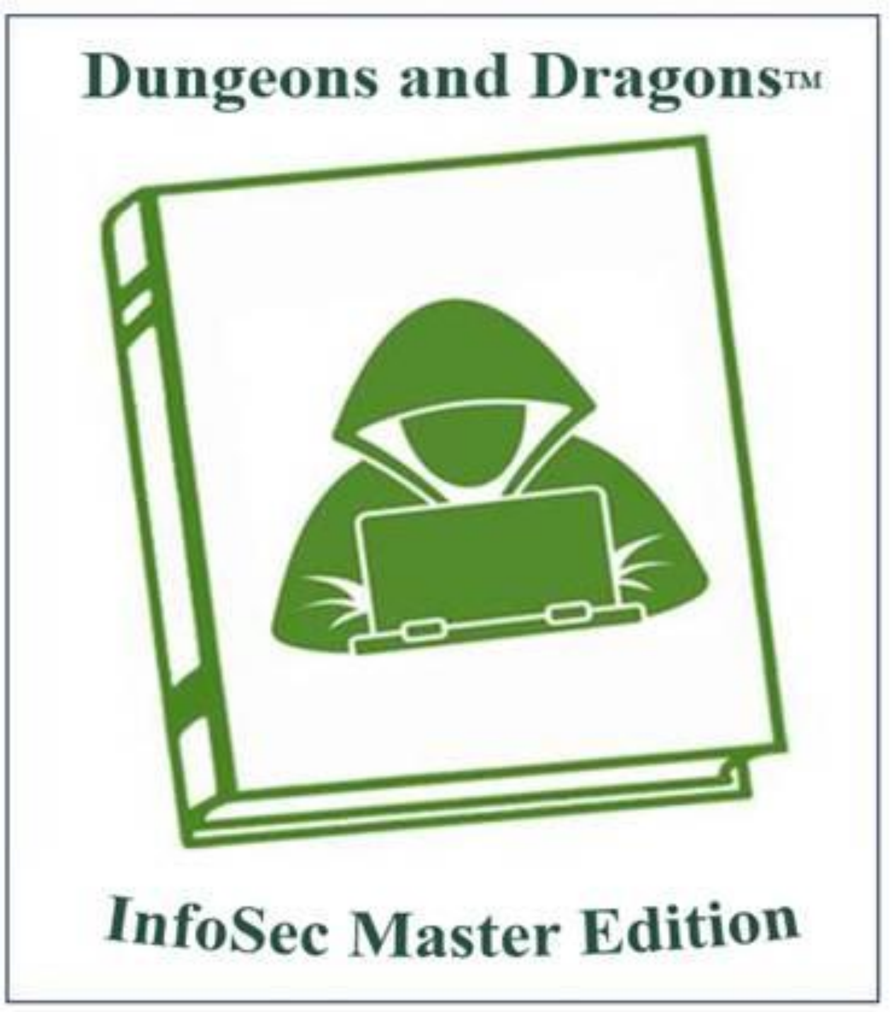
Welcome To The 10th Annual Hacking Conference



The Institute of Internal Auditors
Chicago

ISACA
Chicago Chapter

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session
on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

bakertilly

How to address the new SEC cyber disclosure rule

November. 7, 2023

Meet the presenters

Joe Shusko

Principal, Risk Advisory

P: +1 (312) 228 7269
E: joe.shusko@bakertilly.com

Andres Castillo

Manager, Risk Advisory

P: +1 (513) 675 1751
E: andres.castillo@bakertilly.com

Agenda

- Overview of the cyber disclosure rule
- Actions to assess readiness
- Using the AICPA cyber risk management framework
- Questions

Polling question #1

Have you read the SEC disclosure guidance?

a) Yes, and the guidance was clear as day.

b) Yes, but I could still use clarification on what the guidance means for my organization.

c) No, that's why I'm attending this webinar!

d) No, the guidance does not apply to me/my organization.

