter concerns that the disclosure of certain details required by proposed Item 1.05 could exacerbate security threats, both for the registrants' systems and for systems in the same industry or beyond, and could chill threat information sharing within industries. We agree that a balancing of concerns consistent with our statutory authority is necessary in crafting Item 1.05 to avoid empowering threat actors with actionable information that could harm a registrant and its investors. However, we are not persuaded, as some commenters suggested,¹¹⁸ that we should forgo requiring disclosure of the existence of an incident while it is ongoing to avoid risks, such as the risk of tipping off threat actors. Some companies already disclose material cybersecurity incidents while they are ongoing and before they are fully remediated, but the timing, form, and substance of those disclosures are inconsistent. Several commenters indicated both that investors look for information regarding registrants' cybersecurity incidents and that current disclosure levels are

themselves and their securities is essential to the effective operation of the markets, and specifically recognized the importance of current reporting in this regard by requiring that “[e]ach issuer reporting under Section 13(a) or 15(d) … disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer … as the Commission determines … is necessary or useful for the protection of investors and in the public interest.” 15 U.S.C. 78m(l).

¹¹⁸ See *supra* note 50.

inadequate to their needs in making investment decisions.¹¹⁹ In addition, we note below in Section IV evidence showing that delayed reporting of cybersecurity incidents can result in mispricing of securities, and that such mispricing can be exploited by threat actors, employees, related third parties, and others through trades made before an incident becomes public.¹²⁰ Accordingly, we believe it is necessary to adopt a requirement for uniform current reporting of material cybersecurity incidents.

To that end, and to balance investors' needs with the concerns raised by commenters, we are streamlining Item 1.05 to focus the disclosure primarily on the impacts of a material cybersecurity incident, rather than on requiring details regarding the incident itself. The final rules will require the 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." We believe this formulation more precisely focuses the disclosure on what the company determines is the material impact of the incident, which may vary from incident to incident. The rule's inclusion of "financial condition and results of operations" is not exclusive; companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident.¹²¹ By way of illustration, harm to a company's reputation, customer or vendor relationships, or competitiveness may be examples of a material impact on the company. Similarly, the possibility of litigation or regulatory investigations or actions, including regulatory actions by

¹¹⁹ See letters from Better Markets; CalPERS; CII.

¹²⁰ See *infra* notes 413 and 462.

¹²¹ See also Proposing Release at 16596 (stating that "[a] materiality analysis is not a mechanical exercise" and not solely quantitative, but rather should take into consideration "all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors").

state and Federal Governmental authorities and non-U.S. authorities, may constitute a reasonably likely material impact on the registrant.

We are not adopting, as proposed, a requirement for disclosure regarding the incident’s remediation status, whether it is ongoing, and whether data were compromised. While some incidents may still necessitate, for example, discussion of data theft, asset loss, intellectual property loss, reputational damage, or business value loss, registrants will make those determinations as part of their materiality analyses. Further, we are adding an Instruction 4 to Item 1.05 to provide that a “registrant need not disclose specific or technical information about its planned response to the incident or its 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.” While the Commission provided this assurance in the Proposing Release,¹²² we agree with some commenters that codifying it in the Item 1.05 instructions should provide added clarity to registrants on the type of disclosure required by Item 1.05.

With respect to commenters’ questions concerning the application of Item 1.05 to incidents occurring on third-party systems, we are not exempting registrants from providing disclosures regarding cybersecurity incidents on third-party systems they use, nor are we providing a safe harbor for information disclosed about third-party systems. While we appreciate the commenters’ concerns about a registrant’s reduced control over such systems, we note the centrality of the materiality determination: whether an incident is material is not contingent on where the relevant electronic systems reside or who owns them. In other words, we do not believe a reasonable investor would view a significant breach of a registrant’s data as immaterial merely because the data were housed on a third-party system, especially as

¹²² *Id.* at 16595.

companies increasingly rely on third-party cloud services that may place their data out of their immediate control.¹²³ Instead, as discussed above, materiality turns on how a reasonable investor would consider the incident’s impact on the registrant.

Depending on the circumstances of an incident that occurs on a third-party system, disclosure may be required by both the service provider and the customer, or by one but not the other, or by neither. We appreciate that companies may have reduced visibility into third-party systems; registrants should disclose based on the information available to them. The final rules generally do not require that registrants conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with registrants’ disclosure controls and procedures. This is consistent with the Commission’s general rules regarding the disclosure of information that is difficult to obtain.¹²⁴

Turning to disclosure timing, we believe that the modifications from the proposed rules regarding the disclosures called for by Item 1.05 alleviate many of the concerns some commenters had regarding the proposed disclosure deadline of four business days from the materiality determination. Because the streamlined disclosure requirements we are adopting are focused on an incident’s basic identifying details and its material impact or reasonably likely material impact, the registrant should have the information required to be disclosed under this rule as part of conducting the materiality determination. For example, most organizations’ materiality analyses will include consideration of the financial impact of a cybersecurity

¹²³ See Deloitte, *Global Third-Party Risk Management Survey 2022*, at 15, available at <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-global-tprm-survey-report-2022.pdf> (discussing results of a global survey of 1,309 “senior leaders from a variety of organizations” indicating that “73% of respondents currently have a moderate to high level of dependence on [cloud-service providers]” and “[t]hat is expected to increase to 88% in the years ahead”).

¹²⁴ See 17 CFR 230.409 and 17 CFR 240.12b-21, which provide that information need only be disclosed insofar as it is known or reasonably available to the registrant. Accordingly, we are not providing additional time to comply with Item 1.05 as it relates to third-party incidents, as requested by some commenters.

incident, so information regarding the incident’s impact on the registrant’s financial condition and results of operations will likely have already been developed when Item 1.05 is triggered.¹²⁵ Thus, we believe that the four business day timeframe from the date of a materiality determination will be workable.

The reformulation of Item 1.05 also addresses the concern among commenters that the disclosure may be tentative and unclear, resulting in false positives and mispricing in the market. In the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered. The registrant will develop information after discovery until it is sufficient to facilitate a materiality analysis.¹²⁶ At that point, we believe investors are best served knowing, within four business days after the materiality determination, that the incident occurred and what led management to conclude the incident is material. While it is possible that occasionally there may be incidents that initially appear material but developments after the filing of the Item 1.05 Form 8-K reveal to be not material, the alternative of delaying disclosure beyond the four business day period after a materiality determination has the potential to lead to far more mispricing and will negatively impact investors making investment and voting decisions without the benefit of knowing that there is a material cybersecurity incident.

Commenters posited an array of alternative deadlines for the Item 1.05 Form 8-K, as recounted above. We are not persuaded by commenters’ arguments that disclosure should be delayed until companies mitigate, contain, remediate, or otherwise diminish the harm of the incident, because, as discussed above, Item 1.05 does not require disclosure of the types of

¹²⁵ To the extent any required information is not determined or is unavailable at the time of the required filing, Instruction 2 to Item 1.05, as adopted, directs the registrant to include a statement to this effect in the Form 8-K and then file a Form 8-K amendment containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available. See *infra* Section II.B.3.

¹²⁶ As discussed below, registrants should develop such information without unreasonable delay.

details that have the potential to be exploited by threat actors, but rather focuses on the incident’s material impact or reasonably likely material impact on the registrant. While there may be, as commenters noted, some residual risk of the disclosure of an incident’s existence tipping off threat actors, such risk is justified, in our view, by investors’ need for timely information, and similar risk already exists today with some companies’ current cybersecurity incident disclosure practices. We are also not persuaded that Item 1.05 is sufficiently different from other Form 8-K items such that deviating from the form’s four business day deadline following the relevant trigger would be indicated. While some commenters argued that Item 1.05 is qualitatively different from all other Form 8-K filings in that its trigger is largely outside the company’s control, we disagree because other Form 8-K items may also be triggered unexpectedly, such as Item 4.01 (Changes in Registrant’s Certifying Accountants) and Item 5.02 (Departure of Directors or Principal Officers). And as compared to those items, the information needed for Item 1.05 may be further along in development when the filing is triggered, whereas, for example, a company may have no advance warning that a principal officer is departing.

With respect to the five business day deadline suggested by a few commenters to allow registrants a full calendar week from the materiality determination to the disclosure, we note that in the majority of cases registrants will have had additional time leading up to the materiality determination, such that disclosure becoming due less than a week after discovery should be uncommon. More generally with respect to the various alternative timing suggestions, we observe that the Commission adopted the uniform four business day deadline in 2004 to simplify the previous bifurcated deadlines, and we find commenters have not offered any compelling

rationale to return to bifurcated deadlines.¹²⁷ Form 8-K provides for current reporting of events that tend to be material to investor decision-making, and we see no reason to render the reporting of Item 1.05 less current than other Form 8-K items.

In the Proposing Release, the Commission requested comment on whether to allow registrants to delay filing an Item 1.05 Form 8-K where the Attorney General determines that a delay is in the interest of national security.¹²⁸ In response to comments, we are adopting a delay provision in cases where disclosure poses a substantial risk to national security or public safety. Pursuant to Item 1.05(c), a registrant may delay making an Item 1.05 Form 8-K filing if the Attorney General determines that the disclosure poses a substantial risk to national security or public safety and notifies the Commission of such determination in writing.¹²⁹ Initially, disclosure may be delayed for a time period specified by the Attorney General, up to 30 days following the date when the disclosure was otherwise required to be provided. The delay may be extended for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing.

In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. We are

¹²⁷ See Additional Form 8-K Disclosure Release. See also *Proposed Rule: Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date*, Release No. 33-8106 (June 17, 2002) [67 FR 42914 (June 25, 2002)].

¹²⁸ Proposing Release at 16598.

¹²⁹ We note that the delay provision we are adopting does not relieve a company's obligations under Regulation FD or with respect to the securities laws' antifraud prohibitions that proscribe certain insider trading, including Exchange Act Section 10(b). Under Regulation FD, material nonpublic information disclosed to any investor, for example, through investor outreach activities, would be required to be disclosed publicly, subject to limited exceptions. See 17 CFR 243.100 *et seq.*

providing for the final additional delay period in recognition that, in extraordinary circumstances, national security concerns may justify additional delay beyond that warranted by public safety concerns, due to the relatively more critical nature of national security concerns. Beyond the final 60-day delay, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through Commission exemptive order.¹³⁰

We have consulted with the Department of Justice to establish an interagency communication process to allow for the Attorney General's determination to be communicated to the Commission in a timely manner. The Department of Justice will notify the affected registrant that communication to the Commission has been made, so that the registrant may delay filing its Form 8-K.

We agree with commenters that a delay is appropriate for the limited instances in which public disclosure of a cybersecurity incident may cause harm to national security or public safety. The final rules appropriately balance such security concerns against investors' informational needs. In particular, the provision's "substantial risk to national security or public safety" bases are sufficiently expansive to ensure that significant risks of harm from disclosure may be protected against, while also ensuring that investors are not denied timely access to material information.¹³¹ With respect to commenters who recommended that other Federal

¹³⁰ Any exercise of exemptive authority in these circumstances would need to meet all of the standards of Section 36 of the Exchange Act. Furthermore, Item 1.05 of Form 8-K in no way limits the Commission's general exemptive authority under Section 36.

¹³¹ The delay provision for substantial risk to national security or public safety is separate from Exchange Act Rule 0-6, which provides for the omission of information that has been classified by an appropriate department or agency of the Federal Government for the protection of the interest of national defense or foreign policy. If the information a registrant would otherwise disclose on an Item 1.05 Form 8-K or pursuant to Item 106 of Regulation S-K or Item 16K of Form 20-F is classified, the registrant should comply with Exchange Act Rule 0-6.

agencies and non-Federal law enforcement agencies also be permitted to trigger a delay or who argued that other agencies may be the primary organization in the Federal Government for the response, we note that the rule does not preclude any such agency from requesting that the Attorney General determine that the disclosure poses a substantial risk to national security or public safety and communicate that determination to the Commission. However, we believe that designating a single law enforcement agency as the Commission's point of contact on such delays is critical to ensuring that the rule is administrable.

Turning to other timing-related issues raised by commenters, we are not adopting commenters' suggestion to replace Item 1.05 with periodic reporting of material cybersecurity incidents on Forms 10-Q and 10-K because such an approach may result in significant variance as to when investors learn of material cybersecurity incidents. Based on when an incident occurs during a company's reporting cycle, the timing between the materiality determination and reporting on the next Form 10-Q or Form 10-K could vary from a matter of months to a matter of weeks or less. For example, if two companies experience a similar cybersecurity incident, but one determines the incident is material early during a quarterly period and the other makes such determination at the end of the quarterly period, commenters' suggested approach would have both companies report the incident around the same time despite the first company having determined the incident was material weeks or months sooner, which would result in a significant delay in this information being provided to investors. Such variance would therefore reduce comparability across registrants and may put certain registrants at a competitive disadvantage.

We also decline to use a quantifiable trigger for Item 1.05 because some cybersecurity incidents may be material yet not cross a particular financial threshold. We note above that the

material impact of an incident may encompass a range of harms, some quantitative and others qualitative. A lack of quantifiable harm does not necessarily mean an incident is not material. For example, an incident that results in significant reputational harm to a registrant may not be readily quantifiable and therefore may not cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material. Similarly, whereas a cybersecurity incident that results in the theft of information may not be deemed material based on quantitative financial measures alone, it may in fact be material given the impact to the registrant that results from the scope or nature of harm to individuals, customers, or others, and therefore may need to be disclosed.

In another change from the proposal, and to respond to commenters' concerns that the proposed "as soon as reasonably practicable" language in Instruction 1 could pressure companies to draw conclusions about incidents with insufficient information, we are revising the instruction to state that companies must make their materiality determinations "without unreasonable delay." As explained in the Proposing Release, the instruction was intended to address any concern that some registrants may delay making such a determination to avoid a disclosure obligation.¹³² We understand commenter concerns that the proposed instruction could result in undue pressure to make a materiality determination before a registrant has sufficient information to do so, and we recognize that a materiality determination necessitates an informed and deliberative process. We believe the revised language should alleviate this unintended consequence, while providing registrants notice that, though the determination need not be rushed prematurely, it also cannot be unreasonably delayed in an effort to avoid timely disclosure. For example, for incidents that

¹³² Proposing Release at 16596.

impact key systems and information, such as those the company considers its “crown jewels,”¹³³ as well as incidents involving unauthorized access to or exfiltration of large quantities of particularly important data, a company may not have complete information about the incident but may know enough about the incident to determine whether the incident was material. In other words, a company being unable to determine the full extent of an incident because of the nature of the incident or the company’s systems, or otherwise the need for continued investigation regarding the incident, should not delay the company from determining materiality. Similarly, if the materiality determination is to be made by a board committee, intentionally deferring the committee’s meeting on the materiality determination past the normal time it takes to convene its members would constitute unreasonable delay.¹³⁴ As another example, if a company were to revise existing incident response policies and procedures in order to support a delayed materiality determination for or delayed disclosure of an ongoing cybersecurity event, such as by extending the incident severity assessment deadlines, changing the criteria that would require reporting an incident to management or committees with responsibility for public disclosures, or introducing other steps to delay the determination or disclosure, that would constitute unreasonable delay. In light of the revision to Instruction 1, we find that a safe harbor, as suggested by some commenters, is unnecessary; adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance. Importantly, we remind registrants, as the Commission did in the Proposing Release, that

¹³³ See National Cybersecurity Alliance, *Identify Your “Crown Jewels”* (July 1, 2022), available at <https://staysafeonline.org/cybersecurity-for-business/identify-your-crown-jewels/> (explaining that “[c]rown jewels are the data without which your business would have difficulty operating and/or the information that could be a high-value target for cybercriminals”).

¹³⁴ We note that Form 8-K Item 1.05 does not specify whether the materiality determination should be performed by the board, a board committee, or one or more officers. The company may establish a policy tasking one or more persons to make the materiality determination. Companies should seek to provide those tasked with the materiality determination information sufficient to make disclosure decisions.

“[d]oubts as to the critical nature” of the relevant information “will be commonplace” and should “be resolved in favor of those the statute is designed to protect,” namely investors.¹³⁵

Revised Instruction 1 should also reassure registrants that they should continue sharing information with other companies or government actors about emerging threats. Such information sharing may not necessarily result in an Item 1.05 disclosure obligation. The obligation to file the Item 1.05 disclosure is triggered once a company has developed information regarding an incident sufficient to make a materiality determination, and a decision to share information with other companies or government actors does not in itself necessarily constitute a determination of materiality. A registrant may alert similarly situated companies as well as government actors immediately after discovering an incident and before determining materiality, so long as it does not unreasonably delay its internal processes for determining materiality.

As proposed, we are adding Item 1.05 to the list of Form 8-K items in General Instruction I.A.3.(b) of Form S-3 , so that the untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility.¹³⁶ We note the significant support from commenters regarding this proposal, and as noted in the Proposing Release, continue to believe that the consequences of the loss of Form S-3 eligibility would be unduly severe given the circumstances that will surround Item 1.05 disclosures. Likewise, as supported by many commenters, we are adopting as proposed amendments to Rules 13a-11(c) and 15d-11(c) under the Exchange Act to include new Item 1.05 in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act. This accords with the view the

¹³⁵ Proposing Release at 16596 (quoting *TSC Indus. v. Northway*, 426 U.S. at 448). The Court’s opinion in *TSC Indus.* has a nuanced discussion of the balance of considerations in setting a materiality standard. 426 U.S. at 448-450.

¹³⁶ Because of our decision to exempt asset-backed issuers from the new rules (*see infra* Section II.G.1), we are not amending Form SF-3.

Commission articulated in 2004 that the safe harbor is appropriate if the triggering event for the Form 8-K requires management to make a rapid materiality determination.¹³⁷

We decline to permit registrants to furnish rather than file the Item 1.05 Form 8-K, as suggested by some commenters. While we understand commenters' points that reducing liability may ease the burden on registrants, we believe that treating Item 1.05 disclosures as filed will help promote the accuracy and reliability of such disclosures for the benefit of investors. Of the existing Form 8-K items, only Items 2.02 (Results of Operations and Financial Condition) and 7.01 (Regulation FD Disclosure) are permitted to be furnished rather than filed. The Commission created exceptions for those two items to allay concerns that do not pertain here. Specifically, with respect to Item 2.02, the Commission was motivated by concerns that requiring the information to be filed would discourage registrants from proactively issuing earnings releases and similar disclosures.¹³⁸ Similarly, with respect to Item 7.01, the Commission decided to allow the disclosure to be furnished to address concerns that, if required to be filed, the disclosure could be construed as an admission of materiality, which might lead some registrants to avoid making proactive disclosure.¹³⁹ By contrast, Item 1.05 is not a voluntary disclosure, and it is by definition material because it is not triggered until the registrant determines the materiality of an incident. It is thus more akin to the Form 8-K items other than Items 2.02 and 7.01, in that it is a description of a material event that has occurred about which investors need adequate information. Therefore, the final rules require an Item 1.05 Form 8-K to be filed.

¹³⁷ Additional Form 8-K Disclosure Release at 15607.

¹³⁸ See *Conditions for Use of Non-GAAP Financial Measures*, Release No. 33-8176 (Jan. 22, 2003) [68 FR 4819 (Jan. 30, 2003)].

¹³⁹ See *Selective Disclosure and Insider Trading*, Release No. 33-7881 (Aug. 15, 2000) [65 FR 51715 (Aug. 24, 2000)].

We are not including a new rule to ban trading by insiders during the materiality determination time period, as suggested by some commenters. Those with a fiduciary duty or other relationship of trust and confidence are already prohibited from trading while in possession of material, nonpublic information.¹⁴⁰ And because we are adopting the four business days from materiality determination deadline, we agree with the point raised by some commenters that the risk of insider trading is low given the limited time period between experiencing a material incident and public disclosure. We also note that we recently adopted amendments to 17 CFR 240.10b5-1 (“Rule 10b5-1”) that added a certification condition for directors and officers wishing to avail themselves of the rule’s affirmative defense; specifically, if relying on the amended affirmative defense, directors and officers need to certify in writing, at the time they adopt the trading plan, that they are unaware of material nonpublic information about the issuer or its securities, and are adopting the plan in good faith and not as part of a plan or scheme to evade the insider trading prohibitions.¹⁴¹ Therefore, given the timing of the incident disclosure requirement as well as the recently adopted amendments to Rule 10b5-1, we do not find need for a new rule banning trading by insiders during the time period between the materiality determination and disclosure.

A number of commenters raised concerns about conflicts with other Federal laws and regulations. Of the Federal laws and regulations that we reviewed and commenters raised concerns with, we have identified one conflict, with the FCC’s notification rule for breaches of

¹⁴⁰ *United States v. O’Hagan*, 521 U.S. 642 (1997).

¹⁴¹ See *Insider Trading Arrangements and Related Disclosures*, Release No. 33-11138 (Dec. 14, 2022) [87 FR 80362 (Dec. 29, 2022)].

customer proprietary network information (“CPNI”).¹⁴² Of the remaining Federal laws and regulations noted by commenters as presenting conflicts, our view is that Item 1.05 neither directly conflicts with nor impedes the purposes of other such laws and regulations.

The FCC’s rule for notification in the event of breaches of CPNI requires covered entities to notify the United States Secret Service (“USSS”) and the Federal Bureau of Investigation (“FBI”) no later than seven business days after reasonable determination of a CPNI breach, and further directs the entities to refrain from notifying customers or disclosing the breach publicly until seven business days have passed following the notification to the USSS and FBI.¹⁴³ To accommodate registrants who are subject to this rule and may as a result face conflicting disclosure timelines,¹⁴⁴ we are adding paragraph (d) to Item 1.05 providing that such registrants may delay making a Form 8-K disclosure up to the seven business day period following notification to the USSS and FBI specified in the FCC rule,¹⁴⁵ with written notification to the Commission.¹⁴⁶

¹⁴² 47 CFR 64.2011. CPNI is defined in 47 CFR 222(h)(1) as: “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.”

¹⁴³ We note that the FCC recently proposed amending its rule; among other things, the proposal would eliminate the seven-business day waiting period, potentially eliminating the conflict. Federal Communications Commission, *Data Breach Reporting Requirements*, 88 FR 3953 (Jan. 23, 2023).

¹⁴⁴ Commission staff consulted with FCC staff about a potential delay provision to address any conflict between the FCC rule and the Form 8-K reporting requirements.

¹⁴⁵ The exception we are creating does not apply to 47 CFR 64.2011(b)(3), which provides that the USSS or FBI may direct the entity to further delay notification to customers or public disclosure beyond seven business days if such disclosure “would impede or compromise an ongoing or potential criminal investigation or national security.” If the USSS or FBI believes that disclosure would result in a substantial risk to national security or public safety, it may, as explained above, work with the Department of Justice to seek a delay of disclosure.

¹⁴⁶ Such notice should be provided through correspondence on EDGAR no later than the date when the disclosure required by Item 1.05 was otherwise required to be provided.

We also considered the conflicts commenters alleged with CIRCIA. Specifically, they stated that Item 1.05 is at odds with the goals of CIRCIA, and that it may conflict with forthcoming regulations from CISA. The confidential reporting system established by CIRCIA serves a different purpose from Item 1.05 and through different means; the former focuses on facilitating the Federal Government’s preparation for and rapid response to cybersecurity threats, while the latter focuses on providing material information about public companies to investors in a timely manner. While CISA has yet to propose regulations to implement CIRCIA, given the statutory authority, text, and legislative history of CIRCIA, it appears unlikely the regulations would affect the balance of material information available to investors about public companies, because the reporting regime CIRCIA establishes is confidential.¹⁴⁷ Nonetheless, the Commission participates in interagency working groups on cybersecurity regulatory implementation, and will continue to monitor developments in this area to determine if modification to Item 1.05 becomes appropriate in light of future developments.¹⁴⁸

We also considered the HIPAA-related conflict alleged by commenters, specifically with respect to HHS’s rule on Notification in the Case of Breach of Unsecured Protected Health Information. That rule provides, in the event of a breach of unsecured protected health information, for the covered entity to provide notification to affected individuals “without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.”¹⁴⁹ If the breach involves more than 500 residents of a state or jurisdiction, the rule directs the covered

¹⁴⁷ 6 U.S.C. 681e.

¹⁴⁸ Should a conflict arise in the future with CISA regulations or regulations of another Federal agency, the Commission can address such conflict via rulemaking or other action at that time.

¹⁴⁹ 45 CFR 164.404(b). The notification must describe the breach, the types of unsecured protected health information involved, steps the individuals should take to protect themselves, what the entity is doing to mitigate harm and remediate, and where the individuals can seek additional information. *Id.*

entity to also notify prominent media outlets within the same timeframe.¹⁵⁰ The rule further provides that if a company receives written notice from “a law enforcement official” requesting a delay and specifying the length of the delay, then the company “shall … delay such notification, notice, or posting for the time period specified by the official.”¹⁵¹

We do not view Form 8-K Item 1.05 as implicated by the HHS rule. Importantly, the HHS rule’s delay provision applies specifically to any “notification, notice, or posting required under this subpart,” or in other words notice to affected individuals, media, and the Secretary of HHS.¹⁵² Such notification focuses on the consequences of the breach for the affected individuals; for example, individuals must be told what types of protected health information were accessed, and what steps they should take to protect themselves from harm.¹⁵³ This is different from the disclosure required by Item 1.05, which focuses on the consequences for the company that are material to investors, and whose timing is tied not to discovery but to a materiality determination. The HHS rule does not expressly preclude the latter type of public disclosure, or other potential communications companies experiencing a breach may make. Therefore, we believe that a registrant subject to the HHS rule will not face a conflict in complying with Item 1.05.¹⁵⁴

We also considered the conflicts commenters alleged with regulations and programs of DOD, DOE, DHS, the Federal banking regulatory agencies, state insurance laws, and miscellaneous other Federal agencies or laws. We find that, while there may be some overlap of

¹⁵⁰ 45 CFR 164.406.

¹⁵¹ 45 CFR 164.412.

¹⁵² *Id.*

¹⁵³ 45 CFR 164.404(c).

¹⁵⁴ For the same reason, the Federal Trade Commission’s Health Breach Notification rule, which is similar to HHS’s rule, does not present a conflict either. *See* 16 CFR part 318.

subject matter, Item 1.05 neither conflicts with nor impedes the purpose of those regulations and programs.¹⁵⁵ We disagree with one commenter’s assertion that cybersecurity incident disclosure “falls squarely within the jurisdiction of state insurance commissioners” as state cybersecurity incident reporting regulations would not pertain to the “business of insurance” as courts have interpreted the McCarran-Ferguson Act, and the commenter did not note any particular state insurance laws that would present a conflict.¹⁵⁶ With respect to Federal banking regulatory agencies specifically, we note that, in the event they believe that the disclosure of a material cybersecurity incident would threaten the health of the financial system in such a way that results in a substantial risk to national security or public safety, they may, as explained above, work with the Department of Justice to seek to delay disclosure.

It would not be practical to further harmonize Item 1.05 with other agencies’ cybersecurity incident reporting regulations, as one commenter suggested,¹⁵⁷ because Item 1.05 serves a different purpose—it is focused on the needs of investors, rather than the needs of regulatory agencies, affected individuals, or the like. With respect to state insurance and privacy laws, commenters did not provide any evidence sufficient to alter the Commission’s finding in the Proposing Release that, to the extent that Item 1.05 would require disclosure in a situation where state law would excuse or delay notification, we consider prompt reporting of material cybersecurity incidents to investors critical to investor protection and well-functioning, orderly, and efficient markets.

¹⁵⁵ For example, one commenter alleged conflicts with DHS’s Chemical Facilities Anti-Terrorism Standards program (“CFATS”) and with the Maritime Transportation Security Act (“MTSA”). *See letter from American Chemistry Council.* Both CFATS and MTSA provide for the protection of certain sensitive information, but neither is implicated by cybersecurity incident disclosure to the Commission.

¹⁵⁶ *See, e.g., SEC v. National Sec., Inc.*, 393 U.S. 453 (1969).

¹⁵⁷ *See letter from BIO.*

B. Disclosures about Cybersecurity Incidents in Periodic Reports

1. Proposed Amendments

The Commission proposed to add new Item 106 to Regulation S-K to, among other things, require updated cybersecurity disclosure in periodic reports. If a registrant previously provided disclosure regarding one or more cybersecurity incidents pursuant to Item 1.05 of Form 8-K, proposed 17 CFR 229.106(d)(1) (Regulation S-K “Item 106(d)(1)”) would require such registrant to disclose “any material changes, additions, or updates” on the registrant’s quarterly report on Form 10-Q or annual report on Form 10-K.¹⁵⁸ In addition, proposed Item 106(d)(1) would require disclosure of the following information:

- Any material effect of the incident on the registrant’s operations and financial condition;
- Any potential material future impacts on the registrant’s operations and financial condition;
- Whether the registrant has remediated or is currently remediating the incident; and
- Any changes in the registrant’s policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.¹⁵⁹

The Commission explained that it paired current reporting under Item 1.05 of Form 8-K with periodic reporting under 17 CFR 229.106(d) (Regulation S-K “Item 106(d)”) to balance investors’ need for timely disclosure with their need for complete disclosure.¹⁶⁰ When an Item 1.05 Form 8-K becomes due, the Commission noted, a registrant may not possess complete

¹⁵⁸ Proposing Release at 16598.

¹⁵⁹ *Id.*

¹⁶⁰ *Id.*

information about the material cybersecurity incident. Accordingly, under the proposed rules, a registrant would provide the information known at the time of the Form 8-K filing and follow up in its periodic reports with more complete information as it becomes available, along with any updates to previously disclosed information.

The Commission also proposed 17 CFR 229.106(d)(2) (Regulation S-K “Item 106(d)(2)”) to require disclosure in a registrant’s next periodic report when, to the extent known to management, a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate.¹⁶¹ The Proposing Release explained that this requirement may be triggered where, for example, a threat actor engages in a number of smaller but continuous related cyberattacks against the same company and collectively they become material.¹⁶² Item 106(d)(2) would require disclosure of essentially the same information required in proposed Item 1.05 of Form 8-K, as follows:

- A general description of when the incidents were discovered and whether they are ongoing;
- A brief description of the nature and scope of the incidents;
- Whether any data were stolen or altered in connection with the incidents;
- The effect of the incidents on the registrant’s operations; and
- Whether the registrant has remediated or is currently remediating the incidents.¹⁶³

¹⁶¹ *Id.* at 16599.

¹⁶² *Id.*

¹⁶³ *Id.* at 16619-16620.

2. Comments

Reaction among commenters to proposed Item 106(d)(1) was mixed. Some wrote in support, noting that updated incident disclosure is needed to avoid previously disclosed information becoming stale and misleading as more information becomes available, and saying that updates help investors assess the efficacy of companies' cybersecurity procedures.¹⁶⁴ Others took issue with specific aspects of the proposed rule. For example, some commenters stated that the proposed requirement to disclose "any potential material future impacts" is vague and difficult to apply, and urged removing or revising it.¹⁶⁵ Similarly, other commenters said that registrants should not be required to describe progress on remediation, noting that such information could open them up to more attacks.¹⁶⁶ In the same vein, one commenter suggested that no updates be required until remediation is sufficiently complete.¹⁶⁷ One commenter said the requirement to disclose changes in policies and procedures is unnecessary and overly broad,¹⁶⁸ and another commenter said the requirement should be narrowed to "material changes."¹⁶⁹

More generally, commenters sought clarification on how to differentiate instances where updates should be included in periodic reports from instances where updates should be filed on Form 8-K; they found the guidance in the Proposing Release on this point "unclear."¹⁷⁰ And one

¹⁶⁴ See letters from AICPA; Crindata; R Street. *See also* IAC Recommendation.

¹⁶⁵ See letters from EEI; Prof. Perullo; PWC; SCG.

¹⁶⁶ See letters from BCE; BPI et al.; Enbridge. *See also* letter from EEI (suggesting narrowing the rule to "material remediation," and delaying such disclosure until remediation is complete).

¹⁶⁷ See letter from EEI.

¹⁶⁸ See letter from Prof. Perullo.

¹⁶⁹ See letter from EEI.

¹⁷⁰ See letter from PWC; *accord* letter from Deloitte. The Proposing Release stated: "Notwithstanding proposed Item 106(d)(1), there may be situations where a registrant would need to file an amended Form 8-K to correct disclosure from the initial Item 1.05 Form 8-K, such as where that disclosure becomes inaccurate or materially misleading as a result of subsequent developments regarding the incident. For example, if the impact of the incident is determined after the initial Item 1.05 Form 8-K filing to be significantly more severe than previously disclosed, an amended Form 8-K may be required." Proposing Release at 16598.

commenter argued that, regardless of where the update is filed, the incremental availability of information would make it difficult for companies to determine when the update requirement is triggered.¹⁷¹

With respect to proposed Item 106(d)(2), a large number of commenters expressed concern about the aggregation requirement, saying, for example, that companies experience too many events to realistically communicate internally upward to senior management, and that retaining and analyzing data on past events would be too costly.¹⁷² A number of other commenters relatedly said that, for the aggregation requirement to be workable, companies need more guidance on the nature, timeframe, and breadth of incidents that should be collated.¹⁷³ In this regard, one supporter of the requirement explained in its request for additional guidance that “cybersecurity incidents are so unfortunately common that a strict reading of this section could cause overreporting to the point that it is meaningless for shareholders.”¹⁷⁴

Some commenters suggested revising the rule to cover only “related” incidents.¹⁷⁵ Possible definitions offered for “related” incidents included those “performed by the same malicious actor or that exploited the same vulnerability,”¹⁷⁶ and those resulting from “attacks on the same systems, processes or controls of a registrant over a specified period of time.”¹⁷⁷ Suggestions for limiting the time period over which aggregation should occur included the

¹⁷¹ See letter from Quest.

¹⁷² See letters from ABA; ACLI; AIA; Business Roundtable; EEI; Enbridge; Ernst & Young LLP (“E&Y”); FAH; FedEx; Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies (“FDD”); GPA; Hunton; ITI; ISA; LTSE; Microsoft; Nareit; NAM; NDIA; NRA; Prof. Perullo; SCG; SIFMA.

¹⁷³ See letters from ACC; APCIA; BDO USA, LLP (“BDO”); BPI et al.; CAQ; Chamber; Chevron; Deloitte; EIC; FEI; M. Barragan; PWC; R Street.; TransUnion.

¹⁷⁴ See letter from R Street.

¹⁷⁵ See letters from ABA; APCIA; EEI; E&Y; PWC.

¹⁷⁶ See letter from ABA.

¹⁷⁷ See letter from E&Y.

preceding one year,¹⁷⁸ and the preceding two years.¹⁷⁹ One commenter requested the Commission clarify that a company’s Item 106(d)(2) disclosure need describe only the aggregate material impact of the incidents, rather than describing each incident individually; the commenter was concerned with threat actors becoming informed of a company’s vulnerabilities through overly detailed disclosure.¹⁸⁰ Another commenter suggested granting registrants additional time to come into compliance with Item 106(d)(2) after Commission adoption, so that they can develop system functionality to retain details about immaterial incidents.¹⁸¹

Commenters also wrote in support of the aggregation requirement.¹⁸² One of these commenters stated that aggregation is needed especially where an advanced persistent threat actor¹⁸³ seeks to exfiltrate data or intellectual property over time.¹⁸⁴

3. Final Amendments

In response to comments, we are not adopting proposed Item 106(d)(1) and instead are adopting a new instruction to clarify that updated incident disclosure must be provided in a Form 8-K amendment. Specifically, we are revising proposed Instruction 2 to Item 1.05 of Form 8-K to direct the registrant to include in its Item 1.05 Form 8-K a statement identifying any

¹⁷⁸ See letter from APCIA.

¹⁷⁹ See letter from EEI.

¹⁸⁰ See letter from AGA/INGAA.

¹⁸¹ See letter from Deloitte.

¹⁸² See letters from CII; CSA; R Street; NASAA.

¹⁸³ The National Institute of Standards and Technology explains that an advanced persistent threat “is an adversary or adversarial group that possesses the expertise and resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. The APT objectives include establishing a foothold within the infrastructure of targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, function, program, or organization; or positioning itself to carry out these objectives in the future. The APT pursues its objectives repeatedly over an extended period, adapts to defenders’ efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives.” National Institute of Standards and Technology, *NIST Special Publication 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information* (Feb. 2021), at 2.

¹⁸⁴ See letter from CSA.

information called for in Item 1.05(a) that is not determined or is unavailable at the time of the required filing and then file an amendment to its Form 8-K containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available. This change mitigates commenters' concerns with Item 106(d)(1). In particular, under the final rules, companies will not have to distinguish whether information regarding a material cybersecurity incident that was not determined or was unavailable at the time of the initial Form 8-K filing should be included on current reports or periodic reports, as the reporting would be in an amended Form 8-K; details that commenters suggested raised security concerns, such as remediation status, are not required; and concerns that the proposed rule was vague or overbroad have been addressed by narrowing the required disclosure to the information required by Item 1.05(a). We also believe that use of a Form 8-K amendment rather than a periodic report will allow investors to more quickly identify updates regarding incidents that previously were disclosed.

We appreciate that new information on a reported cybersecurity incident may surface only in pieces; the final rules, however, do not require updated reporting for *all* new information. Rather, Instruction 2 to Item 1.05 directs companies to file an amended Form 8-K with respect to any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing. Other than with respect to such previously undetermined or unavailable information, the final rules do not separately create or otherwise affect a registrant's duty to update its prior statements. We remind registrants, however, that they may have a duty to correct prior disclosure that the registrant determines was untrue (or omitted a material fact

necessary to make the disclosure not misleading) at the time it was made¹⁸⁵ (for example, if the registrant subsequently discovers contradictory information that existed at the time of the initial disclosure), or a duty to update disclosure that becomes materially inaccurate after it is made¹⁸⁶ (for example, when the original statement is still being relied on by reasonable investors). Registrants should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.¹⁸⁷

We are not adopting proposed Item 106(d)(2), in response to concerns that the proposed aggregation requirement was vague or difficult to apply. We are persuaded by commenters that the proposed requirement might be difficult to differentiate from Item 1.05 disclosure, or by contrast, could result in the need for extensive internal controls and procedures to monitor all immaterial events to determine whether they have become collectively material. The intent of the proposed requirement was to capture the material impacts of related incidents, and prevent the avoidance of incident disclosure through disaggregation of such related events. However, upon further reflection, and after review of comments, we believe that the proposed requirement is not necessary based on the scope of Item 1.05.

To that end, we emphasize that the term “cybersecurity incident” as used in the final rules is to be construed broadly, as the Commission stated in the Proposing Release.¹⁸⁸ The definition

¹⁸⁵ See *Backman v. Polaroid Corp.*, 910 F.2d 10, 16-17 (1st Cir. 1990) (en banc) (finding that the duty to correct applies “if a disclosure is in fact misleading when made, and the speaker thereafter learns of this”).

¹⁸⁶ See *id.* at 17 (describing the duty to update as potentially applying “if a prior disclosure ‘becomes materially misleading in light of subsequent events’” (quoting *Greenfield v. Heublein, Inc.*, 742 F.2d 751, 758 (3d Cir. 1984))). But see *Higginbotham v. Baxter Intern., Inc.*, 495 F.3d 753, 760 (7th Cir. 2007) (rejecting duty to update before next quarterly report); *Gallagher v. Abbott Laboratories*, 269 F.3d 806, 808-11 (7th Cir. 2001) (explaining that securities laws do not require continuous disclosure).

¹⁸⁷ Relatedly, registrants should be aware of the requirement under Item 106(b)(2) of Regulation S-K to describe “[w]hether any risks from cybersecurity threats, *including as a result of any previous cybersecurity incidents*, have materially affected or are reasonably likely to materially affect the registrant” (emphasis added). See *infra* Section II.C.1.c.

¹⁸⁸ Proposing Release at 16601.

of “cybersecurity incident” we are adopting extends to “a series of related unauthorized occurrences.”¹⁸⁹ This reflects that cyberattacks sometimes compound over time, rather than present as a discrete event. Accordingly, when a company finds that it has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact could be parceled among the multiple intrusions to render each by itself immaterial. One example was provided in the Proposing Release: the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material.¹⁹⁰ Another example is a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company’s business materially.

C. Disclosure of a Registrant’s Risk Management, Strategy and Governance Regarding Cybersecurity Risks

1. Risk Management and Strategy

a. Proposed Amendments

The Commission proposed to add 17 CFR 229.106(b) (Regulation S-K “Item 106(b)”) to require registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy in their annual reports. The Commission noted the Division of Corporation Finance staff’s experience that most registrants disclosing a cybersecurity incident do not describe their cybersecurity risk oversight or any related policies and procedures, even though companies typically address significant risks by developing risk

¹⁸⁹ See *infra* Section II.C.3.

¹⁹⁰ Proposing Release at 16599.

management systems that often include written policies and procedures.¹⁹¹

Proposed Item 106(b) would require a description of the registrant's policies and procedures, if any, for the identification and management of cybersecurity threats, including, but not limited to: operational risk (*i.e.*, disruption of business operations); intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk. As proposed, registrants would be required to include a discussion, as applicable, of:

- Whether the registrant has a cybersecurity risk assessment program and if so, a description of the program ((b)(1));
- Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program ((b)(2));
- Whether the registrant has policies and procedures to oversee, identify, and mitigate the cybersecurity risks associated with its use of any third-party service provider (including, but not limited to, those providers that have access to the registrant's customer and employee data), including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers ((b)(3));
- Whether the registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents ((b)(4));
- Whether the registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident ((b)(5));

¹⁹¹ *Id.*

- Whether previous cybersecurity incidents have informed changes in the registrant’s governance, policies and procedures, or technologies ((b)(6));
- Whether cybersecurity related risk and incidents have affected or are reasonably likely to affect the registrant’s results of operations or financial condition and if so, how ((b)(7)); and
- Whether cybersecurity risks are considered as part of the registrant’s business strategy, financial planning, and capital allocation and if so, how ((b)(8)).¹⁹²

The Commission anticipated that proposed Item 106(b) would benefit investors by requiring more consistent disclosure of registrants’ strategies and actions to manage cybersecurity risks.¹⁹³ Such risks, the Commission observed, can affect registrants’ business strategy, financial outlook, and financial planning, as companies increasingly rely on information technology, collection of data, and use of digital payments as critical components of their businesses.¹⁹⁴

The Commission noted that the significant number of cybersecurity incidents pertaining to third-party service providers prompted the proposal to require disclosure of registrants’ selection and oversight of third-party entities.¹⁹⁵ The Commission also proposed requiring discussion of how prior cybersecurity incidents have affected or are reasonably likely to affect the registrant, because such disclosure would equip investors to better comprehend the level of cybersecurity risk the company faces and assess the company’s preparedness regarding such

¹⁹² *Id.* at 16599-16600.

¹⁹³ *Id.* at 16599.

¹⁹⁴ *Id.*

¹⁹⁵ *Id.*

risk.¹⁹⁶

b. Comments

Many commenters supported proposed Item 106(b) for requiring information that is vital to investors as they assess companies' risk profiles and make investment decisions.¹⁹⁷ One said cybersecurity disclosures now are "scattered and unpredictable" rather than "uniform," which "diminishes their effectiveness."¹⁹⁸ Similarly, another found that current disclosures "do not provide investors with the information necessary to evaluate whether companies have adequate governance structures and measures in place to deal with cybersecurity challenges."¹⁹⁹ The IAC recommended extending the proposed Item 106(b) disclosure requirements (as well as the proposed Item 106(c) disclosure requirements) to registration statements, stating that "pre-IPO companies may face heightened [cybersecurity] risks."²⁰⁰

By contrast, a number of commenters opposed proposed Item 106(b). In particular, they commented that much of the proposed Item 106(b) disclosure could increase a company's vulnerability to cyberattacks; they expressed particular concern regarding the potential harms from disclosures about whether cybersecurity policies are in place, incident response processes and techniques, previous incidents and what changes they spurred, and third-party service providers.²⁰¹ Another criticism was that proposed Item 106(b) would effectively force companies

¹⁹⁶ *Id.*

¹⁹⁷ See letters of AICPA; BuildingCyberSecurity.org ("BCS"); Better Markets; Bitsight; Blue Lava, Inc. ("Blue Lava"); CalPERS; ITIF; National Association of Corporate Directors ("NACD"); NASAA; PWC; PRI; R Street; SecurityScorecard; Tenable Holdings Inc. ("Tenable"). *See also* IAC Recommendation.

¹⁹⁸ See letter from Better Markets.

¹⁹⁹ See letter from PRI.

²⁰⁰ See IAC Recommendation.

²⁰¹ See letters from ABA; ACLI; APCIA; BIO; BPI et al.; Business Roundtable; Chamber; CSA; CTIA; EIC; Enbridge; FAH; Federated Hermes; GPA; ITI; ISA; Nareit; NAM; NMHC; NRA; National Retail Federation ("NRF"); SIFMA; Sen. Portman; TechNet; TransUnion; USTelecom; Virtu.

to model their cybersecurity policies on the rule’s disclosure elements, rather than the practices best suited to each company’s context.²⁰² One commenter saw proposed Item 106(b) as counteracting the streamlining accomplished in the Commission’s 2020 release modernizing Regulation S-K.²⁰³

Some commenters offered suggestions to narrow proposed Item 106(b) to address their concerns. On proposed paragraph (b)(1), one commenter recommended allowing a registrant to forgo describing its risk assessment program if it confirms that it “uses best practices and standards” to identify and protect against cybersecurity risks and detect and respond to such events.²⁰⁴ On proposed paragraph (b)(3), a few commenters said that registrants should be required to disclose only high-level information relating to third parties, such as confirmation that policies and procedures are appropriately applied to third-party selection and oversight, and should not have to identify the third parties or discuss the underlying mechanisms, controls, and contractual requirements.²⁰⁵

Some commenters opposed proposed paragraph (b)(6)’s requirement to discuss whether “previous cybersecurity incidents informed changes in the registrant’s governance, policies and procedures, or technologies” entirely, stating it would undermine a registrant’s cybersecurity.²⁰⁶ One commenter recommended the proposed (b)(6) disclosure be required only at a high level, without specific details,²⁰⁷ while two commenters appeared to propose only requiring disclosure

²⁰² See letters from BPI et al.; Chamber; EIC; Nareit; NRF; NYSE; SCG; SIFMA; Virtu.

²⁰³ See letter from Nasdaq (citing *Modernization of Regulation S-K Items 101, 103, and 105*, Release No. 33-10825 (Aug. 26, 2020) [85 FR 63726 (Oct. 8, 2020)]).

²⁰⁴ See letter from Cybersecurity Coalition.

²⁰⁵ See letters from BPI et al.; Chamber; SIFMA. Other commenters supported the level of detail required in (b)(3). See letters from AICPA; PRI.

²⁰⁶ See letters from ITI; SCG; Tenable.

²⁰⁷ See letter from Cybersecurity Coalition.

as it pertains to previous material incidents.²⁰⁸ Commenters suggested a materiality filter for proposed paragraph (b)(7)'s requirement to discuss whether "cybersecurity-related risks and previous cybersecurity-related incidents have affected or are reasonably likely to affect the registrant's strategy, business model, results of operations, or financial condition and if so, how," so that the requirement would apply only where a registrant has been materially affected or is reasonably likely to be materially affected.²⁰⁹

More broadly, one commenter recommended replacing the rule's references to "policies and procedures" with "strategy and programs," because in the commenter's experience companies may not codify their cybersecurity strategy in the same way they codify other compliance policies and procedures.²¹⁰ One commenter also suggested offering companies the choice to place the proposed Item 106(b) disclosures in either the Form 10-K or the proxy statement.²¹¹

Several commenters supported requiring registrants that lack cybersecurity policies and procedures to explicitly say so, commenting, for example, that "investors should not be left to intuit the meaning of a company's silence in its disclosures."²¹² One commenter further stated that registrants should be required to explain why they have not adopted cybersecurity policies and procedures.²¹³ By contrast, two commenters opposed requiring registrants that lack

²⁰⁸ See letters from AGA/INGA; American Public Gas Association ("APGA").

²⁰⁹ See letter from PWC.

²¹⁰ See letter from Prof. Perullo.

²¹¹ See letter from Nasdaq.

²¹² See letters from Blue Lava; CSA; Cybersecurity Coalition; ITI; NASAA; Prof. Perullo; Tenable. The quoted language is from NASAA's letter. See also IAC Recommendation (recommending "that issuers that have not developed any cybersecurity policies or procedures be required to make a statement to that effect" because "the vast majority of investors . . . would view the complete absence of cybersecurity risk governance as overwhelmingly material to investment decision-making").

²¹³ See letter from NASAA.

cybersecurity policies and procedures to explicitly say so,²¹⁴ with one commenter saying that “a threat actor may target registrants they perceive to have unsophisticated cybersecurity programs,”²¹⁵ and the other commenter saying “it is highly unlikely that any SEC registrants would not have ‘established any cybersecurity policies and procedures.’”²¹⁶

In response to the Commission’s request for comment about whether to require a registrant to specify whether any cybersecurity assessor, consultant, auditor, or other service provider that it relies on is through an internal function or through an external third-party service provider, several commenters opposed the idea as not useful, with one saying that “a significant majority—possibly the entirety—of SEC registrants” rely on third-party service providers for some portion of their cybersecurity.²¹⁷ Conversely, another commenter supported the third-party specification, and suggested requiring registrants to name the third parties, as over time, this would create more transparency in whether breaches correlate with specific third parties.²¹⁸

Commenters also offered a range of recommended additions to the rule. One commenter recommended modifying proposed paragraph (b)(1) to require registrants to specify whether their cybersecurity programs assess risks continuously or periodically, arguing the latter approach leaves companies more exposed.²¹⁹ The same commenter suggested paragraph (b)(2) require “a description of the class of services and solutions” provided by third parties.²²⁰

²¹⁴ See letters from EIC; IIA.

²¹⁵ See letter from EIC.

²¹⁶ See letter from IIA.

²¹⁷ See letters from BCS; Chevron; EIC; IIA; Prof. Perullo. The quoted language is from the letter of IIA.

²¹⁸ See letter from Blue Lava.

²¹⁹ See letter from Tenable.

²²⁰ *Id.*

A few commenters recommended that we direct registrants to quantify their cybersecurity risk exposure through independent risk assessments.²²¹ Similarly, one commenter urged us to require registrants to explain how they quantify their cybersecurity risk,²²² while another said we should set out quantifiable metrics against which companies measure their cybersecurity systems, though it did not specify what these metrics should be.²²³ Two commenters suggested that we require companies to disclose whether their cybersecurity programs have been audited by a third party.²²⁴ And one commenter recommended that we require registrants to disclose whether they use the cybersecurity framework of the National Institute of Standards and Technology (“NIST”), to ease comparison of registrant risk profiles.²²⁵

c. Final Amendments

We continue to believe that investors need information on registrants’ cybersecurity risk management and strategy, and that uniform, comparable, easy to locate disclosure will not emerge absent new rules. Commenters raised concerns with proposed Item 106(b)’s security implications and what they saw as its prescriptiveness. We agree that extensive public disclosure on how a company plans for, defends against, and responds to cyberattacks has the potential to advantage threat actors. Similarly, we acknowledge commenters’ concerns that the final rule could unintentionally affect a registrant’s risk management and strategy decision-making. In response to those comments, we confirm that the purpose of the rules is, and was at proposal, to inform investors, not to influence whether and how companies manage their cybersecurity risk.

²²¹ See letters from BitSight; Kovrr Risk Modeling Ltd.; SecurityScorecard.

²²² See letter from Safe Security.

²²³ See letter from FDD.

²²⁴ See letters from BCS; Better Markets.

²²⁵ See letter from SandboxAQ. This commenter also recommended registrants be required to disclose whether they use post-quantum cryptography as part of their risk mitigation efforts.

Additionally, to respond to commenters' concerns about security, the final rules eliminate or narrow certain elements from proposed Item 106(b). We believe the resulting rule requires disclosure of information material to the investment decisions of investors, in a way that is comparable and easy to locate, while steering clear of security sensitive details.

As adopted, 17 CFR 229.106(b)(1) (Regulation S-K "Item 106(b)(1)") requires a description of "the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes." We believe this revised formulation of the rule should help avoid levels of detail that may go beyond information that is material to investors and address commenters' concerns that those details could increase a company's vulnerability to cyberattack. We have also substituted the term "processes" for the proposed "policies and procedures" to avoid requiring disclosure of the kinds of operational details that could be weaponized by threat actors, and because the term "processes" more fully compasses registrants' cybersecurity practices than "policies and procedures," which suggest formal codification.²²⁶ We still expect the disclosure to allow investors to ascertain a registrant's cybersecurity practices, such as whether they have a risk assessment program in place, with sufficient detail for investors to understand the registrant's cybersecurity risk profile. The shift to "processes" also obviates the question of whether to require companies that do not have written policies and procedures to disclose that fact. We believe that, to the extent a company discloses that it faces a material

²²⁶ See letter from Prof. Perullo (distinguishing the formality of "policies and procedures" from the informality of "strategy or program"). We have adopted "processes" in place of the commenter's suggestion of "strategy or program" because "processes" is broader and commonly understood. We decline the suggestion from another commenter to allow registrants to avoid this disclosure altogether by confirming they adhere to "best practices and standards," because there is no single set of widely accepted best practices and standards, and industry practices may evolve. See letter from Cybersecurity Coalition.

cybersecurity risk in connection with its overall disclosures of material risks,²²⁷ an investor can ascertain whether such risks have resulted in the adoption of processes to assess, identify, and manage material cybersecurity risks based on whether the company also makes such disclosures under the final rules.

We have also added a materiality qualifier to the proposed requirement to disclose “risks from cybersecurity threats,” and have removed the proposed list of risk types (i.e., “intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk”), to foreclose any perception that the rule prescribes cybersecurity policy. We continue to believe these are the types of risks that registrants may face in this context, and enumerate them here as guidance. We note that registrants will continue to tailor their cybersecurity processes to threats as they perceive them. The rule requires registrants to describe those processes insofar as they relate to material cybersecurity risks.

We have also revised Item 106(b)’s enumerated disclosure elements in response to commenters that raised concerns regarding the level of detail required by some elements of the proposal. Specifically, we are not adopting proposed paragraphs (4) (prevention and detection activities), (5) (continuity and recovery plans), and (6) (previous incidents). We have similarly revised proposed paragraph (3) to eliminate some of the detail it required, consistent with commenter suggestions to require only high-level disclosure regarding third-party service providers. The enumerated elements that a registrant should address in its Item 106(b) disclosure, as applicable, are:

²²⁷ See Item 105 of Regulation S-K.

- Whether and how the described cybersecurity processes in Item 106(b) 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 any such processes; and
- Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.

We have also revised the rule text to clarify that the above elements compose a non-exclusive list of disclosures; registrants should additionally disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes.

We have moved proposed paragraph (7) into a separate paragraph, at 17 CFR 229.106(b)(2) (Regulation S-K “Item 106(b)(2)”), instead of including it in the enumerated list in Item 106(b)(1), and have added a materiality qualifier in response to a comment.²²⁸ Item 106(b)(2) requires a description of “[w]hether any risks from cybersecurity threats, including as a result of any 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.”²²⁹

The final rules will require disclosure of whether a registrant engages assessors, consultants, auditors, or other third parties in connection with their cybersecurity because we

²²⁸ See letter from PWC.

²²⁹ With respect to the Item 106(b)(2)’s requirement to describe any risks as a result of any previous cybersecurity incidents, *see supra* Section II.B.3 for a discussion of the duties to correct or update prior disclosure that registrants may have in certain circumstances. As we note in that section, registrants should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

believe it is important for investors to know a registrant’s level of in-house versus outsourced cybersecurity capacity. We understand that many registrants rely on third-party service providers for some portion of their cybersecurity, and we believe this information is accordingly necessary for investors to assess a company’s cybersecurity risk profile in making investment decisions. However, we are not persuaded, as one commenter contended, that registrants should be required to name the third parties (though they may choose to do so), because we believe this may magnify concerns about increasing a company’s cybersecurity vulnerabilities. For the same reason, we decline the commenter suggestion to require a description of the services provided by third parties.

We are also not persuaded that risk quantification or other quantifiable metrics are appropriate as mandatory elements of a cybersecurity disclosure framework. While such metrics may be used by registrants and investors in the future, commenters did not identify any such metrics that would be appropriate to mandate at this time. Additionally, to the extent that a registrant uses any quantitative metrics in assessing or managing cybersecurity risks, it may disclose such information voluntarily. For similar reasons, we decline commenters’ recommendations to require disclosure of independent assessments and audits, as well as commenters’ recommendations on disclosure of use of the NIST framework, and on distinguishing between continuous and periodic risk assessment.

We decline the commenter suggestion to allow Item 106(b) disclosure to be provided in the proxy statement, as the proxy statement is generally confined to information pertaining to the election of directors. We are also not requiring Item 106 disclosures in registration statements as recommended by the IAC, consistent with our efforts to reduce the burdens associated with the

final rule. However, as discussed further below,²³⁰ we reiterate the Commission’s guidance from the 2018 Interpretive Release that “[c]ompanies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements.”²³¹

Finally, we note that registrants may satisfy the Item 106 disclosure requirements through incorporation by reference pursuant to 17 CFR 240.12b-23 (“Rule 12b-23”).²³²

2. Governance

a. Proposed Amendments

The Commission proposed to add 17 CFR 229.106(c) (Regulation S-K “Item 106(c)”) to require a description of management and the board’s oversight of a registrant’s cybersecurity risk. This information would complement the proposed risk management and strategy disclosure by clarifying for investors how a registrant’s leadership oversees and implements its cybersecurity processes.²³³ Proposed 17 CFR 229.106(c)(1) (Regulation S-K “Item 106(c)(1)”) would focus on the board’s role, requiring discussion, as applicable, of:

- Whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks;
- The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and
- Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

²³⁰ See *infra* text accompanying notes 355 and 356.

²³¹ 2018 Interpretive Release at 8168.

²³² As required by Rule 12b-23, in order to incorporate information by reference in answer, or partial answer, to Item 106, a registrant must, among other things, include an active hyperlink if the information is publicly available on EDGAR.

²³³ Proposing Release at 16600.

Proposed 17 CFR 229.106(c)(2) (Regulation S-K “Item 106(c)(2)”) meanwhile would require a description of management’s role in assessing and managing cybersecurity-related risks, as well as its role in implementing the registrant’s cybersecurity policies, procedures, and strategies, including at a minimum discussion of:

- Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members;
- Whether the registrant has a designated chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the registrant’s organizational chart, and the relevant expertise of any such persons;
- The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and
- Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

The Proposing Release explained that proposed Item 106(c)(1) would reinforce the Commission’s 2018 Interpretive Release,²³⁴ which said that disclosure on how a board engages management on cybersecurity helps investors assess the board’s exercise of its oversight responsibility.²³⁵ The Proposing Release noted that proposed Item 106(c)(2) would be of

²³⁴ *Id.* (citing 2018 Interpretive Release at 8170).

²³⁵ 2018 Interpretive Release at 8170.

importance to investors in that it would help investors understand how registrants are planning for cybersecurity risks and inform their decisions on how best to allocate their capital.²³⁶

b. Comments

A few commenters supported proposed Item 106(c) as providing investors with more uniform and informed understanding of registrants' governance of cybersecurity risks.²³⁷ A number of commenters opposed proposed Item 106(c). They contended that the proposed Item 106(c) disclosures would be too granular to be decision-useful; instead, some of these commenters recommended that we limit the rule to a high-level explanation of management and the board's role in cybersecurity risk oversight.²³⁸

One commenter said proposed Item 106(c)(1) should be dropped because it duplicates existing 17 CFR 229.407(h) (Regulation S-K "Item 407(h)'), which requires reporting of material information regarding a board's leadership structure and role in risk oversight, including how it administers its oversight function.²³⁹ Others saw similarities with Item 407(h) as well and suggested instead that proposed Item 106(c) be subsumed into Item 407, thus co-locating governance disclosures.²⁴⁰

In response to a request for comment in the Proposing Release on whether the Commission should expressly provide for the use of hyperlinks or cross-references in Item 106, one commenter supported the use of hyperlinks and cross-references, but sought clarification of

²³⁶ Proposing Release at 16600.

²³⁷ See, e.g., letters from Better Markets; CalPERS.

²³⁸ See letters from ABA; AGA/INGAA; EEI; Nareit; NYSE.

²³⁹ See letter from Davis Polk. The commenter went on to say that, to the extent Item 106(c) requires disclosure of immaterial information regarding the board, it should be dropped.

²⁴⁰ See letters from ABA; BDO; PWC.

whether the practice is already permitted under Commission rules.²⁴¹ Another commenter opposed, saying Item 407(h)'s more general discussion of board governance is distinct from Item 106(c)(1)'s specific focus on cybersecurity.²⁴² The commenter cautioned that allowing registrants to employ hyperlinks and cross-references in Item 106 would lead to "less detail," resulting in disclosure insufficient to investor needs.²⁴³

One commenter recommended that we move proposed Item 106(c)(2) to the enumerated list of topics called for in proposed Item 106(b).²⁴⁴ Another commenter suggested expanding the rule to include disclosure of management and staff training on cybersecurity, asserting that the information is useful to investors because policies depend on staff for successful implementation.²⁴⁵ Two commenters suggested allowing the Item 106(c) disclosures to be made in the proxy statement.²⁴⁶

c. Final Amendments

In response to comments, and aligned with our changes to Item 106(b), we have streamlined Item 106(c) to require disclosure that is less granular than proposed. Under Item 106(c)(1) as adopted, registrants must "[d]escribe the board's oversight of risks from cybersecurity threats," and, if applicable, "identify any board committee or subcommittee responsible" for such oversight "and describe the processes by which the board or such committee is informed about such risks." We have removed proposed Item 106(c)(1)(iii), which had covered whether and how the board integrates cybersecurity into its business strategy, risk

²⁴¹ See letter from E&Y.

²⁴² See letter from Tenable.

²⁴³ *Id.*

²⁴⁴ See letter from Davis Polk.

²⁴⁵ See letter from PRI.

²⁴⁶ See letters from Business Roundtable; Nasdaq.

management, and financial oversight. While we have also removed the proposed Item 106(c)(1)(ii) requirement to disclose “the frequency of [the board or committee’s] discussions” on cybersecurity, we note that, depending on context, some registrants’ descriptions of the processes by which their board or relevant committee is informed about cybersecurity risks may include discussion of frequency.²⁴⁷

Given these changes, we find that Item 407(h) and Item 106(c)(1) as adopted serve distinct purposes and should not be combined, as suggested by some commenters—the former requires description of the board’s leadership structure and administration of risk oversight generally, while the latter requires detail of the board’s oversight of specific cybersecurity risk. As noted by one commenter,²⁴⁸ to the extent these disclosures are duplicative, a registrant would be able to incorporate such information by reference.²⁴⁹

We have also modified Item 106(c)(2) to add a materiality qualifier, to make clear that registrants must “[d]escribe management’s role in assessing and managing the registrant’s *material* risks from cybersecurity threats” (emphasis added).²⁵⁰ The enumerated disclosure elements now constitute a “non-exclusive list” registrants should consider including. We have revised the first element to require the disclosure of management positions or committees “responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise.” Because this

²⁴⁷ For example, if the board or committee relies on periodic (e.g., quarterly) presentations by the registrant’s chief information security officer to inform its consideration of risks from cybersecurity threats, the registrant may, in the course of describing those presentations, also note their frequency.

²⁴⁸ See letter from E&Y.

²⁴⁹ Rule 12b-23.

²⁵⁰ We have not added a materiality qualifier to Item 106(c)(1) because, if a board of directors determines to oversee a particular risk, the fact of such oversight being exercised by the board is material to investors. By contrast, management oversees many more matters and management’s oversight of non-material matters is likely not material to investors, so a materiality qualifier is appropriate for Item 106(c)(2).

requirement would typically encompass identification of whether a registrant has a chief information security officer, or someone in a comparable position, we are not adopting the proposed second element that would have specifically called for disclosure of whether the registrant has a designated chief information security officer. Given our purpose of streamlining the disclosure requirements, we also are not adopting the proposed requirement to disclose the frequency of management-board discussions on cybersecurity, though, as noted above, discussion of frequency may in some cases be included as part of describing the processes by which the board or relevant committee is informed about cybersecurity risks in compliance with Item 106(c)(1), to the extent it is relevant to an understanding of the board's oversight of risks from cybersecurity threats.

Thus, as adopted, Item 106(c)(2) directs registrants to consider disclosing the following as part of a description of management's role in assessing and managing the registrant's material risks from cybersecurity threats:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
- The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

As many commenters recommended, these elements are limited to disclosure that we believe balances investors' needs to understand a registrant's governance of risks from cybersecurity threats in sufficient detail to inform an investment or voting decision with concerns

that the proposal could inadvertently pressure registrants to adopt specific or inflexible cybersecurity-risk governance practices or organizational structures. We do not believe these disclosures should be subsumed into Item 106(b), as one commenter recommended, because identifying the management committees and positions responsible for risks from cybersecurity threats is distinct from describing the cybersecurity practices management has deployed. We also decline the commenter suggestion to require disclosure of management and staff training on cybersecurity; registrants may choose to make such disclosure voluntarily. Finally, we decline the commenter suggestion to allow Item 106(c) disclosure to be provided in the proxy statement; governance information in the proxy statement is generally meant to inform shareholders' voting decisions, whereas Item 106(c) disclosure informs investors' assessment of investment risk.

3. Definitions

a. Proposed Definitions

The Commission proposed to define three terms to delineate the scope of the amendments: “cybersecurity incident,” “cybersecurity threat,” and “information systems.”²⁵¹ Proposed 229 CFR 229.106(a) (Regulation S-K “Item 106(a)”) would define them as follows:

- *Cybersecurity incident* means 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* means 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.

²⁵¹ Proposing Release at 16600-16601.

- *Information systems* means 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.

As noted above, the Commission explained that what constitutes a “cybersecurity incident” should be construed broadly, encompassing a range of event types.²⁵²

b. Comments

Most commenters that offered feedback on the proposed definitions suggested narrowing them in some fashion. On “cybersecurity incident,” many commenters urged limiting the definition to cases of actual harm, thereby excluding incidents that had only the potential to cause harm.²⁵³ They suggested accomplishing this by replacing “jeopardizes” with phrases such as “adversely affects” or “results in substantial loss of.”²⁵⁴ One of these commenters noted that such a change would more closely align the definition with that in CIRCIA.²⁵⁵ Other commenters objected to the definition’s use of “any information” as overbroad, saying it would lead to inconsistent application.²⁵⁶ One commenter sought clarification of whether the definition encompasses accidental incidents, such as chance technology outages, that do not involve a

²⁵² *Id.* at 16601.

²⁵³ See letters from ABA; BPI et al.; Chamber et al.; Davis Polk; Enbridge; FDD; FEI; Hunton; PWC; SCG; SIFMA.

²⁵⁴ See letters from BPI et al.; Hunton.

²⁵⁵ See letter from BPI et al. (“The word ‘jeopardizes’ should be replaced with ‘results in substantial loss of’ to capture incidents that are causing some actual harm, and to better harmonize the definition with the reporting standard set forth by Congress in CIRCIA.”).

²⁵⁶ See letters from Deloitte; SIFMA.

malicious actor,²⁵⁷ while another commenter advocated broadening the definition to any incident materially disrupting operations, regardless of what precipitated it.²⁵⁸

On “cybersecurity threat,” commenters urged narrowing the rule by replacing the language “may result in” with “could reasonably be expected to result in” or some other probability threshold.²⁵⁹ One stated that “the use of a ‘may’ standard establishes an unhelpfully low standard that would require registrants to establish policies and procedures to identify threats that are potentially overbroad and not appropriately tailored to those threats that are reasonably foreseeable.”²⁶⁰ In a similar vein, two commenters objected to the language “any potential occurrence” as over-inclusive and lacking “instructive boundaries.”²⁶¹

On “information systems,” many commenters favored replacing “owned or used by” with “owned or operated by,” “owned or controlled by,” or like terms, so that registrants’ reporting obligations stop short of incidents on third-party information systems.²⁶² A few commenters said the definition could be construed to cover hard-copy information and should be revised to foreclose such a reading.²⁶³

More broadly, many commenters advised the Commission to align these definitions with comparable definitions in other Federal laws and regulations, such as CIRCIA and NIST.²⁶⁴ One

²⁵⁷ See letter from CSA.

²⁵⁸ See letter from Crindata.

²⁵⁹ See letters from Chevron; Debevoise; NYC Bar.

²⁶⁰ See letter from Debevoise.

²⁶¹ See letters from Chevron; Deloitte.

²⁶² See letters from ABA; APCIA; Business Roundtable; Chamber; Cybersecurity Coalition; ISA; ITI; NAM; NDIA; Paylocity. Other commenters made similar arguments about third party systems without speaking specifically to the definition, saying, for example, that registrants may not have sufficient visibility into third-party systems and may be bound by confidentiality agreements. See letters from AIA; EIC; FAH; NMHC; SIFMA.

²⁶³ See letters from ABA; BPI et al.; Enbridge.

²⁶⁴ See letters from ABA; CAQ; Chevron; FEI; IC; IIA; Microsoft; PWC; SandboxAQ; SIFMA.

commenter explained that “[a]lligning definitions with those in existing federal laws and regulations would help ensure that the defined terms are consistently understood, interpreted and applied in the relevant disclosure.”²⁶⁵ However, another commenter cautioned against aligning with definitions, such as those of NIST, that were developed with a view toward internal risk management and response rather than external reporting; the commenter identified CIRCIA and the Federal banking regulators’ definitions as more apposite.²⁶⁶ One commenter noted that additional proposed defined terms were included in the Commission’s rulemaking release *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*²⁶⁷ that were not included in the Proposing Release and recommended that we “consider whether the defined terms should be consistent.”²⁶⁸

In the Proposing Release, the Commission asked whether to define other terms used in the proposed amendments, and specifically sought comment on whether a definition of “cybersecurity” would be useful.²⁶⁹ Several commenters supported defining “cybersecurity,”²⁷⁰ reasoning, for example, that any rulemaking on cybersecurity should define that baseline term;²⁷¹ that, left undefined, the term would be open to varying interpretations;²⁷² and that details such as whether hardware is covered should be resolved.²⁷³ Separately, two commenters recommended

²⁶⁵ See letter from ABA.

²⁶⁶ See letter from SCG.

²⁶⁷ Release No. 33-11028 (Feb. 9, 2022) [87 FR 13524 (Mar. 9, 2022)].

²⁶⁸ See letter from Deloitte.

²⁶⁹ Proposing Release at 16601.

²⁷⁰ See letters from BCS; Blue Lava; EIC; R. Hackman; R Street.

²⁷¹ See letter from R Street.

²⁷² See letter from Blue Lava.

²⁷³ See letter from BCS.

the Commission define “operational technology,”²⁷⁴ with one explaining that the “proposed definitions understandably focus on data breaches, which are a major cybersecurity threat, but we believe an operational technology breach could have even more detrimental effects in certain cases (such as for ransomware attacks that have impacted critical infrastructure) and warrants disclosure guidance from the Commission.”²⁷⁵

Several commenters also sought either a formal definition or more guidance on the term “material” specific to the cybersecurity space.²⁷⁶ Some read the proposal, particularly the incident examples provided in the Proposing Release, as lowering the bar for materiality and being overly subjective, which they indicated may result in over-reporting of cybersecurity incidents or introduce uncertainty, and they urged the Commission to affirm the standard materiality definition.²⁷⁷ Another commenter sought cybersecurity-specific guidance on materiality, including “concrete thresholds to assist registrants in determining materiality.”²⁷⁸ A few commenters recommended conditioning the materiality determination on the underlying information being verified to “a high degree of confidence” and “unlikely to materially change,”²⁷⁹ while one commenter looked to replace materiality altogether with a significance standard like that in CIRCIA.²⁸⁰

c. Final Definitions

²⁷⁴ See letters from Chevron; EIC.

²⁷⁵ See letter from Chevron.

²⁷⁶ See letters from ACLI; AIC; AICPA; APCIA; Bitsight; Harry Broadman, Eric Matrejek, and Brad Wilson (“Broadman et al.”); Debevoise; EIC; International Information System Security Certification Consortium (“ISC2”); M. Barragan; NYC Bar; Prof. Perullo; R Street; SIFMA; TransUnion; Virtu.

²⁷⁷ See letters from APCIA; ACLI; EIC; Virtu.

²⁷⁸ See letter from SIFMA.

²⁷⁹ See letters from Debevoise; NYC Bar. *See also* letter from AIC (suggesting “unlikely to change,” without “materially”).

²⁸⁰ See letter from National Electrical Manufacturers Association (“NEMA”).

We are adopting definitions for “cybersecurity incident,” “cybersecurity threat,” and “information systems” largely as proposed, with three modifications.

First, on “cybersecurity incident,” we are adding the phrase “or a series of related unauthorized occurrences” to the “cybersecurity incident” definition. This reflects our guidance in Section II.B.3 above that a series of related occurrences may collectively have a material impact or reasonably likely material impact and therefore trigger Form 8-K Item 1.05, even if each individual occurrence on its own would not rise to the level of materiality. Second, we are making a clarifying edit to “information systems.” Some commenters said the definition could be construed to cover hard-copy resources.²⁸¹ We recognize that reading is possible, if unlikely and unintended, and we are therefore inserting “electronic” before “information resources,” to ensure the rules pertain only to electronic resources. Third, we are making minor revisions to the “cybersecurity threat” definition for clarity and to better align it with the “cybersecurity incident” definition.

Accordingly, the definitions are as follows:

- *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.

²⁸¹ See letters from ABA; BPI et al.; Enbridge.

- *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.

We recognize commenters' concern regarding the term "jeopardizes" in the proposed "cybersecurity incident" definition and the resulting scope of the definition. Nonetheless, we note that the definition is not self-executing; rather it is operationalized by Item 1.05, which is conditioned on the incident having been material to the registrant. Typically that would entail actual harm, though the harm may sometimes be delayed, and a material cybersecurity incident may not result in actual harm in all instances. For example, a company whose intellectual property is stolen may not suffer harm immediately, but it may foresee that harm will likely occur over time as that information is sold to other parties, such that it can determine materiality before the harm occurs. The reputational harm from a breach may similarly increase over time in a foreseeable manner. There may also be cases, even if uncommon, where the jeopardy caused by a cybersecurity incident materially affects the company, even if the incident has not yet caused actual harm. In such circumstances, we believe investors should be apprised of the material effects of the incident. We are therefore retaining the word "jeopardizes" in the definition.

We are not persuaded that the proposed "cybersecurity incident" definition's use of "any information" would lead to inconsistent application of the definition among issuers or cause a risk of over-reporting, as suggested by some commenters. As noted above, the "cybersecurity incident" definition is operationalized by Item 1.05. Item 1.05 does not require disclosure

whenever “any information” is affected by an intruder. Disclosure is triggered only when the resulting effect of an incident on the registrant is material.

We are also retaining “unauthorized” in the incident definition as proposed. In general, we believe that an accidental occurrence is an unauthorized occurrence. Therefore, we note that an accidental occurrence may be a cybersecurity incident under our definition, even if there is no confirmed malicious activity. For example, if a company’s customer data are accidentally exposed, allowing unauthorized access to such data, the data breach would constitute a “cybersecurity incident” that would necessitate a materiality analysis to determine whether disclosure under Item 1.05 of Form 8-K is required.

On “cybersecurity threat,” we appreciate commenters’ concerns with the proposed definition’s use of “may result in” and “any potential occurrence.” Unlike with “cybersecurity incident,” where the interplay of the proposed definition with proposed Item 1.05 ensured only material incidents would become reportable, proposed Item 106(b)’s reference to “the identification and management of risks from cybersecurity threats” was not qualified by materiality. We are therefore adding a materiality condition to Item 106(b). As adopted, Item 106(b) will require disclosure of registrants’ processes to address the material risks of potential occurrences that could reasonably result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of a registrant’s information systems. Given the addition of a materiality condition to Item 106(b), we do not believe that further revision to the “cybersecurity threat” definition is warranted.

On “information systems,” we decline to change “owned or used by” to “owned or operated by,” “owned or controlled by,” or similar terms advanced by commenters. Commenters recognized that “used by” covers information resources owned by third parties. That is by

design: covering third party systems is essential to the working of Item 106 of Regulation S-K and Item 1.05 of Form 8-K. As we explain above, in Section II.A.3, the materiality of a cybersecurity incident is contingent neither on where the relevant electronic systems reside nor on who owns them, but rather on the impact to the registrant. We do not believe that a reasonable investor would view a significant data breach as immaterial merely because the data are housed on a cloud service. If we were to remove “used by,” a registrant could evade the disclosure requirements of the final rules by contracting out all of its information technology needs to third parties. Accordingly, the definition of “information systems” contemplates those resources owned by third parties and used by the registrant, as proposed.

In considering commenters’ suggestion to align our definitions with CIRCIA, NIST, and other Federal regulations, we observe that there is no one standard definition for these terms, and that regulators have adopted definitions based on the specific contexts applicable to their regulations. Nonetheless, we also observe that the final “cybersecurity incident” definition is already similar to the CIRCIA and NIST incident definitions, in that all three focus on the confidentiality, integrity, and availability of information systems.²⁸² Our definition of “information systems” also tracks CIRCIA and NIST, as all three cover “information resources” that are “organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition” of information.²⁸³ Of course, the definitions do not match precisely, but some variation is inevitable where various Federal laws and regulations have different purposes, contexts, and goals. We therefore find that further alignment is not needed.

²⁸² For CIRCIA, *see supra* note 19, at sec. 103, 136 Stat. 1039; and 6 U.S.C. 681b(c)(2)(A)(i). For NIST, *see Incident, Glossary, NIST COMPUTER SECURITY RESOURCE CENTER, available at https://csrc.nist.gov/glossary/term/incident.*

²⁸³ For CIRCIA, *see supra* note 19, at sec. 103, 136 Stat. 1039; and 44 U.S.C. 3502(8). For NIST, *see Information System, Glossary, NIST COMPUTER SECURITY RESOURCE CENTER, available at https://csrc.nist.gov/glossary/term/information_system.*

We decline to define any other terms. We acknowledge commenters who asked for additional guidance regarding the application of a materiality determination to cybersecurity or sought to replace materiality with a significance standard. As noted in the Proposing Release, however, we expect that registrants will apply materiality considerations as would be applied regarding any other risk or event that a registrant faces. Carving out a cybersecurity-specific materiality definition would mark a significant departure from current practice, and would not be consistent with the intent of the final rules.²⁸⁴ Accordingly, we reiterate, consistent with the standard set out in the cases addressing materiality in the securities laws, that information is material if “there is a substantial likelihood that a reasonable shareholder would consider it important”²⁸⁵ in making an investment decision, or if it would have “significantly altered the ‘total mix’ of information made available.”²⁸⁶ Because materiality’s focus on the total mix of information is from the perspective of a reasonable investor, companies assessing the materiality of cybersecurity incidents, risks, and related issues should do so through the lens of the reasonable investor. Their evaluation should take into consideration all relevant facts and circumstances, which may involve consideration of both quantitative and qualitative factors. Thus, for example, when a registrant experiences a data breach, it should consider both the immediate fallout and any longer term effects on its operations, finances, brand perception, customer relationships, and so on, as part of its materiality analysis. We also note that, given the fact-specific nature of the materiality determination, the same incident that affects multiple

²⁸⁴ See, e.g., *Basic Inc. v. Levinson*, 485 U.S. 224, 236 (1988) (“[a]ny approach that designates a single fact or occurrence as always determinative of an inherently fact-specific finding such as materiality, must necessarily be overinclusive or underinclusive”).

²⁸⁵ *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976); *Matrixx Initiatives v. Siracusano*, 563 U.S. 27, 38-40 (2011); *Basic*, 485 U.S. at 240.

²⁸⁶ *Id.* See also the definition of “material” in 17 CFR 230.405 [Securities Act Rule 405]; 17 CFR 240.12b-2 [Exchange Act Rule 12b-2].

registrants may not become reportable at the same time, and it may be reportable for some registrants but not others.

We also decline to separately define “cybersecurity,” as suggested by some commenters. We do not believe such further definition is necessary, given the broad understanding of this term. To that end, we note that the cybersecurity industry itself appears not to have settled on an exact definition, and because the field is quickly evolving and is expected to continue to evolve over time, any definition codified in regulation could soon become stale as technology develops. Likewise, the final rules provide flexibility by not defining “cybersecurity,” allowing a registrant to determine meaning based on how it considers and views such matters in practice, and on how the field itself evolves over time.

We decline to define “operational technology” as suggested by some commenters because the term does not appear in the rules we are adopting.

D. Disclosure Regarding the Board of Directors’ Cybersecurity Expertise

1. Proposed Amendments

Congruent with proposed Item 106(c)(2) on the board’s oversight of cybersecurity risk, the Commission proposed adding 17 CFR 229.407(j) (Regulation S-K “Item 407(j)”) to require disclosure about the cybersecurity expertise, if any, of a registrant’s board members.²⁸⁷ The proposed rule did not define what constitutes expertise, given the wide-ranging nature of cybersecurity skills, but included a non-exclusive list of criteria to consider, such as prior work experience, certifications, and the like. As proposed, paragraph (j) would build on existing 17 CFR 229.401(e) (Regulation S-K “Item 401(e)”) (business experience of directors) and Item 407(h) (board risk oversight), and would be required in the annual report on Form 10-K and in

²⁸⁷ Proposing Release at 16601.

the proxy or information statement when action is to be taken on the election of directors. Thus, the Proposing Release said, proposed Item 407(j) would help investors in making both investment and voting decisions.²⁸⁸

The Commission also proposed to include a safe harbor in 17 CFR 229.407(j)(2) (Regulation S-K “Item 407(j)(2)”) providing that any directors identified as cybersecurity experts would not be deemed experts for liability purposes, including under Section 11 of the Securities Act.²⁸⁹ This was intended to clarify that identified directors do not assume any duties, obligations, or liabilities greater than those assumed by non-expert directors.²⁹⁰ Nor would such identification decrease the duties, obligations, and liabilities of non-expert directors relative to identified directors.²⁹¹

2. Comments

Proposed Item 407(j) garnered significant comment. Supporters wrote that understanding a board’s level of cybersecurity expertise is important to assessing a company’s ability to manage cybersecurity risk.²⁹² For example, one commenter said “[b]oard cybersecurity expertise serves as a useful starting point for investors to assess a company’s approach to cybersecurity;”²⁹³ while another commenter said investors need the Item 407(j) disclosure “[t]o cast informed votes on directors.”²⁹⁴ One comment letter submitted an academic study by the

²⁸⁸ *Id.*

²⁸⁹ *Id.* at 16602.

²⁹⁰ *Id.*

²⁹¹ *Id.*

²⁹² See letters from O. Borges; CalPERS; Prof. Choudhary; CII; Digital Directors Network (“DDN”); ISC2; Prof. Lowry et al.; NACD; PRI; SANS Institute; SM4RT Secure.

²⁹³ See letter from PRI.

²⁹⁴ See letter from CII.

authors of the letter and noted that its findings “underscore the importance of understanding the role of boards in cybersecurity oversight.”²⁹⁵

By contrast, many commenters argued cybersecurity risk is not intrinsically different from other risks that directors assess with or without specific technical expertise.²⁹⁶ For example, one reasoned that, given the “ever-changing range of risks confronting a company,” directors require “broad-based skills in risk and management oversight, rather than subject matter expertise in one particular type of risk.”²⁹⁷ Commenters also predicted the disclosure requirement would pressure companies to retain cybersecurity experts on their board, and submitted there is not enough cybersecurity talent in the marketplace at this time for all or most companies to do so.²⁹⁸ One of these commenters further contended that finding such expertise will be harder for smaller reporting companies.²⁹⁹ Another commenter warned that, given the current cybersecurity talent pool, the end result may be lower diversity on boards;³⁰⁰ and one said hiring cybersecurity experts to the board may come at the expense of spending on a company’s cybersecurity defenses.³⁰¹ Commenters also expressed concern that the identified expert

²⁹⁵ See letter from Prof. Lowry et al.

²⁹⁶ See letters from ABA; ACC; AGA/INGAA; AICPA; Auto Innovators; BDO; BPI et al.; Business Roundtable; CAQ; CBA; Chamber; CTA; CTIA; Davis Polk; Deloitte; EEI; EIC; Hunton; ITI; IC; LTSE; Microsoft; Nareit; NAM; NDIA; NRA; NYSE; PPG; Safe Security; SCG; SIFMA; TechNet; USTelecom; Virtu; Wilson Sonsini. See also IAC Recommendation.

²⁹⁷ See letter from ABA.

²⁹⁸ See letters from ACC; APCIA; BIO; Blue Lava; Chamber; FDD; ITI (May 9, 2022); NDIA; NYSE; SCG (May 9, 2022). In this vein, a commenter requested the Commission affirm Item 407(j) is only a disclosure provision and is not intended to mandate cybersecurity expertise on the board. See letter from Federated Hermes.

²⁹⁹ See letter from BIO.

³⁰⁰ See letter from Chamber (“An unintended consequence of the SEC proposal is likely to create new barriers for underrepresented groups to move into cybersecurity leadership roles largely due to the expense of obtaining credentials and other formal certifications. The costs associated with obtaining cybersecurity-related degrees and other credentials could hinder the advancement of individuals who could otherwise rise through the ranks within the field of cybersecurity.”).

³⁰¹ See letter from Wilson Sonsini.

directors would face elevated risks, such as being targeted by nation states for surveillance or hackers attempting to embarrass them, thus creating a disincentive to board service.³⁰²

More generally, sentiment among those opposed to Item 407(j) was that the rule is overly prescriptive and in effect would direct how companies operate their cybersecurity programs.³⁰³ As an alternative, some commenters pushed for other ways to show competency, such as identifying outside experts the board relies on for cybersecurity expertise, disclosing how frequently the board meets with the chief information security officer, listing relevant director training, and relying on adjacent technology skills.³⁰⁴

Whether they supported or opposed the proposed disclosure requirement, commenters largely endorsed the proposed Item 407(j)(2) safe harbor; its absence, they said, could make candidates with cybersecurity expertise reluctant to serve on boards.³⁰⁵ Two commenters requested the Commission define “cybersecurity expertise;”³⁰⁶ one of them said being “duly accredited and certified as a cybersecurity professional” should be a prerequisite, and posited specific industry certifications to establish expertise.³⁰⁷ Another commenter suggested adding participation in continuing education to the 17 CFR 229.407(j)(1)(i) factors considered in assessing expertise.³⁰⁸

³⁰² See letters from BIO; Chevron; EEI; EIC; Hunton; Profs. Rajgopal & Sharp.

³⁰³ See, e.g., letter from ACC.

³⁰⁴ See letters from AGA/INGAA; BPI et al.; Business Roundtable; DDN; LTSE; PRI; Wilson Sonsini.

³⁰⁵ See letters from ABA; BIO; CII; CSA; A. Heighington; NACD; Paylocity; Prof. Perullo.

³⁰⁶ See letters from Federated Hermes; ISC2.

³⁰⁷ See letter from ISC2.

³⁰⁸ See letter from SandboxAQ.

3. Final Amendments

After considering the comments, we are not adopting proposed Item 407(j). We are persuaded that effective cybersecurity processes are designed and administered largely at the management level, and that directors with broad-based skills in risk management and strategy often effectively oversee management’s efforts without specific subject matter expertise, as they do with other sophisticated technical matters. While we acknowledge that some commenters indicated that the proposed Item 407(j) information would be helpful to investors, we nonetheless agree that it may not be material information for all registrants. We believe investors can form sound investment decisions based on the information required by Items 106(b) and (c) without the need for specific information regarding board-level expertise. And to that end, a registrant that has determined that board-level expertise is a necessary component to the registrant’s cyber-risk management would likely provide that disclosure pursuant to Items 106(b) and (c).

E. Disclosure by Foreign Private Issuers

1. Proposed Amendments

The Commission proposed to establish disclosure requirements for FPIs parallel to those proposed for domestic issuers in Regulation S-K Items 106 and 407(j) and Form 8-K Item 1.05.³⁰⁹ Specifically, the Commission proposed to amend Form 20-F to incorporate the requirements of proposed Item 106 and 407(j) to disclose information regarding an FPI’s cybersecurity risk management, strategy, and governance.³¹⁰ With respect to incident disclosure,

³⁰⁹ Proposing Release at 16602. The Commission did not propose to amend Form 40-F, choosing rather to maintain the multijurisdictional disclosure system (“MJDS”) whereby eligible Canadian FPIs use Canadian disclosure standards and documents to satisfy SEC registration and disclosure requirements.

³¹⁰ As noted in the Proposing Release, FPIs would include the expertise disclosure only in their annual reports, as they are not subject to Commission rules for proxies and information statements.

the Commission proposed to: (1) amend General Instruction B of Form 6-K to reference material cybersecurity incidents among the items that may trigger a current report on Form 6-K,³¹¹ and (2) amend Form 20-F to require updated disclosure regarding incidents previously disclosed on Form 6-K.

2. Comments

A few commenters agreed that the Commission should not exempt FPIs from the proposed disclosure requirements, given they face the same threats as domestic issuers.³¹² Another commenter said the Commission should not delay compliance for FPIs, for similar reasons.³¹³ On the other hand, one commenter said the proposal would disproportionately burden FPIs because, under its reading of the proposed amendment to General Instruction B, Form 6-K would require disclosure of all cybersecurity incidents, not just those that are material.³¹⁴ The commenter went on to say that the interplay of the European Union’s Market Abuse Regulation (“MAR”) would render the proposed Form 6-K amendment particularly taxing, because MAR requires immediate announcement of non-public price sensitive information.³¹⁵

On MJDS filers, commenters endorsed the Commission’s determination not to propose to amend Form 40-F, maintaining that Canadian issuers eligible to use MJDS should be permitted to follow their domestic disclosure standards, consistent with other disclosure requirements for those registrants.³¹⁶

³¹¹ A registrant is required under Form 6-K to furnish copies of all information that it: (i) makes or is required to make public under the laws of its jurisdiction of incorporation, (ii) files, or is required to file under the rules of any stock exchange, or (iii) otherwise distributes to its security holders.

³¹² See letters from CSA; Cybersecurity Coalition; Prof. Perullo; Tenable.

³¹³ See letter from Crindata.

³¹⁴ See letter from SIFMA.

³¹⁵ *Id.*

³¹⁶ See letters from ACLI; BCE; Cameco Corporation; CBA; Sun Life Financial Inc.

3. Final Amendments

We are adopting the Form 20-F and Form 6-K amendments as proposed, with modifications that are consistent with those being applied to Item 106 of Regulation S-K and Item 1.05 of Form 8-K. We continue to believe that FPIs' cybersecurity incidents and risks are not any less important to investors' capital allocation than those of domestic registrants. We also do not find that the Form 6-K amendments unduly burden FPIs. Importantly, the language the Commission proposed to add to General Instruction B ("cybersecurity incident") of Form 6-K would be modified by the existing language "that which is material with respect to the issuer and its subsidiaries concerning." Nonetheless, for added clarity, we are including the word "material" before "cybersecurity incident." Thus, for a cybersecurity incident to trigger a disclosure obligation on Form 6-K, the registrant must determine that the incident is material, in addition to meeting the other criteria for required submission of the Form.³¹⁷ Even registrants subject to the European Union's MAR will first have developed the relevant information for foreign disclosure or publication under MAR, so any added burden for preparing and furnishing the Form 6-K should be minor. As the Commission stated in the Proposing Release, we do not find reason to adopt prescriptive cybersecurity disclosure requirements for Form 40-F filers, given that the MJDS generally permits eligible Canadian FPIs to use Canadian disclosure standards and documents to satisfy the Commission's registration and disclosure requirements.³¹⁸ We note that such filers are already subject to the Canadian Securities Administrators' 2017 guidance on the disclosure of cybersecurity risks and incidents.³¹⁹

³¹⁷ See *supra* note 311 for the other criteria.

³¹⁸ Proposing Release at 16603.

³¹⁹ Canadian Securities Administrators, *CSA Multilateral Staff Notice 51-347 – Disclosure of cyber security risks and incidents* (Jan. 19, 2017).

F. Structured Data Requirements

1. Proposed Amendments

The Commission proposed to mandate that registrants tag the new disclosures in Inline XBRL, including by block text tagging narrative disclosures and detail tagging quantitative amounts.³²⁰ The Proposing Release explained that the structured data requirements would make the disclosures more accessible to investors and other market participants and facilitate more efficient analysis.³²¹ The proposed requirements would not be unduly burdensome to registrants, the release posited, because they are similar to the Inline XBRL requirements for other disclosures.³²²

2. Comments

Commenters largely supported the proposal to require Inline XBRL tagging of the new disclosures, as structured data would enable automated extraction and analysis.³²³ Opposition to the requirement centered on filer burden, including an argument that, given the time-sensitive nature of the Item 1.05 Form 8-K disclosure, mandating structured data tagging would unduly add to companies' burden in completing timely reporting.³²⁴

3. Final Amendments

After considering comments, we are adopting the structured data requirements as proposed, with a staggered compliance date of one year.³²⁵ We are not persuaded that Inline

³²⁰ Proposing Release at 16603.

³²¹ *Id.*

³²² *Id.*

³²³ See letters from AICPA; CAQ; Crowe LLP; E&Y; FDD; K. Fuller; NACD; PWC; Professors Lawrence Trautman & Neal Newman; XBRL US.

³²⁴ See letters from NYC Bar; SFA.

³²⁵ We have incorporated modifications of a technical nature to the regulatory text.

XBRL tagging will unduly add to companies' burden in preparing and filing Item 1.05 Form 8-K in a timely fashion, and we believe such incremental costs are appropriate given the significant benefits to investors. Compared to the Inline XBRL tagging companies will already be performing for their financial statements, the tagging requirements here are less extensive and complex. Inline XBRL tagging will enable automated extraction and analysis of the information required by the final rules, allowing investors and other market participants to more efficiently identify responsive disclosure, as well as perform large-scale analysis and comparison of this information across registrants.³²⁶ The Inline XBRL requirement will also enable automatic comparison of tagged disclosures against prior periods. If we were not to adopt the Inline XBRL requirement as suggested by some commenters, some of the benefit of the new rules would be diminished. However, we are delaying compliance with the structured data requirements for one year beyond initial compliance with the disclosure requirements. This approach should both help lessen any compliance burden and improve data.

G. Applicability to Certain Issuers

1. Asset-Backed Issuers

The Commission proposed to amend Form 10-K to clarify that an asset-backed issuer, as defined in 17 CFR 229.1101 (Regulation AB "Item 1101"), that does not have any executive officers or directors may omit the information required by proposed Item 106(c).³²⁷ The Commission noted that asset-backed issuers would likewise be exempt from proposed Item

³²⁶ These considerations are generally consistent with objectives of the recently enacted Financial Data Transparency Act of 2022, which directs the establishment by the Commission and other financial regulators of data standards for collections of information, including with respect to periodic and current reports required to be filed or furnished under Exchange Act Sections 13 and 15(d). Such data standards must meet specified criteria relating to openness and machine-readability and promote interoperability of financial regulatory data across members of the Financial Stability Oversight Council. *See* James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, P.L. 117-263, tit. LVIII, 136 Stat. 2395, 3421-39 (2022).

³²⁷ Proposing Release at 16600.

407(j) pursuant to existing Instruction J to Form 10-K.³²⁸ The Commission further requested comment on whether to generally exempt asset-backed issuers from the proposed rules.

One commenter stated that the proposed rules should not apply to issuers of asset-backed securities, given that they are limited purpose or passive special purpose vehicles with limited activities, no operations or businesses, and no information systems.³²⁹ The commenter also opposed applying the proposed rules to other transaction parties (such as the sponsor, servicer, originator, and trustee), because such parties are neither issuers of nor obligors on an asset-backed security, and “it is extraordinarily unlikely that a transaction party’s financial performance or position would be impacted by a cybersecurity incident to such an extent as to impede its ability to perform its duties and responsibilities to the securitization transaction.”³³⁰ The commenter acknowledged that cybersecurity disclosure rules may make sense for servicers of asset-backed securities, but counseled that any new rules should be tailored to such entities, rather than applying the proposed rules.³³¹

We are exempting asset-backed securities issuers from the final rules.³³² We agree with the commenter that the final rules would not result in meaningful disclosure by asset-backed issuers. In particular, we are persuaded by the fact that asset-backed issuers are typically special purpose vehicles whose activities are limited to receiving or purchasing, and transferring or selling, assets to an issuing entity³³³ and, accordingly, do not own or use information systems,

³²⁸ *Id.* at 16601.

³²⁹ See letter from SFA.

³³⁰ *Id.*

³³¹ *Id.*

³³² See General Instruction G to Form 8-K, and General Instruction J to Form 10-K.

³³³ See letter from SFA (citing the definitions contained in 17 CFR 229.1101(b), 17 CFR 230.191, and 17 CFR 240.3b-19).

whereas the final rules are premised on an issuer’s ownership or use of information systems.³³⁴

To the extent that a servicer or other party to an asset-backed security transaction is a public company, it will be required to comply with the final rules with respect to information systems it owns or uses. Therefore, an investor in an asset-backed security who wants to assess the cybersecurity of transaction parties will be able to do so for those that are public companies. The Commission may consider cybersecurity disclosure rules specific to asset-backed securities at a later date.

2. Smaller Reporting Companies

In the Proposing Release, the Commission did not include an exemption or alternative compliance dates or transition accommodations for smaller reporting companies, but it did request comment on whether to do so.³³⁵ The Commission noted that smaller companies may face equal or greater cybersecurity risk than larger companies, such that cybersecurity disclosures may be particularly important for their investors.³³⁶

A few commenters advocated an exemption for smaller reporting companies, asserting that they face outsized costs from the proposal and lower cybersecurity risk.³³⁷ And some commenters called for a longer compliance phase-in period for smaller reporting companies, to help them mitigate their cost burdens and benefit from the compliance and disclosure experience of larger companies.³³⁸ Other commenters opposed an exemption for smaller reporting

³³⁴ The definition of “cybersecurity incident” focuses on “a registrant’s information systems.” Likewise, the definition of “cybersecurity threat” concerns “a registrant’s information systems or any information residing therein.”

³³⁵ Proposing Release at 16601.

³³⁶ *Id.* at 16613.

³³⁷ See letters from BIO; NDIA.

³³⁸ See letters from BIO; BDO; NACD; Nasdaq. In addition, the Commission’s Small Business Capital Formation Advisory Committee highlights generally in its parting perspectives letter that “exemptions, scaling, and phase-

companies,³³⁹ in part because they may face equal³⁴⁰ or greater³⁴¹ cybersecurity risk than larger companies, or because investors' relative share in a smaller company may be higher, such that small companies' cybersecurity risk "may actually embody the most pressing cybersecurity risk to an investor."³⁴²

Consistent with the proposal, we decline to exempt smaller reporting companies. We believe the streamlined requirements of the final rules will help reduce some of the costs associated with the proposal for all registrants, including smaller reporting companies. Also, we do not believe that an additional compliance period is needed for smaller reporting companies with respect to Item 106, as this information is factual in nature regarding a registrant's existing cybersecurity strategy, risk management, and governance, and so should be readily available to those companies to assess for purposes of preparing disclosure. Finally, given the significant cybersecurity risks smaller reporting companies face and the outsized impacts that cybersecurity incidents may have on their businesses, their investors need access to timely disclosure on material cybersecurity incidents and the material aspects of their cybersecurity risk management and governance. However, we agree with commenters that stated smaller reporting companies would likely benefit from additional time to comply with the incident disclosure requirements.

ins for new requirements where appropriate, allows smaller companies to build their businesses and balance the needs of companies and investors while promoting strong and effective U.S. public markets." *See Parting Perspectives Letter, U.S. Securities and Exchange Commission Small Business Capital Formation Advisory Committee (Feb. 28, 2023), available at* [*https://www.sec.gov/files/committee-perspectives-letter-022823.pdf*](https://www.sec.gov/files/committee-perspectives-letter-022823.pdf). *See also U.S. Securities and Exchange Commission Office of the Advocate for Small Business Capital Formation, Annual Report Fiscal Year 2022 ("2022 OASB Annual Report"), available at* [*https://www.sec.gov/files/2022-oasb-annual-report.pdf*](https://www.sec.gov/files/2022-oasb-annual-report.pdf)*, at 83 (recommending generally that in engaging in rulemaking that affects small businesses, the Commission tailor the disclosure and reporting framework to the complexity and size of operations of companies, either by scaling obligations or delaying compliance for the smallest of the public companies).*

³³⁹ See letters from CSA; Cybersecurity Coalition; NASAA; Prof. Perullo; Tenable.

³⁴⁰ See letter from Cybersecurity Coalition.

³⁴¹ See letters from NASAA and Tenable.

³⁴² See letter from Prof. Perullo.

Accordingly, as discussed below, we are providing smaller reporting companies an additional 180 days from the non-smaller reporting company compliance date before they must begin complying with Item 1.05 of Form 8-K.

H. Need for New Rules and Commission Authority

Some commenters argued that the 2011 Staff Guidance and 2018 Interpretive Release are sufficient to compel adequate cybersecurity disclosure, obviating the need for new rules.³⁴³ In this regard, two commenters highlighted the Proposing Release’s statement that cybersecurity disclosures “have improved since the issuance of the 2011 Staff Guidance and the 2018 Interpretive Release.”³⁴⁴ Another commenter said that Commission staff’s findings that certain cybersecurity incidents were reported in the media but not disclosed in a registrant’s filings and that registrants’ disclosures provide different levels of specificity suggested that “existing guidance is working, because each registrant should always be conducting an individualized, case-by-case analysis” and therefore disclosures “should expectedly vary significantly.”³⁴⁵ One commenter questioned whether the materials cited in the Proposing Release support the Commission’s conclusion there that current cybersecurity reporting may be inconsistent, not timely, difficult to locate, and contain insufficient detail.³⁴⁶ Two commenters recommended that the Commission “reemphasize” the prior guidance and “utilize its enforcement powers to ensure

³⁴³ See letters from BPI et al.; CTIA; ISA; ITI; SCG; SIFMA; Virtu.

³⁴⁴ See letters from Virtu (citing Proposing Release at 16594); BPI et al. (pointing to the Proposing Release’s citation of Stephen Klemash and Jamie Smith, *What companies are disclosing about cybersecurity risk and oversight*, EY (Aug. 10, 2020), available at https://www.ey.com/en_us/board-matters/whatcompanies-are-disclosing-about-cybersecurity-riskand-oversight).

³⁴⁵ See letter from ITI.

³⁴⁶ See letter from BPI et al. (discussing Moody’s Investors Service, Research Announcement, *Cybersecurity disclosures vary greatly in high-risk industries* (Oct. 3, 2019); NACD et al., *The State of Cyber-Risk Disclosures of Public Companies* (Mar. 2021), at 3).

public companies continue to report material cyber incidents.”³⁴⁷ One commenter provided the results from a survey it conducted of its members, finding that “only 10-20% of the 192 respondents reported that their shareholders have requested information or asked a question on” various cybersecurity topics, while “64.3% of the respondents indicated that their investors had not engaged with them” on those topics.³⁴⁸ Another commenter pointed to a 2022 study finding that less than 1% of cybersecurity breaches are “material,” and asserted that current disclosures adequately reflect such a level of material breaches.³⁴⁹ Some commenters also stated that the Commission should forgo regulation of cybersecurity disclosure because other agencies’ regulations are sufficient.³⁵⁰

Other commenters, by contrast, stated that the 2011 Staff Guidance and the 2018 Interpretive Release, while helpful, have not been sufficient to provide investors with the material information they need. One such commenter explained that “[t]he Commission’s past guidance, while in line with our views, does not go far enough. The Proposed Rule is needed to provide clarity regarding what, when, and how to disclose material cybersecurity incident information . . . The improved standardization of disclosures included in the Proposed Rule adds clarity to the reporting process.”³⁵¹ Another commenter stated that “[t]he lack of timely,

³⁴⁷ See letters from Virtu; SIFMA.

³⁴⁸ See letter from SCG.

³⁴⁹ See letter from ISA.

³⁵⁰ See, e.g., letters from CTIA (“The wireless industry is also regulated by the FCC, in several relevant respects . . . In addition to FCC requirements, wireless carriers comply with disclosure obligations under state law, which may require notices to individual consumers and state regulators. Providers are also subject to FCC reporting requirements regarding network outages.”); Sen. Portman (“Congress intended that the Cyber Incident Reporting for Critical Infrastructure Act be the primary means for reporting of cyber incidents to the Federal Government, that such reporting be through CISA, and that the required rule occupy the space regarding cyber incident reporting”); SIFMA (stating the proposal “is unwarranted in light of other, existing regulations and the Commission’s lack of statutory responsibility for cybersecurity regulation of public companies”).

³⁵¹ See letter from CalPERS. *Accord* letter from Better Markets (“Even in instances where a company discloses relevant cybersecurity incidents, board and management oversights and abilities, and policies and procedures in

comprehensive disclosure of material cyber events exposes investors and the community at large to potential harm.”³⁵²

As the Commission explained in the Proposing Release, Commission staff has observed insufficient and inconsistent cybersecurity disclosure notwithstanding the prior guidance.³⁵³ Here, in response to commenters, we emphasize that the final rules supplement the prior guidance but do not replace it. The final rules are aimed at remedying the lack of material cybersecurity incident disclosure, and the scattered, varying nature of cybersecurity strategy, risk management, and governance disclosure, the need for which some commenters confirmed.³⁵⁴ The final rules therefore add an affirmative cybersecurity incident disclosure obligation, and they centralize cybersecurity risk management, strategy, and governance disclosure. While we acknowledge commenters who noted the improvements to certain cybersecurity-related disclosures in response to the 2018 Interpretive Release, and we agree there have been improvements in the areas that the guidance touched upon, we note that the guidance does not mandate consistent or comparable public disclosure of material incidents or otherwise address the topics that are the subject of the final rules. And in response to commenters who suggested that other agencies’ rules on cybersecurity reporting are sufficient, we note that, unlike the final rules, such rules are not tailored to the informational needs of investors; instead, they focus on the needs of regulators, customers, and individuals whose data have been breached.

Accordingly, we believe the final rules are necessary and appropriate in the public interest and

a comprehensive manner, the information is scattered throughout various sections of the Form 10-K. While the 2018 guidance adopted by the Commission successfully identified potential disclosure requirements for companies to think about when disclosing cybersecurity risks, governance, and incidents, it did not solve the problem confronting investors who must search various sections of the Form 10-K for the disclosures.”).

³⁵² See letter from CII.

³⁵³ Proposing Release at 16594, 16599, 16603.

³⁵⁴ See *supra* notes 351 and 352.

for the protection of investors, consistent with the Commission’s authority.

We also note that the 2018 Interpretive Release remains in place, as it treats a number of topics not covered by the new rules. Those topics include, for instance, incorporating cybersecurity-related information into risk factor disclosure under Regulation S-K Item 105, into management’s discussion and analysis under Regulation S-K Item 303, into the description of business disclosure under Regulation S-K Item 101, and, if there is a relevant legal proceeding, into the Regulation S-K Item 103 disclosure.³⁵⁵ The 2018 Interpretive Release also notes the Commission’s expectation that, consistent with Regulation S-X, a company’s financial reporting and control systems should be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as that information becomes available.³⁵⁶

With respect to the Commission’s authority to adopt the final rules, some commenters asserted that the Commission does not have the authority to regulate cybersecurity disclosure.³⁵⁷ These commenters argued that the Proposing Release did not adequately explain which statutory provisions the Commission was relying on to propose the disclosure requirements, that the statutory provisions the Commission did identify do not provide a legal basis to require the proposed disclosures, that the release did not show the requirements were necessary or appropriate to achieve statutory goals, and that the requirements implicate the major questions doctrine and non-delegation principles. Additionally, one commenter stated that “Congress

³⁵⁵ See 2018 Interpretive Release.

³⁵⁶ *Id.*

³⁵⁷ See letters from International Association of Drilling Contractors; NRF; Virtu.

intended that [CIRCIA] be the primary means for reporting of cyber incidents to the federal government.”³⁵⁸

We disagree. Disclosure to investors is a central pillar of the Federal securities laws. The Securities Act of 1933 “was designed to provide investors with full disclosure of material information concerning public offerings of securities.”³⁵⁹ In addition, the Securities Exchange Act of 1934 imposes “regular reporting requirements on companies whose stock is listed on national securities exchanges.”³⁶⁰ Together, the provisions of the Federal securities laws mandating release of information to the market—and authorizing the Commission to require additional disclosures—have prompted the Supreme Court to “repeatedly” describe “the fundamental purpose” of the securities laws as substituting “a philosophy of full disclosure for the philosophy of caveat emptor.”³⁶¹ This bedrock principle of “[d]isclosure, and not paternalistic withholding of accurate information, is the policy chosen and expressed by Congress.”³⁶² Moreover, “[u]nderlying the adoption of extensive disclosure requirements was a

³⁵⁸ See letter from Sen. Portman. We address this comment in Section II.A.3, *supra*.

³⁵⁹ *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 195 (1976); *accord Pinter v. Dahl*, 486 U.S. 622 (1988) (“[t]he primary purpose of the Securities Act is to protect investors by requiring publication of material information thought necessary to allow them to make informed investment decisions concerning public offerings of securities in interstate commerce”).

³⁶⁰ *Ernst & Ernst*, 425 U.S. at 195 (1976); *see also Lawson v. FMR LLC*, 571 U.S. 429, 451 (2014) (referring to the Sarbanes-Oxley Act’s “endeavor to ‘protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws’” (quoting Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, 745 (2002))).

³⁶¹ *Lorenzo v. SEC*, 139 S. Ct. 1094, 1103 (2019); *accord Santa Fe Indus. v. Green*, 430 U.S. 462, 477-778 (1977); *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128, 151 (1972); *SEC v. Capital Gains Research Bureau, Inc.*, 375 U.S. 180, 186 (1963).

³⁶² *Basic*, 485 U.S. at 234. Congress also legislated on the core premise that “public information generally affects stock prices,” *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 272 (2014), and those prices can significantly affect the economy, 15 U.S.C. 78b(2) and (3).

legislative philosophy: ‘There cannot be honest markets without honest publicity. Manipulation and dishonest practices of the market place thrive upon mystery and secrecy.’”³⁶³

Several provisions of the Federal securities laws empower the Commission to carry out these fundamental Congressional objectives. Under the Securities Act, the Commission has authority to require, in a publicly filed registration statement, that issuers offering and selling securities in the U.S. public capital markets include information specified in Schedule A of the Act, including the general character of the issuer’s business, the remuneration paid to its officers and directors, details of its material contracts and certain financial information, as well as “such other information . . . as the Commission may by rules or regulations require as being necessary or appropriate in the public interest or for the protection of investors.”³⁶⁴ In addition, under the Exchange Act, issuers of securities traded on a national securities exchange or that otherwise have total assets and shareholders of record that exceed certain thresholds must register those securities with the Commission by filing a registration statement containing “[s]uch information, in such detail, as to the issuer” in respect of, among other things, “the organization, financial structure and nature of the [issuer’s] business” as the Commission by rule or regulation determines to be in the public interest or for the protection of investors.³⁶⁵ These same issuers must also provide “such information and documents . . . as the Commission shall require to keep reasonably current the information and documents required to be included in or filed with [a] . . .

³⁶³ *Basic*, 485 U.S. at 230 (quoting H.R. Rep. No. 73-1383, at 11 (1934)); *accord SEC v. Zandford*, 535 U.S. 813, 819 (2002) (“Among Congress’ objectives in passing the [Exchange] Act was ‘to insure honest securities markets and thereby promote investor confidence’ after the market crash of 1929” (quoting *United States v. O’Hagan*, 521 U.S. 642, 658 (1997))); *Nat’l Res. Def. Council, Inc. v. SEC*, 606 F.2d 1031, 1050 (D.C. Cir. 1979) (the Securities Act and Exchange Act “were passed during an unprecedented economic crisis in which regulation of the securities markets was seen as an urgent national concern,” and the Commission “was necessarily given very broad discretion to promulgate rules governing corporate disclosure,” which is “evident from the language in the various statutory grants of rulemaking authority”).

³⁶⁴ Securities Act Section 7(a)(1) and Schedule A.

³⁶⁵ Exchange Act Sections 12(b) and 12(g).

registration statement” as the Commission may prescribe as necessary or appropriate for the proper protection of investors and to insure fair dealing in the security.³⁶⁶ Separately, these issuers also must disclose “on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer . . . as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest.”³⁶⁷

These grants of authority are intentionally broad.³⁶⁸ Congress designed them to give the Commission, which regulates dynamic aspects of a market economy, the power and “flexibility” to address problems of inadequate disclosure as they arose.³⁶⁹ As the United States Court of Appeals for the District of Columbia Circuit explained, “[r]ather than casting disclosure rules in stone, Congress opted to rely on the discretion and expertise of the SEC for a determination of what types of additional disclosure would be desirable.”³⁷⁰

The Commission has long relied on the broad authority in these and other statutory provisions³⁷¹ to prescribe rules to ensure that the public company disclosure regime provides

³⁶⁶ Exchange Act Section 13(a). Other issuers that are required to comply with the reporting requirements of Section 13(a) include those that voluntarily register a class of equity securities under Exchange Act Section 12(g)(1) and, pursuant to Exchange Act 15(d), issuers that file a registration statement under the Securities Act that becomes effective.

³⁶⁷ Exchange Act Section 13(l).

³⁶⁸ See *Natural Resources Defense Council, Inc. v. SEC*, 606 F.2d 1031, 1045 (1979); see also H.R. REP. NO. 73-1383, at 6-7 (1934).

³⁶⁹ Courts have routinely applied and interpreted the Commission’s disclosure regulations without suggesting that the Commission lacked the authority to promulgate them. See, e.g., *SEC v. Life Partners Holdings, Inc.*, 854 F.3d 765 (5th Cir. 2017) (applying regulations regarding disclosure of risks and revenue recognition); *SEC v. Das*, 723 F.3d 943 (8th Cir. 2013) (applying Regulation S-K provisions regarding related-party transactions and executive compensation); *Panther Partners Inc. v. Ikanos Commc’ns, Inc.*, 681 F.3d 114 (2d Cir. 2012) (applying Item 303 of Regulation S-K, which requires disclosure of management’s discussion and analysis of financial condition); *SEC v. Goldfield Deep Mines Co.*, 758 F.2d 459 (9th Cir. 1985) (applying disclosure requirements for certain legal proceedings).

³⁷⁰ *Natural Resources Defense Council, Inc.*, 606 F.2d at 1045.

³⁷¹ Securities Act Section 19(a); Exchange Act Section 3(b); and Exchange Act Section 23(a).

investors with the information they need to make informed investment and voting decisions, in each case as necessary or appropriate in the public interest or for the protection of investors.³⁷² Indeed, the Commission’s predecessor agency,³⁷³ immediately upon enactment of the Securities Act, relied upon such authority to adopt Form A-1, precursor to today’s Form S-1 registration statement, to require disclosure of information including, for example, a list of states where the issuer owned property and was qualified to do business and the length of time the registrant had been engaged in its business—topics that are not specifically enumerated in Schedule A of the Securities Act.³⁷⁴ Form A-1 also required disclosures related to legal proceedings, though there is no direct corollary in Schedule A.³⁷⁵

Consistent with the statutory scheme that Congress enacted, the Commission has continued to amend its disclosure requirements over time in order to respond to marketplace developments and investor needs. Accordingly, over the last 90 years, the Commission has eliminated certain disclosure items and adopted others pursuant to the authority in Sections 7 and 19(a) of the Securities Act and Sections 3(b), 12, 13, 15, and 23(a) of the Exchange Act. Those amendments include the adoption of an integrated disclosure system in 1982, which reconciled

³⁷² In considering whether a particular item of disclosure is necessary or appropriate in the public interest or for the protection of investors, the Commission considers both the importance of the information to investors as well as the costs to provide the disclosure. In addition, when engaged in rulemaking that requires it to consider or determine whether an action is necessary or appropriate in the public interest, the Commission also must consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation. *See* Section 2(b) of the Securities Act and Section 3(f) of the Exchange Act.

³⁷³ Prior to enactment of the Exchange Act, the Federal Trade Commission was empowered with administration of the Securities Act.

³⁷⁴ Items 3 through 5 of Form A-1; *see* Release No. 33-5 (July 6, 1933) [not published in the Federal Register]. The Commission’s disclosure requirements no longer explicitly call for this information.

³⁷⁵ This early requirement called for a statement of all litigation that may materially affect the value of the security to be offered, including a description of the origin, nature, and names of parties to the litigation. Item 17 of Form A-1. The Commission has retained a disclosure requirement related to legal proceedings in both Securities Act registration statements and in Exchange Act registration statements and periodic reports. 17 CFR 229.103.

the various disclosure items under the Securities Act and the Exchange Act and was intended to ensure that “investors and the marketplace have been provided with meaningful, nonduplicative information upon which to base investment decisions.”³⁷⁶

In keeping with Congressional intent, the Commission’s use of its authority has frequently focused on requiring disclosures that will give investors enhanced information about risks facing registrants. For example, in 1980, the Commission adopted Item 303 of Regulation S-K to require registrants to include in registration statements and annual reports a management’s discussion and analysis of financial condition (“MD&A”). This discussion is intended to allow investors to understand the registrant’s “financial condition, changes in its financial condition and results of operation” through the eyes of management.³⁷⁷ Item 303 includes a number of specific disclosure items, such as requiring the identification of any known trends or uncertainties that will result in, or that are reasonably likely to result in, a material change to the registrant’s liquidity,³⁷⁸ a material change in the mix and relative cost of the registrant’s capital resources,³⁷⁹ or a material impact on net sales, revenues, or income from continuing operations.³⁸⁰ Item 303 also requires registrants to “provide such other information

³⁷⁶ See *Adoption of Integrated Disclosure System*, Release No. 33-6383 (Mar. 3, 1982) [47 FR 11380 (Mar. 16, 1982)]. Even prior to the adoption of the integrated disclosure system in 1982, the Commission addressed anticipated disclosure issues in particular areas through the use of Guides for the Preparation and Filing of Registration Statements. See *Proposed Revision of Regulation S-K and Guides for the Preparation and Filing of Registration Statements and Reports*, Release No. 33-6276 (Dec. 23, 1980) [46 FR 78 (Jan. 2, 1981)] (discussing the use of Guides); see also *Notice of Adoption of Guide 59 and of Amendments to Guides 5 and 16 of the Guides for Preparation and Filing of Registration Statements Under the Securities Act of 1933*, Release No. 33-5396 (Jun. 1, 1973) (discussing, in response to fuel shortages in 1974, the obligation to disclose any material impact that potential fuel shortages might have and adding a new paragraph relating to disclosure by companies engaged in the gathering, transmission, or distribution of natural gas).

³⁷⁷ See *Management’s Discussion and Analysis of Financial Condition and Results of Operations; Certain Investment Company Disclosures*, Release No. 33-6231 (Sept. 2, 1980) [45 FR 63630 (Sept. 25, 1980)]; see also 17 CFR 229.303(a).

³⁷⁸ See 17 CFR 229.303(b)(1)(i).

³⁷⁹ See 17 CFR 229.303(b)(1)(ii)(B).

³⁸⁰ See 17 CFR 229.303(b)(2)(ii).

that the registrant believes to be necessary to an understanding of its financial condition, changes in financial condition, and results of operation.”³⁸¹ The Commission developed the MD&A disclosure requirements to supplement and provide context to the financial statement disclosures previously required by the Commission.

A few years later, in 1982, the Commission codified a requirement that dated back to the 1940s for registrants to include a “discussion of the material factors that make an investment in the registrant or offering speculative or risky,” commonly referred to as “risk factors.”³⁸² By definition, these disclosures encompass a discussion of risks, or prospective future events or losses, that might affect a registrant or investment. The initial risk factor disclosure item provided examples of possible risk factors, such as the absence of an operating history of the registrant, an absence of profitable operations in recent periods, the nature of the business in which the registrant is engaged or proposes to engage, or the absence of a previous market for the registrant’s common equity.³⁸³

In subsequent years, the Commission expanded both the scope of risks about which registrants must provide disclosures and the granularity of those disclosures. For example, in 1997, the Commission first required registrants to disclose quantitative information about market

³⁸¹ 17 CFR 229.303(b).