Overview of the cyber disclosure rule

Disclosure requirements include

Material incident

- Within Item 1.05 in Form 8-K (or 6-K for FPI)
- Within 4 days of determining incident to be material
- Should consider individual incident and multiple related incidents
- Subsequent filings may be required as additional information becomes available

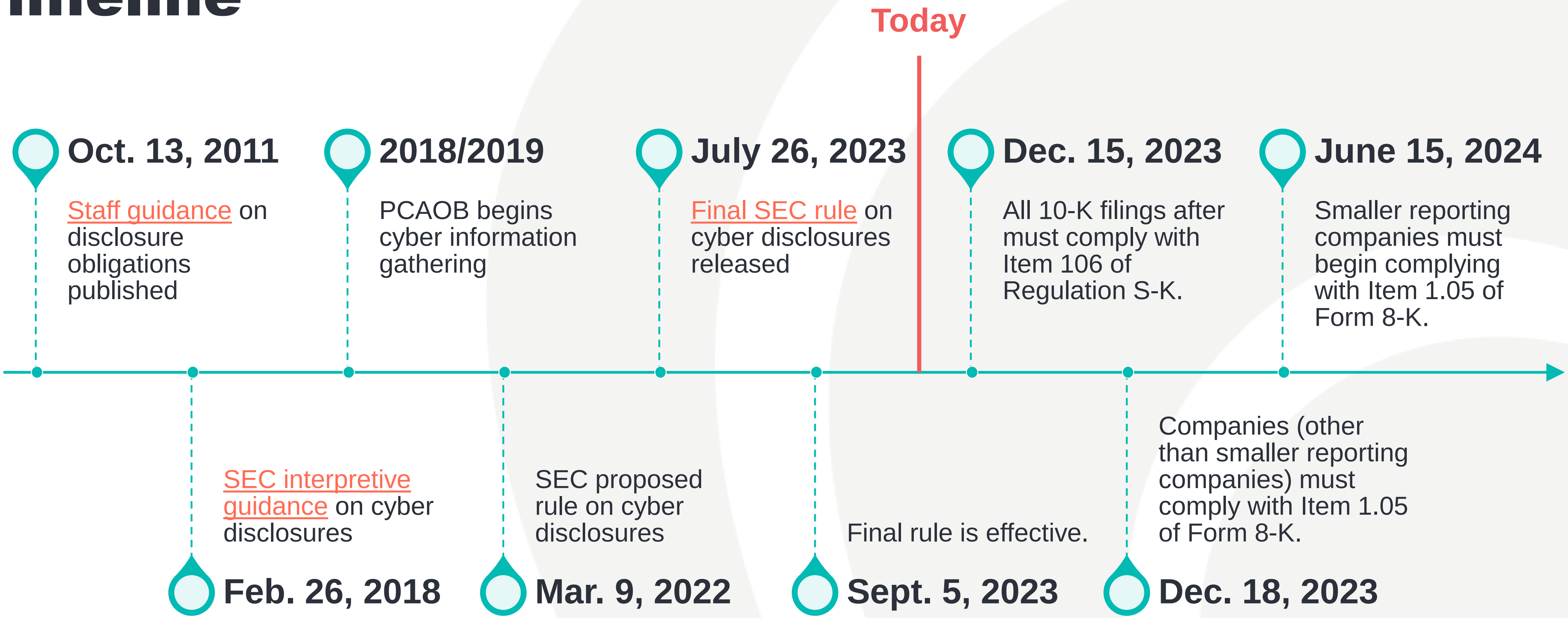
Cyber risk management & strategy

- Within Item 1C in Form 10-K (or Item 16K in Form 20-F for FPI)
- Sufficient detail for an investor to understand process for "assessing, identifying and managing" material cyber risks
- Include consideration for the use of third parties
- Disclose affect on business strategy, operations and financial reporting

Cyber governance

- Within Item 1C in Form 10-K (or Item 16K in Form 20-F for FPI)
- Board's role in oversight of cyber risk
- Management's role and expertise in assessing and managing cyber risk
- How information is shared across those charged with governance

Timeline



Oct. 13, 2011

Staff guidance on disclosure obligations published

Feb. 26, 2018

SEC interpretive guidance on cyber disclosures

2018/2019

PCAOB begins cyber information gathering

Mar. 9, 2022

SEC proposed rule on cyber disclosures

July 26, 2023

Final SEC rule on cyber disclosures released

Sept. 5, 2023

Final rule is effective.

Today

Dec. 15, 2023

All 10-K filings after must comply with Item 106 of Regulation S-K.

Dec. 18, 2023

Companies (other than smaller reporting companies) must comply with Item 1.05 of Form 8-K.

June 15, 2024

Smaller reporting companies must begin complying with Item 1.05 of Form 8-K.

New definitions

- **Cybersecurity incidents:** 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 threats:** 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:** 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.

(Source: SEC Rule, Release Nos. 33-11216; 34-97989)

Assessing readiness

Polling question #2

How far along are you with updating governance documentation for cyber incidents?

a) Have not started

b) Started, but finding it a challenge

c) Started and feeling confident!

d) Complete. We got this covered!

e) This question does not apply to me.

INCIDENT DISCLOSURE

What is your process to identify and report material cybersecurity incidents?