³⁸² See *Adoption of Integrated Disclosure System*, Release No. 33-6383 (Mar. 3, 1982) [47 FR 11380 (Mar. 16, 1982)] (“Release No. 33-6383”) (codifying the risk factor disclosure requirement as Item 503(c) of Regulation S-K); see also 17 CFR 229.105(a). Prior to 1982, the Commission stated in guidance that, if the securities to be offered are of a highly speculative nature, the registrant should provide “a carefully organized series of short, concise paragraphs summarizing the principal factors that make the offering speculative.” See Release No. 33-4666 (Feb. 7, 1964) [29 FR 2490 (Feb. 15, 1964)]. A guideline to disclose a summary of risk factors relating to an offering was first set forth by the Commission in 1968 and included consideration of five factors that may make an offering speculative or risky, including with respect to risks involving “a registrant’s business or proposed business.” See Guide 6, in *Guides for the Preparation and Filing of Registration Statements*, Release No. 33-4936 (Dec. 9, 1968) [33 FR 18617 (Dec. 16, 1968)] (“Release No. 33-4936”).

³⁸³ See Release No. 33-6383.

risk.³⁸⁴ That market risk disclosure included requirements to present “separate quantitative information . . . to the extent material” for different categories of market risk, such as “interest rate risk, foreign currency exchange rate risk, commodity price risk, and other relevant market risks, such as equity price risk.”³⁸⁵ Under these market risk requirements, registrants must also disclose various metrics such as “value at risk” and “sensitivity analysis disclosures.” In addition, registrants must provide certain qualitative disclosures about market risk, to the extent material.³⁸⁶

Each of these disclosure items reflects the Commission’s long-standing view that understanding the material risks faced by a registrant and how the registrant manages those risks can be just as important to assessing its business operations and financial condition as knowledge about its physical assets or material contracts. Indeed, investors may be unable to assess the value of those assets or contracts adequately without appreciating the material risks to which they are subject.³⁸⁷

In addition to risk-focused disclosures, over the decades, the Commission has also required registrants to provide information on a diverse range of topics that emerged as significant to investment or voting decisions, such as the extent of the board’s role in the risk

³⁸⁴ See *Disclosure of Accounting Policies for Derivative Financial Instruments and Derivative Commodity Instruments and Disclosure of Quantitative and Qualitative Information About Market Risk Inherent in Derivative Financial Instruments, Other Financial Instruments, and Derivative Commodity Instruments*, Release No. 33-7386 (Jan. 31, 1997) [62 FR 6044 (Feb. 10, 1997)] (“Release No. 33-7386”) (“In light of those losses and the substantial growth in the use of market risk sensitive instruments, the adequacy of existing disclosures about market risk emerged as an important financial reporting issue.”); see also 17 CFR 229.305.

³⁸⁵ 17 CFR 229.305(a)(1).

³⁸⁶ See 17 CFR 229.305(b).

³⁸⁷ As early as the 1940s, the Commission issued stop order proceedings under Section 8(d) of the Securities Act in which the Commission suspended the effectiveness of previously filed registration statements due, in part, to inadequate disclosure about speculative aspects of the registrant’s business. See *In the Matter of Doman Helicopters, Inc.*, 41 S.E.C. 431 (Mar. 27, 1963); *In the Matter of Universal Camera Corp.*, 19 S.E.C. 648 (June 28, 1945)); see also Release No. 33-4936.

oversight of the registrant,³⁸⁸ the effectiveness of a registrant’s disclosure controls and procedures,³⁸⁹ related-party transactions,³⁹⁰ corporate governance,³⁹¹ and compensation discussion and analysis,³⁹² among many other topics, including on topics related to particular industries,³⁹³ offering structures,³⁹⁴ and types of transactions.³⁹⁵ In all these instances, the Commission’s exercise of its authority was guided by the baseline of the specific disclosures articulated by Congress. But, as Congress expressly authorized,³⁹⁶ the Commission’s exercise of its disclosure authority has not been narrowly limited to those statutorily prescribed disclosures—instead, it has been informed by both those disclosures and the need to protect investors.³⁹⁷ Many of these disclosures have since become essential elements of the public company reporting regime that Congress established.

To ensure the transparency that Congress intended when it authorized the Commission to promulgate disclosure regulations in the public interest or to protect investors,³⁹⁸ the Commission’s regulations must—as they have over time—be updated to account for changing

³⁸⁸ See 17 CFR 229.407.

³⁸⁹ See 17 CFR 229.307.

³⁹⁰ 17 CFR 229.404.

³⁹¹ 17 CFR 229.407.

³⁹² 17 CFR 229.402.

³⁹³ See 17 CFR 229.1200-1208 (Disclosure by Registrants Engaged in Oil and Gas Activities); 17 CFR 1300-1305 (Disclosure by Registrants Engaged in Mining Operations); 17 CFR 1400-1406 (Disclosure by Bank and Savings and Loan Registrants).

³⁹⁴ See 17 CFR Subpart 1100 (Asset-Backed Securities).

³⁹⁵ See 17 CFR subpart 900 (Roll-Up Transactions); 17 CFR 229.1000-1016 (Mergers and Acquisitions).

³⁹⁶ See *supra* notes 364 to 366 and accompanying text.

³⁹⁷ For example, Item 303(b)(2) of Regulation S-K calls for information well beyond the basic profit and loss statement specified in Schedule A by requiring issuers to disclose any unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income—and the extent to which income was so affected—so that investors can better understand the reported results of operations.

³⁹⁸ See *supra* notes 368 to 370 and accompanying text.

market conditions, new technologies, new transaction structures, and emergent risks. In this regard, we disagree with one commenter’s assertion that the Commission’s disclosure authority is “limited to specific types of information closely related to the disclosing company’s value and financial condition.”³⁹⁹ The commenter misstates the scope and nature of the Commission’s authority. There is a wealth of information about a company apart from that which appears in the financial statements that is related to a company’s value and financial condition, including the material risks (cybersecurity and otherwise) a company faces. Nor did Congress dictate that the Commission limit disclosures only to information that is “closely related” to a company’s “value and financial condition.” By also empowering the Commission to require “such other information . . . as the Commission may by rules or regulations require as being necessary or appropriate in the public interest or for the protection of investors,”⁴⁰⁰ Congress recognized that there is information that is vital for investors to understand in making informed investment decisions but does not directly relate to a company’s value and financial condition.⁴⁰¹

The narrow reading of the Commission’s authority advocated by the commenter would foreclose many of these longstanding elements of disclosure that market participants have come to rely upon for investor protection and fair dealing of securities.⁴⁰² Moreover, Congress itself has amended, or required the Commission to amend, the Federal securities laws many times. But Congress has not restricted the Commission’s disclosure authority; rather, Congress has typically sought to further expand and supplement that authority with additional mandated disclosures.

³⁹⁹ See letter from NRF.

⁴⁰⁰ Securities Act Section 7(a).

⁴⁰¹ For example, Schedule A calls for information regarding, among other things: the names of the directors or persons performing similar functions, the disclosure of owners of record of more than 10% of any class of stock of an issuer; commissions paid to underwriters; the renumeration paid to directors and certain officers; and information about certain material contracts.

⁴⁰² See letter from NRF.

We also reject the commenter’s suggestion that the final rules are an attempt to “usurp the undelegated role of maintaining cyber safety in America.”⁴⁰³ The final rules are indifferent as to whether and to what degree a registrant may have identified and chosen to manage a cybersecurity risk. Rather, the final rules reflect the reality, as acknowledged by the same commenter, that “[c]ybersecurity is . . . an area of growing importance to companies across the world.”⁴⁰⁴ When those companies seek to raise capital from investors in U.S. public markets, we believe it is appropriate that they share information about whether and, if so, how they are managing material cybersecurity risks so that investors can make informed investment and voting decisions consistent with their risk tolerance and investment objectives.

Finally, with respect to the commenter’s contention that a broad reading of the Commission’s disclosure authority could raise separation of powers concerns,⁴⁰⁵ we note that a statutory delegation is constitutional as long as Congress lays down by legislative act an intelligible principle to which the person or body authorized to exercise the delegated authority is directed to conform.⁴⁰⁶ In this instance, Congress has required that any new disclosure requirements be “necessary or appropriate in the public interest or for the protection of investors,”⁴⁰⁷ which has guided the Commission’s rulemaking authority for nearly a century. We therefore believe that the final rules are fully consistent with constitutional principles regarding separation of powers.

⁴⁰³ *Id.*

⁴⁰⁴ *Id.*

⁴⁰⁵ *Id.*

⁴⁰⁶ *Gundy v. U.S.*, 139 S. Ct. 2116, 2123 (plurality op.).

⁴⁰⁷ See Securities Act Section 19(a) and Exchange Act Section 23(a); accord *Nat'l Res. Def. Council*, 606 F.2d at 1045, 1050–52.

I. Compliance Dates

The final rules are effective September 5, 2023. With respect to Item 106 of Regulation S-K and item 16K of Form 20-F, all registrants must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. With respect to compliance with the incident disclosure requirements in Item 1.05 of Form 8-K and in Form 6-K, all registrants other than smaller reporting companies must begin complying on December 18, 2023. As discussed above, smaller reporting companies are being given an additional 180 days from the non-smaller reporting company compliance date before they must begin complying with Item 1.05 of Form 8-K, on June 15, 2024.

With respect to compliance with the structured data requirements, as noted above, all registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after the initial compliance date for any issuer for the related disclosure requirement. Specifically:

- For Item 106 of Regulation S-K and item 16K of Form 20-F, all registrants must begin tagging responsive disclosure in Inline XBRL beginning with annual reports for fiscal years ending on or after December 15, 2024; and
- For Item 1.05 of Form 8-K and Form 6-K all registrants must begin tagging responsive disclosure in Inline XBRL beginning on December 18, 2024.

III. OTHER MATTERS

If any of the provisions of these rules, or the application thereof to any person or circumstance, is held to be invalid, such invalidity shall not affect other provisions or application of such provisions to other persons or circumstances that can be given effect without the invalid provision or application.

Pursuant to the Congressional Review Act, the Office of Information and Regulatory Affairs has designated these rules as not a “major rule,” as defined by 5 U.S.C. 804(2).

IV. ECONOMIC ANALYSIS

A. Introduction

We are mindful of the costs imposed by, and the benefits to be obtained from, our rules. Section 2(b) of the Securities Act⁴⁰⁸ and Section 3(f) of the Exchange Act⁴⁰⁹ direct the Commission, when engaging in rulemaking where it is required to consider or determine whether an action is necessary or appropriate in the public interest, to consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation. Further, Section 23(a)(2) of the Exchange Act⁴¹⁰ requires the Commission, when making rules under the Exchange Act, to consider the impact that the rules would have on competition, and prohibits the Commission from adopting any rule that would impose a burden on competition not necessary or appropriate in furtherance of the Exchange Act. The discussion below addresses the economic effects of the final rules, including the likely benefits and costs, as well as the likely effects on efficiency, competition, and capital formation.

Where possible, we have attempted to quantify the benefits, costs, and effects on efficiency, competition, and capital formation expected to result from the final rules. In some cases, however, we are unable to quantify the potential economic effects because we lack information necessary to provide a reasonable estimate. For example, we lack the data to estimate any potential decrease in mispricing that might result from the rule, because we do not know how registrants’ disclosures of cybersecurity risk and governance will change or which

⁴⁰⁸ 15 U.S.C. 77b(b).

⁴⁰⁹ 15 U.S.C. 78c(f).

⁴¹⁰ 15 U.S.C. 78w(a)(2).

cybersecurity incidents that would go undisclosed under the current guidance will be disclosed under the final rules. Where we are unable to quantify the economic effects of the final rules, we provide a qualitative assessment of the effects, and of the impacts of the final rule on efficiency, competition, and capital formation. To the extent applicable, the views of commenters relevant to our analysis of the economic effects, costs, and benefits of these rules are included in the discussion below.

While cybersecurity incident disclosure has become more frequent since the issuance of the 2011 Staff Guidance and 2018 Interpretive Release, there is concern that variation persists in the timing, content, and format of registrants' existing cybersecurity disclosure, and that such variation may harm investors (as further discussed below).⁴¹¹ When disclosures about cybersecurity breaches are made, they may not be timely or consistent. Because of the lack of consistency in when and how companies currently disclose incidents, it is difficult to assess quantitatively the timeliness of disclosures under current practices. According to Audit Analytics data, in 2021, it took on average of 42 days for companies to discover breaches, and then it took an average of 80 days and a median of 56 days for companies to disclose a breach after its discovery.⁴¹² These data do not tell us when disclosure occurs relative to companies' materiality determinations. That said, the report notes that some breaches were disclosed for the first time to investors in periodic reports, the timing of which are unrelated to the timing of the

⁴¹¹ See *supra* Section I. See also *supra* note 18 and accompanying text; Eli Amir, Shai Levi, & Tsafrir Livne, *Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets*, 23 REV. ACCT. STUD. 1177 (2018).

⁴¹² AUDIT ANALYTICS, *Trends in Cybersecurity Breaches* (Apr. 2022), available at https://www.auditanalytics.com/doc/AA_Trends_in_Cybersecurity_Report_April_2022.pdf (“Audit Analytics”) (looking specifically at disclosures by companies with SEC filing requirements and stating that: “[c]ybersecurity breaches can result in a litany of costs, such as investigations, legal fees, and remediation. There is also the risk of economic and reputational costs that can directly impact financial performance, such as reduced revenue due to lost sales.”).

incident or the company’s assessment of the materiality of the incident. This implies at least some cybersecurity incident disclosures were not timely with respect to determination of materiality. Because cybersecurity incidents can significantly affect registrants’ stock prices, delayed disclosure results in mispricing of securities, harming investors.⁴¹³ Incident disclosure practices, with respect to both location and content, currently vary across registrants. For example, some registrants disclose incidents through Form 10-K, others Form 8-K, and still others on a company website, or in a press release. Some disclosures do not discuss whether the cybersecurity incident had material impact on the company.⁴¹⁴ Additionally, evidence suggests registrants may be underreporting cybersecurity incidents.⁴¹⁵ More timely, informative, and standardized disclosure of material cybersecurity incidents may help investors to assess an incident’s impact better.

While disclosures about cybersecurity risk management, strategy, and governance have been increasing at least since the issuance of the 2018 Interpretive Release, they are not currently provided by all registrants. Despite the increasing prevalence of references to cybersecurity risks in disclosures, however, registrants do not consistently or uniformly disclose information related to cybersecurity risk management, strategy, and governance.⁴¹⁶ Registrants currently make such disclosures in varying sections of a company’s periodic and current reports, such as in risk factors, in management’s discussion and analysis, in a description of business and legal proceedings, or in financial statement disclosures, and sometimes include them with other

⁴¹³ See Shinichi Kamiya, et al., *Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms*, 139 J. FIN. ECON. 721 (2021).

⁴¹⁴ Based on staff analysis of the current and periodic reports in 2022 for companies identified by having been affected by a cybersecurity incident.

⁴¹⁵ See BITDEFENDER, *supra* note 18 and accompanying text.

⁴¹⁶ See *supra* Section II.C.1.b. and c.; see also letter from Better Markets.

unrelated disclosures.⁴¹⁷ One commenter noted that current disclosure is “piecemeal” in nature and that the varying content and placement make it difficult for investors and other market participants to locate and understand the cybersecurity risks that registrants face and their preparedness for an attack, and to make comparisons across registrants.⁴¹⁸

As we discuss in more detail below, some commenters supported the proposed rule. Specifically, one commenter noted that markets responded negatively to delayed cybersecurity disclosures, suggesting that timeliness in disclosing incidents is valuable to investors.⁴¹⁹ Further, some academic commenters submitted papers that they authored finding that evidence suggests that companies experiencing data breaches subsequently experience higher borrowing costs.⁴²⁰ On the other hand, other commenters contended that the proposed rules would hinder capital formation, particularly for small registrants,⁴²¹ or that a more cost-effective alternative to the proposed rules would be to look to existing rules to elicit relevant disclosures, as articulated by the 2011 Staff Guidance and the 2018 Interpretive Release.⁴²² Several commenters pointed out that the proposed disclosures on cybersecurity risk management, strategy, and governance might be overly prescriptive and would potentially provide a roadmap for threat actors, and that these rules could increase, not decrease costs.⁴²³ In response to those comments, these provisions have

⁴¹⁷ See Proposing Release at 16606 (Table 1. Incidence of Cybersecurity-Related Disclosures by 10-K Location).

⁴¹⁸ See letter from Better Markets.

⁴¹⁹ See letter from Prof. Choudhary.

⁴²⁰ See letters from Profs. Huang & Wang; Prof. Sheneman.

⁴²¹ See letter from BIO.

⁴²² See letter from NRF.

⁴²³ See letters from ABA; ACLI; APCIA; BIO; BPI et al.; Business Roundtable; Chamber; CSA; CTIA; EIC; Enbridge; FAH; Federated Hermes; GPA; ITI; ISA; Nareit; NAM; NMHC; NRA; NRF; SIFMA; Sen. Portman; TechNet; TransUnion; USTelecom; Virtu.

been modified in the final rule, which should reduce the perceived risk of providing a roadmap for threat actors compared with the proposal.

B. Economic Baseline

1. Current Regulatory Framework

To assess the economic impact of the final rules, the Commission is using as its baseline the existing regulatory framework and market practice for cybersecurity disclosure. Although a number of Federal and State rules and regulations obligate registrants to disclose cybersecurity risks and incidents in certain circumstances, the Commission’s regulations currently do not explicitly address cybersecurity.⁴²⁴

As noted in the Proposing Release, cybersecurity threats and incidents continue to increase in prevalence and seriousness, posing an ongoing and escalating risk to public registrants, investors, and other market participants.⁴²⁵ The number of reported breaches disclosed by public companies has increased almost 600 percent over the last decade, from 28 in 2011 to 131 in 2020 and 188 in 2021.⁴²⁶ Although estimating the total cost of cybersecurity incidents is difficult, as many events may be unreported, some estimates put the economy-wide total costs as high as trillions of dollars per year in the U.S. alone.⁴²⁷ The U.S. Council of Economic Advisers estimated that in 2016 the total cost of cybersecurity incidents was between

⁴²⁴ See Proposing Release at 16593-94 for a detailed discussion of the existing regulatory framework.

⁴²⁵ Unless otherwise noted, when we discuss the economic effects of the final rules on “other market participants,” we mean those market participants that typically provide services for investors and who rely on the information in companies’ filings (such as financial analysts, investment advisers, and portfolio managers).

⁴²⁶ Audit Analytics, *supra* note 412.

⁴²⁷ See CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *Cost of a Cyber Incident: Systemic Review and Cross-Validation* (Oct. 26, 2020), available at https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf (based on a literature review of publications discussing incidents that occurred in the United States or to U.S.-based companies).

\$57 billion and \$109 billion, or between 0.31 and 0.58 percent of U.S. GDP in that year.⁴²⁸ A more recent estimate suggests the average cost of a data breach in the U.S. is \$9.44 million.⁴²⁹ Executives, boards of directors, and investors remain focused on the emerging risk of cybersecurity. A 2022 survey of bank Chief Risk Officers found that they identified managing cybersecurity risk as the top strategic risk.⁴³⁰ In 2022, a survey of audit committee members again identified cybersecurity as a top area of focus in the coming year.⁴³¹

In 2011, the Division of Corporation Finance issued interpretive guidance providing the Division's views concerning operating registrants' disclosure obligations relating to cybersecurity risks and incidents.⁴³² This 2011 Staff Guidance provided an overview of existing disclosure obligations that may require a discussion of cybersecurity risks and cybersecurity incidents, along with examples of potential disclosures.⁴³³ Building on the 2011 Staff Guidance, the Commission issued the 2018 Interpretive Release to assist operating companies in preparing disclosure about cybersecurity risks and incidents under existing disclosure rules.⁴³⁴ In the 2018

⁴²⁸ COUNCIL OF ECON. ADVISERS, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Feb. 2018), available at <https://trumpwhitehouse.archives.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/> (estimating total costs, rather than costs of only known and disclosed incidents).

⁴²⁹ Ponemon Institute & IBM Security, *Cost of a Data Breach Report 2022* (July 2022), available at <https://www.ibm.com/downloads/cas/3R8N1DZJ> (estimating based on analysis of 550 organizations impacted by data breaches that occurred between Mar. 2021 and Mar. 2022).

⁴³⁰ EY AND INSTITUTE OF INTERNATIONAL FINANCE, *12th Annual EY/IIF Global Bank Risk Management Survey*, at 14 (2022), available at https://www.iif.com/portals/0/Files/content/32370132_ey-iif_global_bank_risk_management_survey_2022_final.pdf (stating 58% of surveyed banks' Chief Risk Officers cite "inability to manage cybersecurity risk" as the top strategic risk). See also EY, *EY CEO Imperative Study* (July 2019), available at https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/growth/ey-ceo-imperative-exec-summ-single-spread-final.pdf.

⁴³¹ CENTER FOR AUDIT QUAL. & DELOITTE, *Audit Committee Practices Report: Priorities and Committee Composition* (Jan. 2023) available at <https://www.thecaq.org/audit-committee-practices-report-2023/>. See also CENTER FOR AUDIT QUAL. & DELOITTE, *Audit Committee Practices Report: Common Threads Across Audit Committees* (Jan. 2022), available at <https://www.thecaq.org/2022-ac-practices-report/>.

⁴³² See 2011 Staff Guidance.

⁴³³ *Id.*

⁴³⁴ See 2018 Interpretive Release.

Interpretive Release, the Commission reiterated that registrants must provide timely and ongoing information in periodic reports (Form 10-Q, Form 10-K, and Form 20-F) about material cybersecurity risks and incidents that trigger disclosure obligations.⁴³⁵ Additionally, the 2018 Interpretive Release encouraged registrants to continue to use current reports (Form 8-K or Form 6-K) to disclose material information promptly, including disclosure pertaining to cybersecurity matters.⁴³⁶ Further, the 2018 Interpretive Release noted that to the extent cybersecurity risks are material to a registrant’s business, the Commission believes that the required disclosure of the registrant’s risk oversight should include the nature of the board’s role in overseeing the management of that cybersecurity risk.⁴³⁷ The 2018 Interpretive Release also stated that a registrant’s controls and procedures should enable it to, among other things, identify cybersecurity risks and incidents and make timely disclosures regarding such risks and incidents.⁴³⁸ Finally, the 2018 Interpretive Release highlighted the importance of insider trading prohibitions and the need to refrain from making selective disclosures of cybersecurity risks or incidents.⁴³⁹

In keeping with existing obligations, companies are increasingly acknowledging cybersecurity risks in their disclosures. One analysis of disclosures made by Fortune 100 companies that filed 10-Ks and proxy statements found 95 percent of those companies disclosed a focus on cybersecurity risk in the risk oversight section of their proxy statements filed in the

⁴³⁵ *Id.* at 8168-8170.

⁴³⁶ *Id.* at 8168.

⁴³⁷ *Id.* at 8170.

⁴³⁸ *Id.* at 8171.

⁴³⁹ *Id.* at 8171-8172.

period ending in May 2022, up from 89 percent of filings in 2020 and 76 percent in 2018.⁴⁴⁰

Disclosures of efforts to mitigate cybersecurity risk were found in 99 percent of proxy statements or Forms 10-K, up from 93 percent in 2020 and 85 percent in 2018.⁴⁴¹ The Fortune 100 list is composed of the highest-revenue companies in the United States. As discussed later in this economic analysis, we observed the overall rate of disclosure across not just the largest, but all filers, approximately 8,400, to be approximately 73 percent.⁴⁴² Further, one commenter noted that current disclosures are “scattered and unpredictable” rather than “uniform,” which “diminishes their effectiveness,” and so the final rule should improve investors’ ability to find and compare disclosures.⁴⁴³

Registrants currently are and may continue to be subject to other cybersecurity incident disclosure requirements developed by various industry regulators and contractual counterparties. As discussed in Section II, CIRCIA was passed in March 2022 and requires CISA to develop and issue regulations on cybersecurity reporting. As set forth in CIRCIA, once those regulations are adopted, covered entities will have 72 hours to report covered cybersecurity incidents to CISA and will also be required to report a ransom payment as the result of a ransomware attack within 24 hours of the payment being made.⁴⁴⁴ In addition, Federal contractors may be required to monitor and report cybersecurity incidents and breaches or face liability under the False Claims

⁴⁴⁰ See EY CTR FOR BD MATTERS, *How Cyber Governance and Disclosures are Closing the Gaps in 2022* (Aug. 2022), available at https://www.ey.com/en_us/board-matters/how-cyber-governance-and-disclosures-are-closing-the-gaps-in-2022.

⁴⁴¹ *Id.*

⁴⁴² See *infra* note 456 (describing textual analysis) and accompanying text.

⁴⁴³ See letter from Better Markets. Although uniformity should improve investors’ ability to find and compare disclosures, within that structure the final rule allows customization to capture complexity and avoid unnecessarily simplifying issues for the sake of standardization.

⁴⁴⁴ 6 U.S.C. 681b. See also *supra* notes 21 to 23 and accompanying text.

Act.⁴⁴⁵ An FCC rule directs covered telecommunications providers on how and when to disclose breaches of certain customer data.⁴⁴⁶ HIPAA requires covered entities and their business associates to provide notification following a breach of unsecured protected health information.⁴⁴⁷ Similar rules require vendors of personal health records and related entities to report data breaches to affected individuals and the FTC.⁴⁴⁸ All 50 states have data breach laws that require businesses to notify individuals of security breaches involving their personally identifiable information.⁴⁴⁹ There are other rules that registrants must follow in international jurisdictions. For example, in the European Union, the General Data Protection Regulation mandates disclosure of cybersecurity breaches.⁴⁵⁰

These other cybersecurity incident disclosure requirements may cover some of the material incidents that registrants will need to disclose under the final rules. However, not all registrants are subject to each of these other incident disclosure requirements and the timeliness and public reporting elements of these requirements vary, making it difficult for investors and

⁴⁴⁵ See DEP’T OF JUSTICE, OFFICE OF PUB. AFFAIRS, *Justice News: Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative*, (Oct. 6, 2021), available at <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>; see, e.g., FAR 52.239-1 (requiring contractors to “immediately” notify the Federal Government if they become aware of “new or unanticipated threats or hazards . . . or if existing safeguards have ceased to function”).

⁴⁴⁶ See 47 CFR 64.2011; *see also supra* Section II.A.3.

⁴⁴⁷ See 45 CFR 164.400 through 414 (Notification in the Case of Breach of Unsecured Protected Health Information).

⁴⁴⁸ See 16 CFR 318 (Health Breach Notification Rule).

⁴⁴⁹ Note that there are carve-outs to these rules, and not every company may fall under any particular rule. See NAT’L CONFERENCE OF STATE LEGISLATURES, *Security Breach Notification Laws* (updated Jan. 17, 2022), available at <https://www.ncsl.org/technology-and-communication/security-breach-notification-laws>.

⁴⁵⁰ See Regulation (EU) 2016/679, of the European Parliament and the Council of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), arts. 33 (Notification of a personal data breach to the supervisory authority), 34 (Communication of a personal data breach to the data subject), 2016 O.J. (L 119) 1 (“GDPR”).

other market participants to be alerted to the breaches and to gain an adequate understanding of the impact of such incidents on a registrant.

Some registrants are also subject to other mandates regarding cybersecurity risk management, strategy, and governance. For instance, government contractors may be subject to the Federal Information Security Modernization Act, and use the NIST framework to manage information and privacy risks.⁴⁵¹ Certain financial institutions may be subject to the FTC's Standards for Safeguarding Customer Information Rule, requiring an information security program, including a qualified individual to oversee the security program, and the provision of periodic reports on the cybersecurity program to a company's board of directors or equivalent governing body.⁴⁵² Under HIPAA regulations, covered entities are subject to rules that require protection against reasonably anticipated threats to electronic protected health information.⁴⁵³ International jurisdictions also have cybersecurity risk mitigation measures and governance requirements (see, for example, the GDPR).⁴⁵⁴ These rules and regulations provide varying standards and requirements for disclosing cybersecurity risk management, strategy, and governance, and may not provide investors with public or clear and comparable disclosure regarding how a particular registrant manages its cybersecurity risk profile.

2. Affected Parties

The parties that are likely to be affected by the final rules include investors, registrants, other market participants that use the information provided in company filings (such as financial

⁴⁵¹ See NIST, NIST Risk Management Framework (updated Jan. 31, 2022), available at <https://csrc.nist.gov/projects/risk-management/fisma-background>.

⁴⁵² See 16 CFR 314.

⁴⁵³ See 45 CFR 164 (Security and Privacy); see also *supra* Section II.A.3.

⁴⁵⁴ See, e.g., GDPR, arts. 32 (Security of processing), 37 (Designation of the data protection officer).

analysts, investment advisers, and portfolio managers), and external stakeholders such as consumers and other companies in the same industry as affected companies.

We expect the final rules to affect all registrants with relevant disclosure obligations on Forms 10-K, 20-F, 8-K, or 6-K. This includes (1) approximately 7,300 operating companies filing on domestic forms (of which, approximately 120 are business development companies) and (2) 1,174 FPIs filing on foreign forms, based on all companies that filed such forms or an amendment thereto during calendar year 2022.⁴⁵⁵ Our textual analysis⁴⁵⁶ of all calendar year 2022 Form 10-K filings and amendments reveals that approximately 73 percent of domestic filers made some kind of cybersecurity-related disclosures, whether of incidents, risk, or governance.

We also analyzed calendar year 2022 Form 8-K and Form 6-K filings. There were 71,505 Form 8-K filings in 2022, involving 7,416 filers, out of which 35 filings reported material cybersecurity incidents.⁴⁵⁷ Similarly, there were 27,296 Form 6-K filings in 2022, involving 1,161 filers, out of which 22 filings reported material cybersecurity incidents.

C. Benefits and Costs of the Final Rules

The final rules will benefit investors, registrants, and other market participants, such as financial analysts, investment advisers, and portfolio managers, by providing more timely and informative disclosures relating to cybersecurity incidents and cybersecurity risk management, strategy, and governance, facilitating investor decision-making and reducing information

⁴⁵⁵ Estimates of affected companies here are based on the number of unique CIKs with at least one periodic report, current report, or an amendment to one of the two filed in calendar year 2022.

⁴⁵⁶ In performing this analysis, staff executed computer program-based keyword (and combination of key words) searches. This analysis covered 8,405 Forms 10-K and 10-K/A available in Intelligize (a division of RELX Inc.) filed in calendar year 2022 by 7,486 companies as identified by unique CIK.

⁴⁵⁷ The number of filers in our sample is larger than the number of estimated affected parties because, among other reasons, it includes 8-K filings by companies that have not yet filed their first annual report.

asymmetry in the market. The final rules also will entail costs. A discussion of the anticipated economic costs and benefits of the final rules is set forth in more detail below. We first discuss benefits, including benefits to investors and other market participants. We subsequently discuss costs, including the cost of compliance with the final rules. We conclude with a discussion of indirect economic effects on investors, external stakeholders such as consumers, and companies in the same industry with registrants subject to this rule, or those facing similar cybersecurity threats.

1. Benefits

Existing shareholders, and those seeking to purchase shares in registrants subject to the final rules, will be the main beneficiaries of the enhanced disclosure of both cybersecurity incidents and cybersecurity risk management, strategy, and governance as a result of the final rules. Specifically, investors will benefit because: (1) more informative and timely disclosure will improve investor decision-making by allowing investors to better understand a registrant's material cybersecurity incidents, material cybersecurity risks, and ability to manage such risks, reducing information asymmetry and the mispricing of securities in the market; and (2) more uniform and comparable disclosures will lower search costs and information processing costs. Other market participants that rely on financial statement information to provide services to investors, such as financial analysts, investment advisers, and portfolio managers, will also benefit.

a. More Timely and Informative Disclosure

The final rules provide more timely and informative disclosures, relative to the current disclosure environment, which will allow investors to better understand registrants' cybersecurity incidents, risks, and ability to manage such risks as well as reduce mispricing of

securities in the market. Timeliness benefits to investors will result from the requirement to disclose cybersecurity incidents within four business days of determining an incident was material, as well as the requirement to amend the disclosure to reflect material changes. Information benefits to investors will result from the disclosure of both (1) cybersecurity incidents and (2) cybersecurity risk management, strategy, and governance. Together, the timeliness and information benefits created by the final rules will reduce market mispricing and information asymmetry and potentially lower firms' cost of capital.

We anticipate Item 1.05, governing cybersecurity incident disclosure on Form 8-K, will lead to more timely disclosure to investors.⁴⁵⁸ Currently, there is not a specific requirement for a registrant to disclose a cybersecurity incident to investors in a timely manner after its discovery and determination of material impact.⁴⁵⁹ Item 1.05's requirement to disclose a material cybersecurity incident on Form 8-K within four business days after determining the incident is material will improve the overall timeliness of the disclosure offered to investors—disclosure that is relevant to the valuation of registrants' securities. It is well-documented in the academic literature that the market reacts negatively to announcements of cybersecurity incidents. For example, one study finds a statistically significant mean cumulative abnormal return of -0.84 percent in the three days following cyberattack announcements, which, according to the study, translates into an average value loss of \$495 million per attack.⁴⁶⁰ One commenter argued that

⁴⁵⁸ For foreign issuers, the disclosure is made via Form 6-K.

⁴⁵⁹ See *supra* Sections I and IV.B.1.

⁴⁶⁰ See Shinichi Kamiya, et al., *supra* note 413, at 719-749. See also Lawrence A. Gordon, Martin P. Loeb, & Lei Zhou, *The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?*, 19 (1) J. OF COMPUT. SEC. 33, 33-56 (2011) (finding “the impact of the broad class of information security breaches on stock market returns of firms is significant”); Georgios Spanos & Lefteris Angelis, *The Impact of Information Security Events to the Stock Market: A Systematic Literature Review*, 58 COMPUT. & SEC. 216-229 (2016) (documenting that the majority (75.6%) of the studies the paper reviewed report statistical significance of the impact of security events to the stock prices of companies). But see Katherine Campbell, et al., *The Economic*

the magnitude of stock market reaction to cybersecurity incidents from this study would not be considered significant by market participants, stating that “if a stock had a historical standard deviation of 1 percent and moved 0.8 percent on news, most market participants would suggest that the news was either not significant or the market had priced in that news so the reaction was muted.”⁴⁶¹ We note, however, that a cumulative abnormal return (CAR) of -0.84 percent refers not to the total return but to the return relative to how stocks in similar industries and with similar risk profiles moved; thus, indeed, a statistically significantly negative CAR represents a meaningful reaction and change to how the stock price would have moved that day absent the announcement of the cybersecurity incident. By allowing investors to make decisions based on more current, material, information, Item 1.05 will reduce mispricing of securities and information asymmetry in the market.

Information asymmetries due to timing could also be exploited by the malicious actors who caused a cybersecurity incident, those who could access and trade on material information stolen during a cybersecurity incident, or those who learn about the incident before public disclosure, causing further harm to investors who trade unknowingly against those with inside information.⁴⁶² Malicious actors may trade ahead of an announcement of a data breach that they

Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, 11 (3) J. OF COMPUT. SEC. 432, 431-448 (2003) (while finding limited evidence of an overall negative stock market reaction to public announcements of information security breaches, they also find “the nature of the breach affects this result,” and “a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information;” they thus conclude that “stock market participants appear to discriminate across types of breaches when assessing their economic impact on affected firms”).

⁴⁶¹ See letter from BIO.

⁴⁶² See Joshua Mitts & Eric Talley, *Informed Trading and Cybersecurity Breaches*, 9 HARV. BUS. L. REV. 1 (2019) (“In many respects, then, the cyberhacker plays a role in creating and imposing a unique harm on the targeted company—one that (in our view) is qualitatively different from ‘exogenous’ information shocks serendipitously observed by an information trader. Allowing a coordinated hacker-trader team to capture these arbitrage gains would implicitly subsidize the very harm-creating activity that is being ‘discovered’ in the first instance.”).

caused or pilfer material information to trade on ahead of company announcements. Trading on undisclosed cybersecurity information is particularly pernicious, because profits generated from this type of trading provide incentives for malicious actors to “create” more incidents and proprietary information to trade on, further harming the shareholders of impacted companies.⁴⁶³ Employees or related third-party vendors of a company experiencing a cybersecurity incident may also learn of the incident and trade against investors in the absence of disclosure. More timely disclosure as a result of Item 1.05 will reduce mispricing by reducing windows of information asymmetry in connection with a material cybersecurity incident, thereby reducing opportunities to exploit the mispricing, enhancing investor protection.

A commenter noted that there is risk the rule could, under certain conditions, aid stock manipulation efforts by malicious actors, offsetting these benefits.⁴⁶⁴ One commenter suggested that mandated disclosure timing could make public cybersecurity incident disclosure dates more predictable, and thus trading strategies based on the accompanying negative stock price reaction more consistent, to the extent malicious actors can monitor or control discovery of breaches they cause and correctly anticipate materiality determination timing. Their ability to do this is unclear, but we note that if the final rules increase the precision of strategies by attackers that involve shorting the stock of their targets, that would reduce the benefit of the final rules.

Item 1.05 allows registrants to delay filing for up to 30 days if the Attorney General determines that the incident disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. The delay may be extended

⁴⁶³ *Id.*

⁴⁶⁴ See letter from ISA.

up to an additional 30 days if the Attorney General determines disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. Beyond the final 60-day delay, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through Commission exemptive order. These delay periods and possible exemptive relief would curb the timeliness benefits discussed above but would reduce the costs of premature disclosure such as alerting malicious actors targeting critical infrastructure that their activities have been discovered.

By requiring all material cybersecurity incidents to be disclosed, Item 1.05 will also provide investors more informative disclosure by increasing material cybersecurity incident disclosure.⁴⁶⁵ There are currently reasons that registrants do not disclose cybersecurity incidents. For example, a registrant's managers may be reluctant to release information that they expect or anticipate will cause their stock price to suffer.⁴⁶⁶ Thus an agency problem prevents investors from receiving this useful information. In addition, registrants may consider only the benefits and costs that accrue to them when deciding whether to disclose an incident. As discussed in Section IV.C.3, incident disclosure can create indirect economic effects that accrue to parties other than the company itself. Companies focused on direct economic benefits, however, may not factor in this full range of effects resulting from disclosing cybersecurity incidents, resulting

⁴⁶⁵ See Amir, Levi, & Levine, *supra* note 411.

⁴⁶⁶ See, e.g., Kamiya, et al., *supra* note 413, at 719-749.

in less reporting and less information released to the market. The mandatory disclosure in Item 1.05 should thus lead to more incidents being disclosed, reducing mispricing of securities and information asymmetry in the market as stock prices will more accurately reflect registrants having experienced a cybersecurity incident.

Item 1.05 will also improve the informativeness of the content of cybersecurity incident disclosures. In 2022, when registrants filed a Form 8-K to report an incident, the Form 8-K did not necessarily state whether the incident was material, and in some cases, the Form 8-K stated that the incident was immaterial.⁴⁶⁷ Item 1.05 will require registrants to describe in an 8-K filing the material aspects of the nature, scope, and timing of a material cybersecurity incident and the material impact or reasonably likely material impact on the registrant, including on its financial condition and results of operations. The disclosure must also identify any information called for in Item 1.05(a) that is not determined or is unavailable at the time of the required filing. Registrants will then need to disclose this information in a Form 8-K amendment containing such information within four business days after the information is determined or becomes available. Item 1.05 is thus expected to elicit more pertinent information to aid investor decision-making. Additionally, the materiality requirement should minimize immaterial incident disclosure that might divert investor attention, which should reduce mispricing of securities. Numerous commenters on the Proposing Release agreed that more informative incident disclosure would be useful for investors.⁴⁶⁸

Regulation S-K Items 106(b) and (c) of the final rules provide further benefits by requiring registrants to disclose, in their annual reports on Form 10-K, information about their

⁴⁶⁷ Based on staff analysis of the 10,941 current and periodic reports in 2022 for companies available in Intelligize and identified as having been affected by a cybersecurity incident using a keyword search.

⁴⁶⁸ See, e.g., letters from Better Markets; CalPERS; PWC; Prof. Perullo.

cybersecurity risk management, strategy, and governance. The final rules require disclosure regarding a registrant’s processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as disclosure of the registrant’s board of directors’ oversight of risks from cybersecurity threats and management’s role in assessing and managing material risks from cybersecurity threats.⁴⁶⁹ There are currently no disclosure requirements on Forms 10-K or 10-Q that explicitly refer to cybersecurity risks or governance, and thus Item 106 will benefit investors by eliciting relevant information about how registrants are managing their material cybersecurity risks.

One commenter took issue with the usefulness of the proposed disclosures, arguing, for example, that the particular requirement to disclose whether a registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program was unnecessary because there was no evidence that such third parties improved a registrant’s cyber risk management, and some companies have internal cybersecurity risk management capabilities.⁴⁷⁰ Some, however, have noted that the use of independent third-party advisors may be “vital to enhancing cyber resiliency” by validating that the risk management program is meeting its objectives.⁴⁷¹ As discussed in Section II.C.1.c., it may be important for investors to know a registrant’s level of in-house versus outsourced cybersecurity capacity. Another commenter suggested that the requirement to disclose governance and risk management practices would be of limited value to investors, while being administratively burdensome.⁴⁷²

⁴⁶⁹ See *supra* Sections II.B and C. For foreign issuers, the disclosure is made via Form 20-F.

⁴⁷⁰ See letter from NRF.

⁴⁷¹ See Harvard Law School Forum on Corporate Governance Blog, posted by Steve W. Klemash, Jamie C. Smith, and Chuck Seets, *What Companies are Disclosing About Cybersecurity Risk and Oversight*, (posted Aug. 25, 2020), available at <https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/>.

⁴⁷² See letter from SIMFA.

Other commenters said that the required disclosures about cybersecurity governance and risk management were too granular to be useful and suggested that the specific disclosures be replaced with a more high-level explanation of management's and the board's roles in cybersecurity risk management and governance.⁴⁷³ One such commenter stated that the proposed disclosures would create pressures to provide boilerplate responses to the specific items that would need to be disclosed instead of providing a robust discussion of the way a registrant would manage cybersecurity risk management and governance.⁴⁷⁴ Another commenter stated that granular disclosures "may result in overly detailed filings that have little utility to investors."⁴⁷⁵ These commenters suggested that the specific disclosures should be replaced with a more high-level explanation of management's and the board's roles in cybersecurity risk management and governance.

In response to these comments, the Commission is not adopting certain proposed disclosure requirements, such as disclosure of whether the registrant has a designated chief information security officer. However, Items 106(b) and (c) still require risk, strategy and governance disclosures as we continue to believe disclosures of cybersecurity risk oversight and processes, as well as management's role and relevant expertise, are important to investors.

Improved timeliness and informativeness of cybersecurity disclosures may provide further benefit by lowering companies' cost of capital.⁴⁷⁶ As detailed above, the final rules

⁴⁷³ See letters from ABA; AGA/INGAA; EEI; Nareit; NYSE.

⁴⁷⁴ See letter from ABA.

⁴⁷⁵ See letter from NYSE.

⁴⁷⁶ See Leuz & Verrecchia, *The Economic Consequences of Increased Disclosure*, 38 J. ACCT. RES. 91 (2000) ("A brief sketch of the economic theory is as follows. Information asymmetries create costs by introducing adverse selection into transactions between buyers and sellers of firm shares. In real institutional settings, adverse selection is typically manifest in reduced levels of liquidity for firm shares (e.g., Copeland and Galai [1983], Kyle [1985], and Glosten and Milgrom [1985]). To overcome the reluctance of potential investors to hold firm shares in illiquid markets, firms must issue capital at a discount. Discounting results in fewer proceeds to the

should reduce information asymmetry and mispricing of securities. In an asymmetric information environment, investors are less willing to hold shares, reducing liquidity. Registrants may respond by issuing shares at a discount, increasing their cost of capital. By providing more and more credible disclosure, however, companies can reduce the risk of adverse selection faced by investors and the discount they demand, ultimately increasing liquidity and decreasing the company's cost of capital.⁴⁷⁷ Investors benefit when the companies they are invested in enjoy higher liquidity. Item 1.05 enables companies to provide more credible disclosure because currently, investors do not know whether an absence of incident disclosure means no incidents have occurred, or one has but the company has not yet chosen to reveal it. By requiring all material incidents to be reported, Item 1.05 supplies investors greater assurance that, indeed, barring extraordinary circumstances, no disclosure means the company has not been aware for more than four business days of a material incident having occurred. Similarly, Item

firm and hence higher costs of capital. A commitment to increased levels of disclosure reduces the possibility of information asymmetries arising either between the firm and its shareholders or among potential buyers and sellers of firm shares. This, in turn, should reduce the discount at which firm shares are sold, and hence lower the costs of issuing capital (e.g., Diamond and Verrecchia [1991] and Baiman and Verrecchia [1996]).”).

⁴⁷⁷ See Douglas W. Diamond & Robert E. Verrecchia, *Disclosure, Liquidity, and the Cost of Capital*, 46 J. FIN. 1325, 1325–1359 (1991) (finding that revealing public information to reduce information asymmetry can reduce a company's cost of capital through increased liquidity). See also Christian Leuz & Robert E. Verrecchia, *The Economic Consequences of Increased Disclosure*, 38 J. ACCT. RES. 91 (2000) (providing empirical evidence that increased disclosure lowers the information asymmetry component of the cost of capital in a sample of German companies); see also Christian Leuz & Peter D. Wysocki, *The Economics of Disclosure and Financial Reporting Regulation: Evidence and Suggestions for Future Research*, 54 J. ACCT. RES. 525 (2016) (providing a comprehensive survey of the literature on the economic effect of disclosure). Although disclosure could be beneficial for the company, several conditions must be met for companies to voluntarily disclose all their private information. See Anne Beyer, et al., *The Financial Reporting Environment: Review Of The Recent Literature*, 50 J. ACCT. & ECON. 296, 296-343 (2010) (discussing conditions under which companies voluntarily disclose all their private information, and these conditions include “(1) disclosures are costless; (2) investors know that companies have, in fact, private information; (3) all investors interpret the companies' disclosure in the same way and companies know how investors will interpret that disclosure; (4) managers want to maximize their companies' share prices; (5) companies can credibly disclose their private information; and (6) companies cannot commit ex-ante to a specific disclosure policy”). Increased reporting could also help determine the effect of investment on company value. See Lawrence A. Gordon, et al., *The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective*, 34 (5) J. ACCT. & PUB. POLICY 509, 509-519 (2015) (arguing that “information sharing could reduce the tendency by firms to defer cybersecurity investments”).

106 should also generate more credible disclosure. Currently, voluntary cybersecurity risk management, strategy, and governance disclosures lack standardization and consistency, reducing their comparability and usefulness for investors. Without set topics that must be addressed, companies may disclose only the strongest aspects of their cybersecurity processes, if they disclose at all. By clarifying what registrants must disclose with respect to their cybersecurity risk management, strategy, and governance, Item 106 will reduce information asymmetry and provide investors and other market participants more certainty and easier comparability of registrants' vulnerability to and ability to manage cybersecurity breaches, reducing adverse selection and increasing liquidity. Thus, the final rules could decrease cost of capital across registrants and increase company value, benefiting investors.

One commenter argued that smaller registrants are less likely than larger registrants to experience cybersecurity incidents and that cyberattacks are not material for smaller registrants.⁴⁷⁸ This could imply that the degree of cybersecurity-driven adverse selection faced by investors in small registrants might be less severe. If so, the potential benefit from improvement in liquidity and cost of capital due to the timeliness and information benefits from the final rules might be smaller for small registrants and their investors. The research this commenter cited to support this assertion found larger companies were more susceptible than smaller companies to a particular category of cybersecurity incidents—those involving personal information lost through hacking by an outside party—which composed less than one-quarter of

⁴⁷⁸ See comment letter from BIO. The letter argues that the Commission, when citing the study by Kamiya, et al. (2021) in the Proposing Release, "ignored and omitted" the fact that the mean market capitalization of impacted companies in this study was \$58.9 billion, much higher than the average for small companies, and thus "cyberattacks mainly affect large companies and are not material for smaller companies." We observe that an average market capitalization of impacted companies of \$58.9 billion would generally indicate that companies both larger and smaller than that size were impacted by cyberattacks.

all cyber incidents in the sample (1,580 out of 6,382).⁴⁷⁹ It is possible that malicious strategies that target personal information are particularly suited to larger, well-known companies, and thus the research may overstate the degree to which large companies are more susceptible to cybersecurity incidents generally. These strategies explicitly harm companies' customers, and customer ill will is potentially more newsworthy and consequential for a larger, well-known company as compared to a smaller one. In contrast, ransomware attacks that target non-personal, internal company operations such as an information technology network, for example, are less concerned with causing reputational loss and thus may have an optimal target profile that favors smaller firms as much as larger firms. Additionally, smaller companies may have fewer resources and weaker processes in place to prevent cybersecurity attacks.⁴⁸⁰ Hence, it is not clear that smaller companies experience fewer material cybersecurity incidents generally. Others have noted that small companies are frequently targeted victims of cyberattacks, potentially leading to dissolution of the business.⁴⁸¹ Thus, overall, we maintain that cybersecurity attacks are material for smaller reporting companies and that the final rules will serve to benefit them and their investors.

Overall, Form 8-K Item 1.05 and Regulation S-K Item 106 provide for timely, informative, and up-to-date disclosure of cybersecurity incidents, as well as disclosure that may provide insight into whether a registrant is prepared for risks from cybersecurity threats and has adequate cybersecurity risk management, strategy, and governance measures in place to reduce

⁴⁷⁹ See Kamiya, et al., *supra* note 413.

⁴⁸⁰ See letter from Tenable.

⁴⁸¹ See Testimony of Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College, before the U.S. House of Representatives Committee on Small Business (Apr. 22, 2015), available at <https://docs.house.gov/meetings/SM/SM00/20150422/103276/HHRG-114-SM00-20150422-SD003-U4.pdf> (describing the cybersecurity risks small businesses face and noting “fifty percent of SMB’s have been the victims of cyberattack and over 60 percent of those attacked go out of business”).

the likelihood of future incidents, reducing the likelihood of delayed or incomplete disclosure and benefiting investors and the market.

We believe enhanced information, timing, and completeness of disclosures as a result of Form 8-K Item 1.05 and Regulation S-K Item 106 will benefit not only investors but also other market participants that rely on registrant disclosures to provide services to investors. They, too, will be able to better evaluate registrants' cybersecurity preparations and risks and thus provide better recommendations. We note that the potential benefit of these amendments could be reduced because some registrants already provide relevant disclosures. That said, we expect this same information will become more useful due to added context from, and easier comparisons with, the increased number of other registrants now providing these disclosures.

We are unable to quantify the potential benefit to investors and other market participants as a result of the increase in disclosure and improvement in pricing under the final rules. Such estimation requires information about the fundamental value of securities and the extent of the mispricing. We do not have access to such information and therefore cannot provide a reasonable estimate. One commenter suggested we use existing cyber disclosure models to “empirically determine” the current degree of market mispricing, but did not suggest what data the Commission could use to do so.⁴⁸² The Commission cannot estimate the effects of undisclosed cybersecurity incidents that are creating market mispricing, as the relevant information was never released and the market was unable to react.

b. Greater Uniformity and Comparability

The final rules requiring disclosure about cybersecurity incidents and cybersecurity risk management, strategy, and governance should also lead to more uniform and comparable

⁴⁸² See letter from ISA.

disclosures, in terms of both content and location, benefiting investors by lowering their search and information processing costs. Currently, registrants do not always use Form 8-K to report cybersecurity incidents. Even among registrants that do, reporting practices vary widely.⁴⁸³ Some provide a discussion of materiality, the estimated costs of an incident, or the remedial steps taken as a result of an incident, while others do not provide such disclosure or provide much less detail. Disclosures related to risk management, strategy, and governance also vary significantly across registrants—such information could be disclosed in places such as the risk factors section, the management’s discussion and analysis section, or not at all. For both types of disclosures, the final rules specify the topics that registrants should disclose. As a result, both incident disclosure and risk management, strategy, and governance disclosure should become more uniform across registrants, making them easier for investors and other market participants to compare. The final rules also specify the disclosure locations (e.g., Item 1C of Form 10-K), benefiting investors and other market participants further by reducing the time, cost, and effort it takes them to search for and retrieve information (as pointed out by commenters⁴⁸⁴).

We note that to the extent that the disclosures related to cybersecurity risk management, strategy, and governance become too uniform or “boilerplate,” the benefit of comparability may be diminished. However, we believe that Item 106 requires sufficient specificity, tailored to the registrant’s facts and circumstances, to help mitigate any tendency towards boilerplate disclosures. Item 106 also provides a non-exclusive list of information that registrants should disclose, as applicable, which should help in this regard.

⁴⁸³ See Proposing Release at 16594.

⁴⁸⁴ See, e.g., letters from Better Markets; CalPERS.

The requirement to tag the cybersecurity disclosure in Inline XBRL will likely augment the informational and comparability benefits by making the disclosures more easily retrievable and usable for aggregation, comparison, filtering, and other analysis. XBRL requirements for public operating company financial statement disclosures have been observed to mitigate information asymmetry by reducing information processing costs, thereby making the disclosures easier to access and analyze.⁴⁸⁵ While these observations are specific to operating company financial statement disclosures and not to disclosures outside the financial statements, such as the cybersecurity disclosures, they suggest that the Inline XBRL requirements should directly or indirectly (*i.e.*, through information intermediaries such as financial media, data aggregators, and academic researchers) provide investors with increased insight into cybersecurity-related information at specific companies and across companies, industries, and time periods.⁴⁸⁶ Also, unlike XBRL financial statements (including footnotes), which consist of tagged quantitative and narrative disclosures, the cybersecurity disclosures consist largely of tagged narrative disclosures.⁴⁸⁷ Tagging narrative disclosures can facilitate analytical benefits

⁴⁸⁵ See, e.g., J.Z. Chen, et al., *Information processing costs and corporate tax avoidance: Evidence from the SEC's XBRL mandate*, 40 J. OF ACCT. AND PUB. POL'Y 2 (finding XBRL reporting decreases likelihood of company tax avoidance because “XBRL reporting reduces the cost of IRS monitoring in terms of information processing, which dampens managerial incentives to engage in tax avoidance behavior”). See also P.A. Griffin, et al., *The SEC's XBRL Mandate and Credit Risk: Evidence on a Link between Credit Default Swap Pricing and XBRL Disclosure*, 2014 AMERICAN ACCOUNTING ASSOCIATION ANNUAL MEETING (2014) (finding XBRL reporting enables better outside monitoring of companies by creditors, leading to a reduction in company default risk); E. Blankespoor, *The Impact of Information Processing Costs on Firm Disclosure Choice: Evidence from the XBRL Mandate*, 57 J. OF ACC. RES. 919, 919-967 (2019) (finding “firms increase their quantitative footnote disclosures upon implementation of XBRL detailed tagging requirements designed to reduce information users’ processing costs,” and “both regulatory and non-regulatory market participants play a role in monitoring firm disclosures,” suggesting “that the processing costs of market participants can be significant enough to impact firms’ disclosure decisions”).

⁴⁸⁶ See, e.g., N. Trentmann, *Companies Adjust Earnings for Covid-19 Costs, but Are They Still a One-Time Expense?*, WALL ST. J. (2020) (citing an XBRL research software provider as a source for the analysis described in the article). See also Bloomberg Lists BSE XBRL Data, XBRL.org (2018); R. Hoitash, and U. Hoitash, *Measuring Accounting Reporting Complexity with XBRL*, 93 ACCOUNT. REV. 259 (2018).

⁴⁸⁷ The cybersecurity disclosure requirements do not expressly require the disclosure of any quantitative values; if a company includes any quantitative values that are nested within the required discussion (*e.g.*, disclosing the

such as automatic comparison or redlining of these disclosures against prior periods and the performance of targeted artificial intelligence or machine learning assessments (tonality, sentiment, risk words, etc.) of specific cybersecurity disclosures rather than the entire unstructured document.⁴⁸⁸

In addition, by formalizing the disclosure requirements related to cybersecurity incidents and cybersecurity risk management, strategy, and governance, the final rules could reduce compliance costs for those registrants that are currently providing disclosure about these topics. The compliance costs would be reduced to the extent that those registrants may be currently over-disclosing information out of caution, to increase the perceived credibility of their disclosures, or to signal to investors that they are diligent with regard to cybersecurity. For instance, the staff has observed that some registrants provide Form 8-K filings even when they do not anticipate the incident will have a material impact on their business operations or financial results.⁴⁸⁹ By specifying that only material incidents require disclosure, the final rules should ease some of these concerns and reduce costs to the extent those costs currently exist.⁴⁹⁰ Investors will benefit to the extent the registrants they invest in enjoy lower compliance costs.

number of days until containment of a cybersecurity incident), those values will be individually detail tagged, in addition to the block text tagging of the narrative disclosures.

⁴⁸⁸ To illustrate, without Inline XBRL, using the search term “remediation” to search through the text of all companies’ filings over a certain period of time, so as to analyze the trends in companies’ disclosures related to cybersecurity incident remediation efforts during that period, could return many narrative disclosures outside of the cybersecurity incident discussion (e.g., disclosures related to potential environmental liabilities in the risk factors section). Inline XBRL, however, enables a user to search for the term “remediation” exclusively within the required cybersecurity disclosures, thereby likely reducing the number of irrelevant results.

⁴⁸⁹ Based on staff analysis of the 10,941 current and periodic reports in 2022 for companies available in Intelligize and identified as having been affected by a cybersecurity incident using a keyword search.

⁴⁹⁰ We note that registrants may still over-disclose due to uncertainty over when a cybersecurity incident crosses the threshold of materiality. This may impact how fully costs from immaterial incident disclosure are reduced.

2. Costs

We also recognize that enhanced cybersecurity disclosure would result in costs to registrants, borne by investors. These costs include potential increases in registrants' vulnerability to cybersecurity incidents and compliance costs. We discuss these costs below.

First, the disclosure about cybersecurity incidents and cybersecurity risk management, strategy, and governance could potentially increase the vulnerability of registrants. Since the issuance of the 2011 Staff Guidance, concerns have been raised that providing detailed disclosures of cybersecurity incidents could, potentially, provide a road map for future attacks, and, if the underlying security issues are not completely resolved, could exacerbate the ongoing attack.⁴⁹¹ The concern is that malicious actors could use the disclosures to potentially gain insights into a registrant's practices on cybersecurity. As a result, the final incident disclosure rules could potentially impose costs on registrants and their investors, if, for example, additional threat actors steal more data or hamper breach resolution.

The final rules have been modified from the Proposing Release to mitigate disclosure of details that could aid threat actors, while remaining informative for investors. Form 8-K Item 1.05 will require registrants to timely disclose material cybersecurity incidents, describe the material aspects of the nature, scope, and timing of the incident, and, importantly, describe the material impact or reasonably likely material impact of the incident on the registrant. Focusing on the material impact or reasonably likely material impact of the incident rather than the specific or technical details of the incident should reduce the likelihood of providing a road map

⁴⁹¹ See, e.g., Roland L. Trope & Sarah Jane Hughes, *The SEC Staff's Cybersecurity Disclosure Guidance: Will It Help Investors or Cyber-Thieves More*, 2011 Bus. L. TODAY 2, 1-4 (2011).

that threat actors can exploit for future attacks, and should reduce the risks and costs stemming from threat actors acting in this manner.⁴⁹²

Similar concerns were raised by commenters about the required risk management, strategy, and governance disclosure.⁴⁹³ Items 106(b) and (c) require registrants to provide specified disclosure regarding their cybersecurity risk management processes and cybersecurity governance by the management and board. The required disclosure could provide malicious actors information about which registrants have weak processes related to cybersecurity risk management and allow such malicious actors to determine their targets accordingly.

However, academic research so far has not provided evidence that more detailed cybersecurity risk disclosures necessarily lead to more attacks. For example, one study finds that measures for specificity (*e.g.*, the uniqueness of the disclosure) do not have a statistically significant relation with subsequent cybersecurity incidents.⁴⁹⁴ Another study finds that cybersecurity risk factor disclosures that involve terms about processes are less likely to be related to future breach announcements than disclosures that employ more general language.⁴⁹⁵ On the other hand, we note that the final rules will require more details of cybersecurity processes than what is explicitly required under the current rules, and the uniformity of the final rules might also make it easier for malicious actors to identify registrants with relatively weaker

⁴⁹² Instruction 4 to Item 1.05 provides that a “registrant need not disclose specific or technical information about its planned response to the incident or its 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.”

⁴⁹³ See letters from ABA; ACLI; APCIA; BIO; BPI et al.; Business Roundtable; Chamber; CSA; CTIA; EIC; Enbridge; FAH; Federated Hermes; GPA; ITI; ISA; Nareit; NAM; NMHC; NRA; NRF; SIFMA; Sen. Portman; TechNet; TransUnion; USTelecom; Virtu; *see also supra* note 201 and accompanying text.

⁴⁹⁴ See He Li, Won Gyun No, & Tawei Wang, *SEC’s Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors*, 30 INT’L. J. OF ACCT. INFO. SYS. 40-55 (2018) (“while Ferraro (2013) criticizes that the SEC did little to resolve the concern about publicly revealing too much information [that] could provide potential hackers with a roadmap for successful attacks, we find no evidence supporting such claim”).

⁴⁹⁵ See Tawei Wang, Karthik N. Kannan, & Jackie Rees Ulmer, *The Association Between the Disclosure and the Realization of Information Security Risk Factors*, 24.2 INFO. SYS. RES. 201, 201-218 (2013).

processes. Therefore, these academic findings might not be generalizable to the effects of the final rules.⁴⁹⁶ However, we also note that we have streamlined the disclosure obligations for Items 106 (b) and (c), in response to commenters' concerns, to require a more principles-based discussion of a registrant's processes instead of detailed disclosures on a specific set of items. This change should help ease concerns that the required cybersecurity risk management, strategy, and governance disclosures will help malicious actors choose targets. In addition, the potential costs resulting from the disclosure requirements might be partially mitigated to the extent that registrants decide to enhance their cybersecurity risk management in anticipation of the increased disclosure. This possibility is discussed below under Indirect Economic Effects.

The final rules will also impose compliance costs. Registrants, and thus their investors, will incur one-time and ongoing costs to fulfill the new disclosure requirements under Item 106 of Regulation S-K. These costs will include costs to gather the information and prepare the disclosures. Registrants will also incur compliance costs to fulfill the disclosure requirements related to Form 8-K (Form 6-K for FPIs) incident disclosure.⁴⁹⁷ These costs include one-time costs to implement or revise their incident disclosure practices, so that any registrant that determines it has experienced a material cybersecurity incident will disclose such incident with the required information within four business days. Registrants may also incur ongoing costs to disclose in a Form 8-K report any material changes or updates relating to previously disclosed incidents, and we expect these costs to be higher for registrants with more incidents to disclose. The costs will be mitigated for registrants whose current disclosure practices match or are similar

⁴⁹⁶ We note that the papers we cited above study the effect of voluntary disclosure and the 2011 Staff Guidance, which could also reduce the generalizability of these studies to the mandatory disclosures under the final rules.

⁴⁹⁷ We note that the compliance costs related to Form 6-K filings will be mitigated, because a condition of the form is that the information is disclosed or required to be disclosed elsewhere.

to those that are in the final rules. One commenter suggested that companies could incur costs to reconcile their existing cybersecurity activities and NIST-based best practices with the requirements of the final rules⁴⁹⁸ but, as discussed in Section II.C.3.c, the final rules are not in conflict with NIST and we do not anticipate that significant reconciliation will be needed.

The compliance costs will also include costs attributable to the Inline XBRL tagging requirements. Many commenters supported the XBRL tagging requirement,⁴⁹⁹ while one commenter suggested that it would be burdensome to add tagging given the time-sensitive nature of the disclosure requirements.⁵⁰⁰ Various preparation solutions have been developed and used by operating companies to fulfill XBRL requirements, and some evidence suggests that, for smaller companies, XBRL compliance costs have decreased over time.⁵⁰¹ The incremental compliance costs associated with Inline XBRL tagging of cybersecurity disclosures will also be mitigated by the fact that most companies that will be subject to the requirements are already subject to other Inline XBRL requirements for other disclosures in Commission filings, including financial statement and cover page disclosures in certain periodic reports and registration

⁴⁹⁸ See letter from SIFMA.

⁴⁹⁹ See letters from E&Y; CAQ; PWC; NACD; AICPA; XBRL.

⁵⁰⁰ See letter from NYC Bar.

⁵⁰¹ An AICPA survey of 1,032 reporting companies with \$75 million or less in market capitalization in 2018 found an average cost of \$5,850 per year, a median cost of \$2,500 per year, and a maximum cost of \$51,500 per year for fully outsourced XBRL creation and filing, representing a 45% decline in average cost and a 69% decline in median cost since 2014. See AICPA, *XBRL Costs for Small Companies Have Declined 45% since 2014* (2018), available at <https://us.aicpa.org/content/dam/aicpa/interestareas/frc/accountingfinancialreporting/xbrl/downloadabledocuments/xbrl-costs-for-small-companies.pdf>. See also Letter from Nasdaq, Inc. (Mar. 21, 2019) (responding to Request for Comment on Earnings Releases and Quarterly Reports, Release No. 33-10588 (Dec. 18, 2018) [83 FR 65601 (Dec. 21, 2018)]) (stating that a 2018 NASDAQ survey of 151 listed companies found an average XBRL compliance cost of \$20,000 per quarter, a median XBRL compliance cost of \$7,500 per quarter, and a maximum XBRL compliance cost of \$350,000 per quarter).

statements.⁵⁰² Such companies may be able to leverage existing Inline XBRL preparation processes and expertise in complying with the cybersecurity disclosure tagging requirements. Moreover, the one-year XBRL compliance period extension could further assuage concerns about the transition for registrants to comply with the new requirements.⁵⁰³

Some commenters contended that the Proposing Release failed to consider the costs of the proposed rules adequately.⁵⁰⁴ We are generally unable to quantify costs related to the final rules due to a lack of data. For example, we are unable to quantify the impact of any increased vulnerability to existing or new threat actors arising from the required incident or risk management, strategy, or governance disclosures. Moreover, costs related to preparing cyber-related disclosures are generally private information known only to the issuing firm, hence such data are not readily available to the Commission. There is also likely considerable variation in these costs depending on a given firm's size, industry, complexity of operations, and other characteristics, which makes comprehensive estimates difficult to obtain. We note that the Commission has provided certain estimates for purposes of compliance with the Paperwork Reduction Act of 1995, as further discussed in Section V below. Those estimates, while useful to understanding the collection of information burden associated with the final rules, do not purport to reflect the full costs associated with making the required disclosures.

One commenter provided a numerical cost estimate, stating the initial costs of complying with the proposed rules would be \$317.5 million to \$523.4 million (\$38,690 to \$69,151 per regulated company), and future annual costs would be \$184.8 million to \$308.1 million (\$22,300

⁵⁰² See 17 CFR 229.601(b)(101) and 17 CFR 232.405 (for requirements related to tagging financial statements, including footnotes and schedules in Inline XBRL). See 17 CFR 229.601(b)(104) and 17 CFR 232.406 (for requirements related to tagging cover page disclosures in Inline XBRL).

⁵⁰³ See *supra* Section II.I.

⁵⁰⁴ See, e.g., letters from Chamber and SIFMA.

to \$37,500 per regulated company).⁵⁰⁵ We cannot directly evaluate the accuracy of these estimates because the commenter did not provide any explanation for how they were derived. We believe, however, these estimates likely significantly overstate the costs of the final rules.

First, the commenter overestimates the number of registrants who are likely to bear the full costs of new disclosures. Converting the total and per company cost estimates to registrant counts implies the commenter assumed these costs would be borne by approximately 8,000 companies, which would be nearly every registrant.⁵⁰⁶ As stated in Section IV.B.2 above, however, 73 percent of domestic filers in 2022 already made cybersecurity-related disclosures in Form 10-K filings and amendments, and 35 Form 8-K filings disclosed material cybersecurity incidents.⁵⁰⁷ While the degree to which registrants' existing disclosures already may be in line with the requirements of the final rules varies—some registrants may need to make significant changes while others may not, especially given the guidance from the 2018 Interpretive Release—most registrants should not bear the full costs of compliance. In addition, while cybersecurity incident disclosure is expected to increase as a result of Item 1.05, we do not expect that most companies will need to report in any given year. Extrapolating from the current numbers of incidents reported—for example, public companies disclosed 188 reported breaches in 2021⁵⁰⁸—we expect that the overwhelming majority of registrants will not experience a material breach and will not need to disclose cybersecurity incidents and incur the ongoing

⁵⁰⁵ See letter from Chamber.

⁵⁰⁶ \$317.5 million divided by \$38,690 per registrant equals 8,206 registrants; \$523.4 million divided by \$69,151 per registrant equals 7,569 registrants; \$184.8 million divided by \$22,300 per registrant equals 8,287 registrants; \$308.1 million divided by \$37,500 per registrant equals 8,216 registrants. In Section IV.B.2, *supra*, we find the number of affected parties to include approximately 7,300 operating companies filing on domestic forms and 1,174 FPIs filing on foreign forms.

⁵⁰⁷ See *supra* notes 456 and 457 and accompanying text.

⁵⁰⁸ See *supra* note 426 and accompanying text.

associated costs.⁵⁰⁹ They may, however, revisit their disclosure controls initially, to ensure they are capturing what the rule requires.

Second, we have made changes from the proposed rules that would also reduce costs as compared with the proposal. Some of these changes concerned aspects of the proposed rules that the commenter noted would be burdensome. For example, the commenter states that “potential material incidents in the aggregate would be difficult to identify and operationally challenging to track.”⁵¹⁰ The commenter also states “the SEC underestimates the burdens related to tracking ‘several small but continuous cyberattacks against a company,’ which may or may not prove to be material.”⁵¹¹ These comments refer to proposed Item 106(d)(2), which would have required disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. In response to comments, we are not adopting this aspect of the proposal and instead have added “a series of related unauthorized occurrences” to the definition of “cybersecurity incident,” which may help address this concern about the burden of the proposal. The comment letter also stated that “cybersecurity talent is scar[c]e globally. From a personnel standpoint, it’s unclear where companies would get the so-called cybersecurity experts that the proposed regulation would mandate. There is a well-documented lack of cybersecurity talent for the public and private sectors that would unquestionably affect companies’ recruitment of board cybersecurity experts.”⁵¹² We are not adopting proposed 407(j) about the cybersecurity expertise, if any, of a registrant’s board members, which may have factored into the commenter’s cost estimates. Additionally, the proposal would not have

⁵⁰⁹ This conclusion is based on relative quantities. Note that 188 is very small relative to the total number of registrants, 8,474, from Section IV.B.2 (188 divided by 8,474 is roughly 2%).

⁵¹⁰ See letter from Chamber.

⁵¹¹ *Id.*

⁵¹² *Id.*

mandated recruitment of cybersecurity experts, only disclosure of their presence. Additional streamlining of requirements in the final rules (e.g., reduced granularity of cybersecurity incident disclosure requirements) should further reduce costs from what might have been estimated using the Proposing Release.

Another commenter stated that the Commission’s calculation of costs and benefits does not adequately address the impact of different but overlapping disclosure and reporting requirements that may escalate burdens and costs.⁵¹³ We acknowledge the possibility that to the extent different information has to be reported pursuant to different regulations, laws, or other requirements, there could be a greater cost because of the demands to keep track of and manage the multiple different disclosure regimes. However, to the extent that certain other existing requirements may involve monitoring cybersecurity incidents or assessing an incident’s impact on the registrant, the registrant may be able to leverage existing disclosures to reduce the burden of complying with the final rules. Additionally, as noted in Section II.A.3 those other regulations generally serve different purposes than the final rules, and we believe that the benefits of the final rules justify the costs.

One commenter raised a concern that the costs of the rules reached the threshold of an “economically significant rulemaking” under the Unfunded Mandate Reform Act of 1995 (“UMRA”) and the Small Business Regulatory Enforcement Fairness Act, thus requiring an “enhanced economic analysis.”⁵¹⁴ The requirement to issue an analysis under the UMRA does not apply to rules issued by independent regulatory agencies.⁵¹⁵

⁵¹³ See letter from SIFMA.

⁵¹⁴ See letter from Chamber.

⁵¹⁵ See 2 U.S.C. 658 (“The term ‘agency’ has the same meaning as defined in section 551(1) of title 5, United States Code, but does not include independent regulatory agencies.”). See also Congressional Research Service,

The compliance costs of the final rules could be disproportionately burdensome to smaller registrants, as some of these costs may have a fixed component that does not scale with the size of the registrant.⁵¹⁶ Also, smaller registrants may have fewer resources with which to implement these changes.⁵¹⁷ One commenter suggested this could lead some small companies seeking to conduct an initial public offering to reconsider.⁵¹⁸ Commenters also noted that smaller companies may not yet have a mature reporting regime and organizational structure and would benefit from an onramp to compliance.⁵¹⁹ We are not adopting some proposed requirements (e.g., disclosing whether the board includes a cybersecurity expert), and thus the cost burden of the final rules should not be as high as initially proposed. We also are delaying compliance for incident disclosure for smaller reporting companies by providing an additional phase-in period of 180 days after the non-smaller reporting company compliance date for smaller reporting companies, which will delay compliance with these requirements for 270 days from effectiveness of the rules.⁵²⁰ To the extent smaller reporting companies are less likely than larger companies to have incident disclosure processes in place, they could benefit from additional time to comply. An extended compliance date may also permit smaller reporting companies to benefit from seeing how larger companies implement these disclosures. Investors in these smaller registrants could benefit from higher disclosure quality afforded by the delay, although

Unfunded Mandates Reform Act: History, Impact, and Issues (July 17, 2020), available at <https://sgp.fas.org/crs/misc/R40957.pdf> (noting “[UMRA] does not apply to duties stemming from participation in voluntary federal programs [or] rules issued by independent regulatory agencies”).

⁵¹⁶ See *infra* Section VI.

⁵¹⁷ See, e.g., letter from SBA.

⁵¹⁸ See letter from BIO.

⁵¹⁹ See, e.g., letter from BIO.

⁵²⁰ See *supra* Section II.I.

some benefits, such as the reduction in asymmetric information and mispricing, would also be delayed.

3. Indirect Economic Effects

While the final rules only require disclosures—not changes to risk management practices—the requirement to disclose and the disclosures themselves could result in certain indirect benefits and costs. In anticipating investor reactions to the required disclosures, for example, registrants might devote more resources to cybersecurity governance and risk management in order to be able to disclose those efforts. Although not the purpose of this rule, registrants devoting resources to cybersecurity governance and risk management could reduce both their susceptibility to a cybersecurity attack, reducing the likelihood of future incidents, as well as the degree of harm suffered from an incident, benefiting registrants and investors. The choice to dedicate these resources would also represent an indirect cost of the final rules, to the extent registrants do not already have governance and risk management measures in place. As with compliance costs, the cost of improving cybersecurity governance and risk management could be proportionally higher for smaller companies if these registrants have fewer resources to implement these changes, and to the extent these costs do not scale with registrant size.

In addition, the requirement to tag the cybersecurity disclosure in Inline XBRL could have indirect effects on registrants. As discussed in Section III.C.1.a.(ii), XBRL requirements for public operating company financial statement disclosures have been observed to reduce information processing cost. This reduction in information processing cost has been observed to facilitate the monitoring of registrants by other market participants, and, as a result, to influence registrants’ behavior, including their disclosure choices.⁵²¹

⁵²¹ See *supra* note 485.

The requirement in Item 1.05 that registrants timely disclose material cybersecurity incidents could also indirectly affect consumers, and external stakeholders such as other registrants in the same industry and those facing similar cybersecurity threats. Cybersecurity incidents can harm not only the company that suffers the incident but also other businesses and consumers. For example, a cybersecurity breach at one company, such as a gas pipeline, or a power company, may cause a major disruption or shutdown of a critical infrastructure industry, resulting in broad losses throughout the economy.⁵²² Timely disclosure of cybersecurity incidents required by Item 1.05 could increase awareness by those external stakeholders and companies in the same industry that the malicious activities are occurring, giving them more time to mitigate any potential damage.

To the extent that Item 1.05 increases incident disclosure, consumers may learn about a particular cybersecurity breach and therefore take appropriate actions to limit potential economic harm that they may incur from the breach. For example, there is evidence that increased disclosure of cybersecurity incidents by companies can reduce the risk of identity theft for individuals.⁵²³ Also, consumers may be able to make better informed decisions about which companies to entrust with their personal information.

⁵²² See Lawrence A. Gordon, et al., *Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model*, 6 J. INFO. SEC. 24, 25 (2015) (“Firms in the private sector of many countries own a large share of critical infrastructure assets. Hence, cybersecurity breaches in private sector firms could cause a major disruption of a critical infrastructure industry (e.g., delivery of electricity), resulting in massive losses throughout the economy, putting the defense of the nation at risk.”). See also Collin Eaton and Dustin Volz, *U.S. Pipeline Cyberattack Forces Closure*, WALL ST. J. (MAY 8, 2021), available at <https://www.wsj.com/articles/cyberattack-forces-closure-of-largest-u-s-refined-fuel-pipeline-11620479737>.

⁵²³ See Sasha Romanosky, Rahul Telang, and Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 (2) J. OF POL’Y. ANALYSIS AND MGMT. 272, 256-286 (2011) (finding that the adoption of State-level data breach disclosure laws reduced identity theft by 6.1%).

As discussed above, to the extent that registrants may decide to enhance their cybersecurity risk management in anticipation of the increased disclosure, that could reduce registrants' susceptibility to and damage incurred from a cybersecurity attack. This reduced likelihood of and vulnerability to future incidents could reduce the negative externalities of those incidents, leading to positive spillover effects and a reduction in overall costs to society from these attacks.

However, the magnitude of this and the other indirect effects discussed above would depend upon factors outside of the specific disclosures provided in response to the final rule, and therefore it is difficult to assess with certainty the likelihood or extent of these effects.

D. Effects on Efficiency, Competition, and Capital Formation

We believe the final rules should have positive effects on market efficiency. As discussed above, the final rules should improve the timeliness and informativeness of cybersecurity incident and risk disclosure. As a result of the disclosure required by the final rules, investors and other market participants should better understand the cybersecurity threats registrants are facing, their potential impact, and registrants' ability to respond to and manage risks. Investors and other market participants should thereby better evaluate registrants' securities and make more informed decisions. As a result, the required disclosures should reduce information asymmetry and mispricing in the market, improving market efficiency. More efficient prices should improve capital formation by increasing overall public trust in markets, leading to greater investor participation and market liquidity.

The final rules also could promote competition among registrants with respect to improvement in both their cybersecurity risk management and transparency in communicating their cybersecurity processes. To the extent investors view strong cybersecurity risk

management, strategy, and governance favorably, registrants disclosing more robust processes, more clearly, could benefit from greater interest from investors, leading to higher market liquidity relative to companies that do not. Customers may also be more likely to entrust their business to companies that protect their data. Registrants that to date have invested less in cybersecurity preparation could thus be incentivized to invest more, to the benefit of investors and customers, in order to become more competitive. To the extent that increased compliance costs resulting from the final rules prevent smaller companies from entering the market, as a commenter suggested,⁵²⁴ the final rules could reduce the ability of smaller companies to compete and thereby reduce competition overall.

E. Reasonable Alternatives

1. Website Disclosure

As an alternative to Form 8-K disclosure of material cybersecurity incidents, we considered providing registrants with the option of disclosing this information instead through company websites, if the company disclosed its intention to do so in its most recent annual report, and subject to information availability and retention requirements. While this approach may be less costly for the company because it may involve fewer compliance costs, disclosures made on company websites would not be located in a central depository, such as the EDGAR system,⁵²⁵ and would not be in the same place as other registrants' disclosures of material cybersecurity incidents, nor would they be organized into the standardized sections found in Form 8-K and could thus be less uniform. Even if we required registrants to announce the

⁵²⁴ See letter from BIO.

⁵²⁵ EDGAR, the Electronic Data Gathering, Analysis, and Retrieval system, is the primary system for companies and others submitting documents under the Securities Act, the Exchange Act, the Trust Indenture Act of 1939, and the Investment Company Act. EDGAR's public database can be used to research a public company's financial information and operations.

disclosure, or to alert the Commission to it, the information would still be more difficult for investors and market participants to locate and less uniform than Form 8-K.

The lack of a central repository, and a lack of uniformity of website disclosures, could increase the costs for investors and other market participants to search for and process the information to compare cybersecurity risks across registrants. Additionally, such disclosure might not be preserved on the company's website for as long as it would be on the EDGAR system when the disclosure is filed with the Commission, because registrants may not keep historical information available on their websites indefinitely and it could be difficult to determine whether the website information had moved or changed. Therefore, this approach would be less beneficial to investors, other market participants, and the overall efficiency of the market.

2. Disclosure through Periodic Reports

We also considered requiring disclosure of material cybersecurity incidents through quarterly or annual reports, as proposed, instead of Form 8-K. Reporting material cybersecurity incidents at the end of the quarter or year would allow registrants more time to assess the financial impact of such incidents. The resulting disclosure might be more specific or informative for investors and other market participants to value the securities and make more informed decisions. The compliance costs would be less under this alternative, because registrants would not have to file as frequently. And, it might further reduce the risk that disclosure could provide timely information to attackers.

However, this alternative also would lead to less timely reporting on material cybersecurity incidents. As a result, the market would not be able to incorporate the information related to cybersecurity risk into securities prices in as timely a manner, and investors and other

market participants would not be able to make as informed decisions as they could under the requirements of Item 1.05. Additionally, as previously discussed, less timely reporting could adversely impact external stakeholders, such as other registrants in the same industry and those facing similar cybersecurity threats, and consumers whose data were compromised.

Relatedly, we proposed requiring registrants to disclose material changes and additions to previously reported cybersecurity incidents on Forms 10-K and 10-Q instead of on an amended Form 8-K. However, as discussed above, we believe using Form 8-K would be more timely and consistent;⁵²⁶ all disclosures concerning material cybersecurity incidents, whether new or containing information not determined or unavailable initially, will be disclosed on the same form.

3. Exempt Smaller Reporting Companies

We also considered exempting smaller reporting companies from the final rules.⁵²⁷ Exempting smaller reporting companies from the disclosure requirements of the final rules would avoid compliance costs for smaller companies, including those compliance costs that could disproportionately affect smaller companies.⁵²⁸ As noted earlier, however, we are not adopting some proposed requirements (e.g., disclosing whether the board includes a cybersecurity expert) and modifying others (e.g., requiring a description of cybersecurity “processes” instead of more formal “policies and procedures”), and thus the cost burden of the final rules should not be as high as initially proposed. This should mitigate some of the concerns raised by commenters and would also reduce the potential value of an exemption. Moreover, an exemption would remove the benefit to investors of informative, timely, uniform, and

⁵²⁶ See *supra* Section II.B.3.

⁵²⁷ See *supra* Section II.G.2.

⁵²⁸ See *supra* Section II.G.2

comparable disclosure with regard to smaller companies. And although one commenter argued for an exemption based on a perception that smaller companies are less likely to experience cybersecurity incidents,⁵²⁹ for the reasons explained in Section IV.C.1.b, we believe that smaller companies are still at risk for material cybersecurity incidents. This aligns with comments we received opposing an exemption for smaller reporting companies.⁵³⁰

Lastly, one commenter that argued for an exemption cited the Proposing Release, which noted a potential for increased cost of capital for registrants that do not have cybersecurity programs once disclosures are mandated; the commenter stated that these would disproportionately be smaller registrants.⁵³¹ We have reconsidered the argument that registrants without robust cybersecurity processes in place might face a higher cost of capital and as a result would be priced unfavorably, and no longer believe it to be accurate. It is indeed possible that companies that reveal what investors consider to be less robust cybersecurity risk management, strategy, and governance processes may experience a decline in stock price. However, because the risk of cybersecurity attacks should be idiosyncratic, this decline would likely be due to investors updating their expectations of future cash flows for this firm to incorporate higher likelihood of a future incident—moderating the decline should future incidents occur—not an increase in fundamental market risk and thus cost of capital. In addition, to the extent investors already rationally anticipate that smaller registrants or registrants that have not previously disclosed such information have less robust policies, there may be less or no stock price decline as a result of Item 106, as these disclosures would merely confirm expectations. Thus, increases

⁵²⁹ See letter from BIO.

⁵³⁰ See, e.g., letters from Cybersecurity Coalition; Tenable.

⁵³¹ See letter from BIO.

in cost of capital should not be prevalent in this regard and should not be a reason to exempt small firms from the final rules.

V. PAPERWORK REDUCTION ACT

A. Summary of the Collections of Information

Certain provisions of our rules and forms that will be affected by the final rules contain “collection of information” requirements within the meaning of the Paperwork Reduction Act (“PRA”).⁵³² The Commission published a notice requesting comment on changes to these collections of information in the Proposing Release and submitted these requirements to the Office of Management and Budget (“OMB”) for review in accordance with the PRA.⁵³³

The hours and costs associated with preparing, filing, and sending the forms constitute reporting and cost burdens imposed by each collection of information. An agency may not conduct or sponsor, and a person is not required to comply with, a collection of information unless it displays a currently valid OMB control number. Compliance with the information collections is mandatory. Responses to the information collections are not kept confidential and there is no mandatory retention period for the information disclosed. The titles for the affected collections of information are:⁵³⁴

- “Form 8-K” (OMB Control No. 3235-0060);
- “Form 6-K” (OMB Control No. 3235-0116);
- “Form 10-K” (OMB Control No. 3235-0063); and
- “Form 20-F” (OMB Control No. 3235-0288).

⁵³² 44 U.S.C. 3501 *et seq.*

⁵³³ 44 U.S.C. 3507(d) and 5 CFR 1320.11.

⁵³⁴ The Proposing Release also listed “Schedule 14A” (OMB Control No. 3235-0059), “Schedule 14C” (OMB Control No. 3235-0057), and “Form 10-Q” (OMB Control No. 3235-0070) as affected collections of information. However, under the final rules, these schedules and form are no longer affected.

The Commission adopted all of the existing regulations and forms pursuant to the Securities Act and the Exchange Act. The regulations and forms set forth disclosure requirements for current reports and periodic reports filed by registrants to help shareholders make informed voting and investment decisions.

A description of the final amendments, including the need for the information and its use, as well as a description of the likely respondents, can be found in Section II above, and a discussion of the economic effects of the final amendments can be found in Section IV above.

B. Summary of Comment Letters and Revisions to PRA Estimates

In the Proposing Release, the Commission requested comment on the PRA burden hour and cost estimates and the analysis used to derive the estimates.⁵³⁵ While a number of parties commented on the potential costs of the proposed rules, only one commenter spoke specifically to the PRA analysis, arguing that the proposal “cannot be justified under the Paperwork Reduction Act” because of an “unreasonable” number of separate disclosures and because “the amount of information the Proposal would require to be produced is unwarranted in light of other, existing regulations.”⁵³⁶ The commenter further alleged that the Proposing Release’s “calculation of costs and benefits is skewed” because “[d]ifferent but overlapping disclosure and reporting requirements do not correlate with lower burdens on information providers, but rather, escalated burdens and costs.”

While we acknowledge the commenter’s concerns about costs of the proposal, for the reasons discussed in Section II.H and elsewhere throughout this release, we believe the information required by the final rules is necessary and appropriate in the public interest and for

⁵³⁵ Proposing Release at 16616-16617.

⁵³⁶ See letter from SIFMA.

the protection of investors. Further, a discussion of the economic effects of the final amendments, including consideration of comments that expressed concern about the expected costs associated with the proposed rules, can be found in Section IV above. With regard to the calculation of paperwork burdens, we note that both the Proposing Release's PRA analysis and our PRA analysis of the final amendments here estimate the incremental burden of each new or revised disclosure requirement individually and fully comport with the requirements of the PRA. Our estimates reflect the modifications to the proposed rules that we are adopting in response to commenter concerns, including streamlining some of the proposed rule's elements to address concerns regarding the level of detail required and the anticipated costs of compliance.

C. Effects of the Amendments on the Collections of Information

The following PRA Table 1 summarizes the estimated effects of the final amendments on the paperwork burdens associated with the affected collections of information listed in Section V.A.

PRA Table 1 – Estimated Paperwork Burden of Final Amendments

Final Amendments and Effects	Affected Forms	Estimated Burden Increase	Number of Estimated Affected Responses*
Form 8-K • Add Item 1.05 requiring disclosure of material cybersecurity incidents within four business days following determination of materiality.	Form 8-K	9 hour increase in compliance burden per form	200 Filings
Form 6-K • Add “cybersecurity incident” to the list in General Instruction B of information required to be furnished on Form 6-K.	Form 6-K	9 hour increase in compliance burden per form	20 Filings
Regulation S-K Item 106 • Add Item 106(b) requiring disclosure regarding cybersecurity risk management and strategy. • Add Item 106(c) requiring disclosure regarding cybersecurity governance.	Form 10-K and Form 20-F	Form 10-K: 10 hour increase in compliance burden per form Form 20-F: 10 hour increase in compliance burden per form	8,292 Filings 729 Filings

* The OMB PRA filing inventories represent a three-year average. Averages may not align with the actual number of filings in any given year.

The estimated burden increases for Forms 8-K, 10-K, and 20-F reflect changes from the estimates provided in the Proposing Release. There, the Commission estimated that the average incremental burden for an issuer to prepare the Form 8-K Item 1.05 disclosure would be 10 hours. The proposed estimate included the time and cost of preparing the disclosure, as well as tagging the data in XBRL. The changes we are making to Item 1.05 in the final rules should generally reduce the associated burden by an incremental amount in most cases. We therefore estimate that Form 8-K Item 1.05 will have a burden of 9 hours, on par with the average burdens of existing Form 8-K items, which is 9.21 hours.

In the Proposing Release, the Commission estimated that the average incremental burden for preparing Form 10-K stemming from proposed Item 106 would be 15 hours. Similarly, the Commission estimated that proposed Item 106 would result in an average incremental burden for preparing Form 20-F of 16.5 hours. The proposed estimates included the time and cost of preparing the disclosure, as well as tagging the data in XBRL. We estimate the changes we are

making to Item 106 in the final rules should generally reduce the associated burden by one-third due to the elimination of many of the proposed disclosure items; accordingly, we have reduced the estimated burden to 10 hours from 15 hours for Form 10-K, and to 10 hours from 16.5 hours for Form 20-F.⁵³⁷

We have not modified the estimated number of estimated affected responses for Form 8-K and Form 6-K from what was proposed. As noted in the Proposing Release, not every filing of these forms would include responsive disclosures. Rather, these disclosures would be required only when a registrant has made the determination that it has experienced a material cybersecurity incident. Further, in the case of Form 6-K, the registrant would only have to provide the disclosure if it is required to disclose such information elsewhere.

D. Incremental and Aggregate Burden and Cost Estimates for the Final Amendments

Below we estimate the incremental and aggregate increase in paperwork burden as a result of the final amendments. These estimates represent the average burden for all respondents, both large and small. In deriving our estimates, we recognize that the burdens will likely vary among individual respondents and from year to year based on a number of factors, including the nature of their business.

The burden estimates were calculated by multiplying the estimated number of responses by the estimated average amount of time it would take a registrant to prepare and review disclosure required under the final amendments. For purposes of the PRA, the burden is to be

⁵³⁷ Note that, in the proposal, a portion of the burden for companies reporting on Form 10-K was allocated to Schedule 14A, as a result of certain disclosure items being proposed to be included in Rule 407 of Regulation S-K. By contrast, since registrants reporting on Form 20-F do not have an analogous form to Schedule 14A, the comparable burden to Schedule 14A was attributable to Form 20-F. Since we are not adopting Item 407 as proposed, and we do not expect any disclosures on Schedule 14A, the estimates for Form 10-K and Form 20-F are now aligned.

allocated between internal burden hours and outside professional costs. PRA Table 2 below sets forth the percentage estimates we typically use for the burden allocation for each collection of information. We also estimate that the average cost of retaining outside professionals is \$600 per hour.⁵³⁸

PRA Table 2: Standard Estimated Burden Allocation for Specified Collections of Information

Collection of Information	Internal	Outside Professionals
Form 10-K, Form 6-K, and Form 8-K	75%	25%
Form 20-F	25%	75%

PRA Table 3 below illustrates the incremental change to the total annual compliance burden of affected collections of information, in hours and in costs, as a result of the final amendments.

⁵³⁸ We recognize that the costs of retaining outside professionals may vary depending on the nature of the professional services, but for purposes of this PRA analysis, we estimate that such costs would be an average of \$600 per hour. At the proposing stage, we used an estimated cost of \$400 per hour. We are increasing this cost estimate to \$600 per hour to adjust the estimate for inflation from Aug. 2006.

PRA Table 3. Calculation of the Incremental Change in Burden Estimates of Current Responses Resulting from the Final Amendments

Collection of Information	Number of Estimated Affected Responses (A)*	Burden Hour Increase per Response (B)	Change in Burden Hours (C) = (A) x (B)**	Change in Company Hours (D) = (C) x 0.75 or .25	Change in Professional Hours (E) = (C) x 0.25 or .75	Change in Professional Costs (F) = (E) x \$600
8-K	200	9	1,800	1,350	450	\$270,000
6-K	20	9	180	135	45	\$27,000
10-K	8,292	10	82,920	62,190	20,730	\$12,438,000
20-F	729	10	7,290	1,822.50	5,467.50	\$3,280,500

* The number of estimated affected responses is based on the number of responses in the Commission's current OMB PRA filing inventory. The OMB PRA filing inventory represents a three-year average.

** The estimated changes in Columns (C), (D), and (E) are rounded to the nearest whole number.

The following PRA Table 4 summarizes the requested paperwork burden, including the estimated total reporting burdens and costs, under the final amendments.

PRA Table 4. Requested Paperwork Burden Under the Final Amendments

Form	Current Burden			Program Change			Revised Burden		
	Current Annual Responses (A)	Current Burden Hours (B)	Current Cost Burden (C)	Change in Number of Affected Responses (D)	Change in Company Hours (E) [†]	Change in Professional Costs (F) [‡]	Annual Responses (G) = (A)+(D)	Burden Hours (H) = (B) + (E)	Cost Burden (I) = (C) + (F)
Form 8-K	118,387	818,158	\$108,674,430	200	1,350	\$270,000	118,587	819,508	\$108,944,430
Form 6-K	34,794	227,031	\$30,270,780	20	135	\$27,000	34,814	227,166	\$30,297,780
Form 10-K	8,292	13,988,770	\$1,835,588,919	--	62,190	\$12,438,000	8,292	14,050,960	\$1,848,026,919
Form 20-F	729	478,983	\$576,490,625	--	1,822.50	\$3,280,500	729	480,805.50	\$579,771,125

[†] From Column (D) in PRA Table 3

[‡] From Column (F) in PRA Table 3

VI. FINAL REGULATORY FLEXIBILITY ANALYSIS

The Regulatory Flexibility Act (“RFA”) requires the Commission, in promulgating rules under Section 553 of the Administrative Procedure Act,⁵³⁹ to consider the impact of those rules on small entities. We have prepared this Final Regulatory Flexibility Analysis (“FRFA”) in accordance with Section 604 of the RFA.⁵⁴⁰ An Initial Regulatory Flexibility Analysis (“IRFA”) was prepared in accordance with the RFA and was included in the Proposing Release.⁵⁴¹

A. Need for, and Objectives of, the Final Amendments

The purpose of the final amendments is to ensure investors and other market participants receive timely, decision-useful information about registrants’ material cybersecurity incidents, and periodic information on registrants’ approaches to cybersecurity risk management, strategy, and governance that is standardized and comparable across registrants. The need for, and objectives of, the final rules are described in Sections I and II above. We discuss the economic impact and potential alternatives to the amendments in Section IV, and the estimated compliance costs and burdens of the amendments under the PRA in Section V.

B. Significant Issues Raised by Public Comments

In the Proposing Release, the Commission requested comment on any aspect of the IRFA, and particularly on the number of small entities that would be affected by the proposed amendments, the existence or nature of the potential impact of the proposed amendments on small entities discussed in the analysis, how the proposed amendments could further lower the burden on small entities, and how to quantify the impact of the proposed amendments.

⁵³⁹ 5 U.S.C. 553.

⁵⁴⁰ 5 U.S.C. 604.

⁵⁴¹ Proposing Release at 16617.

We received one comment letter on the IRFA, from the U.S. Small Business Administration’s Office of Advocacy (“Advocacy”).⁵⁴² Advocacy’s letter expressed concern that “the IRFA does not adequately describe the regulated small entities and potential impacts on those entities.”⁵⁴³ In the Proposing Release, the Commission estimated that the proposed amendments would apply to 660 issuers and 9 business development companies that may be considered small entities.⁵⁴⁴ Advocacy’s comment letter stated that this estimate did “not provide additional information, such as the North American Industry Classification System (“NAICS”) classifications of the affected entities” and did not “break down the affected entities into smaller size groups (e.g., based on total assets).”⁵⁴⁵ It also stated that the IRFA did not “adequately analyze the relative impact of costs to small entities.”⁵⁴⁶ In this vein, it suggested that emerging growth companies (“EGCs”) may face particular challenges complying with the proposed rules.⁵⁴⁷ In particular, Advocacy’s comment letter stated that “[e]merging growth companies may have little or no revenue to afford the additional cost burden of the proposed rules and may not have access to the cybersecurity expertise necessary to comply with the new disclosure requirements.”⁵⁴⁸

⁵⁴² See letter from U.S. Small Business Administration Office of Advocacy. We also received some comments that, while not specifically addressed to the IRFA, did concern the impact of the proposed rules on smaller reporting companies. See letters from BDO; BIO; CSA; Cybersecurity Coalition; NACD; NASAA; Nasdaq; NDIA; Prof. Perullo; Tenable. We have addressed those comments in Section II.G.2, *supra*, and incorporate those responses here as applicable to our RFA analysis. We also note the recommendations for all Commission rulemakings from the Office of the Advocate for Small Business Capital Formation. See 2022 OASB Annual Report.

⁵⁴³ *Id.*

⁵⁴⁴ Proposing Release at 16617.

⁵⁴⁵ See letter from Advocacy.

⁵⁴⁶ *Id.*

⁵⁴⁷ *Id.*

⁵⁴⁸ *Id.*

The comment letter from Advocacy also addressed the discussion of alternatives within the IRFA and the Commission’s explanation of why it did not ultimately propose such alternatives. Advocacy stated that “[t]he RFA requires that an IRFA provide significant, feasible alternatives that accomplish an agency’s objectives,” and stated that the IRFA did not satisfy this requirement because it listed “broad categories of potential alternatives to the proposed rules but [did] not analyze any specific alternative that was considered by the SEC,” and because it did not “contain a description of significant alternatives which accomplish the stated SEC objectives and which minimize the significant economic impact of the proposal on small entities.”

1. Estimate of Affected Small Entities and Impact to Those Entities

With respect to the adequacy of the Proposing Release’s estimate of affected small entities, the RFA requires “a description of and, where feasible, an estimate of the number of small entities to which the proposed rule will apply.”⁵⁴⁹ Advocacy’s published guidance recommends agencies use NAICS classifications to help in “identifying the industry, governmental and nonprofit sectors they intend to regulate.”⁵⁵⁰ Here, given that the rulemaking applies to and impacts all public company registrants, regardless of industry or sector, we do not believe that further breakout of such registrants by industry classification is necessary or would otherwise be helpful to such entities understanding the impact of the proposed or final rules. This is not a case in which small entities in certain industries and sectors would be affected more than others, as cybersecurity risks exist across industries.⁵⁵¹ For the same reasons we are not

⁵⁴⁹ 5 U.S.C. 603(b)(3).

⁵⁵⁰ U.S. Small Business Administration Office of Advocacy, *A Guide for Government Agencies: How to Comply with the Regulatory Flexibility Act* (Aug. 2017), at 18, available at <https://www.sba.gov/sites/default/files/advocacy/How-to-Comply-with-the-RFA-WEB.pdf>.

⁵⁵¹ A breakout would be relevant where, for example, the Commission finds that small entities generally would not be affected by a rule but small entities in a particular industry would be affected.

breaking down the affected entities into smaller size groups (e.g., based on total assets) as recommended by Advocacy. Given the nature of the final rules, we believe that our estimate of the number of small entities to which the final rules will apply adequately describes and estimates the small entities that will be affected.⁵⁵²

With respect to Advocacy’s suggestion that the proposed rule may be “particularly problematic” for EGCs, we have discussed in Section IV.C.2 above the anticipated costs of the final rules, including their impact on EGCs. We also note that the category of EGC is not the same as the category of “small entity” for purposes of the RFA, and indeed EGC status is not a reliable indicator of whether a registrant is a small entity.⁵⁵³ While EGC status does include a revenue component, it importantly considers whether the issuer is *seasoned*, meaning, whether it is a new registrant (rather than a registrant with a longer public reporting history). Accordingly, while many EGCs are small entities, there are many that are not. Likewise, many small entities are not EGCs. For purposes of the FRFA, our focus is on the impact on small entities, regardless of whether or not they are EGCs.

We disagree with the statement in the Advocacy comment letter that “SEC expects that the costs associated with the proposed amendments to be similar for large and small entities.” The Commission explained in the IRFA that the proposed amendments would apply to small entities to the same extent as other entities, irrespective of size, and that therefore, the Commission expected that “the *nature* of any benefits and costs associated with the proposed

⁵⁵² See *infra* Section VI.C.

⁵⁵³ An EGC is defined as a company that has total annual gross revenues of less than \$1.235 billion during its most recently completed fiscal year and, as of Dec. 8, 2011, had not sold common equity securities under a registration statement. A company continues to be an EGC for the first five fiscal years after it completes an initial public offering, unless one of the following occurs: its total annual gross revenues are \$1.235 billion or more; it has issued more than \$1 billion in non-convertible debt in the past three years; or it becomes a “large accelerated filer,” as defined in Exchange Act Rule 12b-2.

amendments to be similar for large and small entities” (emphasis added).⁵⁵⁴ The analysis with respect to the *nature* of the costs (and benefits) of the proposed rules detailed in the Economic Analysis of the Proposing Release was referenced in the IRFA to help small entities understand such impacts, not to imply that small entities face the same degree of costs as large entities. Indeed, the Commission went on to state in both the IRFA and the Economic Analysis of the Proposing Release that, while it was unable to project the economic impacts on small entities with precision, it recognized that “the costs of the proposed amendments borne by the affected entities could have a proportionally greater effect on small entities, as they may be less able to bear such costs relative to larger entities.”⁵⁵⁵ Additionally, in Section IV, above, we discuss the economic effects, including costs, of the final amendments across all entities. We recognize that to the extent the costs are generally uniform across all entities, they would have a relatively greater burden on smaller entities. That said, as discussed both above and below, to help mitigate that relatively greater burden and to respond to comment letters including the letter from Advocacy, we have extended the compliance date for smaller reporting companies so as to provide additional transition time and allow them to benefit from the experience of larger companies. Accordingly, we believe that both this FRFA and our prior IRFA adequately describe and analyze the relative impact of costs to small entities.

2. Consideration of Alternatives

The IRFA’s discussion of significant alternatives, and our discussion of alternatives below, satisfy the RFA. The relevant RFA requirement provides that an IRFA “shall also contain a description of any significant alternatives to the proposed rule which accomplish the

⁵⁵⁴ Proposing Release at 16617 (emphasis added).

⁵⁵⁵ Proposing Release at 16617-16618. *See also id.* at 16613 (“smaller companies might incur a cost that is disproportionately high, compared to larger companies under the proposed rules”).

stated objectives of applicable statutes and which minimize any significant economic impact of the proposed rule on small entities.”⁵⁵⁶ In the Proposing Release, the Commission discussed each of the types of significant alternatives noted in Section 603 of the RFA and concluded that none of these alternatives would accomplish the stated objectives of the rulemaking while minimizing any significant impact on small entities. In addition, Section III.E of the Proposing Release discussed reasonable alternatives to the proposed rules and their economic impacts. Similarly, in addition to the discussion in Section VI.E below, in Section IV.E of this release we also discuss reasonable alternatives of the final rules and their economic impacts.

While not commenting on the alternatives raised in the IRFA specifically, two commenters stated that the final rules should exempt smaller businesses. One of these commenters stated that small companies in the biotechnology industry “do not have the capacity, nor the business need, to have institutional structures related to the management, planning, oversight, and maintenance of cybersecurity related systems and suppliers. These companies should not have to hire extra employees specifically for the purposes of implementing cybersecurity related programs.”⁵⁵⁷ The other commenter noted that, with respect to the proposed requirement to require disclosure about the cybersecurity expertise of board members, small companies “have limited resources to begin with, and may find it more difficult than large companies to identify board members with requisite cyber expertise given that there already is a lack of talent in this area.”⁵⁵⁸

With respect to the first of these commenters, we note that neither the proposed nor the final rules require any company to “implement new management structures” or otherwise adopt

⁵⁵⁶ 5 U.S.C. 603(c).

⁵⁵⁷ See letter from BIO.

⁵⁵⁸ See letter from NDIA.

or change “institutional structures related to the management, planning, oversight, and maintenance of cybersecurity related systems and suppliers.”⁵⁵⁹ The final rules instead call for disclosure of a registrant’s processes, *if any*, for assessing, identifying, and managing material cybersecurity risks. To the extent that a registrant does not have such processes, the final rules do not impose any additional costs. With respect to the second of these commenters, we note that, consistent with commenter feedback and for the reasons discussed above, we have not adopted the proposed requirement related to disclosure of board cybersecurity expertise.

Finally, we note that many commenters explicitly opposed exempting smaller businesses from the proposed rules,⁵⁶⁰ in part because they may face equal⁵⁶¹ or greater⁵⁶² cybersecurity risk than larger companies, or because investors’ relative share in a smaller company may be higher, such that small companies’ cybersecurity risk “may actually embody the most pressing cybersecurity risk to an investor.”⁵⁶³ We agree with these analyses,⁵⁶⁴ and accordingly are not exempting small entities from the final rules. However, as discussed above, in response to concerns about the impact of the rules on smaller companies and in order to provide smaller

⁵⁵⁹ The quoted language is from the BIO letter.

⁵⁶⁰ See letters from CSA; Cybersecurity Coalition; NASAA; Prof. Perullo; Tenable.

⁵⁶¹ See letter from Cybersecurity Coalition.

⁵⁶² See letters from NASAA and Tenable.

⁵⁶³ See letter from Prof. Perullo.

⁵⁶⁴ We note that one commenter stated its conclusion that “cyberattacks mainly affect larger companies.” See letter from BIO. The basis of the commenter’s assertion is that mean market capitalization of impacted companies in the relevant study cited in the Proposing Release is \$58.9 billion (Kamiya, et al. (2021)), which it notes is much higher than the average for small companies, and thus concludes that “cyberattacks mainly affect large companies and are not material for smaller companies.” As noted in Section IV, *supra*, an average market capitalization of \$58.9 billion does not preclude the existence of numerous companies much smaller (and larger) than that amount. See *supra* note 478. The commenter additionally notes that the relevant study states that “firms are more likely to experience cyberattacks when they are larger.” To the extent that smaller entities face fewer cyber incidents, that would result in a less frequent need to analyze whether disclosure of such incidents is required under the final rules. However, even if smaller entities are less likely to experience a cyberattack, this would not negate the analysis that such attacks, when they do occur, are more likely to be material for the reasons discussed above.

reporting companies with additional time to prepare to comply with the incident disclosure requirements, we are providing such registrants with an additional 180 days from the non-smaller reporting company compliance date before they must comply with the new Form 8-K requirement.

C. Small Entities Subject to the Final Amendments

The final amendments would apply to registrants that are small entities. The RFA defines “small entity” to mean “small business,” “small organization,” or “small governmental jurisdiction.”⁵⁶⁵ For purposes of the RFA, under our rules, a registrant, other than an investment company, is a “small business” or “small organization” if it had total assets of \$5 million or less on the last day of its most recent fiscal year and is engaged or proposing to engage in an offering of securities that does not exceed \$5 million.⁵⁶⁶ An investment company, including a business development company,⁵⁶⁷ is considered to be a “small business” if it, together with other investment companies in the same group of related investment companies, has net assets of \$50 million or less as of the end of its most recent fiscal year.⁵⁶⁸ We estimate that, as of December 31, 2022, there were approximately 800 issuers and 10 business development companies that may be considered small entities that would be subject to the final amendments.

D. Projected Reporting, Recordkeeping, and other Compliance Requirements

Per the final rules, registrants will be required to report material cybersecurity incidents on Form 8-K and Form 6-K for FPIs, and will be required to describe in their annual reports on Forms 10-K and 20-F certain aspects of their cybersecurity risk management, strategy, and

⁵⁶⁵ 5 U.S.C. 601(6).

⁵⁶⁶ See 17 CFR 240.0-10(a) [Exchange Act Rule 0-10a].

⁵⁶⁷ Business development companies are a category of closed-end investment company that are not registered under the Investment Company Act [15 U.S.C. 80a-2(a)(48) and 80a-53 through 64].

⁵⁶⁸ 17 CFR 270.0-10(a).

governance, if any. The final amendments are described in more detail in Section II above. These requirements generally will apply to small entities to the same extent as other entities, irrespective of size or industry classification, although we are adopting a later compliance date for smaller reporting companies in response to concerns raised by commenters. We continue to expect that the nature of any benefits and costs associated with the amendments to be similar for large and small entities, and so we refer to the discussion of the amendments' economic effects on all affected parties, including small entities, in Section IV above. Also consistent with the discussion in Sections II and IV above, we acknowledge that, in particular to the extent that a smaller entity would be required to provide disclosure under the final rules, it may face costs that are proportionally greater as they may be less able to bear such costs relative to larger entities. However, as discussed in in Section IV, we anticipate that the economic benefits and costs likely could vary widely among small entities based on a number of factors, such as the nature and conduct of their businesses, including whether the company actively manages material cybersecurity risks, which makes it difficult to project the economic impact on small entities with precision. To the extent that the disclosure requirements have a greater effect on small registrants relative to large registrants, they could result in adverse effects on competition. The fixed component of the legal costs of preparing the disclosure would be a primary contributing factor. Compliance with certain provisions of the final amendments may require the use of professional skills, including legal, accounting, and technical skills.

E. Agency Action to Minimize Effect on Small Entities

The RFA directs us to consider alternatives that would accomplish our stated objectives, while minimizing any significant adverse impact on small entities. Accordingly, we considered the following alternatives:

- Exempting small entities from all or part of the requirements;
- Establishing different compliance or reporting requirements that take into account the resources available to small entities;
- Using performance rather than design standards; and
- Clarifying, consolidating, or simplifying compliance and reporting requirements under the rules for small entities.

The rules are intended to better inform investors about cybersecurity incidents and, if any, the cybersecurity risk management, strategy, and governance of registrants of all types and sizes that are subject to the Exchange Act reporting requirements. We explain above in Sections II and IV that current requirements and guidance are not yielding uniform, comparable disclosure sufficient to meet investors' needs. The disclosure that does exist is scattered in various parts of registrants' filings, making it difficult for investors to locate, analyze, and compare across registrants. Staff has also observed that smaller reporting companies generally provide less cybersecurity disclosure as compared to larger registrants, and commenters agreed that there is a need for cybersecurity disclosure from small companies.⁵⁶⁹

Given the current disclosure landscape, exempting small entities or otherwise clarifying, consolidating, or simplifying compliance and reporting requirements under the rules for small entities would frustrate the rulemaking's goal of providing investors with more uniform and timely disclosure about material cybersecurity incidents and about cybersecurity risk management, strategy, and governance practices across all registrants. That said, as discussed in Section II above, we have consolidated and simplified the disclosure requirements for all entities, which should ease small entities' compliance as well. Further, as noted above, smaller

⁵⁶⁹ See *supra* notes 339 to 342 and accompanying text.

companies may face equal or greater cybersecurity risk than larger companies, making the disclosures important for investors in these companies.

On the other hand, we believe the rulemaking’s goals can be achieved by providing smaller reporting companies with additional time to come into compliance. Therefore, we are delaying smaller reporting companies’ required compliance date with the Form 8-K incident disclosure requirement by an additional 180 days from the non-smaller reporting company compliance date. This delay will benefit smaller reporting companies both by giving them extra time to establish disclosure controls and procedures and by allowing them to observe and learn from best practices as they develop among larger registrants.

Similarly, the final rules incorporate a combination of performance and design standards with respect to all subject entities, including small entities, in order to balance the objectives and compliance burdens of the rules. While the final rules do use design standards to promote uniform compliance requirements for all registrants and to address the concerns underlying the amendments, which apply to entities of all size, they also incorporate elements of performance standards to give registrants sufficient flexibility to craft meaningful disclosure that is tailored to their particular facts and circumstances. For example, the final rules require a registrant to describe its “processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes.” The rule also provides a non-exclusive list of disclosure items that a registrant should include in providing responsive disclosure to this performance standard; this design element provides registrants with additional guidance with respect to the type of disclosure topics that could be covered and promotes consistency.

Statutory Authority

The amendments contained in this release are being adopted under the authority set forth in Sections 7 and 19(a) of the Securities Act and Sections 3(b), 12, 13, 15, and 23(a) of the Exchange Act.

List of Subjects in 17 CFR Parts 229, 232, 239, 240, and 249

Reporting and record keeping requirements, Securities.

Text of Amendments

For the reasons set forth in the preamble, the Commission amends title 17, chapter II of the Code of Federal Regulations as follows:

PART 229—STANDARD INSTRUCTIONS FOR FILING FORMS UNDER SECURITIES ACT OF 1933, SECURITIES EXCHANGE ACT OF 1934 AND ENERGY POLICY AND CONSERVATION ACT OF 1975—REGULATION S-K

1. The authority citation for part 229 continues to read as follows:

Authority: 15 U.S.C. 77e, 77f, 77g, 77h, 77j, 77k, 77s, 77z-2, 77z-3, 77aa(25), 77aa(26), 77ddd, 77eee, 77ggg, 77hhh, 77iii, 77jjj, 77nnn, 77sss, 78c, 78i, 78j, 78j-3, 78l, 78m, 78n, 78n-1, 78o, 78u-5, 78w, 78ll, 78mm, 80a-8, 80a-9, 80a-20, 80a-29, 80a-30, 80a-31(c), 80a-37, 80a-38(a), 80a-39, 80b-11 and 7201 *et seq.*; 18 U.S.C. 1350; sec. 953(b), Pub. L. 111-203, 124 Stat. 1904 (2010); and sec. 102(c), Pub. L. 112-106, 126 Stat. 310 (2012).

2. Add § 229.106 to read as follows:

§ 229.106 (Item 106) Cybersecurity.

- (a) *Definitions.* For purposes of this section:

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.

(b) *Risk management and strategy.* (1) Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

- (i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;
- (ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
- (iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

(2) Describe whether any risks from cybersecurity threats, including as a result of any 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.

(c) *Governance*. (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.

(2) Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

- (i) Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
- (ii) The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- (iii) Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Instruction 1 to Item 106(c): In the case of a foreign private issuer with a two-tier board of directors, for purposes of paragraph (c) of this section, the term "board of directors" means the supervisory or non-management board. In the case of a foreign private issuer meeting the requirements of §240.10A-3(c)(3) of this chapter, for purposes of paragraph (c) of this Item, the term "board of directors" means the issuer's board of auditors (or similar body) or statutory auditors, as applicable.

Instruction 2 to Item 106(c): Relevant expertise of management in Item 106(c)(2)(i) may include, for example: Prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity.

(d) *Structured Data Requirement.* Provide the information required by this Item in an Interactive Data File in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.

3. Amend § 229.601 by revising paragraph (b)(101)(i)(C)(I) as follows:

§ 229.601 (Item 601) Exhibits

* * * * *

(b) * * *

(101) * * *

(i) * * *

(C) * * *

(I) Only when:

(i) The Form 8-K contains audited annual financial statements that are a revised version of financial statements that previously were filed with the Commission and that have been revised pursuant to applicable accounting standards to reflect the effects of certain subsequent events, including a discontinued operation, a change in reportable segments or a change in accounting principle. In such case, the Interactive Data File will be required only as to such revised financial statements regardless of whether the Form 8-K contains other financial statements; or

(ii) The Form 8-K includes disclosure required to be provided in an Interactive Data File pursuant to Item 1.05(b) of Form 8-K; and

* * * * *

PART 232—REGULATION S-T—GENERAL RULES AND REGULATIONS FOR ELECTRONIC FILINGS

4. The general authority citation for part 232 continues to read as follows:

Authority: 15 U.S.C. 77c, 77f, 77g, 77h, 77j, 77s(a), 77z-3, 77sss(a), 78c(b), 78l, 78m, 78n, 78o(d), 78w(a), 78ll, 80a-6(c), 80a-8, 80a-29, 80a-30, 80a-37, 80b-4, 80b-6a, 80b-10, 80b-11, 7201 *et seq.*; and 18 U.S.C. 1350, unless otherwise noted.

* * * * *

5. Amend § 232.405 by adding paragraph (b)(4)(v) to read as follows:

§ 232.405 Interactive Data File submissions.

* * * * *

(b) * * *

(4) * * *

(v) Any disclosure provided in response to: §229.106 of this chapter (Item 106 of Regulation S-K); Item 1.05 of §249.308 of this chapter (Item 1.05 of Form 8-K); and Item 16K of § 249.220f of this chapter (Item 16K of Form 20-F).

* * * * *

PART 239—FORMS PRESCRIBED UNDER THE SECURITIES ACT OF 1933

6. The general authority citation for part 239 continues to read as follows:

Authority: 15 U.S.C. 77c, 77f, 77g, 77h, 77j, 77s, 77z-2, 77z-3, 77sss, 78c, 78l, 78m, 78n, 78o(d), 78o-7 note, 78u-5, 78w(a), 78ll, 78mm, 80a-2(a), 80a-3, 80a-8, 80a-9, 80a-10, 80a-13, 80a-24, 80a-26, 80a-29, 80a-30, 80a-37, and sec. 71003 and sec. 84001, Pub. L. 114-94, 129 Stat. 1321, unless otherwise noted.

* * * * *

7. Amend § 239.13 by revising paragraph (a)(3)(ii) to read as follows:

§ 239.13 Form S-3, for registration under the Securities Act of 1933 of securities of certain issuers offered pursuant to certain types of transactions.

* * * * *

(a) * * *

(3) * * *

(ii) Has filed in a timely manner all reports required to be filed during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement, other than a report that is required solely pursuant to Item 1.01, 1.02, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a), 6.01, 6.03, or 6.05 of Form 8-K (§ 249.308 of this chapter). If the registrant has used (during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement) § 240.12b-25(b) of this chapter with respect to a report or a portion of a report, that report or portion thereof has actually been filed within the time period prescribed by that section; and

* * * * *

8. Amend Form S-3 (referenced in § 239.13) by adding General Instruction I.A.3(b).

Note: Form S-3 is attached as Appendix A to this document. Form S-3 will not appear in the Code of Federal Regulations.

PART 240—GENERAL RULES AND REGULATIONS, SECURITIES EXCHANGE ACT OF 1934

9. The authority citation for part 240 continues to read, in part, as follows:

Authority: 15 U.S.C. 77c, 77d, 77g, 77j, 77s, 77z–2, 77z–3, 77eee, 77ggg, 77nnn, 77sss, 77ttt, 78c, 78c–3, 78c–5, 78d, 78e, 78f, 78g, 78i, 78j, 78j–1, 78j–4, 78k, 78k–1, 78l, 78m, 78n, 78n–1, 78o, 78o–4, 78o–10, 78p, 78q, 78q–1, 78s, 78u–5, 78w, 78x, 78dd, 78ll, 78mm, 80a–20, 80a–23, 80a–29, 80a–37, 80b–3, 80b–4, 80b–11, 7201 *et seq.*, and 8302; 7 U.S.C. 2(c)(2)(E); 12 U.S.C. 5221(e)(3); 18 U.S.C. 1350; and Pub. L. 111–203, 939A, 124 Stat. 1376 (2010); and Pub. L. 112–106, sec. 503 and 602, 126 Stat. 326 (2012), unless otherwise noted.

* * * * *

Section 240.15d–11 is also issued under secs. 3(a) and 306(a), Pub. L. 107–204, 116 Stat. 745.

* * * * *

10. Amend § 240.13a-11 by revising paragraph (c) to read as follows:

§ 240.13a-11 Current reports on Form 8-K (§249.308 of this chapter).

* * * * *

(c) No failure to file a report on Form 8-K that is required solely pursuant to Item 1.01, 1.02, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a), 5.02(e), or 6.03 of Form 8-K shall be deemed to be a violation of 15 U.S.C. 78j(b) and § 240.10b-5.

11. Amend § 240.15d-11 by revising paragraph (c) to read as follows

§ 240.15d-11 Current reports on Form 8-K (§ 249.308 of this chapter).

* * * * *

(c) No failure to file a report on Form 8-K that is required solely pursuant to Item 1.01, 1.02, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a), 5.02(e), or 6.03 of Form 8-K shall be deemed to be a violation of 15 U.S.C. 78j(b) and §240.10b-5.

PART 249—FORMS, SECURITIES EXCHANGE ACT OF 1934

12. The authority citation for part 249 continues to read, in part, as follows:

Authority: 15 U.S.C. 78a *et seq.* and 7201 *et seq.*; 12 U.S.C. 5461 *et seq.*; 18 U.S.C. 1350; Sec. 953(b) Pub. L. 111–203, 124 Stat. 1904; Sec. 102(a)(3) Pub. L. 112–106, 126 Stat. 309 (2012), Sec. 107 Pub. L. 112–106, 126 Stat. 313 (2012), Sec. 72001 Pub. L. 114–94, 129 Stat. 1312 (2015), and secs. 2 and 3 Pub. L. 116–222, 134 Stat. 1063 (2020), unless otherwise noted.

Section 249.220f is also issued under secs. 3(a), 202, 208, 302, 306(a), 401(a), 401(b), 406 and 407, Pub. L. 107–204, 116 Stat. 745, and secs. 2 and 3, Pub. L. 116–222, 134 Stat. 1063.

* * * * *

Section 249.308 is also issued under 15 U.S.C. 80a–29 and 80a–37.

* * * * *

Section 249.310 is also issued under secs. 3(a), 202, 208, 302, 406 and 407, Pub. L. 107–204, 116 Stat. 745.

* * * * *

13. Revise Form 20-F (referenced in § 249.220f) by adding Item 16K.

Note: Form 20-F is attached as Appendix B to this document. Form 20-F will not appear in the Code of Federal Regulations.

14. Amend Form 6-K (referenced in § 249.306) by adding, in the second paragraph of General Instruction B, the phrase “material cybersecurity incident;” before the phrase “and any other information which the registrant deems of material importance to security holders.”

15. Revise Form 8-K (referenced in § 249.308) by:

- a. Revising General Instruction B.1.;
- b. Revising General Instruction G.1.; and
- c. Adding Item 1.05.

Note: Form 8-K is attached as Appendix C to this document. Form 8-K will not appear in the Code of Federal Regulations.

16. Revise Form 10-K (referenced in § 249.310) by:

- a. Revising General Instruction J(1)(b); and
- b. Adding Item 1C to Part I.

Note: Form 10-K is attached as Appendix D to this document. Form 10-K will not appear in the Code of Federal Regulations.

* * * * *

By the Commission.

Dated: July 26, 2023.

Vanessa A. Countryman,

Secretary.

Note: The following appendices will not appear in the Code of Federal Regulations.

Appendix A—Form S-3

FORM S-3

* * * * *

INFORMATION TO BE INCLUDED IN THE REPORT

* * * * *

General Instructions

I. Eligibility Requirements for Use of Form S-3

* * * * *

A. Registrant Requirements.

* * * * *

3. * * *

(b) has filed in a timely manner all reports required to be filed during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement, other than a report that is required solely pursuant to Item 1.01, 1.02, 1.04, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a) or 5.02(e) of Form 8-K (§249.308 of this chapter). If the registrant has used (during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement) Rule 12b-25(b) (§240.12b-25(b) of this chapter) under the Exchange Act with respect to a report or a portion of a report, that report or portion thereof has actually been filed within the time period prescribed by that rule.

* * * * *

Appendix B—Form 20-F

FORM 20-F

* * * * *

PART II

* * * * *

Item 16K. Cybersecurity.

(a) *Definitions.* For purposes of this section:

(1) *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.

(2) *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.

(3) *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.

(b) *Risk management and strategy.* (1) Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail

for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

- (i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;
 - (ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
 - (iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.
- (2) Describe whether any risks from cybersecurity threats, including as a result of any 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.

(c) *Governance.* (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.

(2) Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

- (i) Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

- (ii) The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- (iii) Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Instructions to Item 16K(c).

1. In the case of a foreign private issuer with a two-tier board of directors, for purposes of paragraph (c) of this Item, the term “board of directors” means the supervisory or non-management board. In the case of a foreign private issuer meeting the requirements of §240.10A-3(c)(3) of this chapter, for purposes of paragraph (c) of this Item, the term “board of directors” means the issuer’s board of auditors (or similar body) or statutory auditors, as applicable.
2. Relevant expertise of management in paragraph (c)(2)(i) of this Item may include, for example: Prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity.

(d) *Structured Data Requirement.* Provide the information required by this Item in an Interactive Data File in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.

Instruction to Item 16K. Item 16K applies only to annual reports, and does not apply to registration statements on Form 20-F.

* * * * *

Appendix C—Form 8-K

FORM 8-K

* * * * *

GENERAL INSTRUCTIONS

* * * * *

B. Events to be Reported and Time for Filing of Reports.

1. A report on this form is required to be filed or furnished, as applicable, upon the occurrence of any one or more of the events specified in the items in Sections 1 through 6 and 9 of this form.

Unless otherwise specified, a report is to be filed or furnished within four business days after occurrence of the event. If the event occurs on a Saturday, Sunday or holiday on which the Commission is not open for business, then the four business day period shall begin to run on, and include, the first business day thereafter. A registrant either furnishing a report on this form under Item 7.01 (Regulation FD Disclosure) or electing to file a report on this form under Item 8.01 (Other Events) solely to satisfy its obligations under Regulation FD (17 CFR 243.100 and 243.101) must furnish such report or make such filing, as applicable, in accordance with the requirements of Rule 100(a) of Regulation FD (17 CFR 243.100(a)), including the deadline for furnishing or filing such report. A report pursuant to Item 5.08 is to be filed within four business days after the registrant determines the anticipated meeting date. A report pursuant to Item 1.05 is to be filed within four business days after the registrant determines that it has experienced a material cybersecurity incident.

* * * * *

G. Use of this Form by Asset-Backed Issuers.

* * * * *

1. * * *

- (a) Item 1.05, Cybersecurity Incidents;
- (b) Item 2.01, Completion of Acquisition or Disposition of Assets;
- (c) Item 2.02, Results of Operations and Financial Condition;
- (d) Item 2.03, Creation of a Direct Financial Obligation or an Obligation under an Off-Balance Sheet Arrangement of a Registrant;
- (e) Item 2.05, Costs Associated with Exit or Disposal Activities;
- (f) Item 2.06, Material Impairments;
- (g) Item 3.01, Notice of Delisting or Failure to Satisfy a Continued Listing Rule or Standard; Transfer of Listing;
- (h) Item 3.02, Unregistered Sales of Equity Securities;
- (i) Item 4.01, Changes in Registrant's Certifying Accountant;
- (j) Item 4.02, Non-Reliance on Previously Issued Financial Statements or a Related Audit Report or Completed Interim Review;
- (k) Item 5.01, Changes in Control of Registrant;
- (l) Item 5.02, Departure of Directors or Principal Officers; Election of Directors; Appointment of Principal Officers;
- (m) Item 5.04, Temporary Suspension of Trading Under Registrant's Employee Benefit Plans; and
- (n) Item 5.05, Amendments to the Registrant's Code of Ethics, or Waiver of a Provision of the Code of Ethics.

* * * * *

INFORMATION TO BE INCLUDED IN THE REPORT

Section 1 – Registrant's Business and Operations

* * * * *

Item 1.05 Material Cybersecurity Incidents.

(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, 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.

(b) A registrant shall provide the information required by this Item in an Interactive Data File in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.

(c) Notwithstanding General Instruction B.1. to Form 8-K, if the United States Attorney General determines that disclosure required by paragraph (a) of this Item 1.05 poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, the registrant may delay providing the disclosure required by this Item 1.05 for a time period specified by the Attorney General, up to 30 days following the date when the disclosure required by this Item 1.05 was otherwise required to be provided. Disclosure may be delayed for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. Beyond the final 60-day delay under this paragraph, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through Commission exemptive order.

(d) Notwithstanding General Instruction B.1. to Form 8-K, if a registrant that is subject to 47 CFR 64.2011 is required to delay disclosing a data breach pursuant to such rule, it may delay providing the disclosure required by this Item 1.05 for such period that is applicable under 47 CFR 64.2011(b)(1) and in no event for more than seven business days after notification required under such provision has been made, so long as the registrant notifies the Commission in correspondence submitted to the EDGAR system no later than the date when the disclosure required by this Item 1.05 was otherwise required to be provided.

Instructions to Item 1.05.

1. A registrant's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident.
2. To the extent that the information called for in Item 1.05(a) is not determined or is unavailable at the time of the required filing, the registrant shall include a statement to this effect in the filing and then must file an amendment to its Form 8-K filing under this Item 1.05 containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.
3. The definition of the term "cybersecurity incident" in §229.106(a) [Item 106(a) of Regulation S-K] applies to this Item.
4. A registrant need not disclose specific or technical information about its planned response to the incident or its 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.

* * * * *

Appendix D—Form 10-K

FORM 10-K

* * * * *

GENERAL INSTRUCTIONS

* * * * *

J. Use of this Form by Asset-Backed Issuers.

* * * * *

(1) * * *

(b) Item 1A, Risk Factors and Item 1C, Cybersecurity;

* * * * *

Part I

* * * * *

Item 1C. Cybersecurity.

(a) Furnish the information required by Item 106 of Regulation S-K (§ 229.106 of this chapter).

* * * * *

Comptroller's Handbook

Safety and Soundness

Capital Adequacy
(C)

Asset Quality
(A)

Management
(M)

Earnings
(E)

Liquidity
(L)

Sensitivity to
Market Risk
(S)

Other Activities
(O)

Corporate and Risk Governance

Version 2.0, July 2019



Office of the
Comptroller of the Currency

Contents

Introduction.....	1
Risks Associated With Corporate and Risk Governance.....	3
Strategic Risk.....	4
Reputation Risk.....	4
Compliance Risk.....	4
Operational Risk	5
Corporate Governance	6
Board's Role in Corporate Governance	6
Board Composition, Qualifications, and Selection.....	7
Leadership Structure of the Board	9
Outside Advisors and Advisory Directors	9
Board and Board Committee Meeting Minutes	10
Access to Senior Management and Staff	11
Director Orientation and Training	12
Board Compensation.....	12
Board Tenure	13
Board's Responsibilities	13
Provide Oversight	15
Establish an Appropriate Corporate Culture.....	15
Comply With Fiduciary Duties and the Law	17
Select, Retain, and Oversee Management.....	18
Oversee Compensation and Benefits Arrangements.....	21
Maintain Appropriate Affiliate and Holding Company Relationships	24
Establish and Maintain an Appropriate Board Structure	24
Perform Board Self-Assessments	25
Oversee Financial Performance and Risk Reporting	26
Support Efforts to Serve Community Credit Needs	28
Individual Responsibilities of Directors	28
Attend and Participate in Board and Committee Meetings	28
Request and Review Meeting Materials	29
Make Decisions and Seek Explanations	29
Review and Approve Policies	30
Exercise Independent Judgment	30
Planning	32
Strategic Planning	32
New Activities	34
Capital Planning.....	35
Operational Planning	36
Disaster Recovery and Business Continuity Planning.....	36
Information Technology and Information Security	37
Recovery Planning	37

Risk Governance	39
Risk Culture	40
Risk Appetite	40
Risk Management System.....	42
Identify Risk.....	44
Measure Risk	44
Monitor Risk	44
Control Risk.....	44
Risk Assessment Process	45
Policies	45
Processes	46
Personnel.....	46
Control Systems	47
Quality Control	48
Quality Assurance.....	48
Compliance Management System.....	48
Bank Secrecy Act/Anti-Money Laundering Program.....	50
Audit Program.....	51
Management Information Systems	52
Third-Party Risk Management.....	54
Insurance	54
Insurance Record Keeping.....	55
Board and Management's Roles in Risk Governance	55
Board's Responsibilities	55
Management's Responsibilities	56
Examination Procedures	58
Scope.....	58
Board of Directors and Management.....	60
Conclusions.....	89
Internal Control Questionnaire	91
Verification Procedures	96
Appendices.....	98
Appendix A: Board of Directors Statutory and Regulatory Requirements	98
Appendix B: Regulations Requiring Board Approval for Policies and Programs....	101
Appendix C: Common Board Committees	106
Appendix D: Common Types of Insurance	111
Appendix E: Glossary	117
Appendix F: Abbreviations.....	119
References	120

Introduction

The Office of the Comptroller of the Currency's (OCC) *Comptroller's Handbook* booklet, "Corporate and Risk Governance," is prepared for use by OCC examiners in connection with their examination and supervision of national banks, federal savings associations, and federal branches and agencies of foreign banking organizations (collectively, banks). Each bank is different and may present specific issues. Accordingly, examiners should apply the information in this booklet consistent with each bank's individual circumstances. When it is necessary to distinguish between them, national banks¹ and federal savings associations (FSA) are referred to separately.

The general principles and practices discussed in this booklet are important protections against overarching risks to banks. This booklet

- focuses on strategic, reputation, compliance, and operational risks as they relate to governance.
- reinforces oversight of credit, liquidity, interest rate, and price risks.
- combines and updates existing national bank and FSA guidance covering the roles and responsibilities of the board of directors and senior management as well as corporate and risk governance activities and risk management practices.
- supplements other OCC and interagency guidance related to corporate and risk governance and risk management.

Other booklets in the *Comptroller's Handbook* provide detailed risk management information according to subject.

An effective corporate and risk governance framework is essential to maintaining the safe and sound operation of the bank and helping to promote public confidence in the financial system. A bank's corporate and risk governance practices should be commensurate with the bank's size, complexity, and risk profile. In accordance with the OCC's risk-based supervision approach, examiners use the core assessment in the "Community Bank Supervision," "Federal Branches and Agencies Supervision," or "Large Bank Supervision" booklets of the *Comptroller's Handbook* when evaluating the governance of community banks, federal branches and agencies, and midsize and large banks, respectively. Expanded procedures in this and other booklets of the *Comptroller's Handbook* contain detailed guidance for examining activities or products that warrant review beyond the core assessment.

Corporate and risk governance structure and practices should keep pace with the bank's changes in size, risk profile, and complexity. Larger or more complex banks should have more sophisticated and formal board and management structures and practices.

¹ Generally, references to "national banks" throughout this booklet also apply to federal branches and agencies of foreign banking organizations unless otherwise specified. Refer to the "Federal Branches and Agencies Supervision" booklet of the *Comptroller's Handbook* for more information regarding applicability of laws, regulations, and guidance to federal branches and agencies.

Heightened Standards

Specific criteria for covered banks, subject to 12 CFR 30, appendix D, are noted in text boxes like this one throughout this booklet. 12 CFR 30, appendix D.I.E.5, “Covered Bank,” describes banks subject to “OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches” (heightened standards).

The assignment of the “management” rating in CAMELS² under the Uniform Financial Institutions Rating System is based on an assessment of the capability of the board of directors and management, in their respective roles, to identify, measure, monitor, and control the risks of a bank’s activities. The rating reflects their ability to maintain the bank’s safe, sound, and efficient operation in compliance with applicable laws and regulations.³ The “management” rating reflects examiner assessments about the board and management’s willingness and ability to effectively address all aspects of governance, risk management, compliance, bank operations, and financial performance. Examiners also consider Bank Secrecy Act (BSA)/anti-money laundering (AML) examination findings in a safety and soundness context when assigning the management component rating. Serious deficiencies in a bank’s BSA/AML compliance program create a presumption that the bank’s management component rating will be adversely affected because its risk management practices are less than satisfactory.

For purposes of this booklet, the term “board” refers to the board of directors unless otherwise stated. The board is responsible for providing effective oversight over the bank. The term “senior management” refers to bank employees designated by the board as executives responsible for making key decisions and implementing the board’s vision. Senior management may include, but is not limited to, the president, chief executive officer (CEO), chief financial officer, chief risk executive (CRE),⁴ chief information officer (CIO), compliance officer, chief credit officer, chief audit executive (CAE),⁵ and chief bank counsel. Titles and positions vary depending on the bank’s structure, size, and complexity. Unless otherwise noted, the booklet uses the terms “CEO” and “president” to refer to the individual

² A bank’s composite rating under the Uniform Financial Institutions Rating System, or CAMELS, integrates ratings from six component areas: capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk. Evaluations of the component areas take into consideration the bank’s size and sophistication, the nature and complexity of its activities, and its risk profile. Federal branches and agencies are rated using the ROCA rating system, which includes the following component areas: risk management, operational controls, compliance, and asset quality.

³ For more information about the management rating, refer to the “Bank Supervision Process” booklet of the *Comptroller’s Handbook*.

⁴ A CRE is also commonly known as a chief risk officer.

⁵ A CAE is commonly known as a chief auditor.

appointed by the board to oversee the bank’s day-to-day activities. The term “management” refers to bank managers responsible for carrying out the bank’s day-to-day activities, including goals established by senior management.

Corporate governance identifies the authorities and responsibilities of the board and senior management, in their respective roles, to govern the bank’s operations and structure. Corporate governance involves the relationships among the bank’s board, management, shareholders, and other stakeholders. Corporate governance is essential to the safe and sound operation of the bank. Corporate governance includes how the board and senior management, in their respective roles,

- set the bank’s strategy, objectives, and risk appetite.
- establish the bank’s risk governance framework.
- identify, measure, monitor, and control risks.
- supervise and manage the bank’s business.
- protect the interests of depositors, protect the interests of shareholders or members (in the case of a mutual FSA),⁶ and take into account the interests of other stakeholders.
- align corporate culture, activities, and behaviors with the expectation that the bank will operate in a safe and sound manner, operate with integrity, and comply with applicable laws and regulations.

Risk governance is an important element of corporate governance. Risk governance applies the principles of sound corporate governance to the identification, measurement, monitoring, and controlling of risks to help ensure that risk-taking activities are in line with the bank’s strategic objectives and risk appetite. Risk governance is the bank’s approach to risk management and includes the policies, processes, personnel, and control systems that support risk-related decision making.

Risks Associated With Corporate and Risk Governance

From a supervisory perspective, risk is the potential that events will have an adverse effect on a bank’s current or projected financial condition⁷ and resilience.⁸ The OCC has defined eight categories of risk for bank supervision purposes: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. These categories are not mutually exclusive. Any product or service may expose a bank to multiple risks. Risks also may be interdependent and may be positively or negatively correlated. Examiners should be aware of and assess this interdependence. Examiners also should be alert to concentrations that can significantly elevate risk. Concentrations can accumulate within and across products,

⁶ Mutual FSAs do not have shareholders. Voting rights in a mutual FSA are held by members, who are depositors (and also, in some cases, borrowers) of the association. In the context of mutual FSAs, references to “shareholders” in this booklet should be read to mean members.

⁷ Financial condition includes impacts from diminished capital and liquidity. Capital in this context includes potential impacts from losses, reduced earnings, and market value of equity.

⁸ Resilience recognizes the bank’s ability to withstand periods of stress.

business lines, geographic areas, countries, and legal entities. Refer to the “Bank Supervision Process” booklet of the *Comptroller’s Handbook* for an expanded discussion on banking risks and their definitions. Corporate and risk governance is the framework in which all risks are managed at a bank as well as the oversight of the framework. The primary risks associated with corporate and risk governance are strategic, reputation, compliance, and operational. These risks are discussed more fully in the following paragraphs.

Strategic Risk

Strategic risk is the risk to current or projected financial condition and resilience arising from adverse business decisions, poor implementation of business decisions, or lack of responsiveness to changes in the banking industry and operating environment. The board and senior management, collectively, are the key decision makers that drive the strategic direction of the bank and establish governance principles. The absence of appropriate governance in the bank’s decision-making process and implementation of decisions can have wide-ranging consequences. The consequences may include missed business opportunities, losses, failure to comply with laws and regulations resulting in civil money penalties (CMP), and unsafe or unsound bank operations that could lead to enforcement actions or inadequate capital.

Reputation Risk

Reputation risk is the risk to current or projected financial condition and resilience arising from negative public opinion. The strength and level of transparency of a bank’s corporate and risk governance structure influence the bank’s reputation with shareholders, regulators, customers, other stakeholders, and the community at large. A responsible corporate culture and a sound risk culture are the foundation of an effective corporate and risk governance framework and help form a positive public perception of the bank. A bank that fails to implement effective corporate and risk governance principles and practices may hinder the bank’s competitiveness and adversely affect the bank’s ability to establish new relationships and services or to continue servicing existing relationships. Departures from effective corporate and risk governance principles and practices cast doubt on the integrity of the bank’s board and management. History shows that such departures can affect the entire financial services sector and the broader economy.

Compliance Risk

Compliance risk is the risk to current or projected financial condition and resilience arising from violations of laws or regulations, or from nonconformance with prescribed practices, internal bank policies and procedures, or ethical standards. Banks are subject to various laws, rules and regulations. The board is responsible for complying with applicable laws, regulations, and for understanding the legal and regulatory framework applicable to the bank’s activities. The board is also responsible for meeting its fiduciary duties to the bank. Failure to establish a sound compliance program that addresses all laws and regulations, and that includes a BSA program reasonably designed to comply with the record-keeping and

reporting requirements, exposes the bank to increased legal and reputation risks and the potential for enforcement actions (including CMPs) and customer reimbursements.

Operational Risk

Operational risk is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events. The board oversees management's establishment and maintenance of the bank's risk management system through the risk governance framework. Sound corporate governance and risk management systems—including strategic planning, internal controls and assurance of internal controls, management information systems (MIS), and talent management—help to identify, measure, monitor, and control risks. Lapses in corporate and risk governance can increase the bank's risk profile and elevate the risk of fraud, defalcation, and other operational losses.

Corporate Governance

The board and management should be transparent about their corporate and risk governance structure and practices, with particular emphasis on board composition, the director nominating process, management succession plans, compensation, and other issues important to shareholders. The board and senior management should also play an active role in communicating with shareholders and adhering to disclosure practices. Serious errors or omissions in the bank's disclosure requirements may result in violations of law and regulation, which in turn could lead to significant regulatory penalties. The board and management should view enhanced transparency and communication as a means of building trust and public confidence that enhance the bank's value and potentially provide access to capital and funding markets.

Board's Role in Corporate Governance

The board plays a pivotal role in the effective governance of its bank. The board is accountable to shareholders, regulators, and other stakeholders. The board is responsible for overseeing management, providing organizational leadership, and establishing core corporate values. The board should create a corporate and risk governance framework to facilitate oversight and help set the bank's strategic direction, risk culture, and risk appetite. The board also oversees the talent management processes for senior management, which include development, recruiting, succession planning, and compensation.

The board should have a clear understanding of its roles and responsibilities. It should collectively have the skills and qualifications, committee structure, communication and reporting systems, and processes necessary to provide effective oversight. The board should be willing and able to act independently and provide a credible challenge to management.

The corporate and risk governance framework should provide for independent assessments of the quality, accuracy, and effectiveness of the bank's risk management functions, financial reporting, and compliance with laws and regulations. Most often performed by the bank's audit function, independent assurances are essential to the board's effective oversight of management.

The board's role in the governance of the bank is clearly distinct from management's role. The board is responsible for the overall direction and oversight of the bank—but is not responsible for managing the bank day-to-day. The board should oversee and hold management accountable for meeting strategic objectives within the bank's risk appetite. Both the board and management should ensure the bank is operating in a safe and sound manner and complying with laws and regulations.

Board Composition, Qualifications, and Selection

Board composition should facilitate effective oversight. The ideal board is well diversified and composed of individuals with a mix of knowledge and expertise in line with the bank's size, strategy, risk profile, and complexity. Although the qualifications of individual directors will vary, the directors should provide the collective expertise, experience, and perspectives necessary for effectively overseeing the bank. Boards of larger, more complex banks should include directors who have the ability to understand the organizational complexities and the risks inherent in the bank's businesses. Individual directors also should lend expertise to the board's risk oversight and compliance responsibilities. In addition, the board and its directors must meet the statutory and regulatory requirements governing size, composition, and other aspects. Refer to appendix A of this booklet for a list of these requirements.

The board should be willing and able to exercise independent judgment and provide credible challenge to management's decisions and recommendations. The board also should have an appropriate level of commitment and engagement to carry out its duties and responsibilities. To promote director independence, the board should ensure an appropriate mix of "inside" and "outside" directors. Inside directors are bank officers or other bank employees. Outside directors are not bank employees. Directors are viewed as independent if they are free of any family relationships or any material business or professional relationships (other than stock ownership and directorship itself) with the bank or its management. Independent directors bring experiences from their fields of expertise. These experiences provide perspective and objectivity because independent directors oversee bank operations and evaluate management recommendations. This mix of inside and outside directors promotes arms-length oversight. A board that is subject to excessive management influence may not be able to effectively fulfill its fiduciary and oversight responsibilities.

Generally, a director should

- be willing and able to exercise independent judgment and provide credible challenge to management's decisions and recommendations.
- have basic knowledge of the banking industry, financial regulatory system, and laws and regulations that govern the bank's operation.
- have background, knowledge, and experience in business or another discipline to facilitate bank oversight.
- accept fiduciary duties and obligations, including a firm commitment to put the bank's interests ahead of personal interests and to avoid conflicts of interest.
- have firm commitment to regularly attend and be prepared for board and committee meetings.
- have knowledge of the communities that the bank serves.

To fill board vacancies, the board should establish a process to identify, assess, and select director candidates. The bank's size and complexity may warrant the process to be written. Some boards use a nominating committee. The board or nominating committee should consider whether the director candidate has the necessary knowledge, skills, and experience in light of the bank's business and the risks presented by that business as well as sufficient

time to effectively carry out his or her responsibilities. Criteria for desired knowledge, skills, and experience may change over time if, for example, the bank plans to offer new, modified, or expanded products and services. Some boards establish additional criteria depending on certain needs. The director candidate should be willing and able to actively oversee senior management and challenge and require changes in senior management, if necessary. Additionally, inside directors should not use undue influence in selecting board members.

The board candidate should have a record of integrity in his or her personal and professional dealings, a good reputation, and a willingness to place the interests of the bank above any conflicting self-interest. The board candidate should disclose any relationships or potential conflicts of interest that the candidate or any of his or her related interests has with the bank or its affiliates. The board should consider whether a potential candidate with significant conflicts of interest that would require him or her to abstain from consideration of issues or transactions is an appropriate candidate. The bank should conduct background checks on potential board members and periodic checks of existing directors.

Diversity among directors is another important aspect of an effective board. The board should actively seek a diverse pool of candidates, including women and minorities, as well as candidates with diverse knowledge of risk management and internal controls.⁹

In most cases, nominees should be able to serve as directors immediately after they are elected in accordance with the bank’s bylaws. The bank must file a prior notice with the OCC when any of the following circumstances exist:¹⁰

- The bank is in troubled condition, as defined by 12 CFR 5.51.
- The bank is not in compliance with minimum capital requirements as prescribed in 12 CFR 3, “Capital Adequacy Standards.”
- The OCC determines, in writing, in connection with the OCC’s review of a capital restoration plan under 12 USC 1831o, “Prompt Corrective Action,” or otherwise, that such prior notice is appropriate.

The OCC also generally requires prior notice for new directors under additional circumstances, such as de novo banks, change in bank control, or conversions to a federal charter.¹¹

⁹ For more information, refer to OCC Bulletin 2015-30, “Standards for Assessing the Diversity Policies and Practices of Regulated Entities: Final Interagency Policy Statement.”

¹⁰ For more information, refer to 12 USC 1831i, “Agency Disapproval of Directors and Senior Executive Officers of Insured Depository Institutions or Depository Institution Holding Companies,” and 12 CFR 5.51, “Changes in Directors and Senior Executive Officers of a National Bank or Federal Savings Association.” Also, refer to the “Changes in Directors and Senior Executive Officers” and “Background Investigations” booklets of the *Comptroller’s Licensing Manual*.

¹¹ Refer to the “Charters,” “Change in Bank Control,” and “Conversions to Federal Charter” booklets of the *Comptroller’s Licensing Manual* for more information.

Directors should adhere to the attendance policy for regular and special board meetings. A director of a national bank may not participate or vote by proxy.¹² Excessive absences may be grounds for director dismissal. For more information, refer to the “Attend and Participate in Board and Committee Meetings” section of this booklet.

Leadership Structure of the Board

The board should determine the appropriate leadership structure. The individual selected as board chair plays a crucial leadership role in the board’s proper functioning. The board chair should promote candid dialogue, encourage critical discussion, and support directors to express any dissenting views. The chair should strive to promote a well-functioning, informed, independent, and deliberative decision-making process. The chair should also have the requisite qualities, including being a respected and trusted board member, and have appropriate leadership and communication skills.

These are the two most common structures for board leadership:

- The chair is independent of the CEO.
- When the CEO and chair are the same person, the board appoints a lead director who is independent of management.

Both structures can be equally effective. When the board chair and the CEO are different individuals, however, having the separate roles may promote a more appropriate balance of power between the board and senior management.

When the board appoints a lead director in addition to a chair who also is the CEO, the board should clearly define the lead director’s role. For example, a lead director typically maintains ongoing communication with the CEO, leads executive sessions of the board, works with the CEO and the board to set the board agenda, and facilitates communication between the directors and the CEO.

Outside Advisors and Advisory Directors

From time to time, the board and board committees may need to seek advice from outside advisors, who are independent of management. For example, there may be technical aspects of the bank’s business—such as risk assessments, accounting matters, strategic planning, or compensation—where additional expert advice would be useful. The board should have the necessary financial resources to hire external experts to help the board fulfill its fiduciary responsibilities. Audit committees of certain banks must have members with banking or related financial management expertise, have access to their own outside counsel, and not

¹² For national banks, refer to 12 CFR 7.2009, “Quorum of the Board of Directors; Proxies Not Permissible.”

include any large customers of the bank.¹³ These committees may also have their own advisors.

Although qualified consultants can provide needed expertise and counsel, the board should ensure that no improper conflicts of interest exist between the bank and the consultant so that the board receives only objective and independent advice.

To leverage outside expertise, the board may consider using advisory directors. These individuals provide information and advice but do not vote as part of the board. The bank may use advisory directors in a number of situations, including

- when the operations of the bank are geographically dispersed and the board wants input from more segments of the communities served by the bank.
- when the board is small and the directors want direct involvement with a broader array of community leaders.
- to assist in business development.
- to gain access to special expertise to help the board with planning and decision making.
- to help identify likely candidates for future board openings.

Because of their limited role, advisory directors generally are not liable for board decisions. The facts and circumstances of a particular situation determine if an advisory director may have liability for individual decisions. Factors affecting potential liability include

- whether advisory directors were elected or appointed.
- how corporate documents identified advisory directors.
- the extent to which the advisory directors participated in board meetings.
- whether advisory directors exercised significant influence on the voting process.
- how the bank compensated advisory directors for attending board meetings.
- whether the advisory director had a previous relationship with the bank.

Additionally, an advisory director who, in fact, functions as a full director may be liable for board decisions in which he or she participated as if that advisory director were a full director. The OCC expects that individuals will not shield their actions from liability simply by having the word “advisory” in their titles.

Board and Board Committee Meeting Minutes

Minutes of board and board committee meetings are an essential part of the bank’s records capturing the board’s deliberations and actions. Board meeting minutes should be complete and accurate. Minutes should document the board’s review and discussion of material action items on the agenda, any actions taken, follow-up items to be addressed at subsequent

¹³ For more information, refer to 12 CFR 363.5(b), “Committees of Large Institutions.” This pertains to audit committees of any bank with more than \$3 billion in total assets as of the beginning of the fiscal year. Refer to the “Internal and External Audits” booklet of the *Comptroller’s Handbook* for more information on other audit committee independence considerations.

meetings, and any other issues that may arise (including approval of previous meeting minutes and board-approved policies).

Minutes should record the attendance of each director, other attendees, and directors' votes or abstentions. The record of board meetings and activities should include all materials distributed to the board for informational, oversight, or monitoring purposes. Each director should have the opportunity to review and, if appropriate, modify the minutes before the board ratifies them. Board minutes should be timely and presented for approval at the next meeting of the board. In addition, the board should receive regular reports or minutes from the various committee meetings.

The board should address the level of detail required for minutes and records of board meetings. Minutes may be subject to discovery, for example, during stockholder derivative litigation.¹⁴ Board minutes should include sufficient information to reflect that directors were fully informed about the relevant facts, carefully deliberated the issues, provided credible challenge when necessary, and made decisions based on the best interests of the bank and its shareholders.

For stock FSAs, a director's presence at a meeting at which actions are taken on behalf of the bank is considered assenting to the action unless his or her abstention or dissent is entered in the meeting minutes.¹⁵ A director may also file a written dissent to the action with the secretary before the meeting is adjourned or send a written dissent by registered mail to the secretary within five days after the meeting minutes are received.¹⁶

Access to Senior Management and Staff

Directors should have full access to all employees, if needed, but particularly senior management. Direct interaction with key staff can balance viewpoints and help ensure that information going to the board is not overly filtered. Direct interaction also can help directors deal with succession planning and management development. In addition, direct interaction with employees allows directors to assess how the corporate culture has been implemented throughout the bank. Directors can use these contacts to determine what behaviors senior managers promote.

¹⁴ In stockholder derivative litigation, a shareholder sues both the corporation and a third party. The third party, often an executive officer or director of the corporation, is the actual defendant. The shareholder seeks recovery for the corporation from the third party.

¹⁵ For more information, refer to 12 CFR 5.22(l)(10), "Presumption of Assent" (stock FSAs).

¹⁶ Ibid.

Director Orientation and Training

The board should conduct orientation programs for new directors. Orientation programs vary according to bank size and complexity. At a minimum, these programs should explain

- the bank's organizational structure, corporate culture, operations, strategic plans, risk appetite, and significant issues.
- the importance of BSA/AML regulatory requirements, the ramifications of noncompliance with the BSA, and the BSA/AML risk posed to the bank.
- the individual and group responsibilities of board members, the roles of the various board committees, and the roles and responsibilities of senior management.

Directors should understand their roles and responsibilities and deepen their knowledge of the bank's business, operations, risks, and management. The board should periodically assess its skills and competencies relative to the bank's size and complexity, identify gaps, and take appropriate actions.

Management can help the board develop an ongoing education and training program to keep directors informed and current on general industry trends and regulatory developments, particularly regarding issues that pertain to their bank.

Heightened Standards

The board should establish and adhere to a formal, ongoing training program for all directors. This program should consider the directors' knowledge and experience and the covered bank's risk profile. The program should include, as appropriate, training on the following:

- Complex products, services, lines of business, and risks that have a significant impact on the covered bank.
- Laws, regulations, and supervisory requirements applicable to the covered bank.
- Other topics identified by the board.¹⁷

Board Compensation

Directors should be compensated fairly and appropriately. Given the demands on a director's time and the responsibilities, director compensation should be competitive and sufficient to attract and retain qualified individuals. The board or a designated committee sets and periodically reevaluates director compensation. Such compensation should be aligned with industry standards and be commensurate with an individual director's responsibilities. The board also should safeguard against payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to the bank. Excessive compensation is considered an unsafe or unsound practice. Additionally, if the bank falls below required

¹⁷ For more information, refer to 12 CFR 30, appendix D, "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches"; appendix D, III; and appendix D, III.E, "Provide Ongoing Training to All Directors."

capital minimums, the compensation paid to directors should be reassessed. The reassessment may include reducing or eliminating the fees paid.

Board Tenure

A director tenure policy, though not a requirement for either public or nonpublic banks, can help the bank maintain skilled, objective, and engaged board members. A tenure policy or bylaws may, for example, establish

- director term limits.
- a mandatory retirement age.

A tenure policy can provide a road map for the board's natural evolution and create a structured process to obtain fresh ideas and promote critical thinking from new directors. A tenure policy protects against the board losing objectivity and effectiveness if long-time directors become less active, less committed, complacent, or too comfortable with the status quo. On the other hand, mandatory retirement may result in the loss of directors whose contributions to the bank continue to be valuable.

Board's Responsibilities

The board is responsible for

- providing effective oversight.
- exercising independent judgment.
- providing credible challenge to management.
- establishing an appropriate corporate culture and setting the tone at the top.
- understanding the legal and regulatory framework applicable to the bank's activities.
- complying with fiduciary duties and all applicable rules and laws.
- directing and overseeing an effective compliance management system (CMS).
- setting realistic strategic goals and objectives and overseeing management's implementation of those goals and objectives.
- confirming that the bank has a risk management system, including audit, suitable for the bank's size and activities, and understanding the bank's material risks.
- confirming that the bank has an effective system of internal controls.
- holding management accountable for implementing policies and operating within established standards and limits.
- monitoring the bank's operations, overseeing the bank's business performance, and staying informed about the bank's operating and business environment.
- selecting, retaining, and overseeing a competent CEO and senior management team.
- overseeing the compensation and benefits programs.
- setting formal performance standards for senior management, overseeing the talent management process, and approving a management succession policy for the CEO and other key executives.

- establishing and maintaining an appropriate board structure and performing board self-assessments.
- maintaining appropriate affiliate and holding company relationships.
- monitoring and supporting management's efforts to serve the convenience and needs of the communities in which the bank is chartered and its assessment area(s), including the need for credit and deposit services.¹⁸
- approving the bank's BSA/AML compliance program.¹⁹
- confirming that management's actions to correct material weaknesses, including those identified by the bank, its auditors, and regulators, are timely and effective.

Heightened Standards

Each member of a covered bank's board should oversee the covered bank's compliance with safe and sound banking practices. The board also should require management to establish and implement an effective risk governance framework that meets the minimum standards described in these guidelines. The board or the board's risk committee should approve any significant changes to the risk governance framework and monitor compliance with such framework.²⁰

A covered bank's board should actively oversee the covered bank's risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board may rely on risk assessments and reports prepared by independent risk management (IRM) and internal audit to support the board's ability to question, challenge, and, when necessary, oppose recommendations and decisions made by management that could cause the covered bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the bank.²¹

When providing active oversight under paragraph III.B of heightened standards guidelines, each member of the board should exercise sound, independent judgment.²²

The following pages focus on some of the board's key responsibilities.

¹⁸ Refer to 12 CFR 25, "Community Reinvestment Act and Interstate Deposit Production Regulations" (national banks) and 12 CFR 195, "Community Reinvestment" (FSAs). Also refer to OCC Bulletin 2018-17, "Community Reinvestment Act: Supervisory Policy and Processes for Community Reinvestment Act Performance Evaluations," for more information regarding CRA, including OCC supervisory policies and procedures regarding how examiners evaluate bank performance under the CRA.

¹⁹ For more information, refer to 12 CFR 21.21, "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance" and the *Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*.

²⁰ For more information, refer to 12 CFR 30, appendix D, III, and appendix D, III.A, "Require an Effective Risk Governance Framework."

²¹ For more information, refer to 12 CFR 30, appendix D, III, and appendix D, III.B, "Provide Active Oversight of Management."

²² For more information, refer to 12 CFR 30, appendix D, III, and appendix D, III.C, "Exercise Independent Judgment."

Provide Oversight

The key to effective board oversight is qualified and actively involved directors. Effective board oversight can help the bank withstand economic downturns, problems with ineffective management, and other concerns. During challenging times, the board should evaluate the bank's condition, take appropriate sustainable corrective actions, and, when necessary, keep the bank operating until the board obtains capable management to fully resolve the bank's problems.

Board oversight is critical to maintaining the bank's operations in a safe and sound manner and the bank's compliance with laws and regulations. Effective board oversight includes supervising major banking activities and governing senior management. To fulfill its responsibilities, the board relies on senior management to oversee the key decisions and management to carry out the bank's day-to-day activities. The board also relies on management to provide the board with sound advice on organizational strategies, objectives, structure, and significant policies and to provide accurate and timely information about the bank's risks and financial performance. Several *Comptroller's Handbook* booklets and *The Director's Book: Role of Directors for National Banks and Federal Savings Associations* reinforce and expand on supervisory expectations regarding the board's oversight duties and management's roles and responsibilities.

Establish an Appropriate Corporate Culture

Corporate culture refers to the norms and values that drive behaviors within an organization. An appropriate corporate culture for a bank is one that does not condone or encourage imprudent risk taking, unethical behavior, or the circumvention of laws, regulations, or safe and sound policies and procedures in pursuit of profits or business objectives. An appropriate corporate culture holds employees accountable. This starts with the board, which is responsible for setting the tone at the top and overseeing management's role in fostering and maintaining a sound corporate culture and risk culture. Shared values, expectations, and objectives established by the board and senior management promote a sound corporate culture.

To promote a sound corporate culture, the board should

- establish the expectations for desired behaviors; practice and promote the expectations that all business should be conducted in a legal and ethical manner; and oversee adherence to such values by senior management and other employees.
- promote risk awareness within a sound risk culture (refer to the "Risk Culture" section for more information).
- confirm that corporate values and the code of conduct are communicated throughout the bank.
- promote clear lines of authority and accountability.
- hold management accountable for transparent and timely information.

To promote a sound corporate culture, management should

- demonstrate commitment to the corporate culture and expect the same from all employees.
- integrate the culture into the bank’s strategic planning process and risk management practices.
- include desired behaviors in performance reviews and compensation practices.
- engage in continuous employee communication and training regarding risk management practices and standards of conduct.
- report and escalate material risk issues, suspected fraud, and illegal or unethical activities to the board.

Code of Ethics

The board should adopt a written code of ethics (or code of conduct) to set expected standards of behavior and professional conduct for all employees. The board should oversee management’s development and periodic review of the code of ethics and other policies that address board and employee conduct, insider activities, conflicts of interest, and other relevant ethical issues. The code of ethics should encourage the timely and confidential communication of suspected fraud, misconduct, or abuse to a higher level within the bank. Such a code is intended to foster a culture of integrity and accountability.

The bank’s code of ethics should address the following:

- **Conflicts of interest:** A conflict of interest occurs when an individual’s private interests conflict with the bank’s interests.
- **Insider activities:** Directors and executive officers should refrain from financial relationships that are or could be viewed as abusive, imprudent, or preferential. In addition, laws and regulations prohibit certain insider activities.²³
- **Self-dealing and corporate opportunity:** Employees, officers, and directors are prohibited from using corporate property, information, or their positions for personal gain. Usurpation of a corporate opportunity is a breach of fiduciary duty.
- **Confidentiality:** All bank employees, officers, and directors must maintain the confidentiality of bank, customer, and personnel information, as required by law.
- **Fair dealing:** Employees, officers, and directors should not conceal information, abuse privileged information, misrepresent material facts, or engage in any other unfair dealing practice.
- **Protection and use of bank assets:** Company assets should be used for legitimate business purposes.
- **Compliance:** All bank employees, officers, and directors must comply with applicable laws and regulations.
- **Whistle-blower policy:** The bank should have a process for employees to report legitimate concerns about suspected illegal, unethical, or questionable practices with

²³ For more information, refer to 12 USC 1828(z), “General Prohibition on Sale of Assets”; 12 CFR 215, “Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks (Regulation O)”; 12 CFR 31, “Extensions of Credit to Insiders and Transactions With Affiliates”; and the “Insider Activities” booklet of the *Comptroller’s Handbook*.

protection from reprisal. This process includes the ability to escalate operational problems, inappropriate conduct, policy violations, or other risks to the bank for investigation.

- **Consequences:** Employees, officers, and directors should have a clear understanding of the consequences of unethical, illegal, or other behaviors that do not align with the bank’s code of ethics (or code of conduct).

The bank should have an ethics officer, bank counsel, or some other individual from whom employees can seek advice regarding ethics questions. Ethics policies should include a process for the annual review and discussion of ethics rules at all levels of the bank, including the board. Ethics policies should be reinforced as an important part of each director’s, senior manager’s, and employee’s performance review.

Internal audit plays an important role in monitoring the effectiveness of the bank’s ethics program and whistle-blower policy. Internal audit should assess the bank’s corporate culture and standards and ethics processes to identify any governance-related weaknesses. Internal audit should assure the board that suspected fraud and misconduct are promptly reported, investigated, and addressed.

Comply With Fiduciary Duties and the Law

Directors’ activities are governed by common law fiduciary legal principles, which impose two duties—the duty of care and the duty of loyalty.

The duty of care requires that directors act in good faith, with the level of care that ordinarily prudent persons would exercise in similar circumstances and in a manner that the directors reasonably believe is in the bank’s best interests. The duty of care requires directors to acquire sufficient knowledge of the material facts related to proposed activities or transactions, thoroughly examine all information available to them, and actively participate in decision making.

The duty of loyalty requires that directors exercise their powers in the best interests of the bank and its shareholders rather than in the directors’ own self-interest or in the interests of any other person. Directors taking action on particular activities or transactions must be objective, meaning the directors must consider the activities or transactions on their merits, free from any extraneous influences. The duty of loyalty primarily relates to conflicts of interest, confidentiality, and corporate opportunity. Directors of FSAs are also subject to specific conflict of interest and corporate opportunity regulations.²⁴

Each director should personally ensure that his or her conduct reflects the level of care and loyalty required of a bank director. A bank director—like the director of any corporate entity—may be held personally liable in lawsuits for losses resulting from his or her breach of fiduciary duties. Shareholders or members (either individually or on behalf of the bank),

²⁴ For more information, refer to 12 CFR 163.200, “Conflicts of Interest,” and 12 CFR 163.201, “Corporate Opportunity.”

depositors, or creditors who allege injury by a director’s failure to fulfill these duties may bring these suits. In addition, the OCC may take enforcement action, including assessment of CMPs, against a director for breach of fiduciary duty.²⁵ The OCC may assess director liability individually because the nature of any breach of fiduciary duty can vary for each director.

Additionally, a bank director may be criminally liable for his or her actions as a director and may incur criminal liability if the director

- falsifies bank records or causes such records to be falsified.²⁶
- misuses or misapplies bank funds or assets.²⁷
- requests or accepts fees or gifts to influence, or as a reward for, bank business.²⁸
- makes false statements generally.²⁹
- commits or attempts to commit fraud.³⁰
- willfully violates the BSA or its implementing regulations.³¹

Select, Retain, and Oversee Management

A profitable and sound bank is largely the result of the efforts of talented and capable management. Effective management is able to direct day-to-day operations to achieve the bank’s strategic goals and objectives while operating within the risk appetite. Such management has the expertise to help the board plan for the bank’s future in a changing and competitive marketplace as well as generate new and innovative ideas for board consideration. Effective management has the expertise to design and administer the systems and controls necessary to carry out the bank’s strategic plan within the risk governance framework and to comply with laws and regulations.

One of the most important decisions the board makes is selecting the bank’s CEO. The CEO is responsible for executing the bank’s strategic plan and effectively managing the bank’s risks and financial performance. The board should select and retain a CEO who has the leadership skills and the appropriate competence, experience, and integrity to carry out his or her responsibilities.

²⁵ Refer to 12 USC 1818, “Termination of Status as Insured Depository Institution.”

²⁶ For more information, refer to 18 USC 1005, “Bank Entries, Reports, and Transactions.”

²⁷ For more information, refer to 18 USC 656, “Theft, Embezzlement, or Misapplication by Bank Officer or Employee.”

²⁸ For more information, refer to 18 USC 215, “Receipt of Commissions or Gifts for Procuring Loans.”

²⁹ For more information, refer to 18 USC 1001, “Statements or Entries Generally.”

³⁰ For more information, refer to 18 USC 1344, “Bank Fraud.”

³¹ For more information, refer to 31 USC 5322, “Criminal Penalties.”

The board or a board committee should be actively engaged in the CEO selection process. The board should specifically define selection criteria, including experience, expertise, and personal character, and periodically review and update the criteria as appropriate. The CEO should share the board's corporate culture and the vision and philosophy for the bank to promote mutual trust and a close working relationship. For larger banks, a board committee, typically the governance or nominating committee, oversees the CEO selection process. This committee's responsibilities are discussed in more detail in appendix C of this booklet.

Besides selecting a qualified CEO, the board's primary responsibility is to directly oversee the CEO and senior management. In doing so, the board should

- set formal performance standards for senior management consistent with the bank's strategy and financial objectives, risk appetite and culture, and risk management practices; and monitor performance relative to the standards.
- align compensation with performance and ensure that incentive compensation arrangements do not encourage imprudent risk taking.
- oversee the talent management process, which includes establishing a succession plan to replace key senior management.
- approve diversity policies and practices consistent with identified standards.³²
- meet regularly with senior management and maintain appropriate lines of communication.
- hold management accountable for providing sufficient, clear, transparent, and timely information.
- question and critically review explanations, assumptions, and information provided by senior management.
- assess whether senior management's knowledge and expertise remain appropriate given the nature and complexity of the bank's strategy and risk profile.
- take decisive action to address problems or concerns with management performance or misconduct.

Banks proposing to enter into an employment contract or other written agreement regarding compensation with a prospective director, senior executive officer, or employee may be subject to additional requirements.³³

An FSA's board must approve any employment contract that the association enters into.³⁴ 12 CFR 163.39 prohibits unsafe or unsound contracts that could lead to material financial loss or damage to the association or could interfere with the board's duty or discretion to employ or terminate management or employees. For example, a contract with an excessive term could be considered unsafe or unsound. The regulation also requires that employment contracts be in writing and include certain mandatory provisions.

³² For more information, refer to OCC Bulletin 2015-30.

³³ For more information, refer to 12 CFR 359, "Golden Parachute and Indemnification Payments."

³⁴ For more information, refer to 12 CFR 163.39, "Employment Contracts" (FSAs).

The board or a designated board committee should establish a formal performance appraisal process that evaluates the CEO and other senior management. The goal of a CEO evaluation process is to enhance the relationship between the CEO and the board and improve the bank's overall performance through candid conversations about goal setting and performance measurement. The board should give constructive feedback to its CEO to help improve his or her performance in overseeing the bank. This process assists the board in discharging its responsibilities to supervise management and hold the CEO accountable. When the CEO does not fulfill board expectations, the board should be prepared to replace the CEO.

Succession Planning

Succession planning can provide for stability in tumultuous financial times and can lessen the influence of dominant personalities and behaviors. At smaller banks, the depth of talent available for key management positions may be limited. In these instances, smaller banks may consider increasing the formality of management training programs, development, and talent identification. Succession planning in larger banks may involve developing a talent pool of employees who have the necessary qualifications, skills, experience, and exposure to the board and senior management. These larger banks should have more formal processes to identify management succession requirements to develop and prepare individuals for various leadership positions. The bank's succession planning may also help the bank retain key employees.

Succession planning should be a regular topic of board discussion. The board should approve a management succession policy to address the loss of the CEO and other key executives. This policy should identify critical positions that would fall in the scope of a succession plan. This policy also should outline the process by which the board and management would fill vacancies created by death, illness, injury, resignation, or misconduct. If no individual in the bank is suitable, the succession policy should provide for a temporary replacement to serve in the role until the board finds a successor. In addition, the board and senior management should review and update management succession plans at least annually to confirm that the plans remain viable.

The CEO is responsible for appropriate leadership development and management succession planning for major bank functions while effectively preserving the independence of audit and independent risk control functions. Managers should support succession planning by assessing their line-of-business structures as well as the bank's needs. Management also should determine the required knowledge and skills for management positions, identify the best candidates for critical jobs, and initiate development plans for those who show potential for advancement.

Heightened Standards

The board or board committee should review and approve a written talent management program that provides for, among other things, development, recruitment, and succession planning regarding the CEO, CAE, CRE, their direct reports, and other potential successors.³⁵

Oversee Compensation and Benefits Arrangements

The board should determine that compensation practices for the bank's executive officers and employees are safe and sound, are consistent with prudent compensation practices, and comply with laws and regulations governing compensation practices.³⁶ For a mutual FSA or its service corporation, compensation to directors, officers, and employees should be reasonable and commensurate with their duties and responsibilities.³⁷ This includes former directors, officers, and employees who regularly perform services for the FSA or its service corporation under consulting contracts.

The bank is required to maintain safeguards to prevent the payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to the bank.³⁸ If it is unreasonable or disproportionate to the services actually performed, compensation is considered excessive and is therefore prohibited as an unsafe or unsound practice.³⁹

Given the level of authority that executive officers have over all banking activities, the board should oversee this group's compensation, including

- evaluating and approving employment contracts.
- establishing the compensation and benefits of the CEO and other executive officers.
- assessing the reasonableness of the structure and components of executive compensation, including various benefits related to retirement, termination, and change of control.
- confirming that the internal processes for incentive compensation arrangements are consistent with safe and sound banking principles.
- evaluating executive performance relative to board-established goals and objectives.
- considering shareholder concerns.

³⁵ For more information, refer to 12 CFR 30, appendix D, II.L, "Talent Management Processes."

³⁶ For example, refer to 12 CFR 30, appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness"; 12 CFR 163.39; 12 CFR 359; and 12 CFR 1026.36, "Prohibited Acts or Practices and Certain Requirements for Credit Secured by a Dwelling."

³⁷ For more information, refer to OCC Bulletin 2014-35, "Mutual Federal Savings Associations: Characteristics and Supervisory Considerations."

³⁸ For more information, refer to 12 CFR 30, appendix A, section II, I, "Compensation, Fees and Benefits."

³⁹ For more information, refer to 12 CFR 30, appendix A, III, "Prohibition on Compensation That Constitutes an Unsafe and Unsound Practice."

Incentive Compensation

Incentive-based compensation means any variable compensation, fees, or benefits that serve as an incentive or reward for performance. Banks of varying size may have incentive compensation arrangements. Incentive compensation arrangements should balance risk and financial results in a manner that does not encourage employees to expose their banks to imprudent risks.

Incentive compensation can be a useful tool for retaining key talent; it may, however, encourage executives and employees to take imprudent risks that are inconsistent with the bank’s long-term viability and safety and soundness. Strong corporate governance, including active and effective board oversight, should support incentive compensation arrangements.

OCC Bulletin 2010-24, “Incentive Compensation: Interagency Guidance on Sound Incentive Compensation Policies,” provides guidance to all banks that have incentive compensation arrangements, with expanded expectations for the largest, most complex banks.⁴⁰ The principles in OCC Bulletin 2010-24 apply to compensation arrangements of executive officers as well as nonexecutive personnel, collectively referred to as “covered employees,” who have the ability to expose the bank to material amounts of risks. OCC Bulletin 2010-24 outlines that sound incentive compensation principles should include the following:

- Provide employees with incentives that appropriately balance risk and reward.
- Be compatible with effective controls and risk management.
- Be supported by strong corporate governance, including active and effective oversight by the bank’s board.

The board is ultimately responsible for ensuring that incentive compensation arrangements for all covered employees are appropriately balanced and do not jeopardize the bank’s safety and soundness. The board’s oversight should be commensurate with the scope and prevalence of the bank’s incentive compensation arrangements. Independent directors should be actively involved in the oversight of incentive compensation arrangements.

Executive officers play a critical role in managing the overall risk-taking activities of the bank. The board should

- approve executive officers’ incentive compensation arrangements.
- approve and document any material exceptions or adjustments to executive officers’ incentive compensation arrangements.
- consider and monitor the effects of approved exceptions on the balance of the arrangements, the risk-taking incentives of senior executives, and the safety and soundness of the bank.
- monitor incentive compensation payments to senior executives and the sensitivity of these payments to risk results.

⁴⁰ The largest, most complex banks are those supervised by the OCC’s Large Bank Supervision department.

- obtain sufficient information to monitor and review any clawback provisions to determine if the provision was triggered and executed as planned.

In larger banks, the board’s oversight of compensation matters is typically handled by a board compensation committee, as discussed in appendix C of this booklet.

Employee Benefits

“Employee benefits” is an umbrella term that refers to non-wage compensation provided to employees in addition to their normal wages or salaries.

A comprehensive employee benefits package is an important, competitive, and useful tool for attracting and retaining employees. In addition, there may be tax advantages for the bank for establishing certain employee benefits, such as a retirement plan. On the other hand, offering employee benefits can be costly. Administrative costs can be high and may increase year-to-year. There is also the risk of liability from lawsuits and the payment of regulatory fines from mistakes made in benefits administration.

There are two types of employee benefits, mandated and optional. By law, banks must provide mandated benefits. The mandated benefits include Social Security, Medicare, unemployment insurance, and workers’ compensation. Optional benefits are not mandated. If offered, however, optional benefits may be subject to certain requirements. If requirements are not met, the bank could incur lawsuits, penalties, and excise taxes. Optional benefits include

- group health plans.
- disability insurance.
- life insurance.
- retirement plans.
- flexible compensation (cafeteria plans).
- leave.

The board ultimately should be responsible for all decisions relating to the cost and scope of the bank’s employee benefits. The board also should be responsible for overseeing management’s administration of benefits and fulfillment of fiduciary responsibilities. If the board determines the bank should provide its employees with a group health plan or a retirement plan, then the board should ensure the bank’s fiduciary responsibilities are met.⁴¹

Senior management is responsible for establishing an appropriate organizational structure to administer benefits. Management often outsources benefits administration to benefits professionals or may use an internal administrative committee or human resources department to manage some or all employee benefit operations.

⁴¹ For more information, refer to the “Retirement Plan Products and Services” booklet of the *Comptroller’s Handbook*, which contains a detailed discussion of the Employee Retirement Income Security Act of 1974 and its fiduciary standards.

Maintain Appropriate Affiliate and Holding Company Relationships

In the case of affiliated banks and holding companies, the strategic objectives, corporate values, and corporate governance principles of the affiliated bank should align with the holding company. A bank managed as part of a holding company structure can face additional challenges if directors serve on both the holding company board and the bank board. For example, this arrangement may create conflicts of interest or force directors to act on competing priorities.⁴² The bank's board should ensure the interests of the bank are not subordinate to the interests of the parent holding company in decisions that may adversely affect the bank's risk profile, financial condition, safety and soundness, and compliance with laws and regulations.⁴³ Additionally, a director who serves on the board of both the bank and its holding company must comply with the director's fiduciary duties to the bank, including the duty of loyalty.

The primary duty of a subsidiary bank's board is to ensure the bank operates in a safe and sound manner. The subsidiary bank's board should ensure that relationships between the bank and its affiliates and subsidiaries do not pose safety and soundness issues for the bank and are appropriately managed. The bank's board should carefully review holding company policies that affect the bank to confirm that those policies adequately serve the bank. If the bank's board is concerned that the holding company is engaging in practices that may harm the bank or are otherwise inappropriate, the bank's board should notify the holding company and obtain modifications. If the holding company board does not address concerns of the bank's board, bank directors should dissent on the record and consider actions to protect the bank's interests. If necessary, the bank's board should hire an independent legal counsel or accountant. The bank's board also may raise its concerns with its regulators.

Establish and Maintain an Appropriate Board Structure

Board committees are an important component of the corporate and risk governance structure. Board committees help the board carry out oversight duties and responsibilities. Delegation of work to a committee can enhance board effectiveness by enabling the board, through its committees, to cover a wider range of issues with greater depth of analysis. Delegation also allows the directors to better focus their time and attention on areas or subject matters on which they can lend their specific expertise or experience. Committee meetings can encourage directors to thoroughly consider issues, promote more candid discussions, and gain better insight into the bank's activities.

The board should clearly understand and define the responsibilities of each committee. Each committee should have a written charter that outlines the committee's responsibilities,

⁴² For more information, refer to 12 USC 371c, “Banking Affiliates”; 12 USC 371c-1, “Restrictions on Transactions with Affiliates”; 12 CFR 31; and 12 CFR 223, “Transactions Between Member Banks and Their Affiliates (Regulation W).” For more information on national banks, affiliates, and other related organizations, refer to the “Related Organizations” booklet of the *Comptroller’s Handbook*. For FSAs, refer to section 730, “Related Organizations,” of the *OTS Examination Handbook*.

⁴³ For more information, refer to the “Related Organizations” booklet of the *Comptroller’s Handbook* (national banks) and section 730, “Related Organizations,” of the *OTS Examination Handbook* (FSAs).

member qualifications, authorities, independence, and board reporting. The charter should establish requirements that include meeting frequency, conduct, attendance, minutes, and use of advisors. The charter also should address the need for an annual performance evaluation of the committee. The board should approve and disclose the written charter, as appropriate. Disclosure of the committee charters (for example, on websites, in proxy statements, and in policy manuals) improves the transparency of the board's decision-making processes.

The appropriate governance and committee structure depends on the bank's needs and is another key board decision. As the complexity and risk profile of the bank's products and services increase, additional committees may be necessary for the board to provide effective oversight. Similarly, additional skills and expertise of committee members might be needed. Conversely, too many committees can create competing demands and the potential for duplication and confusion about responsibilities.

Directors should be assigned to committees that align with their skills and experience. In some circumstances, directors are required to have specific qualifications to serve on certain committees.⁴⁴ Participation on multiple committees should be balanced with time commitments to avoid overburdening any single director. Some overlap, however, is beneficial in integrating board activities. With smaller boards, directors likely need to serve on multiple committees. Periodically rotating committee membership may help to achieve optimal objectivity, but frequent rotation can sometimes adversely affect the knowledge base and effectiveness of committee members. The board should find the right balance between maintaining institutional knowledge and gaining new perspectives.

The board's responsibility is to determine which committees it needs to effectively govern the bank. The committees vary by bank. Some committees are mandated by laws or regulations. Appendix C, "Common Board Committees," of this booklet describes some key committees.

Perform Board Self-Assessments

A meaningful self-assessment evaluates the board's effectiveness and functionality, board committee operations, and directors' skills and expertise. All boards should periodically undertake some form of self-assessment. Board self-assessments can be valuable in improving the board's overall performance. Further, by acknowledging that the board holds itself responsible for its performance, self-assessments help affirm the "tone at the top." The bank's directors and senior management set the tone at the top, which emphasizes personal integrity and accountability. The tone at the top also involves clearly articulating and consistently enforcing the directors' and senior management's expectations for employee behavior.

Self-assessments may take the form of questionnaires to all directors, a group self-assessment, formal interviews with each director, peer evaluations, or a combination of these

⁴⁴ For example, refer to 12 CFR 363.5, "Audit Committees," for regulatory requirements regarding the composition of audit committees for banks with consolidated total assets greater than \$500 million.

methods. In some circumstances, it may be worthwhile to use an independent third party to administer the self-assessments and provide feedback to the directors.

A board self-assessment addresses the effectiveness of the board's structure, activities, and oversight, including factors such as

- director qualifications.
- level of director participation.
- quality of board meetings and discussions, including whether one director or a group of directors dominates the discussion.
- quality and timeliness of board materials and information.
- relevance and comprehensiveness of meeting agendas.
- the board's relationship with the CEO, including whether the relationship is supportive but independent.
- effectiveness of credible challenge.
- effectiveness of strategic and succession planning.
- effectiveness of executive sessions.
- effectiveness of board committees and committee structure.

An important component of any assessment is to follow up on action items identified to improve performance. The action items should produce measurable results. The board or a designated committee should oversee the implementation of recommendations arising from board self-assessments and independent assessments. As part of its oversight duties, the committee may determine that board composition changes are needed to address skill and competency gaps.

Heightened Standards

A covered bank's board should conduct an annual self-assessment that includes an evaluation of the board's effectiveness in meeting the standards applicable to the board.⁴⁵

Oversee Financial Performance and Risk Reporting

Sound financial performance is a key indicator of the bank's success. The board is responsible for overseeing financial performance and risk reporting. As such, the board should determine the types of reports required to help with its oversight and decision-making responsibilities.⁴⁶ The reports should be accurate, timely, relevant, complete, and succinct. Refer to the "Management Information Systems" section in this booklet for more information. The information requirements, particularly the number and variety of reports, depend on the bank's size, complexity, and risks. The information should be sufficient to keep relevant parties informed of the financial condition and performance of all the bank's

⁴⁵ For more information, refer to 12 CFR 30, appendix D, III.

⁴⁶ For more information on the types of reports and measures the board uses to assist in its oversight responsibilities, refer to *Detecting Red Flags in Board Reports: A Guide for Directors*.

material lines of business. In addition, information requirements should evolve as the bank grows in size and complexity and as the bank's environment or strategic goals change.

Reports presented to the board should highlight important performance measures, trends, and variances rather than presenting the information as raw data. Some banks use dashboard-style reports to communicate the risk and performance indicators to the board.

Performance and risk reports should enable the board to

- understand the drivers of financial performance.
- understand and evaluate the potential impact of business units and their risk on financial performance.
- assess the adequacy of capital, liquidity, and earnings.
- monitor performance trends and projections.
- monitor financial performance against strategic goals.
- monitor risk positions in relation to the risk appetite, limits, and parameters.
- monitor the types, volumes, and impacts of exceptions to policies and operating procedures.
- understand model risks and reliance.
- assess the impact of new, modified, or expanded products or services.
- assess evolving risks related to changing technologies and market conditions.
- monitor risks related to third-party relationships involving critical activities.
- assess potential litigation costs and reserves.

Useful performance reports are likely to include, but are not limited to, the following information:

- Financial statements and peer comparison reports
- Budget variance reports
- Metrics on key risks
- Asset quality indicators and trends
- Allowance for loan and lease losses analysis
- Concentrations of credit
- Liquidity position and trends and contingency funding plans
- Interest rate sensitivity analyses
- Performance metrics for new, modified, or expanded products and services
- Outsourced critical activities
- Off-balance-sheet activity and exposures, including derivative exposures
- Growth rates and projections
- Capital position, trends, and capital adequacy assessments
- Key business unit performance
- Policy exception monitoring reports
- Performance measurements and metrics for risk appetite, performance goals, and strategic goals
- Earnings trends and quality, including non-interest income and expenses

Support Efforts to Serve Community Credit Needs

Banks have a responsibility to help meet the credit needs of their communities, consistent with safe and sound lending practices,⁴⁷ and an obligation to provide fair access and equal treatment to all bank customers.⁴⁸ The Community Reinvestment Act (CRA) is intended to prevent redlining and to encourage banks to help meet the credit needs of the communities they serve, including low- and moderate-income neighborhoods.⁴⁹

The board should understand management's involvement in the community and should develop a high-level understanding of what activities meet the requirements of the CRA to ensure that strategic plans consider activities that qualify under the CRA. As part of its governance responsibilities, the board should work toward fulfilling the credit needs of the bank's community, including unmet or underserved banking needs.

Management should maintain a constructive dialogue with community members. This dialogue helps management and the board better understand where community needs are not being adequately addressed and what role the bank might play in helping to meet those needs. Significant reputation, strategic, and compliance risks and exposure to litigation exist when banks do not help meet the credit needs of their communities consistent with safe and sound lending practices or when they do not provide fair and equal treatment to all bank customers. A failure to do so can adversely affect the bank's expansion plans to acquire branches or other banks.

Individual Responsibilities of Directors

Each director has individual responsibilities and should meet these responsibilities when overseeing the bank's operations.

Attend and Participate in Board and Committee Meetings

Directors should demonstrate a willingness and ability to prepare for, attend, and participate in all board and committee meetings to make a sound contribution to the oversight function. Directors should attend meetings as often as possible. A director's time commitment should be sufficient to stay informed about the bank's risks, business and operational performance, and competitive position in the marketplace. The time commitment is generally a function of the bank's size and complexity as well as the committee work required of the director.

⁴⁷ Refer to 12 USC 2901 et seq., "Community Reinvestment."

⁴⁸ Refer to 15 USC 45(a)(1); 15 USC 1691(a), "Activities Constituting Discrimination"; 42 USC 3604, "Discrimination in the Sale or Rental of Housing and Other Prohibited Practices"; 42 USC 3605, "Discrimination in Residential Real Estate-Related Transactions."

⁴⁹ For more information on national banks, refer to the "Community Reinvestment Act Examination Procedures" booklet of the *Comptroller's Handbook*. For FSAs, refer to section 1500, "Community Reinvestment Act," of the *OTS Examination Handbook*.

Board meetings should be focused and productive by following agendas that permit adequate time for presentation and discussion of material issues. The thoughtful preparation of an agenda for each board meeting should provide directors with reasonable assurance that all important matters are brought to their attention. While the agenda should be carefully planned, it should be flexible enough to accommodate unexpected developments. The board should have a process for soliciting potential agenda items from individual directors and from others within the bank.

Request and Review Meeting Materials

The board should work with management to determine what information the board needs at meetings to monitor the bank's operations, make decisions, and oversee the bank's compliance with laws and regulations. Information should give directors a complete and accurate overview of the bank's condition, activities, and issues. Management is responsible for being transparent and providing information in a concise and meaningful format. Reports to the board should be subject to periodic audits to validate the integrity of the information.

Directors should be provided with information from a variety of sources, including management, board committees, outside experts and advisors, risk management and compliance personnel, and internal and external auditors. The board should agree on a set of key performance measurements and risk indicators that are tracked at each board meeting. For the board to effectively oversee the bank's adherence to the agreed-upon strategy and risk appetite, directors should have sufficient information about the bank's material risks, including emerging risks.

Directors should receive the information in advance of their meetings so there is sufficient time to review the information, reflect on key issues, prepare for discussion, and request supplemental information as necessary. The board meeting materials should be kept confidential because of the sensitive nature of the information.

The chair or lead director should periodically review the content of the meeting materials with the other directors and provide useful feedback to management. For example, instead of being inundated with technical detail, the board might request that all pre-meeting reading materials include one- to two-page executive summaries, as well as questions the directors should be prepared to address at meetings. When feasible, directors might also have access to secure online analytical tools that allow them to review additional information as needed or compare the bank's performance with a custom peer group and established benchmarks.

Make Decisions and Seek Explanations

The board's decision-making process should include constructive, credible challenge to the information and views provided by management. The ability to provide credible challenge is predicated on the qualifications of the directors and receipt of accurate, complete, and timely information. The quality of information received by the directors affects their ability to perform the board oversight function effectively. If a director is unable to make an informed decision because of inadequate information provided by management, the decision should be

postponed until sufficient information is provided and the board has additional time to discuss and review the information. If this is a recurring problem, the board should review the format of board proceedings or management's responsiveness to director inquiries. Directors should take the initiative to address potential problems.

Effective directors ask incisive questions and require accurate, timely, and honest answers. Effective directors also demonstrate a commitment to the bank, its business plan, and long-term shareholder value. In addition, they are open to other opinions and are willing to raise tough questions in a manner that encourages a constructive and engaging boardroom atmosphere.

Review and Approve Policies

Policies set standards and courses of action to achieve specific goals and objectives established by the board. The directors should approve a clear set of policies that guides management and staff in the operation and administration of the bank. The policies should cover all key areas of the bank's operations. Policies should be consistent with the bank's goals, risk appetite, and regulatory requirements. Furthermore, certain statutes and regulations require written policies governing specific activities or programs. Refer to appendix B of this booklet for a list of policies and programs subject to board approval.

The board or its designated committees should periodically review policies and oversee revisions. As appropriate, the board should approve risk limits for specific policies and monitor the limits periodically. If exceptions to a particular policy are approaching or breaching risk limits, the board should take appropriate action, which includes assessing the policy, risk appetite, or strategy. Adjustments to the strategy may include a slowdown of growth, placing a temporary moratorium on activities, or exiting the line of business. The board should modify bank policies when necessary to respond to significant changes in the bank's resources, activities, or business conditions. The board also should specify means to measure and monitor compliance with board-approved policies.

Exercise Independent Judgment

Independence is the core of effective board oversight. The board should exercise independent judgment in carrying out its responsibilities. Each director should examine and consider management's recommendations thoroughly, but exercise independent judgment. Effective credible challenge among directors is healthy and can suggest that the board is independent and not operating under undue influence by management or from an individual director.

To promote objectivity and impartiality, the bank should have a conflict of interest policy that provides clear independence standards and conflict of interest guidelines for its directors. This policy should provide sufficient guidance to address behaviors or activities that may diminish directors' ability to make objective decisions and act in the best interests of the institution. Directors should also structure their business and personal dealings with the bank to avoid even the appearance of a conflict of interest. Such dealings must comply with legal and regulatory requirements. The policy should also describe situations when directors must

abstain from decision making. Conflicts of interest should be promptly reported to the board.⁵⁰ Refer to the “Establish an Appropriate Corporate Culture” section in this booklet for more information.

To strengthen board independence, the independent directors should convene executive sessions as needed. Executive sessions allow the independent directors to discuss the effectiveness of management, the quality of board meetings, and other issues or concerns without the potential influence of management. Executive sessions make it easier for independent directors to ask questions, express unpopular opinions, and test their instincts without the risk of being seen as uninformed or undermining the CEO’s authority. Executive sessions also can provide a forum for director training and meetings with advisors and regulators.

Heightened Standards

To promote effective, independent oversight of a covered bank’s management, at least two members of the board

- should not be an officer or employee of the parent company or covered bank and should not have been an officer or employee of the parent company or covered bank during the previous three years.
- should not be a member of the immediate family⁵¹ of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank.⁵²
- should qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the OCC’s satisfaction.⁵³

⁵⁰ For more information, refer to the “Insider Activities” booklet of the *Comptroller’s Handbook*.

⁵¹ As defined in 12 CFR 225.41(b)(3), “Immediate Family.”

⁵² As defined in 12 CFR 215.2(e)(1), “Executive Officer.”

⁵³ Refer to 12 CFR 30, appendix D, III.D, “Include Independent Directors.”

Planning

The board sets the bank's strategic focus and significant goals and provides the necessary oversight for the bank to have the personnel as well as the financial, technological, and organizational capabilities to achieve those goals. Because of ongoing changes in the banking industry, a bank should have a clear strategic plan as well as operational plans.

Strategic Planning

A strategic plan defines the bank's long-term goals and its strategy for achieving those goals. The bank should have a strategic planning process that results in a board-approved, written strategic plan. The strategic plan should be consistent with the bank's risk appetite, capital plan, and liquidity requirements.

The bank's strategic planning process should answer the following four questions for the board and senior management:

- 1. Where are we now?** Senior management should evaluate the bank's internal and external environment and its strengths, weaknesses, opportunities, and threats. The internal review identifies the bank's strengths and weaknesses. The external analysis helps to recognize threats and opportunities including regulatory, economic, competitive, and technological matters.
- 2. Where do we want to be?** Senior management should establish or confirm the bank's missions, goals, and objectives. A mission statement should reflect the bank's purpose and values. Goals are general statements about what should be achieved and stem from the mission and the board's vision. Objectives are statements of specific, measurable tasks that the bank, board, management, or staff needs to perform to reach its goals.
- 3. How do we get there?** Senior management should design the bank's strategic plan to achieve the bank's goals and objectives. The plan should be tailored to fit the bank's internal capabilities and business environment. An effective plan should be based on realistic assumptions, consider the associated risks, and be aligned with the bank's risk appetite. The plan should take into account the resources needed to reach the bank's goals and objectives, as well as potential effect on earnings, capital, and liquidity. Technology requirements and constraints also should be considered.
- 4. How do we measure our progress?** Regular measurement and reporting on the bank's objectives keep the board and senior management focused on whether the bank is achieving established goals in the strategic plan. A periodic progress report or scorecard should indicate whether timelines and objectives are being met and if additional or alternative actions need to be implemented.

As the bank grows in size and complexity and its risk profile increases, the process should become more formalized. A formalized process should define the board's and management's

roles and responsibilities, indicate timing and frequency of activities, and establish monitoring activities.

Typically, the strategic plan spans a three- to five-year period and includes the bank's goals and the objectives to achieve those goals. Strategic planning should be linked to the bank's risk management and capital planning processes. The strategic plan should be consistent with the board's articulated risk appetite and liquidity requirements as well as the bank's capital base. The strategic plan should be dynamic; as changes occur, planning and implementation should be adjusted to reflect current conditions. If the bank is a subsidiary of a holding company, the board may consider developing one consolidated strategic plan. Continuous monitoring of activities should allow management to measure the actual and potential risks associated with achieving the bank's strategic goals and objectives and the board to monitor progress. This monitoring includes whenever the bank introduces new, expanded, or modified products and services. When the bank engages in merger or acquisition activities, it should perform a retrospective review of the merger's or acquisition's success. The retrospective review should consider the impact on financial performance, information technology (IT) infrastructure, system integration, and human resources.

The board is responsible for overseeing the bank's strategic planning process and management's implementation of the resulting strategic plan. During the planning phase, the board should provide a credible challenge to management's assumptions and recommendations. The board should understand the risks associated with the success and failure of the plan. With the help of progress reports, the board should carefully monitor and assess the strategic plan. The board should ensure that management actions and decisions remain consistent with the bank's strategic plan. In addition, the board should recognize whether the bank has a reasonable strategy and, if not, challenge management's decisions, drive sustainable corrective actions, or change the strategic direction, as appropriate. The board should require management to have a contingency plan if the original plan fails to achieve its objectives.

Senior management, in consultation with the board and business line managers, should develop a strategic planning process that results in a board-approved, written strategic plan. Management is responsible for implementing the bank's strategic plan, developing policies and processes to guide the plan's execution, and monitoring the plan's implementation. Reports should include outcomes, key performance indicators, and key risk indicators that are compared with established targets and risk limits.

Heightened Standards

The CEO should be responsible for developing a written strategic plan with input from frontline units, IRM, and internal audit. The board should evaluate and approve the strategic plan and monitor management's efforts to implement the strategic plan at least annually.

The strategic plan should cover, at a minimum, a three-year period and

- contain a comprehensive assessment of risks that have an impact on the covered bank or that could have an impact on the covered bank during the period covered by the strategic plan.
- articulate an overall mission statement and strategic objectives for the covered bank, and include an explanation of how the covered bank will achieve those objectives.
- explain how the covered bank will update, as necessary, the risk governance framework to account for changes in the covered bank's risk profile projected under the strategic plan.
- be reviewed, updated, and approved, as necessary, due to changes in the covered bank's risk profile or operating environment that were not contemplated when the strategic plan was developed.⁵⁴

New Activities

A key consideration in the bank's strategic planning process is growth and new profit opportunities for the bank. These opportunities include expanding existing products and services and introducing new ones. To stay relevant in a rapidly changing and evolving financial service industry, the bank should adapt as customer demographics, needs, and demands evolve. Remaining nimble may lead to opportunities for growth in new lines of business.

New activities, including new, modified, or expanded products and services, often require infrastructure support, expertise, substantial lead time, and significant financial investment. As such, management and the board should understand the impact of new activities on the bank's financial performance, strategic planning process, risk profile, banking model, and ability to remain competitive.⁵⁵ Insufficient planning could lead to an incomplete assessment and understanding of associated risks involved with new activities and may result in inadequate oversight and control.

The board should oversee management's implementation of the risk management system for new activities, including execution of control programs and the audit of such activities. Management should design an effective risk management system when developing and implementing new activities that includes adequate due diligence; policies, procedures, and controls; change management; and, performance and monitoring. Specifically, management should

- clearly understand the rationale for engaging in new activities and how proposed new activities meet the bank's strategic objectives.

⁵⁴ For more information, refer to 12 CFR 30, appendix D, II.D, "Strategic Plan."

⁵⁵ For more information, refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

- establish and implement policies and procedures that provide guidance on risk management of new activities.
- have effective change management processes to manage and control the implementation of new or modified operational processes, as well as the addition of new technologies into the bank's existing technology architecture.
- have appropriate performance and monitoring systems, including MIS, to assess whether the activities meet operational and strategic expectations and legal requirements and are within the bank's risk appetite.

While all banks should include these components in their risk management system for new activities, the sophistication of the risk management system should reflect the bank's size, complexity, and risk profile. The bank's risk management system should evolve to be sufficiently robust to keep pace with additional complexities and planned activities.

Depending on the bank's size, complexity, and risk profile, the bank's board or management may consider establishing senior management positions or independent risk committees that include internal stakeholders from business units and other ad hoc members with expertise in applicable functions to oversee new activities.

Capital Planning

Capital planning is essential for a bank's safe and sound operations and viability.⁵⁶ Banks are expected to have capital commensurate with the nature and extent of their risks as well as their current and anticipated needs. Because raising capital normally becomes more difficult and expensive when the bank has problems, any capital raising events should begin before major issues materialize. The board and senior management should regularly assess capital to ensure that levels remain adequate, not just at one point in time, but over time.

Capital planning is a dynamic and continuous process that should be forward-looking. The capital planning process and the resulting capital plan should evolve as the bank's overall risks, activities, and risk management practices change. The most effective capital planning considers short- and long-term capital needs over at least three years. In addition, capital planning should align with the bank's strategic planning process. The content and depth of the bank's capital planning process should be commensurate with the overall risks, complexity, and corporate structure. For example, mutual savings associations build capital almost exclusively through retained earnings, so they have very limited means to increase capital quickly. Capital planning is critical for a federal mutual savings association.

Stress testing is an important element of the capital planning process. Banks can use stress testing to establish and support a reasonable risk appetite and limits, set concentration limits, adjust strategies, and appropriately plan for and maintain adequate capital levels.

⁵⁶ For more information on capital planning and stress testing, refer to the "Capital and Dividends" booklet of the *Comptroller's Handbook*.

Operational Planning

The planning process begins with developing a strategic plan. The responsibility for establishing and implementing operational plans and budgets to meet strategic plans rests with the CEO and management. Operational plans flow logically from the strategic plan by translating long-term goals into specific, measurable targets. The board should approve the operational plans after concluding that they are realistic and compatible with the bank's risk appetite and strategic objectives.

Operational plans are narrower in scope than strategic plans, have more detail, are in effect for shorter periods of time, and provide the means of monitoring progress toward achieving strategic goals. Common examples of operational plans are budgets, annual staffing, marketing, liquidity,⁵⁷ and contingency plans. The size and complexity of the bank's operations, as well as the bank's risk appetite, are important considerations when reviewing the level of formality and depth of the operational planning process.

Disaster Recovery and Business Continuity Planning

Disruptions to operations can result in loss of bank premises or systems supporting customer activities, such as online and mobile applications. Sound business continuity plans allow banks to respond to such adverse events as natural disasters, technology failures, cyber threats, human error, and terrorism. Banks should be able to restore information systems, operations, and customer services quickly and reliably after any adverse event. Banks therefore should have resilient business operations and minimize customer service disruptions.⁵⁸

Banks' business continuity plans should forecast how departure from a business routine caused by a major operational loss could affect customer services or bank resources. Business continuity plans should address backup procedures, alternate facilities, and business resumption processes.

The board should review and approve adequate disaster recovery and business continuity plans at least annually. The board should also oversee implementation and approve policies relating to disaster recovery and business continuity. Additionally, the board should ensure management continually updates the business continuity plan to reflect the current operating environment and adequately tests the plan to confirm its viability.

Senior management is responsible for establishing and implementing policies and procedures and defining responsibilities for bank-wide business continuity planning. Management should document, maintain, and test the bank's business continuity plan and backup systems periodically to mitigate the consequences of system failures, natural and other disasters, and

⁵⁷ For more information on liquidity planning, refer to the "Liquidity" booklet of the *Comptroller's Handbook*.

⁵⁸ For more information, refer to the "Business Continuity Planning" booklet of the *FFIEC IT Examination Handbook*.

unauthorized intrusions. Management also should report the tests of the plan and backup systems to the board annually.

Information Technology and Information Security

Banks are critically dependent on their information and technology assets, such as hardware, software, and data. Management should protect information and technology assets for operational continuity, financial viability, and the trust of customers. The unauthorized loss, destruction, or disclosure of confidential information can adversely affect the bank's reputation, earnings, and capital.

Interagency guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.⁵⁹ The guidelines also discuss assigning specific responsibility for implementing an information security program and reviewing reports from management.

Based on the guidelines, the board should oversee management's development, implementation, and maintenance of a comprehensive, written information security program. The guidelines require the board or a board committee to approve the bank's written information security program at least annually.

Management should develop an information system program to protect the security and confidentiality of customer information. A robust risk assessment drives the information security program. The risk assessment provides guidance for the selection and implementation of security controls and the timing and nature of testing those controls.

Banks may employ a CIO, a chief information security officer (CISO), a chief operating officer (COO), or a chief technology officer (CTO). Titles and positions vary depending on the bank's structure, size, and complexity. This designated individual or individuals (CIO, CISO, COO, or CTO) should provide periodic updates on the bank's IT infrastructure, operations, and information security-related risks to the board.

Recovery Planning

A recovery plan's purpose is to provide a covered bank⁶⁰ with a framework to effectively and efficiently address the financial effects of severe stress events and avoid failure or resolution.⁶¹ A recovery plan's components should generally draw from and should align with other risk management processes, such as those governing capital, liquidity, stress

⁵⁹ For more information, refer to 12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards," and the "Information Security" booklet of the *FFIEC IT Examination Handbook*.

⁶⁰ "Covered Bank" is defined at 12 CFR 30, appendix E, E.3.

⁶¹ For more information, refer to 12 CFR 30, appendix E, "OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches," and the "Recovery Planning" booklet of the *Comptroller's Handbook*. Refer also to 83 Fed. Reg. 66604.

testing, business continuity, or resolution planning. An effective recovery plan helps the management of a covered bank identify when the covered bank is or may be encountering a severe stress event that threatens or may threaten its financial strength and viability. In such an event, the recovery plan should prompt management to take appropriate actions to restore the bank's financial strength and viability. The recovery plan is important to the bank's resilience, should be integrated into the bank's risk governance framework, and should play an important role in crisis management. The recovery plan should recognize the bank's transitions from business as usual to early warning of severe stress to severe stress, and it should be linked to the resolution plan in the event that financial deterioration is not rectified.

The covered bank's recovery planning process should be ongoing. The process should complement the covered bank's risk governance functions and support its safe and sound operation. The process of developing and maintaining a recovery plan should cause the covered bank's management and board to enhance their focus on risk governance with a view toward lessening the financial impact of future unforeseen events.

Risk Governance

Risk governance, which is part of the corporate governance framework, is the bank's approach to risk management. Risk governance applies the principles of sound corporate governance to the identification, measurement, monitoring, and controlling of risks. Risk governance helps ensure that risk-taking activities are in line with the bank's strategy and risk appetite. Key components of risk governance include the risk culture, the risk appetite, and the bank's risk management system.

A risk governance framework, as shown in figure 1, is an essential component in effectively managing the bank's enterprise-wide risks.⁶² The framework is the means by which the board and management, in their respective roles,

- establish and reinforce the bank's risk culture.
- articulate and monitor adherence to the risk appetite.
- establish a risk management system with three lines of defense to identify, measure, monitor, and control risks.

Figure 1: Risk Governance Framework



The framework should cover all risk categories applicable to the bank—credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. These categories of risk and their risk to the bank's financial condition and resilience are discussed in the “Bank Supervision Process” booklet of the *Comptroller’s Handbook*. Risk governance frameworks vary among banks. Banks should have a risk governance framework commensurate with the sophistication of the bank's operations and business strategies.

⁶² Refer to 12 CFR 30, appendix D.II.

Heightened Standards

A covered bank should establish and adhere to a formal written risk governance framework designed by IRM and approved by the board or the board's risk committee.⁶³ The risk governance framework should include delegations of authority from the board to management committees and executive officers as well as the risk limits established for material activities.⁶⁴ IRM should review and update the risk governance framework at least annually and as often as needed to address improvements in industry risk management practices and changes in the covered bank's risk profile caused by emerging risks, its strategic plans, or other internal and external factors.⁶⁵ As a general matter, a covered bank board may adopt the parent company's risk governance framework, if the parent company's framework meets the applicable regulatory standards and if the risk profiles of the parent company and covered bank are substantially the same.⁶⁶

Risk Culture

Risk culture is the shared values, attitudes, competencies, and behaviors throughout the bank that shape and influence governance practices and risk decisions. As a subset of corporate culture, risk culture pertains to the bank's risk approach and is critical to a sound risk governance framework. To promote a sound risk culture

- the board should take the lead in establishing the tone at the top by promoting risk awareness within a sound risk culture. The board should convey its expectations to all employees that the board does not support excessive risk taking and that all employees are responsible for operating within the established risk appetite and limits.
- senior management should implement and reinforce a sound risk culture and provide incentives that reward appropriate behavior and penalize inappropriate behavior. Management should recognize, escalate, and address material risks and risk-taking activities exceeding the risk appetite in a timely manner.

Risk Appetite

The bank's risk appetite is another essential component of an effective risk governance framework and reinforces the risk culture. The bank's risk appetite is the aggregate level and types of risk that the board and management are willing to assume to achieve the bank's goals, objectives, and operating plan, consistent with applicable capital, liquidity, and other requirements. The development of a risk appetite should be driven by both top-down board leadership and bottom-up management involvement. Successful implementation depends on effective interactions among the board, senior management, IRM, and frontline units.

The board's role is to review and approve the bank's risk appetite and risk limits, including concentration limits. The risk appetite should be communicated throughout the bank. For

⁶³ For more information, refer to 12 CFR 30, appendix D, II.A, "Risk Governance Framework."

⁶⁴ Ibid.

⁶⁵ Ibid.

⁶⁶ For more information, refer to 12 CFR 30, appendix D, I, "Introduction."

larger, more complex banks, the board should have a written statement that outlines the risk appetite. The board should reevaluate and approve the risk appetite at least annually.

Senior management, in consultation with the board, develops the risk appetite. Senior management's responsibility is to execute the strategic, capital, and operating plans within the board-approved risk appetite and established limits. Consistent with the board-approved risk appetite, senior management should

- establish, in consultation with the board, risk limits for specific risk categories, business units, and lines of business (e.g., concentration limits).⁶⁷
- establish appropriate metrics for measuring and monitoring risk results.
- develop timely, accurate, and transparent MIS and reports regarding risks, across the institution as well as up to the board and senior management.
- report and develop action plans, when appropriate, when limits are approached or breached.
- establish a process for material weaknesses or problems to be escalated to the appropriate level of management or the board (without fear of retribution), the CRE, and the risk committee or designated committee, as appropriate.

Heightened Standards

A covered bank should have a comprehensive written statement that articulates the bank's risk appetite and serves as the basis for the risk governance framework. The risk appetite statement provides the basis for the common understanding and communication of risk throughout the bank. The risk appetite statement should include both qualitative components and quantitative limits. The qualitative components should describe a safe and sound risk culture and how the bank will assess and accept risks, including those that are difficult to quantify. Quantitative limits should incorporate sound stress testing processes and address the bank's earnings, capital, and liquidity.⁶⁸ To be effective, the bank's risk appetite statement must be communicated and implemented throughout the bank.⁶⁹

The board or its risk committee should review and approve the bank's risk appetite statement at least annually or more frequently, as warranted, based on the size and volatility of risks, and any material changes in the covered bank's business model, strategy, risk profile, or market conditions.⁷⁰

The risk appetite statement should be communicated to all employees in a manner that causes all employees to align their risk-taking decisions with applicable aspects of the bank's risk appetite statement. IRM should establish and adhere to enterprise policies that include concentration risk limits. These policies should state how aggregate risks are effectively identified, measured, monitored, and controlled, consistent with the bank's risk appetite statement. Frontline units and IRM have monitoring and reporting responsibilities.⁷¹

⁶⁷ In smaller, less complex banks, the board, instead of senior management, may approve business line risk limits and concentrations.

⁶⁸ For more information, refer to 12 CFR 30, appendix D, II.E, "Risk Appetite Statement."

⁶⁹ For more information, refer to 12 CFR 30, appendix D, II.G, "Risk Appetite Review, Monitoring, and Communication Processes."

⁷⁰ Ibid.

⁷¹ For more information, refer to 12 CFR 30, appendix D, II.E and II.G.

Risk Management System

The bank's risk management system comprises its policies, processes, personnel, and control systems. A sound risk management system identifies, measures, monitors, and controls risks. Because market conditions and company structures vary, no single risk management system works for all banks. The sophistication of the risk management system should be commensurate with the bank's size, complexity, and risk profile.

A common risk management system used in many banks, formally or informally, involves three lines of defense: (1) frontline units, business units, or functions that create risk; (2) IRM, loan review, compliance officer, and chief credit officer to assess risk independent of the units that create risk; and (3) internal audit, which provides independent assurance.

1. The first line of defense is the frontline units, business units, or functions that create risk. These groups are accountable for assessing and managing that risk. These groups are the bank's primary risk takers and are responsible for implementing effective internal controls and maintaining processes for identifying, assessing, controlling, and mitigating the risks associated with their activities consistent with the bank's established risk appetite and risk limits.
2. The second line of defense is commonly referred to as IRM, which oversees risk taking and assesses risks independent of the frontline units, business units, or functions that create risk. IRM complements the frontline unit's risk-taking activities through its monitoring and reporting responsibilities, including compliance with the bank's risk appetite. IRM also provides input into key risk decisions. Additionally, IRM is responsible for identifying, measuring, monitoring, and controlling aggregate and emerging risks enterprise-wide. In some banks, the second line of defense is less formal and includes such functions and roles as loan review, a compliance officer, or a chief credit officer.
3. The third line of defense is internal audit, which provides independent assurance to the board on the effectiveness of governance, risk management, and internal controls. Internal audit may be in-house, outsourced, or co-sourced.

While many banks have not formally adopted the three lines of defense, most banks have the basic elements. In smaller, noncomplex banks, risk management processes and internal controls are often integrated in the frontline units. In larger banks, the three lines of defense are more clearly defined and visible. In these banks, IRM is under the direction of a CRE or equivalent. The board or risk committee should be involved in the selection, oversight, and dismissal of the CRE. The CRE should have unfettered access to the board or board committees to discuss risk concerns identified through risk management activities.

Heightened Standards

The risk governance framework should include well-defined risk management roles and responsibilities for frontline units, IRM, and internal audit.⁷² Frontline units should assess, on an ongoing basis, the material risks associated with their activities.⁷³ IRM should oversee the covered bank's risk-taking activities; assess risk and issues independent of frontline units; and identify and assess concentrations across the bank and material aggregate risks.⁷⁴

Internal audit should, among other things, ensure that the covered bank's risk governance framework complies with the applicable regulatory standards and is appropriate for the bank's size, complexity, and risk profile. Internal audit should maintain a complete and current inventory of all the covered bank's material processes, product lines, services, and functions, and assess the risks, including emerging risks, associated with each, which collectively provide a basis for the audit plan.⁷⁵

A covered bank's board should actively oversee the covered bank's risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board may rely on risk assessments and reports prepared by IRM and internal audit to support the board's ability to question, challenge, and, when necessary, oppose recommendations and decisions made by management that could cause the covered bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the covered bank.⁷⁶

Within a sound risk management system, the bank should have internal controls and information systems that are appropriate to the bank's size and the nature, scope, and risk of the bank's activities.⁷⁷

Regardless of the bank's size and complexity, a sound risk management system should identify, measure, monitor, and control risk. A risk management system comprises policies, processes, personnel, and control systems. All of these elements are essential to an effective risk management system. If any of these areas are deficient, the bank's risk management may also be deficient.

To determine and confirm appropriate coverage and inform the board, management should address insurance needs as part of the bank's risk management system that identifies risk to be retained versus risk to be transferred to another party through insurance. Refer to the "Insurance" section of this booklet for more information.

⁷² For more information, refer to 12 CFR 30, appendix D, II.C, "Roles and Responsibilities."

⁷³ For more information, refer to 12 CFR 30, appendix D, II.C.1, "Role and Responsibilities of Front Line Units."

⁷⁴ For more information, refer to 12 CFR 30, appendix D, II.C.2, "Role and Responsibilities of Independent Risk Management."

⁷⁵ For more information, refer to 12 CFR 30, appendix D, II.C.3, "Role and Responsibilities of Internal Audit."

⁷⁶ For more information, refer to 12 CFR 30, appendix D, III.B.

⁷⁷ For more information on national banks, refer to the "Internal Control" booklet of the *Comptroller's Handbook*. For FSAs, refer to section 340, "Internal Control," of the *OTS Examination Handbook*.

Identify Risk

To properly identify risks, the board and management should recognize and understand existing risks and risks that may arise from new business initiatives, including risks that originate in nonbank subsidiaries, affiliates, and third-party relationships, and those that arise from external market forces or regulatory or statutory changes. Risk identification should be a continual process and should occur at the transaction, portfolio, and enterprise levels. For larger, more complex banks, management also should identify and report to the board on the interdependencies and correlations across portfolios and lines of business that may amplify risk exposures. Proper risk identification is critical for banks undergoing mergers and consolidations to appropriately address risks. Risk identification in merging companies begins with establishing uniform definitions of risk. A common language helps with the merger's success.

Measure Risk

Accurate and timely measurement of risks is essential to effective risk management systems. A bank that does not have a risk measurement system has limited ability to control or monitor risk levels. Further, the bank needs more sophisticated measurement tools as the complexity of the risk increases. Management should periodically conduct tests to verify that the bank's measurement tools are accurate. Sound risk measurement systems assess the risks at the individual transaction, portfolio, and enterprise levels. During bank mergers and consolidations, the effectiveness of risk measurement tools is often impaired because of the incompatibility of the merging systems or other problems of integration. Consequently, management of the resulting company should make a concerted effort to confirm that risks are appropriately measured across the merged entity. Larger, more complex companies should assess the effect of increased transaction volumes across all risk categories.

Monitor Risk

Management should monitor risk levels to review risk positions and exceptions to established limits in a timely manner. Monitoring reports should be timely and accurate and should be distributed to appropriate individuals including the board to ensure action, when needed. For larger, more complex banks, monitoring is vital to confirming that management's decisions are implemented for all geographies, products and services, and legal entities. Well-designed monitoring systems allow the board to hold management accountable for operating within established risk appetites.

Control Risk

The board and management, in their respective roles, should establish and communicate risk limits through policies, standards, and procedures that define responsibility and authority. These limits should serve as a means to control exposures to the various risks associated with the bank's activities. The limits should be tools that management can adjust when conditions or risk appetites change. Management also should have a process to authorize and document exceptions to risk limits when warranted. In banks merging or consolidating, the transition

should be tightly controlled; business plans, lines of authority, and accountability should be clear. Large, diversified banks should have strong risk controls covering all geographies, products and services, and legal entities to prevent undue concentrations of risk.

The board or audit committee should require a periodic independent assessment of the bank's overall risk governance and risk management practices, which may be conducted by internal audit. The reports should provide an overall opinion on the design and effectiveness of the bank's risk governance framework, including its system of internal controls. In smaller, less complex banks, the board should consider how internal audit reviews incorporate overall risk management.

Risk Assessment Process

A risk assessment process should be part of a sound risk governance framework. A well-designed risk assessment process promotes the identification of emerging risks at an early stage and allows for the development and implementation of appropriate strategies to mitigate the risks before they have an adverse effect on the bank's safety and soundness or financial condition. The completed risk assessments should be integrated into the bank's strategic planning process and risk management activities.

The board should oversee management's implementation of the bank's risk assessment process. The board should periodically receive information about the bank's risk assessments.

Management should perform risk assessments on material bank activities at least annually, or more frequently as warranted. Completing risk assessments helps management identify current, emerging, and aggregate risks and determine if actions need to be taken to strengthen risk management. Risk assessments should measure the inherent risk, which is the risk that an activity would pose if no controls or other mitigating factors were in place. A residual risk rating should be assigned after controls are taken into account. The risk assessment process should be candid and self-critical.

Policies

Policies are statements of actions that the bank adopts to pursue certain objectives. Policies guide decisions and often set standards (on risk limits, for example) and should be consistent with the bank's underlying mission, risk appetite, and core values.

While the board or a designated board committee is responsible for approving designated policies, management is responsible for developing and implementing the policies. The CEO and management should periodically review policies for effectiveness. Policies should control the types of risks that arise from the bank's current and planned activities. To be effective, policies should clearly delineate accountability and be communicated throughout the bank.

All banks should have policies addressing their significant activities and risks. The scope and detail of those policies and procedures vary depending on bank size and complexity. A smaller, noncomplex bank whose management is heavily involved in day-to-day operations should have, at a minimum, basic policies addressing the significant areas of operations. Larger, more complex banks should have more detailed policies in which senior management relies on a widely dispersed staff to implement complex business strategies. Before introducing new activities, management should establish appropriate policies and procedures that outline the standards, responsibilities, processes, and internal controls for ensuring that risks are well understood and mitigated within reasonable parameters.

Processes

Processes are the procedures, programs, and practices that impose order on the bank's pursuit of its objectives. Processes define how activities are carried out and help manage risk. Effective processes are consistent with the underlying policies and are governed by appropriate checks and balances (such as internal controls).

Management should establish processes to implement significant bank policies. The bank's size and complexity determine the amount of detail that is needed in the policies. The design of the bank's risk management procedures, programs, and practices should be tailored to the bank's operations, activities, and business strategies and be consistent with the bank's risk appetite. Examples of bank programs include the bank's risk governance framework, audit program, CMS, and compensation program, which are discussed throughout this booklet. Refer to other booklets of the *Comptroller's Handbook* for more information about other processes for specific areas of examination.

Management is responsible for establishing a system of internal controls⁷⁸ that provides for

- an organizational structure that establishes clear lines of authority and responsibility.
- monitoring adherence to established policies.
- processes governing risk limit breaches.
- an effective risk assessment process.
- timely and accurate financial, operational, and regulatory reports.
- adequate procedures to safeguard and manage assets.
- compliance with applicable laws and regulations.

Personnel

Personnel are the bank managers and staff who execute or oversee processes. Capable management and staff are essential to effective risk management. Personnel should understand the bank's mission, risk appetite, core values, policies, and processes.

Personnel should be qualified and competent, have clearly defined responsibilities, and be held accountable for their actions. The skills and expertise of management and staff should

⁷⁸ Ibid.

be commensurate with the bank's products and services offered to customers. The skills required for larger, more complex banks are generally greater and more varied than those required in smaller, less diversified, and less complex banks. As the complexity and risk profile of the bank increase, the higher the need for qualified personnel with specific areas of expertise. Management should anticipate and assess the bank's needs and develop plans for maintaining staffing commensurate with the bank's risk profile.

Management should design programs to attract, develop, and retain qualified personnel. An effective recruitment program enhances the continuity of executive and middle management, and assists in the recruitment of individuals with the requisite skills and knowledge for various positions within the bank. Training and professional development programs are important for developing and maintaining a talent pool and further developing required skills and knowledge. For banks with limited staff or overlapping responsibilities, training and development are particularly important for continuous and consistent operations.

Compensation programs should be designed to appropriately balance risk taking and reward. Management should continually assess the bank's recruitment, training and development, and compensation programs for the appropriate depth and breadth of staff.

Management should create and maintain an organizational structure with clear lines of responsibility, accountability, and oversight. Personnel in risk management and audit should have sufficient independence and stature. Position descriptions and a formal appraisal process reinforce responsibility and accountability for employees and managers. The appraisal review process provides important feedback about achieving performance goals. Effective communication promotes open dialogue, clear expectations and accountability, good decision making, and less duplication of effort.

Control Systems

Control systems are the functions (such as internal and external audits, risk review, quality control, and quality assurance) and information systems that bank managers use to measure performance, make decisions about risk, and assess the effectiveness of processes and personnel. Control functions should have clear reporting lines, sufficient resources, and appropriate access and authority. MIS should provide timely, accurate, and relevant feedback.

The effectiveness of internal controls is assessed through the bank's risk reviews (often second line of defense) and audit program (third line of defense). Risk reviews may include loan review, stress testing, compliance reviews, and back testing. Management should determine the risk reviews that should be performed in the bank. Audit programs are the independent control function that verifies the effectiveness of the bank's risk management system. Unlike risk reviews, audit managers and the board should make decisions regarding the audit program to maintain appropriate independence.

Quality Control

Quality control provides assurance that the bank consistently applies standards, complies with laws and regulations, and adheres to policies and procedures. An independent party performs the quality-control review concurrently with the bank activity. The quality-control review may be performed internally or outsourced to a third party. Quality control promotes an environment in which management and employees strive for the highest standards. An effective quality-control process significantly reduces or eliminates errors before they become systemic issues or have a negative impact on the bank's operations. Management, in consultation with the board, should determine what activities require a quality-control review, for example, secondary market mortgage loan originations, retail lending, and call center. Management also should determine the method and frequency of reporting of quality-control reviews based on regulatory requirements and risk exposure to the bank.

Quality Assurance

Quality assurance is designed to verify that established standards and processes are followed and consistently applied. An independent party performs the quality assurance review. The quality assurance review is normally performed after the bank completes the activity. Management uses the results of the quality assurance review to assess the quality of the bank's policies, procedures, programs, and practices in a specific area (for example, mortgage banking, retail lending, and internal audit). The results help management identify operational weaknesses, risks associated with the specific area, training needs, and process deficiencies. Management should determine which areas of the bank require a quality assurance review and should confirm that results of the reviews are reported to appropriate personnel.

Compliance Management System

Banking laws and regulations cover a wide range of areas, such as corporate structure, governance, bank activities, bank assets, authorities, AML, consumer protections, and political contributions.⁷⁹ Therefore, CMSs should extend beyond consumer protection laws and regulations and factor in all applicable laws and regulations as well as prudent ethical standards and contractual obligations.⁸⁰ The board and management should recognize the scope and implications of laws and regulations that apply to the bank and its activities. The board and management should understand the potential consequences of violations of laws and regulations that could result in financial losses, reputation and legal risks, and enforcement actions (including CMPs).

⁷⁹ For more information on political contributions for national banks and FSAs, refer to 52 USC 30101 et seq., "Federal Election Campaign Act of 1971," and 11 CFR 114.2, "Prohibitions on Contributions, Expenditures and Electioneering Communications." For national banks, also refer to 11 CFR 100, subpart B, "Definition of Contribution," and OCC Bulletin 2007-31, "Prohibition on Political Contributions by National Banks: Updated Guidance."

⁸⁰ For more information regarding the aspects of the bank's CMS covering consumer protection-related laws and regulations, refer to the "Compliance Management Systems" booklet of the *Comptroller's Handbook*.

The CMS should consist of the policies, procedures, and processes as well as the monitoring and testing programs that verify compliance with applicable laws and regulations and adherence to the bank's policies. All banks, regardless of size, should have a CMS that is commensurate with the risk inherent in the bank's products and services. The bank should also have monitoring in place that allows the board and management to assess the effectiveness of the bank's CMS and assists in the detection of fraud or violations of laws and regulations.

The bank's internal audit system⁸¹ should include a periodic and independent review of the bank's CMS to provide the board and management reasonable assurance of the bank's consumer compliance-related risk management.

Many banks establish a separate compliance function headed by a compliance officer or committee. Compliance officers, or individuals in an equivalent role, should

- have a process to identify the laws and regulations applicable to the bank and its related organizations, maintain an inventory of such laws and regulations, and implement appropriate change management processes in response to new regulations or changes to regulations.⁸²
- oversee the establishment of compliance monitoring and testing programs. For larger, more complex banks, this testing occurs in a second-line function that is independent of the business units.
- establish reporting processes in an effort to provide relevant information to appropriate parties.
- develop reports and metrics to monitor performance.
- implement and oversee compliance-related training programs for all employees and directors. Proper training programs reflect subject matter, depth, and frequency appropriate to job responsibilities. Escalation and reporting procedures should be in place for employees who do not complete the required training.

The board should oversee the bank's CMS. For larger, more complex banks, the board should receive periodic reports on the bank's state of compliance. The board is responsible for establishing a culture that places a high priority on compliance and holds management accountable.

Management should establish and clearly communicate compliance roles, responsibilities, and expectations that compliance with all laws and regulations is an organizational priority for all employees. Management is responsible for the timely correction of deficiencies found by compliance personnel, risk managers, internal and external auditors, and regulators. Management is responsible for implementing processes that promptly escalate material issues

⁸¹ Refer to 12 CFR 30, appendix A, II.A, "Operational and Managerial Standards," and the "Internal and External Audits" booklet of the *Comptroller's Handbook* for information regarding internal audit systems, including compliance audit systems.

⁸² The designation of responsibility over the change management process is a senior management decision and may vary from bank to bank.

to senior management and the board. Management also should implement and maintain a mechanism for employees to confidentially raise concerns about illegal activities, violations, and nonadherence to bank policies.

Bank Secrecy Act/Anti-Money Laundering Program

The BSA is intended to safeguard the U.S. financial system and the banks that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions. The BSA requires banks to establish a BSA/AML compliance program to fulfill its record-keeping and reporting requirements and to confirm the identity of bank customers.⁸³ The board is responsible for approving and overseeing management's implementation of the BSA/AML compliance program. The program must include⁸⁴

- a system of internal controls to ensure ongoing compliance.
- independent testing of BSA/AML compliance.
- a designated individual or individuals responsible for managing BSA compliance (BSA compliance officer).
- training for appropriate personnel.
- a customer identification program.⁸⁵

The program should also contain appropriate risk-based procedures for conducting ongoing customer due diligence, including⁸⁶

- understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile.
- conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.⁸⁷

Senior management should communicate and reinforce the BSA/AML compliance culture established by the board. Senior management is also responsible for implementing and enforcing the board-approved BSA/AML compliance program.⁸⁸

⁸³ For more information, refer to the *FFIEC BSA/AML Examination Manual*.

⁸⁴ For more information, refer to 12 CFR 21.21, “Procedures for Monitoring Bank Secrecy Act Compliance.”

⁸⁵ For more information, refer to 12 CFR 21.21(c)(2), “Customer Identification Program.”

⁸⁶ For more information, refer to 31 CFR 1020.210, “Anti-Money Laundering Program Requirements for Financial Institutions Regulated Only by a Federal Functional Regulator, Including Banks, Savings Associations, and Credit Unions.”

⁸⁷ Ibid.

⁸⁸ Refer to 12 CFR 21.21(c) “Establishment of a BSA Compliance Program,” and 12 CFR 21.21(d)(3).

Audit Program

Well-planned, properly structured audit programs are essential to effective risk management and internal control systems and are also a critical defense against fraud.⁸⁹ The audit program consists of an internal audit function and an external audit function. An internal audit program provides assurance to the board and senior management not only on the quality of the bank's internal controls but also on the effectiveness of risk management, financial reporting, MIS, and governance practices. Internal auditors should be independent of the audited activities and have sufficient stature, authority, and board support to carry out their assignments with objectivity. The external audit function complements the internal audit function by providing management and the board with an independent and objective view of the reliability of the bank's financial statements and the adequacy of its system of internal controls over the bank's financial statements. When a third party provides both audit and consulting services, special care should be taken to preserve audit independence. Specifically, the firm should not audit the activities for which it provided consultation services.⁹⁰

The board may delegate the design, implementation, and monitoring of the system of internal controls to management and delegate the testing and assessment of internal controls to internal auditors or other external third parties. Establishing an independent audit committee to oversee and maintain the audit functions is a good, and sometimes required, practice.⁹¹ See appendix C, "Common Board Committees," of this booklet for more information on audit committee responsibilities. The board and senior management are responsible for having an effective system of internal controls and an effective audit system in place.⁹²

The chief auditor is the person assigned responsibility for the internal audit function.⁹³ The chief auditor reports directly to the audit committee or the board in the absence of the audit committee. The OCC expects the chief auditor to be a bank employee, but the chief auditor may have dual reporting relationships. The objectivity of internal audit is best served when the chief auditor is functionally accountable to the audit committee but reports administratively to the CEO. The chief auditor may also be a dual employee of the holding

⁸⁹ For more information on effective audit functions, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook*.

⁹⁰ For more information, refer to OCC Bulletin 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing."

⁹¹ 12 CFR 363.5(a), "Composition and Duties," requires insured banks with \$500 million or more in total assets to have a dedicated audit committee. 12 CFR 363, appendix A.27, "Composition," outlines audit committee requirements as they should be applied to banks and insured branches of foreign banks. Refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook* for more information on audit committees.

⁹² Refer to 12 CFR 30, appendix A, II.A. Internal control systems include internal controls and information systems.

⁹³ Refer to OCC Bulletin 2003-12. In small banks that do not have a formal internal or external audit program, internal audit responsibilities may lie with an officer or employee. Refer the "Internal and External Audits" booklet of the *Comptroller's Handbook* for more information.

company. The chief auditor implements the audit program and reports audit activities to the audit committee. The chief auditor should have the appropriate stature and authority in the bank to perform his or her duties, and, in certain larger banks, regulation requires the position rest one level below the CEO.⁹⁴ When the bank outsources the internal audit activities, the board and senior management should designate an audit liaison to coordinate audit activities.

Heightened Standards

The audit committee reviews and approves internal audit's overall charter and audit plans. The audit committee should approve all decisions regarding the appointment or removal and annual compensation and salary adjustment of the CAE. The committee may oversee the CAE's administrative activities or designate them to the CEO.⁹⁵

The heightened standards impose additional requirements on audit plans, as well as additional circumstances in which the internal audit should make reports to the audit committee. The audit committee should be aware of and monitor the internal audit's compliance with these heightened standards.⁹⁶

Management Information Systems

Banks rely heavily on IT to process bank transactions, maintain critical records, and supply reports to the board and management about managing business risk.⁹⁷ As such, a bank's IT systems should have the capability to aggregate risks across the bank in a timely manner and under stress situations. Information provided by management in reports should be accurate, timely, and sufficiently detailed to oversee the bank's safe and sound operation.

MIS broadly refers to a comprehensive process, supported by computer-based systems, that provides the information necessary to manage the bank. To function effectively as an interactive, interrelated, and interdependent feedback system for management and staff, MIS should be useable. The five elements of a useable MIS are timeliness, accuracy, consistency, completeness, and relevance. The effectiveness of MIS is hindered whenever one or more of these elements is compromised.

Timeliness: To simplify prompt decision making, the bank's MIS should be capable of providing and distributing current information to appropriate users. Information systems should be designed to expedite reporting of information. The system should be able to quickly collect and edit data, summarize results, and adjust and correct errors.

Accuracy: A sound system of automated and manual internal controls should exist throughout all information systems processing activities. Information should receive appropriate editing, balancing, and internal control checks. The bank should employ a

⁹⁴ Refer to 12 CFR 30, appendix D, I.E.2, "Chief Audit Executive."

⁹⁵ For more information, refer to 12 CFR 30, appendix D, I.E.8, "Internal Audit."

⁹⁶ For more information, refer to 12 CFR 30, appendix D, II.C.3.

⁹⁷ For more information, refer to the "Management" booklet of the *FFIEC IT Examination Handbook*.

comprehensive internal and external audit program to validate the adequacy of internal controls.

Consistency: To be reliable, data should be processed and compiled consistently and uniformly. Variations in how the bank collects and reports data can distort information and trend analysis. In addition, because data collection and reporting processes change over time, management should establish sound procedures to allow for systems changes. These procedures should be well defined and documented, be clearly communicated to appropriate employees, and include an effective monitoring system.

Completeness: Decision makers need complete and pertinent information in summarized form. Management should capture and aggregate all of the bank's material risk exposures, including those that are off-balance-sheet. Data should be available by groupings, such as by business line, asset type, and industry, that are relevant for the risk in question. Also, the data groupings should allow for the identification and reporting on risk exposures, concentrations, and emerging risks.

Relevance: Information provided to management should be relevant. Information that is inappropriate, unnecessary, or too detailed for effective decision making has no value. MIS should be appropriate to support the management level using the information. The relevance and level of detail provided through MIS should directly correlate to the needs of the board, senior management, departmental or area mid-level managers, and others in the performance of their jobs.

MIS do not necessarily reduce expenses. Development of meaningful systems and their proper use lessen the probability that erroneous decisions will be made because of inaccurate or untimely information. Erroneous decisions invariably misallocate or waste resources, which may adversely affect earnings or capital.

Heightened Standards

The risk governance framework should include a set of policies, supported by appropriate procedures and processes, designed to provide risk data aggregation and reporting capabilities appropriate for the size, complexity, and risk profile of the covered bank, and to support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for the following:

- The design, implementation, and maintenance of a data architecture and IT infrastructure that support the covered bank's risk aggregation and reporting needs during both normal times and times of stress.
- The capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board and the OCC.⁹⁸
- The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.⁹⁹

⁹⁸ For more information, refer to 12 CFR 30, appendix D, II.J, "Risk Data Aggregation and Reporting."

⁹⁹ For more information, refer to the Basel Committee on Banking Supervision's "Principles for Effective Risk Data Aggregation and Risk Reporting," January 2013.

Third-Party Risk Management

Banks increasingly rely on third-party relationships to provide technological, administrative, and operational services on the bank's behalf. The bank's use of third parties does not diminish the board and senior management's responsibility to ensure that the activity is performed in a safe and sound manner and complies with applicable laws and regulations.

Management should adopt third-party risk management processes commensurate with the level of risk and complexity of the bank's third-party relationships and organizational structure.¹⁰⁰ The board and management should provide more comprehensive and rigorous oversight and management of third-party relationships that involve critical activities.

Management should adopt a third-party risk management process that follows a continuous life cycle for all relationships and incorporates planning, due diligence, and third-party selection, contract negotiation, ongoing monitoring, and termination.

Insurance

The board should be responsible for the adequacy of insurance coverage and other insurance needs. As part of an effective risk management system, the board should determine the uninsured loss the bank is able and willing to assume. Management can implement additional controls to minimize and retain risk. Management may transfer the risk to another party through insurance or contractual transfer, self-insure the risk, or use any combination of these options. A basic tenet of risk management is that risks carrying the potential for catastrophic or significant loss should not be retained. Conversely, it typically is not cost-justified to insure losses that are relatively predictable and not severe. Teller drawer shortages are an example. It would be less costly to improve controls or training procedures intended to reduce those shortages than to pay additional insurance premiums to cover the losses.

The board should determine the maximum loss the bank is able and willing to assume. Once the decision is made to insure a particular risk, a knowledgeable, professional insurance agent can help with selecting an underwriter. Management should assess the financial capacity of the insurance underwriter to determine that the company has the ability to make payment should a significant loss occur. Additionally, the board and management should review the bank's insurance annually.

Appendix D of this booklet explains major types of insurance coverage available to banks.

¹⁰⁰ For more information, refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"; OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures"; OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"; and the "Outsourcing Technology Services" booklet of the *FFIEC IT Examination Handbook*.

Insurance Record Keeping

The breadth of available insurance policies and differences in the coverage emphasize the importance of maintaining a concise, easily referenced schedule of insurance coverage. These records should include the

- coverage provided, detailing major exclusions.
- underwriter.
- deductible amount.
- upper limit.
- term of the policy.
- date premiums are due.
- premium amount.

Records of losses also should be maintained and included whether or not the bank was reimbursed. These records indicate where internal controls may need to be improved and are useful in measuring the level of risk exposure in a particular area.

Board and Management's Roles in Risk Governance

The board or risk committee and senior management play critical roles in the bank's risk governance by (1) setting the tone at the top, (2) setting the bank's strategic objectives and risk appetite, and (3) establishing an appropriate risk management system to manage the risks associated with meeting the strategic objectives.

Risks may arise from bank activities or activities of subsidiaries, affiliates, counterparties, or third-party relationships. Any product, service, or activity may expose the bank to multiple risks. These risks may be interdependent—an increase in one category of risk may cause an increase in others. Because of the interrelationship of the bank's risks and the potential impact on its earnings, capital, and strategic objectives, the risks should be assessed, evaluated, and managed enterprise-wide. This concept is commonly referred to as enterprise risk management (ERM). ERM helps the board and management view the bank's risks in a comprehensive and integrated manner. ERM also helps identify concentrations that may arise across multiple business lines that, when aggregated, represent concentration risk that may require board attention and management actions. To be successful, ERM should be supported by the board and senior management. If the bank is a subsidiary of a holding company, it may be appropriate to implement ERM corporate-wide.

Board's Responsibilities

The board should oversee the design and implementation of the risk governance framework. The board should require periodic independent assessments to determine the framework's effectiveness.

The board should oversee the bank's risk management system to confirm that the system identifies, measures, monitors, and controls risks. If the bank does not have a CRE, the board

should appoint a qualified individual or committee to oversee the bank's ERM process. While a qualified individual independent of day-to-day frontline management is preferred, it may not be practical for every bank. When impractical, the board should consider selecting a senior-level staff member who has a good understanding of the bank's operations across the various business lines. This person should have access to the board or risk committee to convey risk concerns.

The board should oversee the bank's compliance management programs. The board is responsible for creating a culture that places a high priority on compliance and holds management accountable.

The OCC expects the board to be responsible for confirming that a system of internal controls is in place.¹⁰¹ The board should periodically receive information about the effectiveness of the bank's internal controls and information systems. The board should demonstrate that it has an adequate understanding of the bank's IT infrastructure, inherent risks, and existing controls.

Management's Responsibilities

The OCC expects senior management to be responsible for developing and maintaining the risk governance framework and system of internal controls, which enables management to effectively identify, measure, monitor, control, and report risk exposures consistent with the board-established risk appetite. Senior management should report to the board on the bank's overall risk profile, including aggregate and emerging risks. Senior management should provide the board timely, accurate, and reliable information about current and potential risk exposures and their potential impact on earnings, capital, and strategic objectives, particularly under adverse or stress scenarios. Risk reporting should readily identify significant and emerging risks and issues as well as determine areas that need improvement.

Capable management is essential to an effective risk management system. Senior management should be responsible for the implementation, integrity, and maintenance of the risk management system. Senior management should

- keep directors adequately informed about the level and direction of risk.
- implement the bank's or holding company's strategy.
- develop policies that define the bank's risk appetite that are compatible with the strategic goals.
- ensure the strategic direction and risk appetite are effectively communicated and adhered to throughout the bank.
- oversee the development and maintenance of timely, accurate, consistent, complete, and relevant MIS.

The CEO and senior management play a critical role in communicating to the board and managing the bank. Effective communication is important for corporate and risk governance.

¹⁰¹ Refer to 12 CFR 30, appendix A, II.A. Internal control systems include internal controls and information systems.

The board delegates authority to senior management for directing and overseeing day-to-day management of the bank. Senior management should be responsible for developing and implementing policies, procedures, and processes that translate the board's goals, strategic objectives, and risk appetite and limits into prudent standards for the safe and sound operation of the bank.

Management carries out the bank's day-to-day activities and financial performance. Management should optimize the bank's earnings by investing in good quality assets. Management should measure performance against strategic and operational objectives and ensure that risk exposures remain within risk limits. Management should ensure that capital and liquidity levels (1) are commensurate with the bank's risk profile; (2) support short- and long-term growth plans; and (3) can withstand economic downturns.

Specifically, the CEO and his or her senior management team should be responsible for

- directing and overseeing day-to-day management of the bank.
- implementing a strong risk culture and ethical standards and providing incentives to reward appropriate behavior.
- complying with laws, regulations, and internal bank policies, including policies governing ethics and insider activities.
- developing and implementing an effective CMS.
- executing the bank's strategic plan, and ensuring the adequacy of capital and resources in carrying out the plan.
- developing and administering a risk governance framework that enables management to effectively identify, measure, monitor, and control risk.
- establishing and maintaining an effective system of internal controls.
- maintaining processes, including stress testing when appropriate, to ensure capital and liquidity levels are commensurate with the bank's risks in normal and stressed conditions.
- developing accurate and reliable management information and reporting systems to keep the board apprised of the bank's strategic direction, risk profile, risk appetite, business operations, financial performance, and reputation.
- appropriately allocating staff resources and effectively overseeing personnel.
- establishing talent management and compensation and employee benefit arrangements.
- implementing a corporate governance structure that provides for effective policies and control systems over relationships with related organizations and transactions with insiders.

Management committees may be used to facilitate oversight of day-to-day banking activities. Management should determine which committees are appropriate for its bank and how formal the committees' structure should be. Typical management committee areas include asset liability, credit, compliance, and IT steering.

Examination Procedures

This booklet contains expanded procedures for examining specialized activities or specific products or services that warrant extra attention beyond the core assessment contained in the “Community Bank Supervision,” “Federal Branches and Agencies Supervision,” and “Large Bank Supervision” booklets of the *Comptroller’s Handbook*. Examiners determine which expanded procedures to use, if any, during examination planning or after drawing preliminary conclusions during the core assessment.

Scope

These procedures are designed to help examiners tailor the examination to each bank and determine the scope of the corporate and risk governance examination. This determination should consider work performed by internal and external auditors and other independent risk control functions and by other examiners on related areas. Examiners need to perform only those objectives and steps that are relevant to the scope of the examination as determined by the following objective. Seldom will every objective or step of the expanded procedures be necessary.

Objective: To determine the scope of the examination of corporate and risk governance and identify examination objectives and activities necessary to meet the needs of the supervisory strategy for the bank.

1. Review the following sources of information and reports. Note any previously identified problems related to corporate and risk governance that require follow-up:

- Supervisory strategy.
- Examiner-in-charge’s (EIC) scope memorandum.
- The OCC’s supervisory information systems.
- Previous reports of examination and work papers.
- Internal and external audit reports and work papers.
- Bank management’s responses to previous reports of examination and audit reports.
- Customer complaints and litigation. Examiners should review customer complaint data from the OCC’s Customer Assistance Group, the bank, and the Consumer Financial Protection Bureau (when applicable). When possible, examiners should review and leverage complaint analysis already performed during the supervisory cycle to avoid duplication of effort.
- Financial reports (e.g., the Uniform Bank Performance Report) and applicable OCC analytical tools. Identify changes since the prior review.

2. Obtain and review policies, procedures, and reports bank management uses to supervise corporate and risk governance. Consider

- bylaws of the bank.
- the national bank’s articles or the FSA’s charter.

- a list of directors.
 - board meeting packages.
 - board-level financial performance and key risk reports.
 - board and board-level committee reports and meeting minutes.
 - board-level committees' written charters.
 - director orientation and education material.
 - board self-assessments.
 - the strategic plan and reports used to monitor the plan.
 - operational plans.
 - a list of new, modified, or expanded products and services and documentation of the approval process.
 - third-party relationship risk management, including policies and processes.
 - the capital plan.
 - the risk governance framework, including the risk management system in place.
 - executive and frontline unit reports.
 - internal risk assessments.
 - policies and procedures.
 - quality control reviews.
 - quality assurance reviews.
 - the employee compensation and benefits program information.
 - the compliance management program, including the BSA program. (Refer to the *FFIEC BSA/AML Examination Manual* for procedures to evaluate the BSA/AML compliance program.)
 - the current CRA public evaluation.
 - a schedule of the insurance policies.
3. In discussions with bank management, determine if there have been any significant changes (for example, new executive officers; new directors; changes in corporate structure; changes in the corporate and risk governance framework; strategic and capital plans; changes to charters, policies, procedures, or reports regarding corporate and risk governance; compensation and benefits; and insurance) since the previous examination of corporate and risk governance.
 4. Based on an analysis of information obtained in the previous steps, as well as input from the EIC, determine the scope and objectives of the corporate and risk governance examination.
 5. Select from the following examination procedures the necessary steps to meet examination objectives and the supervisory strategy.

Board of Directors and Management

Conclusion: The board of directors is (effective or ineffective) in its fiduciary duties and establishing a corporate and risk governance framework to facilitate oversight of bank activities.

Management is (effective or ineffective) in directing and overseeing the day-to-day activities of the bank.

Board Composition and Qualifications

Objective: To determine if the board is composed of individuals with a balance of skills, expertise, and diversity who can exercise independent judgment; provide a credible challenge to management's recommendations and decisions; and comply with board-related laws and regulations.

Statutory and Regulatory Requirements

Objective: To assess compliance with laws, regulations, and prudent banking practices relating to board composition and qualifications.¹⁰²

1. Obtain a list of directors that includes the following information for each director:
 - Home address, when appropriate (if the director was appointed or elected since the previous examination, indicate the number of years residing at his or her present address).
 - Years as a director of the bank.
 - Occupation.
 - Citizenship (for national banks).
 - Common stock ownership (beneficial, direct, or indirect) for national banks or membership for mutual FSAs.
 - Bonus, fees, and any other compensation.
 - Attendance record at board meetings.
2. Determine if the number of directors aligns with the bank's bylaws.
3. Determine whether the bank complies with the following laws and regulations regarding director qualifications:
 - Do all directors of national banks possess sufficient stock to qualify as directors? (12 USC 72 and 12 CFR 7.2005)

¹⁰² For a list of the requirements regarding size, composition, and other aspects, refer to this booklet's appendix A, "Board of Directors Statutory and Regulatory Requirements."

- For a stock FSA, do the bylaws require a director to be a stockholder? If so, do all directors meet this requirement? (12 CFR 5.22(l))
 - For a mutual FSA, are all directors members of the association? (12 CFR 5.21(j)(2))
 - Are all national bank directors citizens of the United States? If not, has the Comptroller waived the citizenship requirement? (12 USC 72) (The majority of directors must be U.S. citizens.)
 - Do the majority of national bank directors reside in the state, territory, or district in which the bank is located, or within 100 miles of the bank's main office? If not, has the Comptroller waived the residency requirements? (12 USC 72)
 - Did the majority of the national bank directors reside in the state, territory, or district in which the bank is located, or within 100 miles of the bank's main office, for one year before their election? If not, has the Comptroller waived the residency requirements? (12 USC 72)
 - Did all national bank directors take an oath of office? (12 USC 73 and 12 CFR 7.2008)
 - Did the national bank forward a copy of the oath of office to the OCC? (12 USC 73 and 12 CFR 7.2008)
 - Has it been determined that no director is an indenture trustee? (15 USC 77jjj)
4. For FSAs, determine if the bank complies with 12 CFR 163.33.
- Are the majority of the directors not salaried officers or employees of the FSA or any subsidiary thereof?
 - Are no more than two of the directors members of the same immediate family?
 - Is there no more than one director who is an attorney with a particular law firm?
5. For FSAs, determine if there was a director removed for cause. Cause is defined in 12 CFR 5.21(j)(2)(x)(B) to include personal dishonesty; incompetence; willful misconduct; breach of fiduciary duty involving personal profit; intentional failure to perform stated duties; willful violation of any law, rule, or regulation (other than traffic violations or similar offenses); or final cease-and-desist order.
- Was a meeting of shareholders called expressly for the purpose of removal for cause, as required? If so, other requirements apply for votes for removal. (12 CFR 5.22(l)(6) for stock FSAs)
6. For FSAs, determine, through examination findings and discussions with examiners, whether the person who has a fiduciary duty to the FSA advanced his or her personal or business interests at the expense of the bank. (12 CFR 163.200)
7. For FSAs, determine, through examination findings and discussions with examiners, if the director, officers, or persons having power to direct management or policies, or persons otherwise owing a fiduciary obligation to the FSA, have taken advantage of corporate opportunities that belonged to the bank. (12 CFR 163.201)

8. Determine if the bank complies with the following laws and regulations regarding board structure:

- Is the number of directors consistent with the bylaws and no fewer than five and no more than 25 for national banks? (12 USC 71a) If the national bank has more than 25 directors, has the Comptroller waived the 25-director maximum?
- For FSAs, do the bylaws state a specific number of directors and not a range? (12 CFR 5.22(l)(2) for stock FSAs and 12 CFR 5.21(j)(2)(viii) for mutual FSAs)
- Is the number of directors consistent with the bylaws and no fewer than five and no more than 15 for FSAs? (12 CFR 5.22(l)(2) for stock FSAs and 12 CFR 5.21(j)(2) for mutual FSAs) If not, has the Comptroller waived the requirements?
- Did the board appoint directors to fill vacancies? (12 USC 74 for national banks, and 12 CFR 5.22(l)(5) for stock FSAs and 12 CFR 5.21(j)(2) for mutual FSAs)
- Did shareholders or members elect directors at their regular annual meeting? (12 USC 71 for national banks, and 12 CFR 5.22(k)(1) for stock FSAs and 12 CFR 5.21(j)(2)(i) for mutual FSAs)
- For national banks, if shareholders did not elect directors at their regular annual meeting, were the elections held within 60 days thereof? (12 USC 75)
- For FSAs, did the FSA hold an annual meeting for the election of directors within 150 days after the end of the association's fiscal year? (12 CFR 5.22(k)(1) for stock FSAs and 12 CFR 5.21(j)(2)(i) for mutual FSAs)
- Did the mutual FSA establish a nominating committee, if the bylaws permitted, before the submission of nominations? (12 CFR 5.21(j)(2)(xiii))
- For national banks, is the president a member of the board? (12 USC 76 and 12 CFR 7.2012)
- For FSAs, do the bylaws require the president to be a director? If so, has the FSA met this requirement?
- Is the term of office for a director between one and three years for FSAs and not more than three years for national banks? (12 USC 71 and 12 CFR 7.2024(b) for national banks, 12 CFR 5.22(l)(2) for stock FSAs, and 12 CFR 5.21(j)(2)(viii) for mutual FSAs)

9. Determine compliance with the following laws and regulations regarding restrictions on board activities:

- Has a quorum been present for all board meetings? (12 CFR 7.2009 for national banks, and 12 CFR 5.22(l)(4) for stock FSAs and 12 CFR 5.21(j)(2)(ix) for mutual FSAs)
- For national banks, do board procedures preclude any director from casting a vote by proxy? (12 CFR 7.2009)
- For FSAs, were board actions approved by a majority of directors present at any meeting at which there was a quorum? (12 CFR 5.22(l)(4) for stock FSAs and 12 CFR 5.21(j)(2)(ix) for mutual FSAs)
- If any management officials of the bank or its holding company or holding company affiliates are management officials of an unaffiliated depository bank or depository

- holding company, do any of the statutory exceptions (12 USC 3201 et seq.) or regulatory exemptions (12 CFR 26) apply?
- If any directors have been appointed to the board for purposes other than filling vacancies, do the articles provide for such appointments? (12 CFR 7.2007(a))
10. Determine compliance with the following laws and regulations regarding regulatory reporting:
- If embezzlements, defalcations, misappropriations, mysterious disappearances, or thefts have occurred since the previous examination, did the bank file a Suspicious Activity Report with the appropriate law enforcement agencies and with the U.S. Department of the Treasury? (12 CFR 21.11 for national banks and 12 CFR 163.180(d) for FSAs)
 - Was the Suspicious Activity Report promptly reported to the board as required? (12 CFR 21.11 for national banks and 12 CFR 163.180(d) for FSAs)
 - If the bank has a class of equity securities held by 2,000 or more shareholders and total assets exceeding \$10 million, did the bank file reports with the OCC, as required by federal securities law? (12 CFR 11)
 - Was the OCC notified of any change in control or, if in troubled condition, change in senior executive officers since the last examination? (12 USC 1817(j), 12 USC 1831i, 12 CFR 5.50, and 12 CFR 5.51)
 - Does the bank maintain records of directors, executive officers, and principal shareholders and the related interests of these persons and of extensions of credit to these persons? (12 CFR 31 and 12 CFR 215)
 - Has the bank notified executive officers and directors of the requirements to report to the board the outstanding amount of any credit that was extended to the executive officer or directors and was secured by the bank's shares? (12 CFR 31 and 12 CFR 215)
 - For national banks, if the board contains honorary or advisory members, has the bank distinguished between honorary or advisory directors and active directors in published reports? (12 CFR 7.2004)
11. If it was not done in previous examinations, review and brief the bylaws and articles of association of the bank, including any specific provisions related to the requirements of directors, and if a brief exists from previous examinations, update it as appropriate.
12. Read and brief the minutes of shareholders or members' meetings since the last examination. The brief should include a list of directors elected at the annual meeting, the number of shares present and voted (for national banks and stock FSAs), individuals acting as proxies, and specific action approved by shareholders or members.
13. For stock FSAs, assess whether the minutes reflect a director's dissent or abstention to the board's action to avoid the appearance of approval. (12 CFR 5.22(l)(10))
14. Determine whether all requirements were met (e.g., shareholder approval) for any of the following actions that the board took since the last examination:

- Any change in location of the main or home office. (12 CFR 5.40)
 - Any issuance of preferred stock. (12 CFR 5.46 for national banks and 12 CFR 5.22(g)(4)(B) for stock FSAs)
 - Any increase in capital stock, either through sale or through a stock dividend. (12 CFR 5.46 for national banks and 12 CFR 5.22(g)(4) for stock FSAs)
 - Any reduction in capital stock. (12 CFR 5.46(h) for national banks and 12 CFR 5.22(g)(4) for stock FSAs)
 - Any stock split. (12 CFR 5.46 for national banks and 12 CFR 5.22(g) for stock FSAs)
 - Any bank pension plan established. (29 USC 1001 et seq.)
 - Any bank involvement in a conversion, merger, or consolidation. (12 CFR 5.24 and 12 CFR 5.33 for national banks, and 12 CFR 5.23 and 12 CFR 5.33 for FSAs)
 - Matters subject to vote at shareholder meetings. Verify that
 - for national banks, shares held by the bank as sole trustee or in its nominee name are not voted for directors unless applicable requirements are satisfied. (12 USC 61)
 - for stock FSAs, treasury shares held by the FSA and shares held by another corporation, if a majority of the shares entitled to vote for the election of directors of such other corporation are held by the FSA, shall not vote for directors. (12 CFR 5.22(k)(6)(ii) “”)
 - for national banks, no officer, clerk, teller, or bookkeeper acted as a proxy. (12 USC 61 and 12 CFR 7.2002)
15. Review any stock option or stock purchase plan adopted since the preceding examination, and review such action for compliance with the articles of association and the various conditions of the articles of association.
16. Determine if any candidate was nominated director, other than the slate nominated by bank management, and whether shareholders submitted new business, and review for compliance with the requirements in 12 CFR 5.22(k)(7) for stock FSAs and 12 CFR 5.21(j)(2)(xiii) and 12 CFR 5.21(j)(2)(xiv) for mutual FSAs.

Core Competencies of the Board

Objective: To determine if the board is well-diversified and composed of individuals with a mix of knowledge and expertise in line with the bank’s size, business strategy, risk profile, and complexity.

1. Are background checks performed on board candidates?
2. In the director’s selection process, are the candidate’s ethical standards and integrity in his or her personal and professional dealings considered?
3. Has the board established a board meeting attendance policy?
4. Is attendance monitored to determine the director’s level of involvement and participation?

5. Is there evidence of a credible challenge of management's decisions and recommendations recorded in the board meeting minutes?
6. For national banks, verify that directors have not voted by proxy.

Board Independence

Objective: To determine if the board exercises independent judgment.

1. In assessing whether the board exercises independent judgment, consider whether
 - there is a mix of independent and management directors.
 - there is a dominant management or director(s).
 - the board has adopted standards on conflicts of interest and independence.
 - the board convenes executive sessions without management's influence.
2. Determine if the CEO also serves as the board chair. If so, does the bank also have a lead director who is independent of management to provide a balance of power?
3. For covered banks, verify that at least two members of the board are independent directors. (12 CFR 30, appendix D)
 - Independence means the individual
 - is not an officer or employee of the bank or parent company and has not been an officer or employee of the bank or its parent company in the past three years.
 - is not an immediate family member of a person who has been an executive officer of the bank or its parent company in the past three years.
 - qualifies as an independent director under the listing standards of a national securities exchange.

Outside Advisors and Advisory Board

Objective: To determine if the board uses advisors to leverage expertise independent of bank management, when appropriate.

1. Determine if the board has a process in place to solicit outside advisors, when appropriate.
2. Determine if the board has used an outside advisor since the last examination. If so, obtain a copy of the engagement letter and the information and expert advice provided to the board or designated committee.
3. Assess if the fees charged are reasonable and in line with the services rendered.
4. If the bank uses advisory directors, does the board ensure that they do not have voting privileges?

Board Practices

Objective: To determine if the board adopted practices that permit effective oversight based on the size, strategy, risk profile, and complexity of the bank.

Board Information

Objective: To determine if the information provided to the board is adequate to make informed decisions and allow directors to provide a credible challenge to management assertions.

1. Determine whether management provides information to the board that is accurate, complete, and timely and is presented in a meaningful format to allow for effective oversight.
2. Determine whether the information is periodically reviewed by internal audit for integrity.
3. Does the information include key performance measurements and key risk indicators to monitor adherence to the bank's strategy and risk appetite?
4. Does the board periodically reevaluate the information it receives to determine if it has sufficient information to make informed decisions?

Meetings and Minutes

Objective: To determine if board meetings and minutes reflect the material issues of the bank and comply with board meeting-related laws and regulations.

1. For national banks, mutual FSAs, and stock FSAs, determine the date of the annual shareholders' or members' meeting, and verify that the date was in compliance with the bylaws. (12 USC 71 for national banks, 12 CFR 5.21(j)(2)(i) for mutual FSAs, and 12 CFR 5.22(k)(2) for stock FSAs)
2. Review the bank's practice of notifying shareholders or members of special or regular meetings.
 - For national banks, at least 10 days' notice is required, and the notice must include the time, place, and purpose of the meeting. Longer periods may be required by the articles of association, the bylaws, or other laws and regulations applicable to a national bank. (12 USC 75 and 12 CFR 7.2001)
 - For stock FSAs, notice delivered not fewer than 20 days nor more than 50 days is required. The notice must state the place, day, hour, and purpose of the meeting. (12 CFR 5.22(k)(2))
 - Mutual FSAs must publish notice for two successive weeks immediately before the week in which the meeting will convene, in a newspaper of general circulation in the city or county in which the principal place of business of the association is located.

Alternatively, the FSA may mail notice at least 15 days and not more than 45 days before the date of the meeting to each of its members. In addition to following one of these alternatives, the mutual FSA must post a notice of the meeting in a conspicuous place in each of its offices during the 14 days immediately preceding the date of the meeting. (12 CFR 5.21(j)(2)(iii))

3. For mutual FSAs, determine if directors receive notice of a board meeting at least 24 hours in advance unless the directors waived notice. (12 CFR 5.21(j)(2)(ix))
4. For stock FSAs, determine if directors receive notice of special board or board committee meetings at least 24 hours in advance unless the directors waived notice. (12 CFR 5.22(l)(8))
5. Determine if the frequency of board and board committee meetings is sufficient to manage the affairs of the bank.
6. Determine if the board receives board packets in advance to allow directors to prepare for meetings.
7. Determine whether the information packets cover key risks of the bank.
8. Read and brief the minutes of all meetings of the board since the last examination. Note the following:
 - Any actions taken in contravention of the bylaws.
 - Actions taken by the board that are not part of a normal monthly meeting.
 - Resolutions or discussions about entrance into a new geographic area, customer service, asset or liability category, or other new undertaking. This also should include a discussion of updates to the strategic plan and how any new activities fit in with the plan.
 - Creation of any special committee and its mission.
 - Ratification by the full board of actions taken by standing committees.
 - Any transactions with directors or their interests, or abstention of any interested director. If the minutes do not mention any director-related transactions that are uncovered during the examination, determine why the identified transaction was not discussed during a board meeting. Also determine how the director-related transaction was approved and whether the interested party refrained from voting.
 - Director attendance to determine the levels of interest and dedication, and how the directors fulfill fiduciary responsibilities.
 - Participation of individual directors to determine if any one, or a certain group of directors, dominates the board discussions.
 - Re-booked charged-off loans approved by the board and the rationale for re-booking. (**Note:** The re-booking of charged-off loans is inconsistent with both generally accepted accounting principles and the call report. It is an unacceptable practice.) Distribute list to examiner assigned Loan Portfolio Management and inform the EIC.
 - Reviews of correspondence between the OCC and the bank.

- Reports of examinations and audits reviewed and actions taken or plans to effect correction of deficiencies.
 - Whether directors of an FSA reviewed the results of operations with respect to interest rate risk exposure at least quarterly and made appropriate adjustments as necessary. (12 CFR 163.176)
 - Whether directors reviewed and approved written policies, at least annually, that establish appropriate limits and standards for extensions of credit that are secured by real estate. (12 CFR 34, subpart D, and subpart D, appendix A, for national banks and 12 CFR 160.101 and appendix for FSAs)
 - Whether directors designate a security officer to report at least annually on the implementation, administration, and effectiveness of the security program. (12 CFR 21, subpart A, for national banks and 12 CFR 168 for FSAs)
9. Determine if documentation of board meeting minutes is sufficient to determine
- the board's review and discussion of material action items on the agenda.
 - actions taken.
 - abstention of votes.
 - follow-up items to be addressed at a later meeting.
 - attendance of each director and other attendees.
 - previous board meeting minutes' approval.
 - board-approved policies.

Policy Review and Approval

Objective: To determine if the board has a process to review and approve policies.

1. Are policies that are statutorily required to be reviewed and approved by the board done so in accordance with the respective regulations?¹⁰³
2. Does the board require periodic reviews of policies to confirm that they are consistent with the bank's strategic objectives, risk appetite, and regulatory requirements?
3. Has the board established a method to measure and monitor compliance with board-approved policies?
4. Assess the board's process to address instances when the bank is approaching or has breached a policy limit.

¹⁰³ For a list of the statutorily required policies and programs requiring board approval, refer to this booklet's appendix B.

Director Orientation and Education

Objective: To determine if the board has an education program that keeps its members apprised of major bank operations and industry trends.

1. Determine if the bank has an orientation and education program to provide training on the bank's business, risks, and operations, and to help directors stay apprised of industry trends and regulatory developments.
2. Determine if there is a process to periodically assess the skills and competencies of members and address any identified gaps.
3. For covered banks, has the board established and complied with a formal, continuous training program for all directors? (12 CFR 30, appendix D)
4. When appropriate, does the board engage outside advisors to gain technical expertise? If so, has it ensured that there is no conflict of interest that would prohibit the consultant from providing objective, independent advice?

Board Oversight

Objective: To determine if the board is fulfilling its responsibility to effectively supervise the affairs of the bank.

Corporate Culture

Objective: To determine if the board and management, in their respective roles, have established a sound corporate and risk culture.

1. What measures has the board taken to set the tone at the top?
2. Determine through discussions with management and employees if they are aware of the bank's risk culture, the parameters that they must operate in, and the steps that they should take if there is any breach of the bank's risk appetite and limits.
3. Has the board adopted a code of ethics and respective policies that set expected standards of behavior for all employees and directors?
4. How is adherence to the code of ethics monitored and managed?
5. Are consequences clearly communicated and consistently enforced for behaviors that contravene the bank's code of ethics?
6. Determine whether suspected fraud; illegal or unethical activities; and material risk issues are thoroughly and independently investigated by management and escalated to the board promptly.

7. Is there an ethics officer, bank counsel, or other individual from whom employees can seek advice for ethics questions?
8. Does the bank's internal auditor periodically assess the effectiveness of the bank's code of ethics program?

Board Committees

Objective: To determine if the board committees enable the board to carry out its oversight duties and responsibilities.

1. Has the board established a committee structure based on the bank's needs? Does each board committee have a charter?
2. Determine the level of involvement of directors based on a review of the committee meeting minutes.
3. Is director participation on various committees aligned with the directors' experience and expertise?
4. Are committee members periodically rotated to promote objectivity and different perspectives?
5. Read and brief the minutes of the board's annual organization meeting and list standing committees and their members. Some examples of committees a bank may have, depending on its size, scope of operations, risk profile, and board composition, include
 - executive committee.
 - audit committee (required by 12 CFR 363 for banks with assets over \$500 million).
 - credit committee.
 - asset-liability management committee.
 - risk committee.
 - fiduciary committee.
 - fiduciary audit committee (required by 12 CFR 9 (national banks) and 12 CFR 150 (FSAs) if trust powers are active).
 - compensation committee.
 - corporate governance/nominating committee.
6. Read and brief the minutes of the standing committees as well as ad hoc committees in their assigned areas, specifically noting whether each committee's mission, authority, and responsibilities are clear and followed.
7. Note major areas of operation that are not monitored by specific committees and determine if this information is communicated to the board.

Board Self-Assessments

Objective: To determine if the board periodically evaluates its performance.

1. Determine if the board conducts self-assessments. If so, has the board satisfactorily addressed any identified gaps or weaknesses to strengthen its effectiveness and oversight?
2. Determine whether the content of the assessment is linked to the board's charter and activities (i.e., roles and responsibilities)?
3. If the board does not perform a self-assessment, what other means does it use to evaluate its performance?

Risk Governance Framework

Objective: To determine if the board and management, in their respective roles, established a risk governance framework to manage the enterprise-wide risks.

1. Has management developed a risk governance framework commensurate with the sophistication of the bank's operations and business strategies? Has it been reviewed and approved by the board?
2. Does the risk governance framework cover all applicable risks of the bank?
3. Does the board require periodic independent assessments on the effectiveness of the risk governance framework or the components thereof?
4. For covered banks,
 - has IRM designed a written risk governance framework?
 - has the board or a board-level committee reviewed and approved the framework?
 - does IRM review and update the framework at least annually?
 - if the bank has adopted the parent company's risk governance framework, does it meet the standards established in 12 CFR 30, appendix D?

Risk Culture

Objective: To determine if the board and senior management have conveyed the bank's risk culture throughout the bank.

1. Determine how risk awareness is communicated throughout the bank.
2. Are the employees aware of consequences for excessive risk taking?

3. Are material risks and risk-taking activities that exceed the bank's risk appetite escalated and addressed by management or the board in a timely manner?

Risk Appetite

Objective: To determine if the board has established a risk appetite that aligns with the bank's strategic objectives, capital plans, and liquidity requirements.

1. Has the board established a risk appetite that articulates the aggregate level of risk and types of risk the board and management are willing to assume? Has it been formalized as a written risk appetite statement, when appropriate? Is it reviewed and updated periodically?
2. Has the risk appetite been communicated throughout the bank?
3. Have risk parameters and limits been established for specific business lines and for aggregate risks (including concentrations)?
4. If the bank approached or breached a risk limit, was the issue reported to the board or a board-level committee and senior management? Was a plan of action developed to address the risk-limit breach?
5. Has management established an escalation process that escalates weaknesses or problems to the board and senior management, when appropriate?
6. For covered banks,
 - does the bank have a written statement that articulates the bank's risk appetite?
 - does the board or risk committee review and approve the risk appetite statement at least annually?
 - does the statement include both quantitative limits and qualitative components?
 - is the risk appetite statement integrated and consistent with the overall strategy?
 - has IRM established enterprise policies that include concentration risk limits?

Risk Assessment

Objective: To determine if the bank has an effective risk assessment process to continuously identify current and emerging risks.

1. Does the bank prepare risk assessments on material activities at least annually?
2. Are risk assessments integrated into the bank's strategic planning process and risk management activities?
3. Do the risk assessments identify current risks and controls as well as new and emerging risks? Are the risk assessments candid and self-critical?

4. Are the assessments used to determine if actions need to be taken to strengthen risk management or reduce risk?

Risk Management System

Objective: To determine if the bank has adopted a risk management system commensurate with its size, complexity, and risk profile.

1. Does the structure of the risk management system allow for the bank's risks to be appropriately identified, measured, monitored, controlled, and reported to the board and senior management?
2. When appropriate, is there an IRM function that oversees the risk activities of the bank?
3. If there is not an IRM function, does the bank have sufficient management oversight of the bank's risk-taking activities, aggregate risks, and concentrations to confirm compliance with the bank's risk appetite?
4. If the bank does not have a CRE, has the board appointed a qualified individual or committee to oversee the bank's ERM program?
5. If the bank has adopted the three lines of defense,
 - is the first line of defense (frontline units or business units) accountable for assessing and managing the risk that the frontline units create?
 - has the first line of defense established internal controls that are consistent with the established risk appetite and risk limits?
 - has the first line of defense established controls for compliance with laws and regulations?
 - is the second line of defense (IRM) led by a CRE who has sufficient stature in the bank?
 - does the IRM function oversee risk-taking activities and assess risk independent of the frontline units?
 - is IRM monitoring compliance with the risk appetite and reporting findings to the board?
 - is IRM involved in management's key risk decisions?
 - is IRM identifying, measuring, monitoring, and controlling aggregate and emerging risk enterprise-wide?
 - is the third line of defense (internal audit) providing assurance on the effectiveness of the bank's risk management system?
6. For covered banks, determine compliance with 12 CFR 30, appendix D.
 - Does the risk governance framework include risk management roles and responsibilities for frontline units, IRM, and internal audit?

- Do the frontline units continuously assess the material risks associated with their activities?
 - Does IRM oversee the bank's risk-taking activities, assess risk and issues independent of frontline units, and identify and assess aggregate risks and concentrations across the bank?
 - Does internal audit ensure that the bank's risk governance framework complies with the guidelines?
 - Does internal audit maintain an inventory of the bank's material processes, product lines, services, and functions and assess the risk associated with each when developing the audit plan?
 - Does the board actively oversee the bank's risk-taking activities and hold management accountable for adhering to the risk governance framework?
 - Does the board conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the standards in section III of 12 CFR 30, appendix D?
7. Has the board or audit committee required a periodic independent assessment of the bank's overall risk governance framework and risk management practices? If so, was an opinion provided on the design and effectiveness of the framework?

Audit Program

Consult with the examiner assigned the audit review. For expanded examination procedures, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook*.

Objective: To determine the effectiveness of the board's oversight of the internal and external audit functions.

1. Based on the results of the examination of the bank's internal audit function, assess the adequacy of the function within the risk governance framework. Consider
 - independence of auditors, including reporting lines.
 - qualification of auditors.
 - adequacy and appropriateness of audit program.
 - degree and effectiveness of audit committee oversight.

Strategic Planning

Objective: To determine the effectiveness of the bank's strategic planning process.

1. Does the bank have a board-approved written strategic plan? If not, how are strategic objectives communicated throughout the bank?
2. Is the strategic plan aligned with the bank's risk appetite, capital plan, and liquidity requirements?

3. Does the bank have a strategic planning process that considers
 - an analysis of the bank's strengths, weaknesses, opportunities, and threats including regulatory, economic, competitive, and technological matters?
 - the bank's mission, goals, and measurable objectives?
 - assessment of risk associated with the strategies and whether they are in line with the bank's risk appetite?
 - the resources needed to achieve objectives, including technology requirements and constraints?
 - the contingency plans for significant unanticipated events?
 - the formality of the planning process based on the bank's size, complexity, and risk profile?
4. When the bank has engaged in merger or acquisition activities, has the bank performed a retrospective review of the merger that considered, at a minimum, the effect on
 - financial performance (sales, costs, etc.)?
 - accounting?
 - IT infrastructure (system integration, capacity, etc.)?
 - human resources?
5. Determine whether the long-term (strategic) plan provides the framework for developing short-term (operating) plans.
6. Determine how management verifies compatibility between the short-term and long-term plans by considering the
 - annual financial plan and budget.
 - capital plan.
 - asset-liability plan.
 - marketing plan.
 - fixed-asset plan.
7. Determine whether management weighs the effects of plans on its operations. Consider
 - risk.
 - regulatory requirements.
 - financial condition of the bank.
 - management ability and human resource demands.
 - physical facilities.
 - adequacy of MIS and operating systems to handle growth.
 - current product mix and future product development.
 - technological environment.
 - public perception.

8. Determine if the bank has monitoring and reporting routines to determine the bank's progress in achieving its strategic objectives. Consider

- frequency and method of evaluation.
- CEO and board of director involvement.
- accountability of managers to implement plans and achieve objectives.
- if there is a system in place to make changes.
- if there is a system in place to report on progress toward goals.
- flexibility in the plan to allow for contingencies or changes.

9. For covered banks, does the strategic plan cover, at a minimum, a three-year period and comply with the standards in section II of 12 CFR 30, appendix D?

New Activities

Objective: To determine the adequacy of the bank's risk management system to identify, measure, monitor, report, and control risks when developing and implementing new activities. Refer to OCC Bulletin 2017-43 for more information.

1. Determine the adequacy of the bank's due diligence and approval process for new activities. Due diligence should allow management to fully understand the risks and benefits before implementing new activities. Management should inform the board of all material new activities, including due diligence findings and plans that clearly articulate and appropriately manage risks and returns. The board or a delegated board committee should consider whether new activities are consistent with the bank's strategic goals and risk appetite. Consider whether due diligence includes

- identifying the customer demand for the proposed new activities. Consider the types of market research the bank uses, such as surveys, focus groups, and outside services.
- assessing whether the risks associated with the proposed new activities are consistent with the bank's strategic plan, risk profile, and risk appetite.
- assessing how the new activity affects the bank's current and projected capital position.
- consulting with relevant functional areas, which include credit, asset management, payments, compliance, accounting, audit, independent risk management, legal, operations, IT, information security, marketing, and the treasury/asset liability committee, to identify risks, concerns, and necessary controls.
- determining the requirements of applicable laws and regulations and considering the principles set forth in agency guidance.
- identifying potential conflicts of interest, actual or perceived.
- assessing potential negative effect on the bank's reputation.
- appropriately protecting any intellectual property rights.
- determining the expertise needed to effectively manage the new activities, including the possible need to hire or otherwise acquire additional expertise.

- determining the operational infrastructure requirements to support the new activities, including controls and technology architecture.
 - conducting appropriate research and analysis on relevant third-party service providers.
 - developing a business and financial plan that includes
 - expected costs.
 - sales revenue targets.
 - an assessment of the bank's competitive position if the bank engages in the new activities.
 - objectives and strategies for how the new activities will be brought to market.
 - consideration of fair access to financial services and fair treatment of customers in all aspects related to the new activities.
 - performance or risk metrics that signal the need to pursue an exit strategy.
 - viable alternatives, including an exit strategy, in case the new activities fail to perform as expected
2. Assess whether management has established appropriate policies, processes, and control systems for new activities. Consider whether
- policies and procedures outline the processes, roles, and responsibilities for implementation and adherence to an adequate risk management system for new activities.
 - management expands or amends, as appropriate, existing policies and procedures to adequately address the new activities. Do policies and procedures identify key business lines, establish management's responsibility for monitoring the process, and provide for exception reporting?
 - management develops and deploys MIS as necessary to monitor adherence to established objectives and to properly evaluate the new activities, and, if warranted, effectuate a timely response.
 - new activities are incorporated into the bank's independent risk management, CMS, and audit processes to verify adherence to bank policies and procedures and customer safeguards.
 - the bank has adequate third-party risk management policies and procedures in place, when applicable.
3. Assess the effectiveness of change management processes to manage and control the implementation of new or modified operational processes, as well as the addition of new technologies into the bank's existing technology architecture. Consider whether change management processes include
- reviews by appropriate risk management, line managers, and senior managers in applicable business units (such as lending, finance, treasury, deposits, payments, compliance, audit, legal, technology, and information security) before implementing the new or modified operational process.
 - proper testing of new or modified operational systems, processes, and technology.

- risk parameters and exception reporting that have been approved by appropriate management.
- mechanisms for confirming that delivery to customers occurs as intended.
- an exit strategy that identifies and limits the adverse effect to the bank and its customers in the event of a failed or flawed implementation.
- employee training in the new or modified operational process associated with the new activities.

4. Assess the bank's performance and monitoring systems for new activities. Consider whether such systems

- include limits on the size of risk exposure that management and the board are willing to accept with the addition of new activities.
- identify specific objectives and performance criteria to evaluate whether the new activities are successful, including processes to periodically compare actual results with projections, and quantitative and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner.
- include processes to periodically test the effectiveness of operational controls and safeguards.
- include periodic testing to ensure compliance with applicable laws, regulatory requirements, and the bank's policies and procedures. This should include consideration of potential risks for unfair or deceptive acts or practices.
- trigger changes in the business plan for the activities, based on performance results, including an exit strategy for activities that fail to achieve projections.

Capital Planning

Consult with the examiner assigned to review the capital component area. For examination procedures, refer to the "Capital and Dividends" booklet of the *Comptroller's Handbook*.

Recovery Planning

For examination procedures, refer to the "Recovery Planning" booklet of the *Comptroller's Handbook*. These procedures only apply to covered banks subject to 12 CFR 30, appendix E.

Operational Planning

Objective: To determine the adequacy of the bank's operational plans that translate long-term strategic objectives and goals into measureable targets.

1. Determine what operational plans are in place. Consider

- budgets.
- marketing plans.

- staffing plans.
 - contingency plans.
2. Assess the formality of the operational planning process to determine whether it is commensurate with the bank's size, complexity, and risk profile.
 3. Confirm that operational plans are board-approved and are periodically reviewed and updated.
 4. Determine the adequacy of operational plans. Consider whether plans
 - are consistent with the bank's risk appetite and strategic plan.
 - adequately translate long-term strategic objectives and goals into measurable targets.

Disaster Recovery and Business Continuity Planning

Consult with the examiner assigned to review the IT component area. For examination procedures, refer to the "Business Continuity Planning" booklet of the *FFIEC IT Examination Handbook*.

IT and Information Security

Consult with the examiner assigned the IT component area to assess the bank's IT infrastructure. For examination procedures, refer to the "Information Security" and other booklets of the *FFIEC IT Examination Handbook*.

Management Selection, Retention, and Oversight

Objective: To determine whether the directors have accepted their responsibility for selecting and retaining competent management.

1. Determine if the board has defined specific selection criteria, including experience, expertise, and personal character, for the CEO selection process.
2. Determine how the board assesses senior management's performance. Has the board adopted a performance appraisal process for the CEO and other key executives?
3. Determine whether the board or a committee thereof reviews the CEO's performance at least annually. If so, review the criteria considered for reasonableness. Evaluation criteria may include
 - the bank's record of compliance with laws and regulations.
 - weaknesses contained in audit and examination reports, and their resolution.
 - management's responsiveness to board directives, including compliance with board-approved policies.
 - the timeliness, quality, and accuracy of management's recommendations and reports.

- management's presentations to the board.
4. Determine if the board or a committee thereof reviews the performance of key management members at least annually. Coordinate the assessment of such performance reviews with the EIC and the examiner assigned to the management component rating in CAMELS.
 5. Determine if a board-approved management succession policy exists to address the loss of the CEO and other key executives.
 6. Discuss planned changes to management positions with the EIC and appropriate bank officials. Determine the rationale for changes.
 7. If vacancies exist in senior-level management positions, determine if, when, and how the vacancies will be filled. Also determine the board's criteria to fill those vacancies.
 8. Obtain a copy of any management contracts. Brief the pertinent points and determine whether the bank has had appropriate legal review of the contracts and whether any terms would result in unsafe or unsound practices.
 9. For FSAs, determine whether the board annually reviews and approves all employment contracts and compensation arrangements for senior officers and directors.
(12 CFR 163.39)
 10. Determine the reasonableness of compensation of executive officers, how compensation is determined, and who makes decisions concerning executive salaries. (12 CFR 30, appendix A)
 11. Note any titled individual who, by action of the board or by the bylaws, is specifically excluded from being an executive officer. (12 CFR 31 and 12 CFR 215.2(e)) Be alert for any policymaking decisions made by any titled officer specifically excluded from being an executive officer.
 12. Is succession planning regularly discussed at board or board committee meetings?
 13. For covered banks, has the board or board committee reviewed and approved a written talent management program for the CEO, CAE, and CRE; their direct reports; and other potential successors?

Compensation and Benefits Programs

Objective: To determine if compensation and benefits programs are prudent and comply with applicable laws and regulations.

1. Obtain a list of the compensation and benefits of senior management and the board.

2. Determine the reasonableness of the compensation and benefits of senior management and the board given the financial condition and risk profile of the bank.
3. Determine whether appropriate internal controls are in place for employee benefits and are functioning as designed. Complete the internal control questionnaire (ICQ) in this booklet, if necessary to make this determination.
4. Has the board confirmed that compensation practices for directors, executive officers, employees, and principal shareholders are reasonable, are consistent with regulatory guidelines (12 CFR 30, appendix A), and comply with applicable regulations (e.g., 12 CFR 359 and 12 CFR 1026.36 (national banks and FSAs), and 12 CFR 163.39(a) (FSAs))?
5. Does the board oversee and set the compensation of the CEO and other executive-level officers? If so, is the board
 - evaluating employment contracts?
 - periodically assessing the reasonableness of the compensation structure and components, including various benefits and perks related to retirement, termination, and change in control?
 - evaluating executive performance relative to board-established goals and objectives?
6. Determine the degree to which incentive compensation arrangements are used.
7. If incentive compensation arrangements are in place, select a sample and assess the following:
 - Incentives appropriately balance risk and reward.
 - Compensation is compatible with the bank's controls and risk management.
 - Oversight of incentive compensation arrangements is supported by strong corporate governance, including active oversight by the board.
8. Does the bank have risk management practices for benefits administration that safeguard against regulatory fines and lawsuits?
9. Verify that the board oversees the cost and scope of employee benefits and management's role in the administration of benefits.
10. If the benefits administration is outsourced, does management provide oversight to the function to confirm compliance with applicable laws and regulations?
11. If the bank offers a group health plan or retirement plan, assess whether a process is in place to meet the bank's fiduciary responsibilities under the Employee Retirement Income Security Act of 1974 (29 USC 1001 et seq.).

12. Determine if internal audit periodically reviews the bank's compensation and benefits programs.

Financial Performance

Objective: To determine if the board has accepted its responsibility to oversee business performance.

1. Review the board-level financial performance and key risk reports to determine the adequacy of information to assist in decision making and for oversight and monitoring purposes.
2. Determine if the board reports
 - are appropriate for the bank's size, complexity, and risk.
 - enable the board to understand key drivers of financial performance.
 - assess the adequacy of capital, liquidity, and earnings, and monitor trends.
 - compare financial performance with strategic objectives.
 - monitor risk exposure compared with the bank's risk appetite.
 - disclose model risks and reliance.
 - highlight risks related to technologies and market conditions.
 - inform the board of potential litigation costs.
3. Determine if the board compares the bank's performance with that of its peers and, if so, how that comparison is used.

Corporate Structure and Affiliate Relationships

Objective: To determine if the board maintains appropriate affiliate and holding company relationships.

1. Assess whether the bank maintains sufficient independence in its relationships with its parent company and other related organizations so that the bank's interests are adequately protected and not subordinate to those of the related organizations. For examination procedures for national banks, refer to the "Related Organizations" booklet of the *Comptroller's Handbook*. For FSAs, refer to section 730, "Related Organizations," of the *OTS Examination Handbook*.

Community Reinvestment Act

Objective: To determine if the board understands management's involvement in the community and assessed the bank's efforts toward meeting the credit needs of the bank's communities.

1. Discuss the bank's CRA efforts with the examiner conducting the CRA evaluation and the EIC. If a CRA evaluation is not being done concurrently, discuss the bank's efforts with the President or CEO and review the following information:
 - Current CRA public file.
 - Most recent CRA performance evaluation.
 - Information contained in the OCC database (i.e., community contacts and community group protests).
2. Have the board and management, in their respective roles, assessed how the bank is helping to meet the credit needs of its community as part of the strategic planning process?

Policies

Objective: To determine if management has developed adequate policies for all significant areas of the bank.

1. Determine the adequacy of the policymaking process, taking into account
 - regulatory requirements.
 - risks and risk appetite.
 - strategic, operating, and capital plans and liquidity requirements.
 - the bank's condition.
 - differences between planned goals and current conditions.
 - the process to review, update, and revise policies.
2. Obtain or update a list of all board-approved policies and verify that they cover the significant activities and risks of the bank.
3. Determine how management verifies that adopted policies are followed and that exceptions are documented.
4. Determine if policies are appropriate and consistent with the bank's strategic objectives and risk appetite. (Some testing may be necessary to complete this procedure.) This should be done in conjunction with the examiners reviewing each area of the bank.
5. Verify that policies assign accountability and are communicated to appropriate personnel.
6. Review findings from examination work papers or in discussion with other examiners to determine the overall adequacy of the bank's policymaking process.

Processes

Objective: To determine the adequacy of bank operating procedures, programs, and practices.

1. Confer with the EIC and other examiners to determine the adequacy of the bank's procedures, programs, and practices regarding their areas of review. Consider whether
 - procedures are in place for key policies.
 - procedures are communicated to appropriate personnel and made readily available for reference.
 - procedures are periodically reviewed and updated to reflect current practices.
 - appropriate programs are in place to manage key banking activities and risks.
 - bank practices are in line with
 - strategic goals and objectives.
 - risk appetite.
 - laws and regulations.
 - policies.

Personnel

Objective: To determine the skills and qualifications of personnel to fulfill duties and determine if management provides adequate oversight of personnel activities.

1. Determine if the bank has written job descriptions and responsibilities that are clear and reflect assigned duties. Consider the
 - appropriateness of the required knowledge and skills.
 - basis for performance appraisals.
 - method used to develop or oversee the job description process.
 - relationship to compensation program.
2. Assess how management determines that the bank has adequate staff at all levels. Consider
 - recruitment methods.
 - performance standards.
 - training programs.
 - management succession plans.
 - compensation programs.
 - employee benefits.
3. Determine how management assesses employees' performance.
4. Determine how management verifies that salaries and benefits are equitable and competitive.
5. Determine how management promotes effective communication, including the following venues:

- Staff meetings.
- Employee interviews.
- Employee handbooks, bulletins, etc.
- Memorandums, e-mails, and other communications to employees.

Control Systems

Objective: To determine if management has established effective control functions to fulfill its responsibilities and comply with laws and regulations.

1. Determine the control functions that management uses to measure performance, make decisions about risk, and assess the effectiveness of processes, including
 - quality assurance and quality control.
 - audit.
 - risk reviews (including loan review).
 - compliance management.
2. In consultation with the examiner assigned to the audit review, determine if internal and external audit evaluate whether
 - the board and management, in their respective roles, review insider transactions for compliance with laws, regulations, and policies, as well as look for suspicious activity.
 - management takes timely corrective action to address deficiencies noted by the regulatory examination, audit, compliance, or internal loan review functions.
3. Determine the extent to which management is involved in control functions. Consider
 - adequacy, timeliness, and distribution of various reports.
 - periodic review to determine adherence to policies and procedures.
4. Determine the process used by management to confirm that internal controls function properly. Consider
 - sources and accuracy of information.
 - review of internal controls when changes in operations occur.
 - stakeholders involved in the development of new products or changes in operations (audit, IRM, legal, and compliance).
 - training of personnel regarding the bank's policies and procedures.
 - efforts made by directors and managers to correct deficiencies.
5. Determine what quality control activities, if any, the bank performs and assess the effectiveness of the reviews. Consider

- industry standards.
 - risk exposures of activities.
 - independence of personnel performing review.
 - timing of the review.
 - results of quality control reports and how they are used to improve risk management.
6. Determine what quality assurance activities, if any, the bank performs and assess the effectiveness of the reviews. Consider
- industry standards.
 - risk exposures of activities.
 - independence of personnel performing review.
 - timing of the review.
 - results of quality assurance reports and how they are used to improve risk management.

Management Information Systems

Objective: To determine if MIS policies or practices, processes, objectives, and internal controls are adequate.

Note: IT examiner support should be considered to enhance the depth of coverage for the MIS review if there are known MIS issues or deficiencies that represent an undue level of risk or if MIS activities are particularly complex or sophisticated.

1. Evaluate if MIS applications provide the board and management with timely, accurate, consistent, complete, and relevant information.
2. In consultation with the examiners reviewing their assigned areas, determine management's knowledge of information systems and the use of data for decision making.
3. Assess the types and level of risk associated with MIS and the quality of controls over those risks.
4. Determine whether appropriate internal controls are in place for MIS and functioning as designed. Complete the ICQ in this booklet, if necessary, to make this determination.
5. Determine if MIS applications and enhancements to existing systems adequately support corporate and strategic goals.
6. Determine if MIS is being developed in compliance with an approved MIS policy.
7. Determine if management is committed to providing the resources needed to develop the required MIS.

8. For covered banks, determine if the bank has policies, procedures, and processes in place for risk data aggregation and reporting capabilities.
9. If substantive safety and soundness concerns remain unresolved regarding the bank's MIS that may have a material adverse effect on the bank, further expand the scope of the examination by completing verification procedures.

Compliance Management

Consult with the examiners assigned to the consumer compliance and BSA/AML reviews when assessing the effectiveness of the bank's compliance management program. For expanded examination procedures regarding the bank's program for compliance with consumer protection-related laws and regulations, refer to the "Compliance Management Systems" booklet of the *Comptroller's Handbook*.

Objective: To determine the effectiveness of the bank's CMS.

1. Confirm that the CMS consists of a compliance program (policies and procedures) as well as a compliance audit function. This includes a BSA compliance program.

Note: Refer to the *FFIEC BSA/AML Examination Manual* for procedures to evaluate the BSA/AML compliance program.

2. Determine if the board or management has appointed a compliance officer or equivalent who has the authority and stature to effectively manage the compliance function.
3. Have the compliance officer's duties and responsibilities been established and clearly communicated? Responsibilities may include
 - developing a process to identify and stay apprised of all applicable laws and regulations.
 - overseeing and maintaining the inventory of all laws and regulations applicable to the bank and its related organizations.
 - implementing appropriate change management to identify systems, processes, and procedures that are affected by laws and regulation changes.
 - overseeing the establishment of compliance monitoring and testing programs and confirming their adequacy.
 - developing and overseeing metrics for continuous compliance monitoring.
 - overseeing training on all relevant compliance issues.
4. Does the bank's CMS extend beyond consumer protection laws and regulations to include all applicable laws and regulations, prudent ethical standards, and contractual obligations?
5. Is there evidence that the board places a high priority on compliance with laws and regulations? If so, is it communicated throughout the bank?

6. Does the board confirm timely correction and hold management accountable for noncompliance with laws and regulations?

BSA/AML Program

Consult with the examiner assigned the BSA/AML review. Refer to the *FFIEC BSA/AML Examination Manual* for procedures to evaluate the BSA/AML compliance program.

Third-Party Risk Management

Refer to OCC Bulletin 2017-7, “Third-Party Relationships: Supplemental Examination Procedures,” for procedures to evaluate third-party risk management.

Insurance

Objective: To determine the effectiveness of the bank’s risk transference indemnification and insurance.

1. Determine whether the bank has a designated risk manager who is responsible for loss control. If not, determine who handles the risk management and insurance function.
2. Determine whether appropriate internal controls are in place and function as designed for indemnification and insurance. Complete the ICQ in this booklet, if necessary, to make this determination.
3. Determine whether the board has established appropriate maximum guidelines for risk retention.
4. Obtain the bank’s schedule of insurance policies in place. If the bank does not maintain a schedule, ask management to create a schedule of existing insurance coverage.
5. Using the insurance schedule prepared by the bank, determine whether coverage conforms to the guidelines for maximum loss exposure established by the board. The summary should include
 - coverage provided, detailing major exclusions.
 - underwriter.
 - deductible amount.
 - upper limit.
 - term of the policy.
 - date premiums are due.
 - premium amount.
6. Determine whether insurance coverage provides adequate protection for the bank.

Conclusions

Conclusion: Corporate and risk governance practices are (strong, satisfactory, insufficient, or weak).

Objective: To determine, document, and communicate overall findings and conclusions regarding the examination of corporate and risk governance.

1. Determine preliminary examination findings and conclusions and discuss them with the EIC.

- Quantity of associated risks (as noted in the “Introduction” section of this booklet)
- Quality of risk management
- Aggregate level and direction of associated risks
- Overall risk in corporate and risk governance
- Violations and other concerns

Summary of Risks Associated With Corporate and Risk Governance				
Risk category	Quantity of risk	Quality of risk management	Aggregate level of risk	Direction of risk
	(Low, moderate, high)	(Weak, insufficient, satisfactory, strong)	(Low, moderate, high)	(Increasing, stable, decreasing)
Operational				
Compliance				
Strategic				
Reputation				

2. Discuss examination findings with bank management, including violations, deficient practices, and conclusions about the corporate and risk governance structure and practices. If necessary, obtain commitments for corrective action.
3. Compose conclusion comments, highlighting any issues that should be included in the report of examination. If necessary, compose matters requiring attention and violation write-ups.
4. Update the OCC’s supervisory information systems and any applicable report of examination schedules or tables.
5. Document recommendations for the supervisory strategy (e.g., what the OCC should do to effectively supervise corporate and risk governance in the bank, including time periods, staffing, and workdays required).

6. Update, organize, and reference work papers in accordance with OCC policy.
7. Appropriately dispose of or secure any paper or electronic media that contain sensitive bank or customer information.

Internal Control Questionnaire

An ICQ helps an examiner assess a bank's internal controls for an area. ICQs typically address standard controls that provide day-to-day protection of bank assets and financial records. The examiner decides the extent to which it is necessary to complete or update ICQs during examination planning or after reviewing the findings and conclusions of the core assessment.

Employee Benefits

1. Are directors or a designated committee informed at least annually of important matters relating to employee benefits, such as costs and administration problems, which would assist them in formulating any changes or modifications deemed desirable or necessary?
2. Have employee benefit plans been reviewed by bank counsel for consistency with all applicable requirements before implementation?
3. Does the bank compare its program of employee benefits with those of other banks in its peer group, and, if so, is an analysis of that comparison included in a report to the board at least annually?
4. Have all employee benefits programs currently in effect received proper board approval before the plans' inception, with appropriate documentation in the minutes?
5. Have procedures been established to confirm that all expenses related to employee benefits are correctly identified in accordance with the call report instructions and generally accepted accounting principles?
6. Are procedures in effect that call for periodic independent determinations that those individuals receiving benefits from the bank are eligible?
7. Are economies sought through the use of "standard benefits packages" that can be more efficiently administered by a bank trust department, an insurance firm, or other specialists in the industry?
8. When administration of an employee benefit plan is being handled by a third party, has the bank retained the managerial or final decision-making function about types and amounts of investments?
9. Are detailed and timely reports received that enable the bank to accurately monitor the plan?
10. Are officers and employees in sensitive positions, including personnel who have direct or indirect control of bank general ledger accounts, required to be absent for at least two consecutive weeks each year?

Conclusion

1. Is this information adequate for evaluating internal controls in that there are no significant additional internal auditing procedures, accounting controls, administrative controls, or other circumstances that impair any controls or mitigate any weaknesses noted above (explain negative answers briefly, and indicate conclusions as to their effect on specific examination procedures)?
2. Based on answers to the foregoing questions, internal control for employee benefits is considered (strong, satisfactory, insufficient, or weak).

Management Information Systems

Policies or Processes

1. Has management developed and maintained MIS policies and processes?
2. Do policies and processes provide guidance in the following areas:
 - The definition, purpose, and fundamental components of MIS?
 - How to achieve effective two-way communication between management and employees and specific avenues to maintain such communication?
 - Processes for initiating, developing, and completing MIS enhancements?
 - Guidelines for installing MIS enhancements in a controlled change environment?
 - Procedures for acquiring, merging, manipulating, and uploading data to other systems?
 - Guidance for delineating the need for internal/external audit coverage and testing?
3. Are policies and processes reviewed and updated regularly?
4. Are policies and written processes distributed to appropriate employees?
5. Do policies and processes incorporate or require
 - user approval for each phase of development?
 - installation of MIS enhancements in a controlled change environment?
 - employees to follow the policy and established processes as data are acquired, merged, manipulated, and uploaded to other systems?
 - employees to be sufficiently trained for new systems and subsequent enhancements?

Development

1. Does the internal planning process consider and incorporate the importance of MIS at both the strategic and tactical level?

- Are longer-term strategic goals (beyond two years) supported by the development of appropriate MIS?
 - Are shorter-term tactical goals over the immediate one- to two-year period regularly and appropriately reviewed and monitored by management?
2. Do project objectives address reported MIS weaknesses and meet business unit requirements?
 3. Does management have a process for monitoring project schedules?
 4. Does management use a project management technique to monitor MIS development schedules?
 5. Does the bank use a consistent and standardized approach or a structured methodology for MIS projects?
 6. Does the methodology encompass the following phases:
 - Analysis of the concept, organization of tasks, completions of phases, and approvals?
 - Development of the program and contracting for equipment and software?
 - Development of user manuals and testing of the system?
 - Post-review of the system and future maintenance of it?

User Training and Instructions

1. Are MIS user manuals meaningful, easy to understand, and current?
2. Do user manual requirements include the following information:
 - A brief description of the application or system?
 - Input instructions, including collection points and times to send updated information?
 - Balancing and reconciliation instructions?
 - A full listing of output reports, including samples?

Communication

1. Does management encourage communication lines to meet the following objectives:
 - To effectively link senior management, other appropriate users, and information systems employees?
 - To promote effective two-way communication between management and employees?
 - To document the MIS process?

Audit

1. Have MIS been audited according to bank's audit schedule?
 - If not, meet with audit management to determine what its plans are regarding an audit of MIS.

Conclusion

1. Is this information adequate for evaluating internal controls of MIS activities? This question presumes that there are no additional significant internal auditing procedures, accounting controls, administrative controls, or other circumstances that impair any controls or mitigate any weaknesses noted above. (**Note:** Explain negative answers briefly, and indicate conclusions as to their effect on specific examination or verification procedures.)
2. Based on answers to the previous questions, internal control for MIS is considered to be (strong, satisfactory, insufficient, or weak).

Insurance

1. Does the bank have established insurance guidelines that provide for
 - a reasonably frequent, at least annual, determination of risks the bank should assume or transfer?
 - periodic appraisals of major fixed assets to be insured?
 - a credit or financial analysis of the insurance companies that have issued policies to the bank?
2. Has management established operating procedures for filing fidelity bond claims that include
 - taking prompt action when fraudulent activity is suspected to avoid further losses after what may later be regarded by the insurer as the date of discovery?
 - considering obtaining the advice and assistance of legal counsel, consultants, or accountants in filing claims?
 - ensuring adherence with insurance policy filing and notification requirements?
 - allocating human and monetary resources as warranted by the significance of the claim?
 - conducting adequate monitoring and follow-up after the claim is filed?
3. Does the bank have a risk manager who is responsible for risk control?
4. Does the bank use the services of an insurance agent or broker to assist in selecting and providing advice on alternative means of providing insurance coverage?

5. Does the bank's security officer coordinate his or her activities with the person responsible for handling the risk management function?
6. Does the bank maintain a schedule of existing insurance coverage?
7. Does the bank maintain records, by type of risk, to facilitate an analysis of the bank's experience in costs, claims, losses, and settlements under the various insurance policies in force?
8. Is a complete schedule of insurance coverage presented to the board, at least annually, for its review?

Conclusion

1. Is this information adequate for evaluating internal controls in that there are no significant additional internal auditing procedures, accounting controls, administrative controls, or other circumstances that impair any controls or mitigate any weaknesses noted above (explain negative answers briefly, and indicate conclusions as to their effect on specific examination procedures)?
2. Based on answers to the foregoing questions, internal control for indemnification and insurance is considered (strong, satisfactory, insufficient, or weak).

Verification Procedures

Verification procedures are used to verify the existence of assets and liabilities, or test the reliability of financial records. Examiners generally do not perform verification procedures as part of a typical examination. Rather, verification procedures are performed when substantive safety and soundness concerns are identified that are not mitigated by the bank's risk management systems and internal controls.

Management Information Systems

1. Using an appropriate sampling technique, select an additional MIS project(s) from the bank's development plan.
 - Review project objectives, and determine if they address reported MIS weaknesses and meet business unit plans.
 - Determine whether the MIS project(s) follow an approved and implemented development methodology that encompass the following phases:
 - Analysis of system alternatives, organization of tasks, and approval of phases by system users and owners.
 - Program development and contracts for equipment and software vendors.
 - Development of user instructions and testing the system changes.
 - Installation and maintenance of the system.
2. Using the expanded sample, check copies of relevant user instructions. Verify whether the guidelines are meaningful, easy to understand, and current.
3. Test whether user manuals provide adequate guidelines in the following areas:
 - Complete description of the system and how to use it.
 - Input instructions, including collection points and times to send updated information.
 - Reconciliation instructions.
 - Full listing of output reports, including sample formats.
4. Obtain workflows from the user manuals or managers showing data from the point-of-entry, through user processes, to final product.
 - Test the processes with users to determine if they know where the data are coming from, where data are going, and how data get there.
 - Identify the points in which data adjustments occur, if applicable.
 - Identify the individuals accountable for contributing to data and reports. Compare information with the material acquired in the step immediately preceding this step.
 - Test the preparation and reconciliation processes to verify the integrity of information.
 - Determine if data adjustments are adequately documented, if applicable.

5. Expand the sample by interviewing additional managers and experienced unit employees to determine their perceptions of MIS.
 - Discuss MIS elements of timeliness, accuracy, consistency, completeness, and relevancy.
 - Determine if the employees hold any significant perceptions that the MIS are ineffective.
6. If available, obtain samples of key senior management reports for the targeted MIS area(s). Test the following areas to determine if
 - information originates from the expected business unit.
 - users of the information are the employees one would expect and the data are being used for the correct purposes.
 - the reports are distributed to the appropriate users.
7. Review a sample of audit work papers relating to reports that disclosed material MIS weaknesses, if applicable.
 - Review documents to determine if auditors tested MIS activities against policies or practices and processes.
 - Test to determine if documented findings support the audit scope and report findings.

Appendices

Appendix A: Board of Directors Statutory and Regulatory Requirements

National banks and FSAs are subject to certain statutory and regulatory requirements governing size, composition, and other aspects of the board and the directors. The following table highlights these requirements but does not intend to be all-inclusive, nor is it meant to be an authoritative restatement of the regulations. The regulations are subject to updates and revisions.

Table 1: Statutory and Regulatory Requirements

National banks	FSAs
Citizenship	
All national bank directors must be U.S. citizens. The OCC may waive the citizenship requirement for a minority of the total number of directors. ¹⁰⁴	No similar statutory or regulatory requirement.
Residency	
A majority of directors must reside in the state where the national bank is located (i.e., the state where the national bank has its main office or branches) or within 100 miles of the bank's main office for at least one year immediately preceding the election and must be a resident of the state or within 100 miles of the state. ¹⁰⁵	No similar statutory or regulatory requirement.
Conflicts of interest	
Although national bank directors and officers are not subject to a regulation regarding conflicts of interest, they have a fiduciary responsibility to the national bank. In addition, the common law duty of loyalty requires directors and management to act in the best interest of the national bank and to ensure insiders do not abuse their position by benefiting personally at the national bank's expense.	Directors, officers, or persons having the power to direct an FSA's management or policies or who otherwise owe a fiduciary duty to an FSA are prohibited from advancing their own personal or business interests at the expense of the FSA. Also, he or she must follow certain requirements when he or she has an interest in a matter before the board. ¹⁰⁶
Usurpation of corporate opportunity	
Although national bank directors and officers are not subject to a regulation regarding usurpation of corporate opportunity, they owe a common law fiduciary duty of loyalty to the bank. The usurpation of corporate opportunity doctrine, a part of the duty of loyalty, prevents insiders from improperly taking business opportunities away from the bank.	Directors, officers, or persons having the power to direct an FSA's management or policies or who otherwise owe a fiduciary duty to an FSA must not take advantage of corporate opportunities belonging to the FSA. The OCC will not deem a person to have taken advantage of a corporate opportunity belonging to the FSA if a disinterested and

¹⁰⁴ For more information, refer to 12 USC 72, "Qualifications."

¹⁰⁵ Ibid.

¹⁰⁶ For more information, refer to 12 CFR 163.200.

National banks	FSAs
	independent majority of the board, after receiving a full and fair presentation of the matter, rejected the opportunity as a matter of sound business judgment. ¹⁰⁷
Attorney	
No similar prohibition.	Not more than one director may be an attorney with a particular law firm. ¹⁰⁸
Stock interest	
A national bank director must own a qualifying equity interest in a national bank or a company that has control of the national bank. A minimum qualifying equity interest is common or preferred stock that has not less than an aggregate par value of \$1,000, an aggregate shareholder's equity of \$1,000, or an aggregate fair market value of \$1,000. ¹⁰⁹	A director of a stock FSA need not be a stockholder of the FSA unless the bylaws so require. ¹¹⁰ A director of a mutual FSA is required to be a member of the FSA. ¹¹¹
President as director	
The president (but not the CEO) of the national bank is required to be a member of the board. The board may elect a director other than the president to be chair of the board. ¹¹²	No similar statutory or regulatory requirement. Certain FSAs have bylaws, however, that require the president or CEO to be a member of the board.
Number of directors	
The number of directors of each national bank is authorized by the bylaws and limited to not less than five or more than 25, unless the OCC exempts the national bank from the 25 limit. The OCC may appoint a receiver for a national bank with fewer than five directors. ¹¹³	The number of directors of each FSA is authorized by the bylaws and limited to not fewer than five or more than 15, unless otherwise approved by the OCC. ¹¹⁴

¹⁰⁷ For more information, refer to 12 CFR 163.201.

¹⁰⁸ For more information, refer to 12 CFR 163.33, “Directors, Officers, and Employees.”

¹⁰⁹ For more information, refer to 12 USC 72, and 12 CFR 7.2005.

¹¹⁰ For more information, refer to 12 CFR 5.22(l)(1), “General Powers and Duties.”

¹¹¹ For more information, refer to 12 CFR 5.21(j)(2)(viii), “Number of Directors, Membership.”

¹¹² For more information, refer to 12 USC 76, “President of Bank as Member of Board; Chairman of Board,” and 12 CFR 7.2012, “President as Director; Chief Executive Officer.”

¹¹³ For more information, refer to 12 USC 71a, “Number of Directors; Penalties”; 12 USC 191, “Appointment of Receiver for a National Bank”; and 12 CFR 7.2024, “Staggered Terms for National Bank Directors and Size of Bank Board.”

¹¹⁴ For more information, refer to 12 CFR 5.22(l)(2), “Number and Term,” for stock associations and 12 CFR 5.21(j)(2)(viii) for mutual associations.

National banks	FSAs
Family	
No similar prohibition.	Not more than two of the directors may be members of the same immediate family. ¹¹⁵
Officers or employees	
No similar statutory or regulatory requirement.	A majority of the directors must not be salaried officers or employees of the FSA or any subsidiary. ¹¹⁶
Term limits	
Any national bank director may hold office for a term that does not exceed three years and until his or her successor is elected and qualified. Any national bank may adopt bylaws that provide for staggering the terms of its directors. National banks shall provide the OCC with copies of any bylaws so amended. ¹¹⁷	Directors shall be elected for a term of one to three years and until their successors are elected and qualified. If a staggered board is chosen, the directors shall be divided into two or three classes as nearly equal in number as possible, and one class shall be elected by ballot annually. ¹¹⁸
Committee member requirements	
Refer to the "Establish and Maintain an Appropriate Board Structure" section and appendix C of this booklet.	Refer to the "Establish and Maintain an Appropriate Board Structure" section and appendix C of this booklet.

¹¹⁵ For more information, refer to 12 CFR 163.33.

¹¹⁶ Ibid.

¹¹⁷ For more information, refer to 12 USC 71, "Election," and 12 CFR 7.2024.

¹¹⁸ For more information, refer to 12 CFR 5.22(l)(2) for stock associations and 12 CFR 5.21(j)(2)(viii) for mutual associations.

Appendix B: Regulations Requiring Board Approval for Policies and Programs

The board must approve and oversee management's implementation of written policies and certain programs and practices. The following table does not intend to be all-inclusive, nor is it meant to be an authoritative restatement of the regulations. The regulations are subject to updates and revisions.

Table 2: Regulatory Requirements

Policy	National banks and FSAs	National banks only	FSAs only
BSA compliance program	The board must approve the BSA compliance program, which establishes and maintains procedures reasonably designed to assure and monitor compliance with BSA requirements. ¹¹⁹		
Compensation and employment contracts of officers, directors, and employees	Refer to the "Safe and sound banking practices" row later in this table. Also refer to the "Incentive Compensation" section of this booklet.	Officers serve at will. ¹²⁰	The board must approve all employment contracts and compensation arrangements for senior officers and directors. ¹²¹

¹¹⁹ For more information, refer to 12 CFR 21.21.

¹²⁰ For more information, refer to 12 USC 24(Fifth), "Corporate Powers of Association."

¹²¹ For more information, refer to 12 CFR 163.39.

Policy	National banks and FSAs	National banks only	FSAs only
Fiduciary compensation and powers		<p>A national bank may not permit any officer or employee to retain any compensation for acting as co-fiduciary with the bank in the administration of a fiduciary account, except with the specific approval of the board.¹²²</p> <p>A national bank's asset management activities shall be managed by or under the direction of its board.¹²³</p> <p>A national bank exercising fiduciary powers shall adopt and follow written policies and procedures adequate to maintain its fiduciary activities in compliance with applicable law.¹²⁴</p>	<p>An FSA must adopt and follow written policies and procedures adequate to maintain its fiduciary activities in compliance with applicable law.¹²⁵</p> <p>The exercise of fiduciary powers must be managed by or under the direction of the board.¹²⁶</p>
Financial derivatives		No equivalent regulation.	The board is responsible for effective oversight of financial derivative activities and must establish written policies and procedures governing such activities. ¹²⁷

¹²² For more information, refer to 12 CFR 9.15(b), "Compensation of Co-Fiduciary Officers and Employees."

¹²³ For more information, refer to 12 CFR 9.4, "Administration of Fiduciary Powers."

¹²⁴ For more information, refer to 12 CFR 9.5, "Policies and Procedures."

¹²⁵ For more information, refer to 12 CFR 150.140, "Must I Adopt and Follow Written Policies and Procedures in Exercising Fiduciary Powers?"

¹²⁶ For more information, refer to 12 CFR 150.150, "Who Is Responsible for the Exercise of Fiduciary Powers?"

¹²⁷ For more information, refer to 12 CFR 163.172, "Financial Derivatives."

Policy	National banks and FSAs	National banks only	FSAs only
Heightened standards	Banks with average total consolidated assets of \$50 billion or greater or those that are OCC-designated, which are referred to as covered banks, should have robust governance as outlined in the guidelines. ¹²⁸		
Identity theft prevention program	The board must approve the initial, written identity theft prevention program that establishes and maintains policies and procedures reasonably designed to monitor, detect, and mitigate identity theft. ¹²⁹		
Information security standards	The board or an appropriate committee of the board shall approve a written information security program and oversee the program's development, implementation, and maintenance. ¹³⁰		
Interbank liabilities	The board must review and approve written policies and procedures to prevent excessive exposure to any individual correspondent in relation to the condition of the correspondent. ¹³¹		

¹²⁸ For more information, refer to 12 CFR 30, appendix D.

¹²⁹ For more information, refer to 12 CFR 41.90(d), “Establishment of an Identity Theft Prevention Program”; 12 CFR 41.90(e), “Administration of the Program”; and 12 CFR 41, appendix J, “Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.”

¹³⁰ For more information, refer to 12 CFR 30.

¹³¹ For more information, refer to 12 CFR 206, “Limitations on Interbank Liabilities (Regulation F).”

Policy	National banks and FSAs	National banks only	FSAs only
Interest rate risk management	A bank should provide for periodic reporting to management and the board regarding interest rate risk with adequate information for management and the board to assess the level of risk. ¹³²		The board must review the association's interest rate risk exposure and devise and adopt policies for the management of interest rate risk. The board must review the results of operations at least quarterly and make appropriate adjustments as necessary. ¹³³
Real estate lending standards, interagency, and supplemental lending limits	A bank eligible to participate in the supplemental lending limits program for residential real estate and small business loans must submit an application to, and receive approval from, its supervisory office before using the supplemental lending limits in 12 CFR 32.7(a)(1), (2), and (3). ¹³⁴	The board must, at least annually, review and approve written policies that establish appropriate limits and standards for extensions of credit that are secured by real estate. ¹³⁵	The board must, at least annually, review and approve written policies that establish appropriate limits and standards for extensions of credit that are secured by real estate. ¹³⁶
Report of condition and income		The bank's president, a vice president, the cashier, or any other officer designated by the board must sign the report, and three directors must attest to the report's correctness. ¹³⁷	Two directors must attest to the report's correctness. ¹³⁸
Safe and sound banking practices	The board must oversee the bank's compliance with safe and sound banking practices. ¹³⁹		

¹³² For more information, refer to 12 CFR 30, appendix A, II.E, "Interest Rate Exposure."

¹³³ For more information, refer to 12 CFR 163.176, "Interest-Rate-Risk-Management Procedures."

¹³⁴ For more information, refer to 12 CFR 32.7(b), "Application Process."

¹³⁵ For more information, refer to 12 CFR 34, subpart D, "Real Estate Lending Standards," and subpart D, appendix A, "Interagency Guidelines for Real Estate Lending."

¹³⁶ For more information, refer to 12 CFR 160.101, "Real Estate Lending Standards."

¹³⁷ For more information, refer to 12 USC 161, "Reports to Comptroller of the Currency," and 12 USC 1817(a)(3).

¹³⁸ For more information, refer to 12 USC 1464(v), "Reports of Condition," and 12 USC 1817(a)(3).

¹³⁹ For more information, refer to 12 CFR 30, "Safety and Soundness Standards."

Policy	National banks and FSAs	National banks only	FSAs only
Security program and designation of a security officer	The board must approve and oversee the adoption, implementation, and maintenance of a written security program for the main and branch offices. ¹⁴⁰ The board must designate a security officer to report at least annually on the implementation, administration, and effectiveness of the security program. ¹⁴¹		
Specific funds availability	To meet the requirements of a specific availability policy disclosure under 12 CFR 229.17 and 12 CFR 229.18(d), a bank shall provide a disclosure describing the bank's policy on when funds deposited in an account are available for withdrawal. ¹⁴²		

¹⁴⁰ For more information, refer to 12 CFR 30, Appendix B, III.A., “Development and Implementation of Information Security Program.”

¹⁴¹ For national banks, refer to 12 CFR 21, subpart A, “Minimum Security Devices and Procedures.” For FSAs, refer to 12 CFR 168, “Security Procedures.”

¹⁴² For more information, refer to 12 CFR 229.16, “Specific Availability Policy Disclosure,” and 12 CFR 229, appendix C, “Model Availability Policy Disclosures, Clauses, and Notices; Model Substitute Check Policy Disclosure and Notices.”

Appendix C: Common Board Committees

This list provides examples of common board committees. Some committees are mandated by laws or regulations.

Table 3: Common Board Committees

Committee	Description
Executive committee	<p>Some boards choose to use an executive committee. The executive committee generally</p> <ul style="list-style-type: none"> • addresses matters requiring board review that arise between full board meetings. • relieves the full board of detailed reviews of information and operational activities. • coordinates the work of other board committees. <p>When used, the board traditionally authorizes the executive committee to act on the board's behalf but limits the authority to exercise all of the board's powers. For example, the full board should reserve the right to execute extraordinary contracts, such as mergers and acquisitions. The full board should review the executive committee charter and verify that the charter clearly specifies the committee's authority and what the committee may approve on the board's behalf.</p> <p>The use of an executive committee should not lead to a two-tiered class of directors in which the executive committee wields all the power. All directors share the same responsibilities and liabilities. Additionally, the executive committee should not be confused with executive sessions of the independent directors of the board.</p>
Audit committee	<p>The audit committee should oversee the bank's audit program and ensure that it is sufficiently robust to identify, test, and report on all key activities in the bank. Establishing an independent audit committee to oversee and maintain the audit functions is a good, and sometimes required, practice. The bank's size and activities dictate the composition of the audit committee.</p> <p>The audit committee's responsibilities should include the following:¹⁴³</p> <ul style="list-style-type: none"> • Work with internal and external auditors to confirm that the bank has comprehensive audit coverage to meet the risks and demands posed by its current and planned activities. • Hold senior management accountable for establishing and maintaining an adequate and effective internal control system and processes. • Carry out the appointment and termination, setting of compensation, and oversight of the chief auditor or equivalent and the independent public accountant or external auditor. • Ensure external auditors are independent and objective in their findings and consistent with their independence principles and rules. • Monitor the financial reporting process and oversee the bank's establishment of accounting policies and practices. • Establish and maintain whistle-blower procedures for bank employees to submit confidential and anonymous concerns for accounting, controls, or auditing matters. • Monitor, track, and hold management accountable for effectively addressing in a timely manner deficiencies that auditors or regulators identify.

¹⁴³ For more information on audit committee requirements and responsibilities, refer to the “Internal and External Audits” booklet of the *Comptroller’s Handbook*.

Committee	Description
Credit committee	<p>The credit committee oversees the bank's credit risk and its associated risk management practices. The credit committee should</p> <ul style="list-style-type: none"> • establish and guide the bank's lending strategy, credit risk appetite, and risk limits. • review and approve lending policies and underwriting standards that reflect the bank's risk appetite. • approve loans as outlined in the bank's lending policy for credits involving large dollar amounts relative to the bank's size and capital levels. • monitor the loan portfolio's performance, exceptions, and the allowance for loan and lease losses. • oversee the bank's compliance with credit-related policies, limits, laws, and regulations. • receive periodic reports from the loan review function that opine on the effectiveness of the bank's loan rating systems and credit risk management practices.
Asset-liability committee	<p>In most banks, the board delegates responsibility for overseeing liquidity and interest rate risk and its associated risk management to a committee of senior managers. If there is a board-level asset-liability committee, the committee should</p> <ul style="list-style-type: none"> • establish and guide the bank's asset-liability strategies, rate risk appetites, and limits. • review liquidity and interest rate risk reports and understand key assumptions. • monitor the bank's performance and overall liquidity position and interest rate risk profile and compliance with policies, strategies, limits, and regulations. • verify that asset-liability strategies remain prudent and supported by adequate capital and liquidity levels. • identify senior managers who have authority and responsibility for managing these risks and verify that adequate resources are devoted to asset-liability management. <p>Regulations require FSA boards to monitor financial derivatives activities and interest rate risk. FSA boards must adopt appropriate policies and procedures and periodically review them.¹⁴⁴ While the regulations apply only to FSAs, the guidelines contain sound practices that all banks should follow.</p>

¹⁴⁴ For more information, refer to 12 CFR 163.172 and 12 CFR 163.176.

Committee	Description
<p>Risk committee</p>	<p>The risk committee's primary responsibility is risk oversight. While not required, banks that have increased complexity customarily establish a separate risk committee. For smaller banks, the audit committee sometimes assumes the oversight of risk management activities. Although it is not required, larger banks often have a risk committee. The risk committee should include independent directors who review and approve a sound risk management system commensurate with the bank's size, complexity, and risk profile.</p> <p>The risk committee's roles and responsibilities should be explicitly defined and may include</p> <ul style="list-style-type: none"> • helping to define the bank's risk appetite. • working with the board and management to confirm that the bank's strategic, liquidity, and capital plans are consistent with the bank's risk appetite statement and that material risks are addressed in the bank's risk management process. • reviewing and approving risk limits. • confirming the bank has appropriate policies and procedures for risk governance, risk management practices, and the risk control infrastructure. • working with management to establish processes for identifying and reporting risks. • addressing the bank's material risks in aggregate and by risk type. • addressing the effect of the risks to capital, earnings, and liquidity under normal and stressed conditions. • confirming the independence of the risk management functions. • overseeing and directing the work of the CRE or equivalents. • confirming effective and timely escalation of material issues to the board and holding management accountable for timely and appropriate corrective action.
	<p>Heightened Standards</p> <p>The board or its risk committee should approve the risk governance framework and any significant changes.¹⁴⁵ The board or its risk committee also should monitor compliance with the risk governance framework.¹⁴⁶ Each CRE should have unrestricted access to the board risk committee regarding risk and issues identified through IRM activities.¹⁴⁷ The board or its risk committee approves the appointment and removal of a CRE and the CRE's annual compensation and salary adjustment.¹⁴⁸</p>

¹⁴⁵ For more information, refer to 12 CFR 30, appendix D, II.A.

¹⁴⁶ Ibid.

¹⁴⁷ For more information, refer to 12 CFR 30, appendix D, I.E.7, "Independent Risk Management."

¹⁴⁸ Ibid.

Committee	Description
Fiduciary committee	<p>A bank with fiduciary (trust) powers must comply with a host of state and federal laws and regulations governing fiduciary activities in addition to trust accounts' governing instruments.¹⁴⁹ The board typically establishes three fiduciary committees to oversee fiduciary activities and asset management products and services, including fiduciary compliance: one for administrative decisions, one relating to investment oversight, and a fiduciary audit committee.¹⁵⁰ Smaller, less complex banks may have a variation of these committees, such as a trust committee and a fiduciary audit committee.</p> <p>A bank with fiduciary powers must have an audit of fiduciary activities as well as a fiduciary audit committee.¹⁵¹ Regulations outline the composition requirements of the fiduciary audit committee. The committee oversees the bank's audit of significant fiduciary activities. The audit could be conducted annually or continuously, depending on the audit's setup. The committee should note results of the audit and actions taken in the minutes of the board or the fiduciary audit committee.</p>
Compensation committee	<p>A bank may have a compensation committee to oversee compensation arrangements. The compensation committee typically</p> <ul style="list-style-type: none"> • oversees the design and implementation of any incentive compensation arrangements for covered employees as discussed in the "Oversee Compensation and Benefits Arrangements" section of this booklet. • reviews and recommends compensation for directors, including the board and board committee fee structure. • works closely with board-level risk and audit committees to confirm that all committee decisions align with the bank's strategic objectives and risk appetite, and appropriately balance risk and reward. • has an understanding of all the bank's compensation and benefits arrangements, including the relationship between the arrangements and the risks or behaviors that the arrangements may incentivize; whether the arrangements are designed to promote long-term shareholder value and not promote excessive risk taking; and the legal requirements governing such arrangements. • provides periodic reports to the full board on compensation and benefits matters. <p>The compensation committee may assume other responsibilities, such as overseeing the bank's employee benefits plans. If the committee oversees these activities, it should confirm the bank has a process to appropriately administer benefits and meet the bank's fiduciary responsibilities.</p> <p>The compensation committee may engage consultants for compensation studies and assistance with developing incentive compensation arrangements. In addition, the compensation committee may be responsible for monitoring administrative costs paid to third-party professionals. If the bank has an employee benefit plan, the committee should also determine that no more than reasonable compensation is paid to the third party out of employee benefit plan assets.</p>

¹⁴⁹ For more information on a national bank's fiduciary responsibilities refer to 12 CFR 9, "Fiduciary Activities of National Banks," and to the "Asset Management" booklet of the *Comptroller's Handbook*. For information on FSAs refer to 12 CFR 150, "Fiduciary Powers of Federal Savings Associations."

¹⁵⁰ For more information on audits of fiduciary activities, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook*.

¹⁵¹ For more information, refer to 12 CFR 9.9, "Audit of Fiduciary Activities" (national banks), and 12 CFR 150.440-480, "Audit Requirements" (FSAs).

Committee	Description
Corporate governance/nominating committee	<p>At many banks, the corporate governance/nominating committee duties involve</p> <ul style="list-style-type: none"> • establishing criteria for board and committee membership, including qualifications and independence requirements. • recommending nominees for election to the board, evaluating new nominees, and assessing the contributions of current directors in connection with their re-nomination. • reviewing and approving a management succession policy and plan for senior management positions. • overseeing the bank's corporate governance practices with regard to board composition and independence. • verifying that the board reflects a mix of talent, expertise, and perspectives that is appropriate to the bank's needs, its strategic plans, and the overall effectiveness of the board. <p>A mutual FSA must have a nominating committee if the association's bylaws provide for submission of nominations for directors before the annual meeting. This committee submits nominations to the secretary of the association.¹⁵²</p> <p>Other responsibilities of the corporate governance/nominating committee can include</p> <ul style="list-style-type: none"> • overseeing the evaluation of board performance and individual director contributions. • conducting an evaluation of its own performance. • assisting other board committees with their self-assessments. • periodically assessing board size and composition. • establishing director tenure policies that address procedures for the retirement or replacement of directors. • assessing the reporting channels and mechanisms through which the board receives information and the quality and timeliness of the information. • overseeing director education and training. • establishing and overseeing procedures for shareholder communications, including the solicitation of shareholder recommendations for the nomination of directors to the board. <p>If the bank does not have a compensation committee to review and recommend changes to the bank's director compensation policies, the corporate governance/nominating committee should perform these duties.</p>

¹⁵² For more information, refer to 12 CFR 5.21(j)(2)(xiii), "Nominations for Directors."

Appendix D: Common Types of Insurance

This appendix explains some of the common types of insurance policies and coverage available to banks. The names of the insurance policies or coverage may differ among banks or providers.

Indemnification Agreements

A bank director may be named as a defendant in lawsuits that challenge his or her business decisions or activities, or allege a breach of fiduciary duty. Directors and officers, however, may obtain some protection against judgments and legal and other costs through indemnification agreements and insurance.

Banks may enter into indemnification agreements with directors. Such agreements generally provide that the bank will advance funds to, or reimburse directors for, reasonable expenses incurred in defense of legal actions. The agreement must be consistent with applicable laws and regulations and should be consistent with safe and sound banking practices.

Regulations limit indemnification agreements.¹⁵³ Banks generally may not make or agree to make indemnification payments to an institution-affiliated party (IAP) (e.g., directors, officers, employees, or controlling stockholders)¹⁵⁴ for liability or legal expenses resulting from administrative proceedings or civil actions instituted by any federal banking agency that results in a final order or settlement pursuant to which an IAP is

- assessed a CMP.
- removed from office or prohibited from service.
- required to cease and desist or take any described affirmative action with the bank.¹⁵⁵

Reasonable indemnification payments with respect to an administrative proceeding or civil action initiated by any federal banking agency are permitted subject to the board making specific determinations and following specific procedures.¹⁵⁶ Reasonable indemnification payments are also permitted in other situations.¹⁵⁷ FSAs—but not national banks—are required to obtain OCC non-objection before making any indemnification payments.

¹⁵³ For more information, refer to 12 CFR 359.

¹⁵⁴ Refer to 12 USC 1813(u), “Institution-Affiliated Party,” for the full definition.

¹⁵⁵ For more information, refer to 12 CFR 359.1(l), “Prohibited Indemnification Payment,” and 12 CFR 359.3, “Prohibited Indemnification Payments.”

¹⁵⁶ For more information, refer to 12 CFR 359.5, “Permissible Indemnification Payments.”

¹⁵⁷ For national banks, refer to 12 CFR 7.2014, “Indemnification of Institution-Affiliated Parties.” For more information regarding FSAs, refer to 12 CFR 145.121, “Indemnification of Directors, Officers and Employees.”

Directors' and Officers' Liability Insurance

Director and officer (D&O) liability insurance protects directors and officers who prudently discharge their duties and helps banks attract and retain qualified personnel. D&O insurance can cover the expense of defending suits alleging director or officer misconduct, and damages that may be awarded in such lawsuits. D&O insurance can reimburse the bank for any payments made to directors or officers under an indemnification agreement. Generally, the insuring company requires a deductible for this type of coverage. This insurance does not cover criminal or dishonest acts, when involved persons obtained personal gain, or when a conflict of interest was apparent.

Insurers may add exclusionary language to insurance policies that directors and officers should clearly understand, as it has the potential to limit coverage and leave officers and directors liable for claims not covered by these policies. For instance, during times of economic slowdown, a regulatory exclusion may be added to preclude coverage for lawsuits by federal and state banking regulators. Because there is no industry standard for D&O insurance, directors should be aware of the insuring agreements and exclusions that are most critical to their personal protection. The board's choice of coverage in a D&O insurance policy should be based on a well-informed analysis of the cost and benefits, and the potential impact that could result from exclusions. When considering renewals and amendments to existing policies, directors and officers should consider the following:

- What protections do I want from my bank's D&O insurance policy?
- What exclusions exist in my bank's D&O insurance policy?
- Are any of the exclusions new, and, if so, how do they change my D&O insurance coverage?
- What is my potential personal financial exposure arising from each D&O insurance policy exclusion?

D&O liability insurers have filed suits to rescind coverage against directors and officers in cases involving restatement of financials or other alleged financial misconduct. The insurers typically claim that the policy should be rescinded on the grounds that it was fraudulently procured. Directors and officers may consider a clean non-rescindable clause, providing that the insurer cannot rescind the policy based on alleged corporate wrongdoing or misrepresentations in the application process. Such a clause is generally not included in standard policies, and insurers charge a significant premium for its inclusion.

The severability clause of the D&O policy generally provides that no knowledge or statement by anyone insured in procuring coverage can be imputed to any other insured individual, limiting the potential that coverage will be adversely affected for one individual as the result of the actions of another. The practical effect of the severability clause is to require an insurer seeking to rescind a policy to prove knowledge of each insured person separately. Narrowly tailored severability clauses may limit the insurer's potential exposure.

Refer to the "Indemnification Agreements" section of this booklet for the instances in which the bank may and may not purchase D&O insurance to pay or reimburse an IAP.

Fidelity Bond

Fidelity insurance includes reimbursement for loss, not only from employee dishonesty but also from robbery, burglary, theft, forgery, mysterious disappearance, and, in specified instances, damage to offices or fixtures of the insured. Fidelity bond coverage applies to all banking locations except automated teller machines, for which coverage must be specifically added by a rider. Standard procedure for insurance companies is to write fidelity bonds on a “discovery” basis. Under this method, the insurance company is liable up to the full amount of the policy for losses covered by the terms of the bond and discovered while the bond is in force, regardless of the date on which the loss was actually sustained by the bank. This procedure applies even though lower coverage amounts or more restrictive terms might have been in effect on the date the loss was sustained.

All fidelity bonds require that a loss be reported to the bonding company within a specified time after a reportable item comes to the attention of management. Management should diligently report all potential claims to the bank’s insurance company because failure to file a timely report may jeopardize coverage for that loss.

Many banks also obtain an excess coverage policy. The coverage extends the basic protection provided under the fidelity bond in areas in which the dollar volume of assets or exposure is particularly high. Fidelity bond protection can be extended by purchasing optional riders.

If the bank discontinues efforts to obtain insurance after the policy lapses or is canceled, the board should be aware that

- the failure of directors to require bonds with adequate sureties and in sufficient amounts may make the directors personally liable for any losses the bank sustains because of the absence of such bonds. Common law standards have held directors liable in their “personal and individual capacity” for negligently failing to require an indemnity bond to cover employees with access to cash, notes, and securities.
- management should determine the reason for any denial of insurance or unreasonable terms; confirm that action is taken to correct any deficiencies and, when beneficial, provide additional information; and obtain insurance when feasible.
- although establishing a fund to cover losses is not a viable alternative to insurance, it may be used while attempting to obtain insurance (to be applied to premiums or to offset losses), or it may be used in addition to insurance to offset a high deductible. Establishing such a fund does not mean that an insurance cost or liability has been incurred. Therefore, estimated losses should not be reported as an expense in the call report until the losses actually occur.

When the bank is a subsidiary of a bank holding company, and the holding company has purchased one fidelity bond to cover all affiliated banks, the bank should be careful when determining that the policy is sufficient to cover the bank’s exposures.

Bank-Owned Life Insurance

Bank-owned life insurance (BOLI) is a form of life insurance purchased by banks in which the bank is the beneficiary or owner. This form of insurance is a tax shelter for the administering bank. The cash flows from a BOLI policy generally are income tax-free if the bank holds the policy for its full term. Banks are not authorized to purchase BOLI as an investment. BOLI can, however, provide attractive tax-equivalent yields to help offset the cost of employee benefits. Banks are expected to establish sound risk management processes, including meaningful risk limits, before implementing and adding to a BOLI program.¹⁵⁸

Specialized Bank Insurance

Management, in consultation with the board, may decide that they should obtain other bank insurance coverage to transfer risks. The following are some of the most frequently purchased types of specialized bank insurance:

Automobile, public liability, and property damage: Protects against property and liability losses arising from injury or death when a bank-owned, -rented, or -repossessed vehicle is involved. Non-ownership liability insurance should be considered if officers or employees use their own cars for bank business.

Boiler and machinery: Provides coverage for loss due to explosion or other forms of destruction of boilers, heating or cooling systems, and similar types of equipment.

Business disruption expense: Provides funds for the additional costs of reestablishing the bank's operations after a disaster.

Combination safe depository, coverage A: Covers losses when the bank is legally obligated to pay for the loss (including damage or destruction) of a customer's property held in safe deposit boxes. **Coverage B:** Covers loss, damage, or destruction of property in customers' safe deposit boxes, whether or not the bank is legally liable, when such loss results from activities other than employee dishonesty. This policy commonly provides for reimbursement of legal fees in conjunction with defending suits involving alleged loss of property from safe deposit boxes.

Cybersecurity: Provides coverage to mitigate losses for a variety of cyber incidents, including data breaches, business interruption, and network damage.

Fine arts: Provides coverage for works of art on display at a bank, whether owned by the bank or on consignment. Protection typically is all risk and requires that appraisals of the objects be made regularly to establish the insurable value.

Fire: Covers all loss directly attributed to fire, including damage from smoke, water, or chemicals used to extinguish the fire. Additional fire damage for the building contents may

¹⁵⁸ For more information, refer to OCC Bulletin 2004-56, "Bank-Owned Life Insurance: Interagency Statement on the Purchase and Risk Management of Life Insurance."

be included but often is written in combination with the policy on the building and permanent fixtures. Most fire insurance policies contain “co-insurance” clauses, meaning that insurance coverage should be maintained at a fixed proportion of the replacement value of the building.

First class, certified, and registered mail insurance: Provides protection on shipment of property sent by various types of mail and during transit by messenger or carrier to and from the U.S. Postal Service. This coverage is used principally for registered mail over the maximum \$25,000 insurance provided by the U.S. Postal Service.

Fraudulent accounts receivable and fraudulent warehouse receipts: Covers losses resulting from the pledging of fraudulent or nonexistent accounts receivable and warehouse receipts, or from situations in which the pledger does not have title. In addition, this insurance offers protection against loss arising from diversion of proceeds through acts of dishonesty.

General liability: Covers possible losses arising from a variety of occurrences. General liability insurance provides coverage against specified hazards, such as personal injury, medical payments, landlords’ or garage owners’ liability, or other specific risks that may result in or create exposure to a suit for damages against the bank. “Comprehensive” general liability insurance covers all risks, except specific exclusions.

Key person insurance: Insures the bank on the life of an officer when the death of such officer, or key person, would be of such consequence as to give the bank an insurable interest.

Mortgage errors and omissions: Protects the bank, as mortgagee, from loss when fire or all-risk insurance on real property held as collateral inadvertently has not been obtained. This insurance is not intended to overcome errors in judgment, such as inadequate coverage or insolvency of an original insurer.

Single interest: Covers losses for uninsured vehicles that are pledged as collateral for an extension of credit.

Transit cash letter insurance: Covers loss of cash letter items in transit for collection or to a clearinghouse of which the insured bank is a member. This coverage also includes costs for reproducing cash letter items. Generally, such coverage does not include items sent by registered mail or air express or losses due to dishonest acts of employees.

Trust operations errors and omissions: Indemnifies against claims for damages arising from alleged acts resulting from error or omissions while acting as administrator under a trust agreement.

Umbrella liability: Provides excess coverage over existing liability policies, as well as basic coverage for most known risks not covered by existing insurance.

Valuable papers and destruction of records: Covers cost of reproducing records damaged or destroyed. This coverage also includes the cost of research needed to develop the facts required to replace books of accounts and records.

Appendix E: Glossary

Control functions: Those functions that have a responsibility to provide independent and objective assessment, reporting, and assurance. They include the risk review, compliance, and internal audit functions.

Corporate governance: A set of relationships among a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and by which the means of attaining those objectives and monitoring performance are determined.

Credible challenge: The method that directors use to hold management accountable by being engaged and asking questions and eliciting any facts necessary, when appropriate, to satisfy themselves that management's strategies are viable and in the bank's best interests.

Duty of care: The duty of a board member to decide and act in an informed and prudent manner with respect to the bank. Often interpreted as requiring a board member to approach the affairs of the company the same way that a "prudent person" would approach his or her own affairs.

Duty of loyalty: The duty of a board member to act in good faith in the interest of the company. The duty of loyalty should prevent an individual director from acting in his or her own interest, or in the interest of another individual or group, at the expense of the company and all shareholders.

Independent director: A director is viewed as independent if he or she is free of any family relationship or any material business or professional relationship (other than stock ownership and the directorship itself) with the bank, its holding company, its affiliate, or its management.

Management director: A member of the board (such as a director) who also has management responsibilities within the bank.

Risk appetite statement: The written statement of the aggregate level and types of risk that a bank is willing to assume to achieve its strategic objectives and business plan. It includes quantitative measures expressed relative to earnings, capital, risk measures, liquidity, and other relevant measures as appropriate. It should include qualitative statements to address reputation risk as well as money laundering and unethical practices.

Risk culture: The bank's norms, attitudes, and behaviors related to risk awareness, risk taking, and risk management, and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during day-to-day activities and affects the risks they assume.

Risk governance framework: A part of the corporate governance framework, through which the board and management, in their respective roles, establish and make decisions

about the bank's strategy and risk approach; articulate and monitor adherence to risk appetite and risk limits consistent with the bank's strategy; and identify, measure, monitor, and control risks.

Risk limits: Specific quantitative measures based on, for example, forward-looking assumptions that allocate the bank's risk appetite to business lines; legal entities as relevant, specific risk categories; concentrations; and, as appropriate, other measures.

Risk management: The processes established to identify, measure, monitor, and control material risks and associated risk concentrations.

Risk profile: Point-in-time assessment of the bank's risks, aggregated within and across each relevant risk category based on current and forward-looking assumptions.

Appendix F: Abbreviations

AML	anti-money laundering
BOLI	bank-owned life insurance
BSA	Bank Secrecy Act
CAE	chief audit executive
CAMELS	capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk
CEO	chief executive officer
CFR	Code of Federal Regulations
CIO	chief information officer
CISO	chief information security officer
CMP	civil money penalty
CMS	compliance management system
COO	chief operating officer
CRA	Community Reinvestment Act
CRE	chief risk executive
CTO	chief technology officer
D&O	director and officer
EIC	examiner-in-charge
ERM	enterprise risk management
Fed. Reg.	Federal Register
FFIEC	Federal Financial Institutions Examination Council
FSA	federal savings association
IAP	institution-affiliated party
ICQ	internal control questionnaire
IRM	independent risk management
IT	information technology
MIS	management information systems
OCC	Office of the Comptroller of the Currency
OTS	Office of Thrift Supervision
ROCA	risk management, operational controls, compliance, and asset quality
USC	U.S. Code

References

Listed references apply to national banks and FSAs unless otherwise noted.

Laws

- 12 USC 24(Fifth), “Corporate Powers of Association” (national banks)
- 12 USC 61, “Shareholders’ Voting Rights; Cumulative and Distributive Voting; Preferred Stock; Trust Shares; Proxies, Liability Restrictions; Percentage Requirement Exclusion of Trust Shares” (national banks)
- 12 USC 71, “Election” (national banks)
- 12 USC 71a, “Number of Directors; Penalties” (national banks)
- 12 USC 72, “Qualifications” (national banks)
- 12 USC 73, “Oath” (national banks)
- 12 USC 74, “Vacancies” (national banks)
- 12 USC 76, “President of Bank as Member of Board; Chairman of Board” (national banks)
- 12 USC 161, “Reports to Comptroller of the Currency” (national banks)
- 12 USC 191, “Appointment of Receiver for a National Bank” (national banks)
- 12 USC 371c, “Banking Affiliates”
- 12 USC 1464(v), “Reports of Condition” (FSAs)
- 12 USC 1813(u), “Institution-Affiliated Party”
- 12 USC 1817(a), “Reports of Condition; Access to Reports”
- 12 USC 1817(j), “Change in Control of Insured Depository Institutions”
- 12 USC 1818, “Termination of Status as Insured Depository Institution”
- 12 USC 1828(z), “General Prohibition on Sale of Assets”
- 12 USC 1831i, “Agency Disapproval of Directors and Senior Executive Officers of Insured Depository Institutions or Depository Institution Holding Companies”
- 12 USC 1831o, “Prompt Corrective Action”
- 12 USC 2901 et seq., “Community Reinvestment”
- 12 USC 3201 et seq., “Depository Institution Management Interlocks”
- 15 USC 45, “Unfair Methods of Competition Unlawful; Prevention by Commission”
- 15 USC 77jjj, “Eligibility and Disqualification of Trustee”
- 15 USC 1691(a), “Activities Constituting Discrimination”
- 18 USC 215, “Receipt of Commissions or Gifts for Procuring Loans”
- 18 USC 656, “Theft, Embezzlement, or Misapplication by Bank Officer or Employee”
- 18 USC 1001, “Statements or Entries Generally”
- 18 USC 1005, “Bank Entries, Reports, and Transactions”
- 18 USC 1344, “Bank Fraud”
- 29 USC 1001 et seq., “Employee Retirement Income Security Program”
- 31 USC 5322, “Criminal Penalties”
- 42 USC 3604, “Discrimination in the Sale or Rental of Housing and Other Prohibited Practices”
- 42 USC 3605, “Discrimination in Residential Real Estate-Related Transactions”
- 52 USC 30101 et seq., “Federal Election Campaign Act of 1971”

Regulations

- 11 CFR 100, subpart B, “Definition of Contribution”
- 11 CFR 114.2, “Prohibitions on Contributions, Expenditures and Electioneering Communications”
- 12 CFR 3, “Capital Adequacy Standards”
- 12 CFR 5.21, “Federal Mutual Savings Association Charter and Bylaws” (mutual FSAs)
- 12 CFR 5.22, “Federal Stock Savings Association Charter and Bylaws” (stock FSAs)
- 12 CFR 5.23, “Conversion to Become a Federal Savings Association” (FSAs)
- 12 CFR 5.24, “Conversion to Become a National Bank” (national banks)
- 12 CFR 5.40, “Change in Location of a Main Office of a National Bank or Home Office of a Federal Savings Association”
- 12 CFR 5.46, “Changes in Permanent Capital of a National Bank” (national banks)
- 12 CFR 5.50, “Change in Control of a National Bank or Federal Savings Association; Reporting of Stock Loans”
- 12 CFR 5.51, “Changes in Directors and Senior Executive Officers of a National Bank or Federal Savings Association”
- 12 CFR 7.2002, “Director or Attorney as Proxy” (national banks)
- 12 CFR 7.2004, “Honorary Directors or Advisory Boards” (national banks)
- 12 CFR 7.2005, “Ownership of Stock Necessary to Qualify as Director” (national banks)
- 12 CFR 7.2007(a), “Increasing Board of Directors” (national banks)
- 12 CFR 7.2008, “Oath of Directors” (national banks)
- 12 CFR 7.2009, “Quorum of the Board of Directors; Proxies Not Permissible” (national banks)
- 12 CFR 7.2012, “President as Director; Chief Executive Officer” (national banks)
- 12 CFR 7.2014, “Indemnification of Institution-Affiliated Parties” (national banks)
- 12 CFR 7.2024, “Staggered Terms for National Bank Directors and Size of Bank Board” (national banks)
- 12 CFR 9, “Fiduciary Activities of National Banks” (national banks)
- 12 CFR 11, “Securities Exchange Act Disclosure Rules”
- 12 CFR 21, subpart A, “Minimum Security Devices and Procedures” (national banks)
- 12 CFR 21.11, “Suspicious Activity Report” (national banks)
- 12 CFR 21.21, “Procedures for Monitoring Bank Secrecy Act Compliance”
- 12 CFR 25, “Community Reinvestment Act and Interstate Deposit Production Regulations” (national banks)
- 12 CFR 26, “Management Official Interlocks”
- 12 CFR 30, “Safety and Soundness Standards”
- 12 CFR 30, appendix A, “Interagency Guidelines Establishing Standards for Safety and Soundness”
- 12 CFR 30, appendix B, “Interagency Guidelines Establishing Information Security Standards”
- 12 CFR 30, appendix D, “OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches”

- 12 CFR 30, appendix E, “OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches”
- 12 CFR 31, “Extensions of Credit to Insiders and Transactions With Affiliates”
- 12 CFR 32.7, “Residential real estate loans, small business loans, and small farm loans ('Supplemental Lending Limits Program')”
- 12 CFR 34, subpart D, “Real Estate Lending Standards” (national banks)
- 12 CFR 34.62, subpart D, appendix A, “Interagency Guidelines for Real Estate Lending” (national banks)
- 12 CFR 41.90, “Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft”
- 12 CFR 41, appendix J, “Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.”
- 12 CFR 145.121, “Indemnification of Directors, Officers and Employees” (FSAs)
- 12 CFR 150, “Fiduciary Powers of Federal Savings Associations” (FSAs)
- 12 CFR 160.101, “Real Estate Lending Standards” (FSAs)
- 12 CFR 160.101, appendix, “Interagency Guidelines for Real Estate Lending Policies” (FSAs)
- 12 CFR 163.33, “Directors, Officers, and Employees” (FSAs)
- 12 CFR 163.39, “Employment Contracts” (FSAs)
- 12 CFR 163.172, “Financial Derivatives” (FSAs)
- 12 CFR 163.176, “Interest-Rate-Risk-Management Procedures” (FSAs)
- 12 CFR 163.180(d), “Suspicious Activity Reports” (FSAs)
- 12 CFR 163.200, “Conflicts of Interest” (FSAs)
- 12 CFR 163.201, “Corporate Opportunity” (FSAs)
- 12 CFR 168, “Security Procedures” (FSAs)
- 12 CFR 195, “Community Reinvestment” (FSAs)
- 12 CFR 206, “Limitations on Interbank Liabilities (Regulation F)”
- 12 CFR 215, “Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks (Regulation O)”
- 12 CFR 223, “Transactions Between Member Banks and Their Affiliates (Regulation W)”
- 12 CFR 225.41(b)(3), “Immediate Family”
- 12 CFR 229, “Availability of Funds and Collection of Checks (Regulation CC)”
- 12 CFR 359, “Golden Parachute and Indemnification Payments”
- 12 CFR 363, “Annual Independent Audits and Reporting Requirements”
- 12 CFR 1026.36, “Prohibited Acts or Practices and Certain Requirements for Credit Secured by a Dwelling”
- 31 CFR 1020.210, “Anti-Money Laundering Program Requirements for Financial Institutions Regulated Only by a Federal Functional Regulator, Including Banks, Savings Associations, and Credit Unions”

Federal Register

83 Fed. Reg. 66604

Comptroller's Handbook

“Asset Management”
“Bank Supervision Process”
“Capital and Dividends”
“Community Bank Supervision”
“Community Reinvestment Act Examination Procedures” (national banks)
“Compliance Management Systems”
“Federal Branches and Agencies Supervision”
“Insider Activities”
“Internal and External Audits”
“Internal Control” (national banks)
“Large Bank Supervision”
“Liquidity”
“Recovery Planning”
“Related Organizations” (national banks)
“Retirement Plan Products and Services”

OTS Examination Handbook (FSAs)

Section 1500, “Community Reinvestment Act”
Section 340, “Internal Control”
Section 730, “Related Organizations”

Comptroller's Licensing Manual

“Background Investigations”
“Change in Bank Control”
“Changes in Directors and Senior Executive Officers”
“Charters”
“Conversions to Federal Charter”

OCC Issuances

Detecting Red Flags in Board Reports: A Guide for Directors
OCC Bulletin 2003-12, “Interagency Policy Statement on Internal Audit and Internal Audit
Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing”
OCC Bulletin 2004-56, “Bank-Owned Life Insurance: Interagency Statement on the
Purchase and Risk Management of Life Insurance”
OCC Bulletin 2007-31, “Prohibition on Political Contributions by National Banks: Updated
Guidance”
OCC Bulletin 2010-24, “Incentive Compensation: Interagency Guidance on Sound Incentive
Compensation Policies”
OCC Bulletin 2013-29, “Third-Party Relationships: Risk Management Guidance”
OCC Bulletin 2014-35, “Mutual Federal Savings Associations: Characteristics and
Supervisory Considerations”

- OCC Bulletin 2015-30, “Standards for Assessing the Diversity Policies and Practices of Regulated Entities: Final Interagency Policy Statement”
- OCC Bulletin 2017-21, “Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29”
- OCC Bulletin 2017-43, “New, Modified, or Expanded Bank Products and Services: Risk Management Principles”
- OCC Bulletin 2017-7, “Third-Party Relationships: Supplemental Examination Procedures”
- OCC Bulletin 2018-17, “Supervisory Policy and Processes for Community Reinvestment Act Performance Evaluations”
- The Director’s Book: Role of Directors for National Banks and Federal Savings Associations*

Other

- Basel Committee on Banking Supervision’s “Principles for Effective Risk Data Aggregation and Risk Reporting,” January 2013
- FFIEC BSA/AML Examination Manual*
- FFIEC IT Examination Handbook*

Deloitte.



Cyber Strategy Framework
A unique platform for
managing your Cyber Strategy

A unique framework for managing your Cyber Strategy

Deloitte's Cyber Strategy Framework is a unique approach to creating a cybersecurity strategy - helping organizations to manage cyber resilience with confidence.

Our Cyber Strategy Framework incorporates a business-driven and threat-based methodology supported by an intuitive online platform, which includes dashboards for reporting to an operational, managerial and executive audience. The Cyber Strategy Framework is our global approach to conducting cyber strategy assessments and is used by leading organizations across numerous industries.



A unique framework for managing your Cyber Strategy

Deloitte recognizes that no organization has unlimited resources to dedicate to cybersecurity. Therefore, it is important that organizations invest in those cybersecurity capabilities that will contribute most to their overall cyber resilience. The Cyber Strategy Framework is the result of more than four years of research and investment in Cyber Strategy by Deloitte and incorporates a proven methodology to determine the current and target maturity of an organization's cyber capabilities and design a roadmap to improve the overall cyber resilience of the organization to internal and external threats.

Our framework also includes content packs, which enable maturity assessments to be conducted against a range of industry standards, including the ISO/IEC 27001, the NIST Cybersecurity Framework and the Deloitte Cyber Capability model. The Deloitte Cyber Capability Model recognizes that while being **Secure** is important, organizations must also be **Vigilant** and **Resilient** against cyber threats, and have a comprehensive Cyber Strategy to ensure continued business value.

Methodology
A proven methodology based around three components: business, threats and capabilities.



Content Packs
Content packs which enable maturity assessments against particular standards.



Platform
A versatile platform which supports our methodology and includes an array of customizable dashboards.



Deloitte
Underpinned by our experience in cyber risk management and strategy.

Cyber Resilience delivered

Deloitte's Cyber Strategy Framework leverages our proven methodology and our unique insight and experience to deliver improved cyber resilience and several other business benefits.

These include:

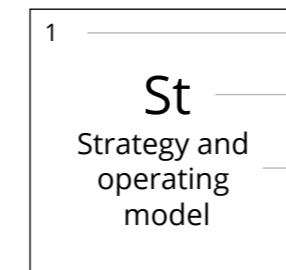
- Enhanced value from cyber investments by focusing on the right priorities.
- Enhanced risk governance and management.
- Improved communication with internal and external stakeholders, including regulators.
- Create a common framework for managing cyber resilience at an operational, managerial and executive level.

Deloitte Cyber Strategy Framework Periodic Table

Deloitte's CSF Periodic tables encapsulates the fundamentals to our services delivered in a manner that is concise and digestible for our clients.

Governance

1	St Strategy and operating model
---	---



Capability #

Symbol

Capability name

Resilient

32	Ip Incident readiness
----	---------------------------------

Secure

Vigilant

2	Pa Policies, standars and architecture	5	Cs Cloud Security	9	S Secure software development lifecycle	13	Es End-user device security	17	Idm Identity lifecycle management	21	Dlp Data loss prevention	25	Cti Cyber threat intelligence	29	Sp Security platform administration	33	Ir Incident response
3	Aw Cyber Risk Culture and behaviour	6	Tp Third-party Risk management	10	Ap Post-development app protection	14	Am Asset management	18	Pam Privileged acces management	22	E Enryption	26	Bp Brand Protection	30	Pvm Patch and Vulnerability management	34	Bc Business continuity Management and resilience
4	Rm Cyber Risk Management, Metrics and reporting	7	Hs Human Resource security	11	Mp Malware protection	15	Ss System security	19	Rbac Role-based Acces control	23	Dp Data privacy	27	Td Thread detection	31	Pvi Penetration testing and vulnerability identification		● Incident management ● Business resilience
	● Cybersecurity management	8	Ps Physical security	12	Nc Network security	16	Ua User acces control	20	Ic Information classification	24	Ilm Information Lifecycle management	28	Th Thread hunting		● Vulnerability identification		

● Extended enterprise
● People and workplace

● Application security

● Infrastructure security

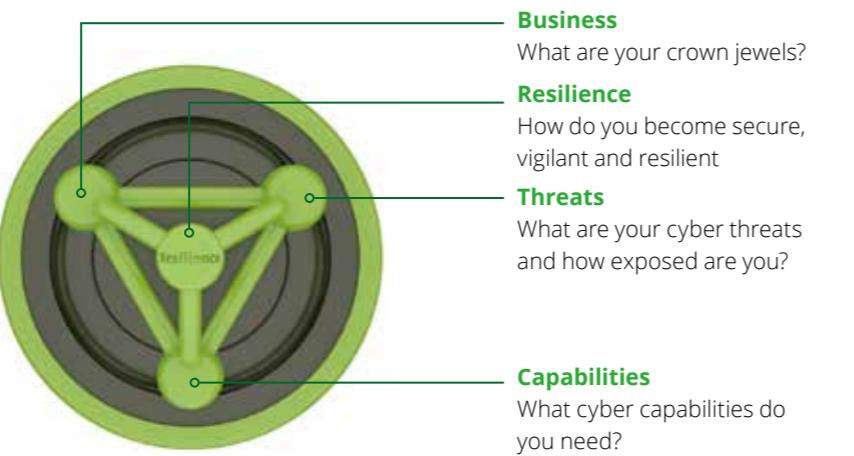
● Identity and access management

● Data security

● Threat intelligence
● Security operations

A comprehensive approach to managing cyber resilience with confidence

Deloitte's Cyber Strategy Framework incorporates a proven methodology based around three core components: **Business**, **Threats** and **Capabilities**. To define the right cyber strategy for an organization we typically follow a five-phase approach to assess the current and the targeted maturity level of cyber capabilities. We define an actionable roadmap which organizations can immediately act upon and which aim to improve their cyber resilience.



PHASE 1: Business profiling	PHASE 2: Threat assessment	PHASE 3: Current state assessment	PHASE 4: Target states and recommendations	PHASE 5: Reporting and roadmap

We start with understanding the organization's business context, including its operating model and strategy, in order to identify its critical business assets (crown jewels). In this phase, we analyze the organization's threat environment to determine the most relevant threat actors and techniques, and use these to determine the organization's exposure to specific threat scenarios. We assess the maturity of the organization's existing cyber capabilities. Our assessment is supported by our platform, which can automatically calculate the current state maturity of each capability based on the responses received to specific statements. In this phase, we define an appropriate target maturity for the organization's cyber capabilities based on its specific threat landscape. Again, our platform can automatically calculate the most appropriate maturity based on the organization's specific threat exposure. Finally, we report on the organization's cyber resilience using the customizable dashboards available in our platform, and use the results of our assessments to define a structured roadmap to improve the maturity of the organization's capabilities and guide the organization towards its target state.

Contact us

Director, Risk Advisory



Dejan Perić

Director

Serbia

E-mail: deperic@deloittece.com

Tel.: +381 (0)11 3812 110

Mob.: +381 (0)65 224 6870

Manager, Risk Advisory



Borko Mijić

Manager

Serbia

E-mail: bmijic@deloittece.com

Tel.: +381 (0) 11 3812 218

Mob.: +381 (0) 65 222 55 90

Manager, Risk Advisory



Aleksandar Mirković

Manager

Serbia

E-mail: almirkovic@deloittece.com

Mob.: +382 (0)69 376 627



Deloitte is a leading global organization that provides audit and assurance services, business, financial, tax and legal consulting, and risk management consulting. Deloitte supports the world's largest companies (four out of five Fortune Global 500® companies) through a globally connected network of member firms in more than 150 countries. To learn more about how Deloitte's approximately 312,000 professionals contribute not only to the success of clients, but to the entire community, visit www.deloitte.com.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms and their related entities (collectively: the "Deloitte Organization"). DTTL (also known as: "Deloitte Global") and all its member companies and related entities are legally separate and independent entities, which cannot be obligated to each other or liable to third parties. DTTL and each DTTL member company and related entity is responsible only for its own acts and omissions, and is not responsible for the actions of others. Deloitte does not provide services to clients. For more information, please visit www2.deloitte.com/rs/en/about-us.

In the Republic of Serbia, services are provided by Deloitte Advisory d.o.o. Belgrade and Deloitte d.o.o. Belgrade (hereinafter collectively: "Deloitte Serbia") which are members of Deloitte Central Europe Holdings Limited. Deloitte Serbia is one of the leading companies for providing professional services in the field of audit, tax, business, financial and consulting in risk management in Serbia, with over 250 experts from the country and abroad.

This business communication contains general information only and accordingly, no member firm of the Deloitte Touche Tohmatsu Limited ("DTTL") global network or any of its affiliates (collectively the "Deloitte Organization") is rendering professional advice or services through this publication. Before making any decision or taking any action that may affect your finances or business, you should consult a qualified professional advisor.

No representations or warranties (express or implied) are made as to the accuracy or completeness of the information in this communication, and DTTL, its member companies, affiliates, employees or agents shall not be liable for any damages that may be suffered by any person directly or indirectly through the use of the information from this publication. DTTL and its member companies are legally separate and independent entities.

© 2022. For information, contact Deloitte Serbia.
© 2022. For information, contact Deloitte Central Europe.