Identification of key roles and responsibilities in monitoring cyber risks

Conducting a periodic cyber risk assessment to identify most likely threats

Establishing cyber communication to share relevant information both internally and externally

Engaging with appropriate third parties; legal, cyber forensics, insurance, etc.

Appropriate escalation protocols with the disclosure committee

INCIDENT DISCLOSURE

How do you plan to measure the materiality of incidents?

- Required disclosure based on law or regulation
- Had a material effect on financial position or operations
- Resulted in ransomware payout
- Caused withdrawal from material markets
- Caused cancellation of material contracts
- Potential recovery through cyber insurance

INCIDENT DISCLOSURE

How reliable is the information needed to perform your disclosure analysis?

- Process for assessing completeness and accuracy of information needed
- Dependence on third parties and their potential exposure
- Timely availability and recoverability of data
- Whether data is subject to processing integrity controls ensuring their reliability
- Estimates of recoverability from insurance claims
- Protection against subsequent attacks
- Consideration of potential unknown impacts

INCIDENT DISCLOSURE

How will you document your rationale and conclusions?

How much information is necessary to capture conclusions

How the rationale was informed by a cyber risk assessment

Consideration for timing, audience, and nature of information captured in conclusions

Whether there is need for third party involvement or if the documentation should be performed under privilege

Whether the incident was an indication of a breakdown of controls

Who will be responsible for review and oversight of rationale

Will you be able to report the right amount of information within the 4-day timeline following materiality determination?

Identified relevant stakeholders (internal and external) needed to support disclosure

Established a disaster scenario for cyber incident that includes protocol for disclosure

Exercised the disclosure scenario in a tabletop to support the ability to respond timely

It is important to note that disclosure timeliness requirements are AFTER determination of materiality.

Are your policies, procedures and controls sufficient?

- The existence of a formal security policy and/or incident response policy
- Aligned with the nature of the business and information potentially at risk
- Whether the security program aligns with an accepted framework (e.g., NIST, ISO, CIS, etc.)
- Considering the security awareness of your workforce and contractors
- Cybersecurity objectives that include commitments to third parties, compliance with laws and regulations, industry standards, etc.
- Determination of risk appetite and who within management has authority to accept risk
- Consideration for dependence on third parties in both operations and cybersecurity posture

Is your cybersecurity risk assessment sufficient?

Processes are defined and accepted by those charged with governance

Key process influencers are accountable for their actions surrounding cyber risk

Tools and enablers are in place to maintain efficient and timely incident detection, management and response

Assessments evolve in tandem with emerging threats

Assessments are performed periodically to re-evaluate cyber risk posture

Are management practices and expertise appropriate to monitor cybersecurity risk?

Clearly defined roles and required expertise for management's cyber function

Level of dependence on third parties to achieve cybersecurity objectives

What tone at the top is established by management and the board

Established accountability and reporting lines

Monitoring of third-party risk

GOVERNANCE

Is the board receiving the right information to oversee cybersecurity risk?

Role of the board and their access to cyber expertise

Board committee designated to oversee cyber risk

Frequency and detail of information presented to the board related to cyber risk

Approval over management’s cybersecurity objectives

Process by which the board is informed of the results of management’s cyber monitoring

Process by which the board is informed of security incidents

Polling question #3

How familiar are you with the AICPA cyber risk management framework?

a) Very

b) Somewhat

c) Not at all

AICPA cybersecurity risk management program

Background

- AICPA defines an entity's cybersecurity risk management program as *the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, migrate, and recover from, on a timely basis, security events that are not prevented.*
- The AICPA published its cybersecurity risk management reporting framework for two primary purposes:

Management

To be used when preparing a description of the entity's cybersecurity risk management program

Practitioners

To be used when evaluation an entity's description in connection with services performed on that entity's cybersecurity risk management program

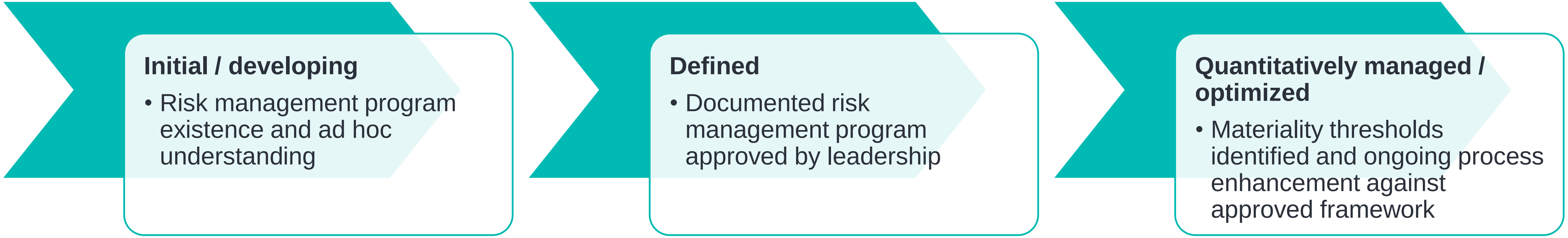
AICPA cybersecurity risk management reporting framework

The 19 description criteria are organized in the following categories:

- Nature of business and operations
- Nature of information at risk
- Cybersecurity risk management program objectives
- Factors that have a significant effect on inherent cybersecurity risk
- Cybersecurity risk governance structure
- Cybersecurity risk assessment process
- Cybersecurity communications and the quality of cybersecurity information
- Monitoring of the cybersecurity risk management program
- Cybersecurity control processes

Advantages of applying a cyber risk framework

- Leveraging a defined framework supports a more mature program
- Framework serves as an independent implementation guide
- Bias is lessened when defining programs and processes against a framework



Initial / developing

- Risk management program existence and ad hoc understanding

Defined

- Documented risk management program approved by leadership

Quantitatively managed / optimized

- Materiality thresholds identified and ongoing process enhancement against approved framework

The AICPA cybersecurity risk management reporting framework addresses topics consistent with the adopted SEC cyber disclosure rule, including:

- Data security, confidentiality, availability
- Internal and external environment
- Laws, regulations and enforcement
- Risk management and appetite
- Oversight, communication and monitoring
- Third-party risk management

Steps in using the AICPA cybersecurity risk management framework

- Compare and document your existing cybersecurity risk management program against the AICPA cybersecurity risk management description criteria
- Identify potential gaps/weaknesses in your cybersecurity risk management program compared to the AICPA cybersecurity risk management description criteria
- Compare and identify gaps/weaknesses in your cybersecurity risk management program to the SEC cyber disclosure rule
- Remediate gaps/implement improvements to your cybersecurity risk management program
- Evaluate the maturity of your cybersecurity risk management program controls and implement improvements based on your risk appetite

Polling question #4

Do you have board members with cyber expertise?

a) Yes

b) No

c) I don't know

d) This question does not apply to me

Recap

The U.S. Securities and Exchange Commission (SEC) adopted final rules requiring disclosure of material cybersecurity incidents on Form 8-K and periodic disclosure of a registrant's cybersecurity risk management, strategy and governance in annual reports.

New Form 8-K Item 1.05

- Disclosure required within four (4) business days following management determination that a cyber incident is material.

New Regulation S-K Item 106

- Describe process for identifying, assessing and managing material risks from cyber threats. Describe cyber risk governance roles and responsibilities for the board of directors and management.

Forms 20-F and 6-K

- Amended to require foreign private issuers to provide disclosures regarding the board's oversight of risks from cybersecurity threats and management's role in assessing and managing material risks from cybersecurity threats. Additional requirements include disclosure of material cybersecurity incidents.

Governance, Risk, and Compliance Leadership Actions (as needed)

- ✓ Identify and address current process gaps in current disclosure controls and procedures and ensure responsiveness to comply with the disclosure requirements.
- ✓ Clarify reporting lines and communication channels for escalating and disclosing material incidents.
- ✓ Determine thresholds and qualifiers in assessing materiality of a breach, or its impact on business operations and agree to how these determinations will be documented.
- ✓ Review and enhance third-party terms and conditions to include relevant cyber incident disclosure requirements.
- ✓ Enhance governance and process documentation with the revised key definitions.
- ✓ Assess cybersecurity risk oversight practices, both by management and the board and realign subcommittee directives, as necessary.

Closing remarks and questions

Stay in touch

Joe Shusko
Principal, Risk Advisory

P: +1 (312) 228 7269
E: joe.shusko@bakertilly.com

Andres Castillo
Manager, Risk Advisory

P: +1 (513) 675 1751
E: andres.castillo@bakertilly.com

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought. Tax information, if any, contained in this communication was not intended or written to be used by any person for the purpose of avoiding penalties, nor should such information be construed as an opinion upon which any person may rely. The intended recipients of this communication and any attachments are not subject to any limitation on the disclosure of the tax treatment or tax structure of any transaction or matter that is the subject of this communication and any attachments. Baker Tilly US, LLP, trading as Baker Tilly, is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities.

bakertilly

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter