CRIMSON VISTA

NORTON ROSE FULBRIGHT

The SEC's New Cybersecurity Rules for Public Companies

WHAT YOU NEED TO KNOW TO STAY COMPLIANT: BEYOND THE CHECKBOX

November 21, 2024

BDO

With You Today

CRISTINA DOLAN

Executive Cybersecurity Advisor

MODERATOR

Crimson Vista

JAMEY LOUPE

Risk Advisory Services Principal

BDO USA

SETH NIELSON

Founder and Chief Scientist

Crimson Vista

WILL DAUGHERTY

Partner - Head of Cybersecurity

Norton Rose Fulbright

Learning Objectives

- Describe SEC Cybersecurity Disclosure Requirements
- Identify the Role of Management in Cyber Disclosure Compliance
- Design Effective Control Practices for Cyber Disclosure Compliance
- Construct Governance Protocols for Active Cyber Risk Management
- Employ Continuous Cyber Risk Defense and Disclosure Practices

Cristina Dolan

EXECUTIVE CYBERSECURITY ADVISOR, **CRIMSON VISTA**

Cristina Dolan is a renowned cybersecurity executive, and advisor for Crimson Vista, currently serving on the boards and audit committees of several prominent public technology companies. At RSA Security, Netwitness, she held key leadership roles, including Managing Director for LATAM, Head of the Americas Channel, and Global Head of Alliances. An accomplished entrepreneur, Cristina launched startups such as iXledger, a cyber insurance marketplace focused on advanced technologies. She is also a co-founder of Additum, a European 'Value Based Healthcare' ecosystem. Currently, Cristina is a Senior Lecturer at Columbia University's Technology Management Program and has contributed to the World Economic Forum's cybersecurity publications and authored books on ESG and Data. Her career includes executive roles at IBM, Oracle, Disney, and Hearst, as well as leading the MIT AI spin-out, Wordstream. Cristina's achievements have been recognized with numerous accolades, including the Harold E. Lobdell Distinguished Service Award from MIT and the Coup de Coeur du CEFCYS Cybersecurity Europe award.

EDUCATION

- Master of Science degree from the MIT Media Lab
- Master of Computer Science
- Bachelor of Electrical Engineering degree

917-226-6626
cristinadolan@gmail.com

Jamey Loupe

RISK ADVISORY SERVICES PRINCIPAL, **BDO USA**

Jamey Loupe is a Principal in BDO's Risk Advisory Services practice where he focuses on IT risk advisory solutions. He has more than 15 years of progressive experience leading and organizing teams and projects and has provided audit and advisory services to various Fortune 500 and mid-size multinational companies in multiple industries. Prior to joining BDO, Jamey worked in the internal audit and information technology (IT) security functions for oil and gas services companies. Prior to that he was with a Big Four Firm. His experience includes:

- Leading, managing and conducting IT internal audits
- Managing complex IT Sarbanes-Oxley (SOX) compliance projects
- Recommending and implementing IT process improvements
- Conducting and leading enterprise resource planning (ERP) pre- and post-implementation reviews
- Conducting IT security assessments

EDUCATION

- Cybersecurity Certificate, Harvard University
- M.L.A., Information Management Systems, Harvard University Extension
- B.A., Information Systems Decision Sciences, Louisiana State University

713-407-3935
jloupe@bdo.com

Seth Nielson, PhD

FOUNDER AND CHIEF SCIENTIST, **CRIMSON VISTA**

Dr. Nielson is the Founder and Chief Scientist of Crimson Vista Inc. In addition to his work at Crimson, he is also Adjunct Faculty at the University of Texas at Austin.

Dr. Nielson has consulted on a wide range of technical projects including the development of security communications, commodity hardware acceleration, secure file systems, privacy, auditing, vulnerability analysis, and cryptographic implementation. He has also been retained by companies ranging from start-ups to Fortune-100 for security evaluation and advising. Additionally, Dr. Nielson is active in research in areas such as formal security proofs, distributed systems, and ransomware mitigation.

Beyond technical consulting, Dr. Nielson has also consulted on a wide range of legal cases and has given expert testimony in trial. He has submitted or contributed to dozens of reports on topics including: high-frequency trading, antivirus software, advanced firewall filtration, e-commerce transmissions, cryptographic protocols, and many others.

EDUCATION

- Master of Science degree from the MIT Media Lab
- Master of Computer Science
- Bachelor of Electrical Engineering degree

512-387-4310

seth@crimsonvista.com

Will Daugherty

HEAD OF CYBERSECURITY, **NORTON ROSE FULBRIGHT**

Will Daugherty is a nationally recognized leader in data protection and privacy and is a partner in the Norton Rose Fulbright's data protection, privacy and cybersecurity group. Clients in a broad-range of industries turn to Will for his experience, practical solutions, and thought leadership on managing risks associated with data and technology, including assessing organizations' security postures; developing information security programs; privacy and cybersecurity training for boards, executives and employees; privacy compliance; incident response preparedness; and leading organizations through data security incidents.

713-651-5684

will.daugherty@nortonrosefulbright.com

Agenda

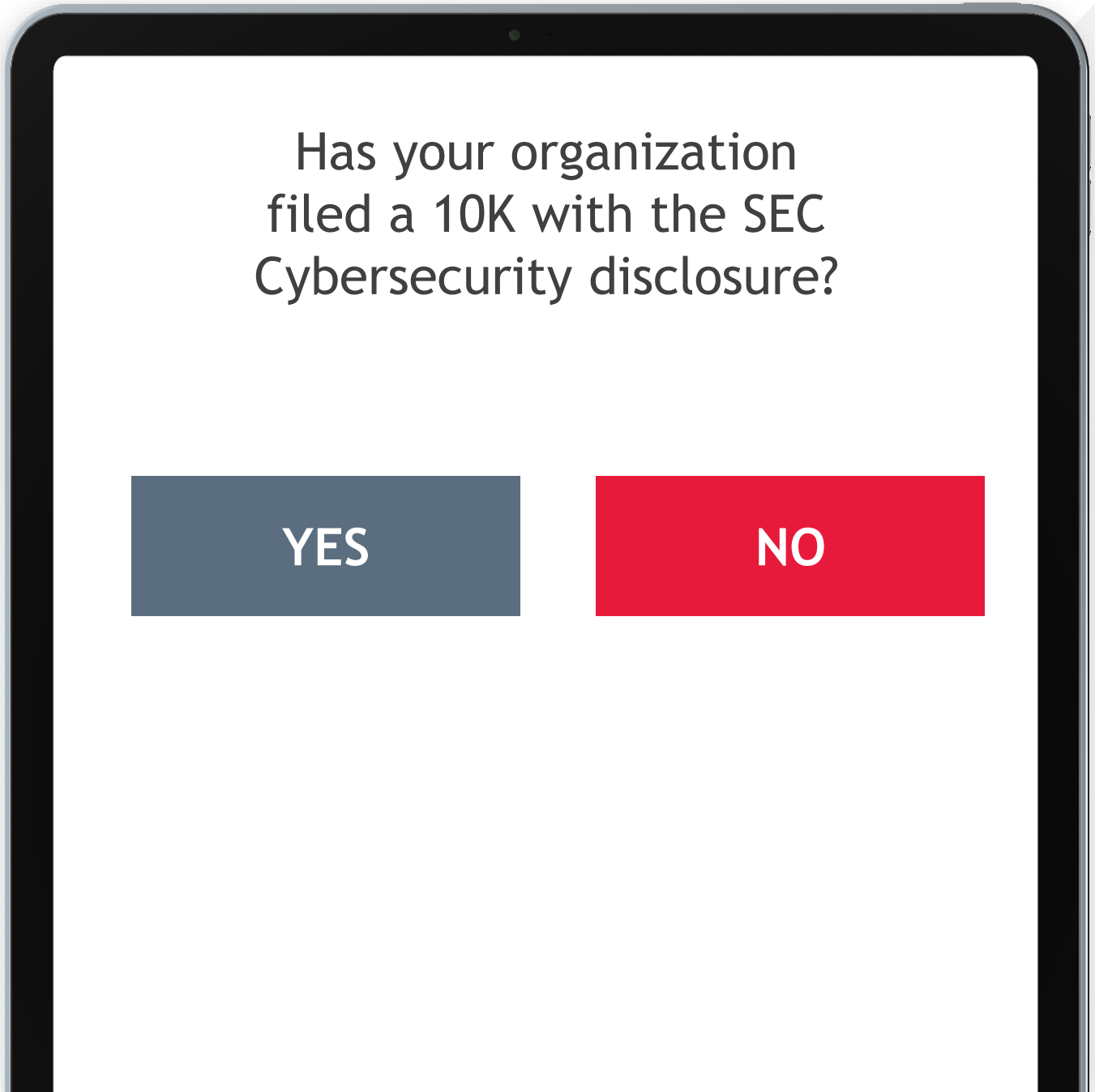
SEC’s Cyber Disclosure Requirements

The Role of Internal Audit in Cyber Disclosure Compliance

Effective Internal Audit Practices for Cyber Disclosure Compliance

Continuous Cyber Risk Defense and Disclosure Practices

Knowledge Check 1



SEC FINAL RULES

Cybersecurity Risk Management, Governance, & Disclosure

WHY SHOULD YOU CARE

- **10-K requirement:** All SEC registrants to provide disclosures on the maturity of their cybersecurity controls around incident detection, response and reporting on their next 10-K filing
- **8-K requirement:** Disclose cybersecurity incidents (An Item 1.05 Form 8-K must be filed) within four business days from the date they determine the incident(s) to be material

WHEN DO YOU NEED IT

- **10-K requirement:** 10-K requirement begins with annual reports for FY ending on or after December 15, 2023
- **8-K requirement:** All registrants other than smaller reporting companies (SRCs) must begin complying on the latter of 90 days after publication in the Federal Register or December 18, 2023. SRCs will have an additional 180 days and must begin complying on the latter of 270 days from the effective date of the rules or June 15, 2024

WHAT IS NEEDED

- **10-K requirement:** Describe processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats
  - Recommend clients have an independent party perform a cybersecurity maturity assessment specifically addressing the SEC disclosure requirements
- **8-K Requirement:** When a security incident occurs a disclosure is triggered, the registrant must disclose the material:
  - Aspects of the scope, nature, and timing of the cybersecurity incident
  - Impact or reasonably likely material impact on the registrant's financial condition and results of operations

CLICK HERE for Final SEC Rule

CLICK HERE for SEC Fact Sheet

CLICK HERE for BDO Bulletin

Cybersecurity Governance

DISCLOSURES

Cybersecurity Governance

Cybersecurity Risk Management

1. Use of External Cybersecurity Consultants
2. Third-Party Service Provider Risk Management
3. Cybersecurity Incident Prevention and Mitigation
4. Business Continuity and Recovery Plans

Material Cybersecurity Incidents

COMPANY ACTIVITIES

Disclosure Requirement:

- Describe board oversight of cybersecurity risks
- Explain management's role in assessing and managing risks
- Disclose relevant experience of responsible personnel
  - Who are the responsible personnel?
  - What are their roles and what do they do?
  - What do you need? CISO? Security Analyst?
  - Are there inconsistencies between disclosed practices and actual operations?

Cybersecurity Risk Management

DISCLOSURES

Cybersecurity Governance

Cybersecurity Risk Management

1. Use of External Cybersecurity Consultants
2. Third-Party Service Provider Risk Management
3. Cybersecurity Incident Prevention and Mitigation
4. Business Continuity and Recovery Plans

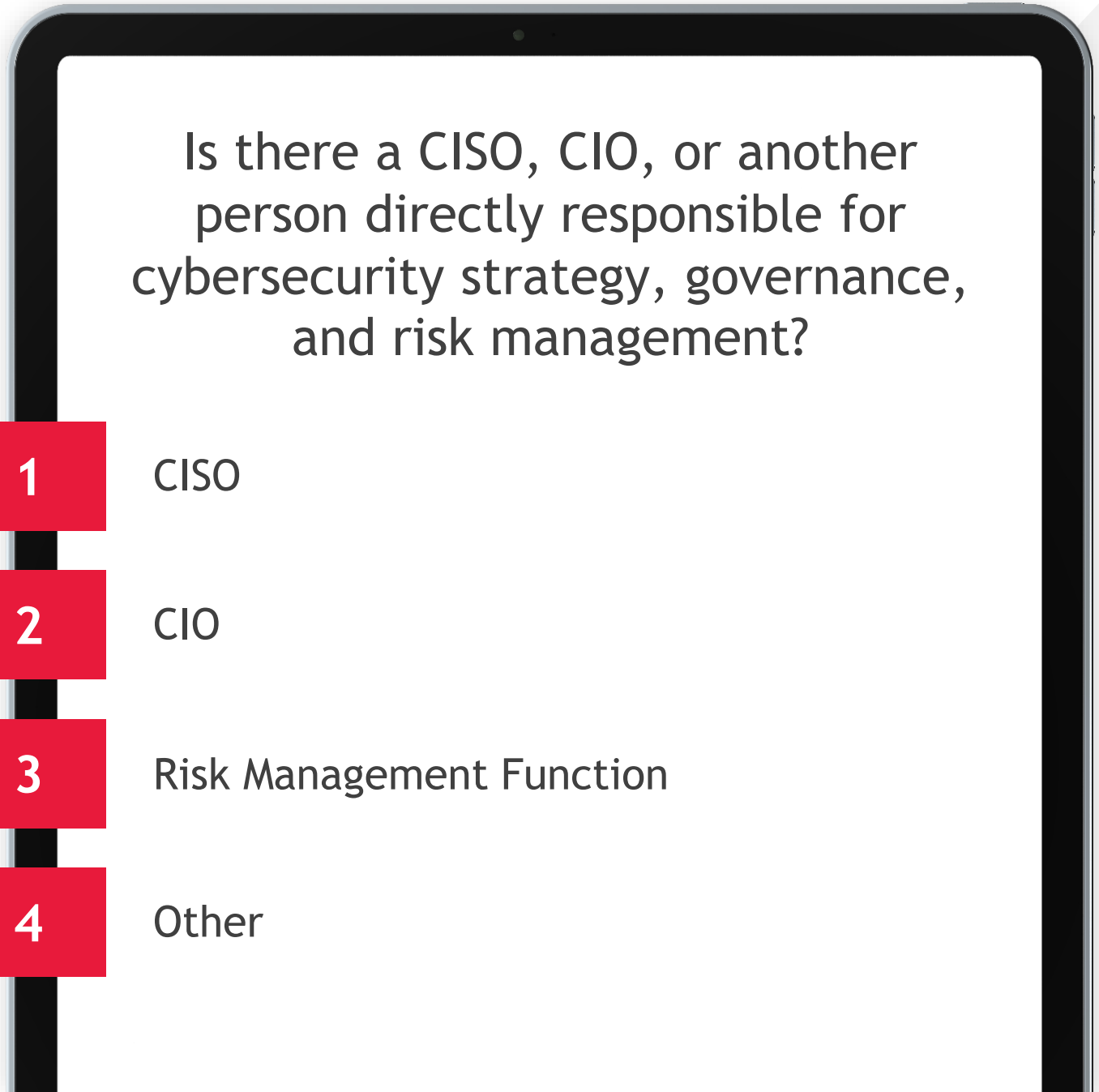
Material Cybersecurity Incidents

COMPANY ACTIVITIES

Disclosure Requirement:

- Disclose the organization's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for reasonable investor to understand the processes
  - Do not need to include level of detail that increase risk of vulnerability to cyber attack
  - Must include non-exclusive list of topics in the disclosures
- Describe whether any risks from material "cybersecurity threats" have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial conditions, and if so how.
  - What types of threats need to be considered?

Knowledge Check 2



Cybersecurity Risk Management

DISCLOSURES

Cybersecurity Governance

Cybersecurity Risk Management

1. Use of External Cybersecurity Consultants
2. Third-Party Service Provider Risk Management
3. Cybersecurity Incident Prevention and Mitigation
4. Business Continuity and Recovery Plans

Material Cybersecurity Incidents

COMPANY ACTIVITIES

Disclosure Requirement:

- Disclose if the organization includes Cybersecurity Risk Management in their Enterprise Risk Management program
- Disclose if the company has a cybersecurity risk assessment program
- Provide risk assessment program description
- Disclose the processes for auditing, assessing, identifying, and managing cybersecurity risks (i.e., NIST Guidelines)
- Disclose the use of third-party cybersecurity assessments
  - What is risk assessment?
  - Is the assessment complete and up to date?
  - Is there a consistent use of risk assessment methodologies and are all material risks addressed?
  - What are the NIST Guidelines?

External Cybersecurity Consultants

DISCLOSURES

Cybersecurity Governance

Cybersecurity Risk Management

1. **Use of External Cybersecurity Consultants**
2. Third-Party Service Provider Risk Management
3. Cybersecurity Incident Prevention and Mitigation
4. Business Continuity and Recovery Plans

Material Cybersecurity Incidents

COMPANY ACTIVITIES

Disclosure Requirement:

- Disclose whether the company engages Third-Party vendors, consultants, or auditors for cybersecurity assessments
- Describe the role of the external cybersecurity consultants
- Disclose the use of third-party cybersecurity assessments
  - What is the role of external cybersecurity consultants?
  - Reliance on third-party assessments
  - Validation of third-party assessments
  - Disclosure of conflicts of interest
  - Consistent criteria for selecting or evaluating assessors

Knowledge Check 3

Third-Party Risk Management

DISCLOSURES

Cybersecurity Governance

Cybersecurity Risk Management

1. Use of External Cybersecurity Consultants
2. **Third-Party Service Provider Risk Management**
3. Cybersecurity Incident Prevention and Mitigation
4. Business Continuity and Recovery Plans

Material Cybersecurity Incidents

COMPANY ACTIVITIES

Disclosure Requirement:

- Disclose processes, policies, and procedures for overseeing and mitigating cybersecurity risks from third-party providers
  - Why and how third-party service providers introduce risk?
  - Solutions for managing third-party risk
  - Is there a complete inventory of third-party relationships?
  - Is there adequate due diligence on vendor selection?
  - Is there ongoing monitoring of third-party risks?
  - Are sub-contractors (fourth-party) risks included?

Cybersecurity Incident Prevention and Mitigation

DISCLOSURES

Cybersecurity Governance

Cybersecurity Risk Management

1. Use of External Cybersecurity Consultants
2. Third-Party Service Provider Risk Management
3. **Cybersecurity Incident Prevention and Mitigation**
4. Business Continuity and Recovery Plans

Material Cybersecurity Incidents

COMPANY ACTIVITIES

Disclosure Requirement:

- Describe activities to prevent, detect, and minimize the effects of cybersecurity incidents
- Disclose the use of cybersecurity tools and technologies

Example Activities:

- Pen tests, security tools/software/devices, code reviews

Tools:

- Intrusion detection, endpoint hardening/monitoring, cloud monitoring
  - Focus on both prevention and detection/response programs
  - Disclosing security details that create additional vulnerabilities
  - Failure to keep up with evolving threats and apply consistent security measures across the organization

Business Continuity and Recovery Plans

DISCLOSURES

Cybersecurity Governance

Cybersecurity Risk Management

1. Use of External Cybersecurity Consultants
2. Third-Party Service Provider Risk Management
3. Cybersecurity Incident Prevention and Mitigation
4. **Business Continuity and Recovery Plans**

Material Cybersecurity Incidents

COMPANY ACTIVITIES

Disclosure Requirement:

- Disclose the existence of business continuity, contingency, and recovery plans in the event of a cybersecurity incident
- Describe key components of these plans including:
  - **Exercises:** table-top, training
  - **Tools:** backup, redundancy, fallback
  - **Incident Response:** containment, remediation

Disclosure, Insurance, External Cybersecurity Consultants, Audit, Attribution

- Defense in depth: 'Assume Compromise" …now what?
- Rehearse exercises, and test the up-to-date plans
- Address all critical business functions
- Coordination with third-party providers in recovery plans
- Accurately state the effectiveness of recovery capabilities

Material Cybersecurity Incidents

DISCLOSURES

Cybersecurity Governance

Cybersecurity Risk Management

1. Use of External Cybersecurity Consultants
2. Third-Party Service Provider Risk Management
3. Cybersecurity Incident Prevention and Mitigation
4. Business Continuity and Recovery Plans

Material Cybersecurity Incidents

COMPANY ACTIVITIES

Disclosure Requirement:

- Determine the materiality of incidents and the impact of a breach
- Disclose within 4 business days of materiality determination
- Describe the nature, scope, and timing of the incident
- Assess the material impact on operations: **Lawsuits (standard of care, negligence) Regulatory Investigations, Fines, Impact, Reputation**
  - Timely material determinations
  - Consistent criteria for assessing materiality
  - Complete disclosure of incident impacts with updates as new information becomes available
  - Accurate estimation of reputational or long-term financial impacts

Knowledge Check 4

Summary of Corporate Cyber Risk Management Best Practices

- Cyber Risk Management Program which includes:
  - Risk Assessments
  - Active Management and Defense
  - Responsible Parties and Roles
  - Third Party Risk Management
  - Tested Plans and Exercises
- Third Party Providers
- Incident Prevention and Mitigation
- Business Continuity and Recovery
- Incident Response

Final Thoughts & Takeaways

TAKEAWAY 1

Board Oversight Requirements

- Cybersecurity Governance
- Cybersecurity Risk Management

TAKEAWAY 2

Cybersecurity As a Process

- Obtain insight
- Manage incidents
- Improve operations
- Measure indicators

TAKEAWAY 3

Compliance and Auditors Role

- Internal Audit
  - Independent Assessments for Board oversight
- External Audit
  - Independent Assessment for investors oversight

Questions?

Thank you

CRISTINA DOLAN

Executive Cybersecurity Advisor

MODERATOR

Crimson Vista

JAMEY LOUPE

Risk Advisory Services Principal

BDO USA

SETH NIELSON

Founder and Chief Scientist

Crimson Vista

WILL DAUGHERTY

Partner - Head of Cybersecurity

Norton Rose Fulbright

Appendix

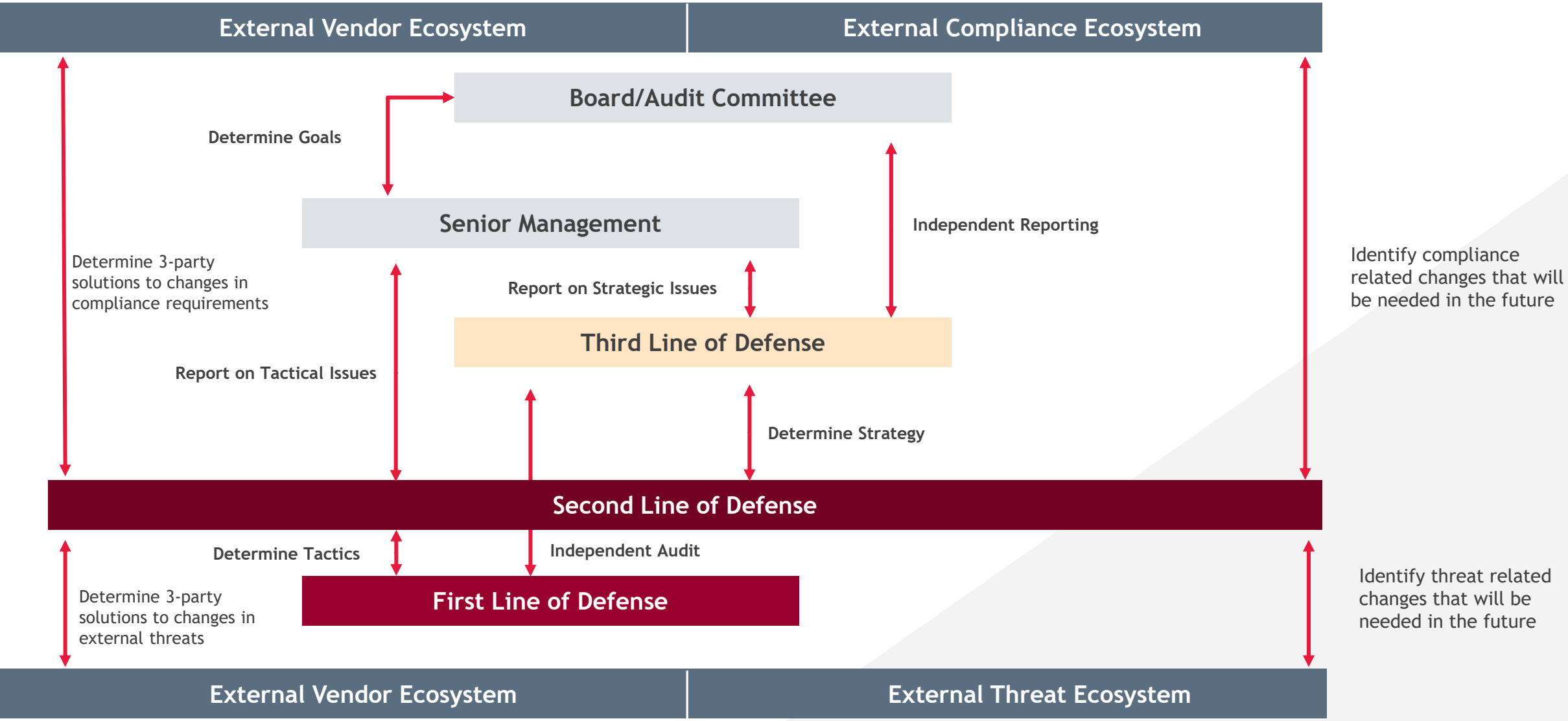
SEC Cybersecurity Risk Disclosure Requirements

DISCLOSURE REQ.	COMPANY ACTIVITIES	AUDITOR ACTIVITIES	FILING TYPE
Cybersecurity Governance	▶ Describe board oversight of cybersecurity risks ▶ Explain management's role in assessing and managing risks ▶ Disclose relevant expertise of responsible personnel	▶ Assess governance structure disclosures ▶ Evaluate board and management oversight processes ▶ Review expertise disclosures	**Form 10-K** (U.S.) **Form 20-F** (Foreign Private Issuers)
Cybersecurity Risk Management	▶ Disclose if the company has a cybersecurity risk assessment program ▶ Provide risk assessment program description ▶ Disclose the processes for auditing, assessing, identifying, and managing cybersecurity risks (i.e., NIST Guidelines) ▶ Disclose the use of third-party cybersecurity assessments	▶ Evaluate adequacy of risk management disclosures ▶ Assess consistency with known information ▶ Review risk assessment processes	**Form 10-K** (U.S.) **Form 20-F** (Foreign Private Issuers)
1. Use of External Cybersecurity Consultants	▶ Disclose whether the company engages third-party assessors, consultants, or auditors for cybersecurity assessments. ▶ Describe the role of the third-party assessor	▶ Understand the process for engaging third-party assessors. Determine competency and thoroughness.	**Form 10-K** (U.S.) **Form 20-F** (Foreign Private Issuers)
2. Third-Party Service Provider Risk Management	▶ Disclose processes, policies, and procedures for overseeing and mitigating cybersecurity risks from third-party providers	▶ Evaluate third-party risk management processes ▶ Assess adequacy of oversight disclosures	**Form 10-K** (U.S.) **Form 20-F** (Foreign Private Issuers)

SEC Cybersecurity Risk Disclosure Requirements

DISCLOSURE REQ.	COMPANY ACTIVITIES	AUDITOR ACTIVITIES	FILING TYPE
3. Cybersecurity Incident Prevention and Mitigation	▶ Describe activities to prevent, detect, and minimize the effects of cybersecurity incidents ▶ Disclose the use of cybersecurity tools and technologies ▶ Example activities: pen tests, security tools/software/devices, code reviews ▶ Tools: Intrusion detection, endpoint hardening/monitoring, cloud monitoring	▶ Review prevention and mitigation strategies ▶ Assess effectiveness of disclosed measures	**Form 10-K** (U.S.) **Form 20-F** (Foreign Private Issuers)
4. Business Continuity and Recovery Plans	▶ Disclose the existence of business continuity, contingency, and recovery plans in the event of a cybersecurity incident. ▶ Describe key components of these plans including: ▶ Exercises: table-top, training; Tools: backup, redundancy, fallback; ▶ Incident Response: containment, remediation; Disclosure, Insurance, Third-party Assessment, Audit, Attribution	▶ Evaluate adequacy of continuity and recovery plans ▶ Assess disclosure of plan components	**Form 10-K** (U.S.) **Form 20-F** (Foreign Private Issuers)
Material Cybersecurity Incidents	▶ Determine the materiality of incidents and the impact of a breach ▶ Disclose within 4 business days of materiality determination ▶ Describe the nature, scope, and timing of the incident ▶ Assess the material impact on operations: Lawsuits (standard of care, negligence) Regulatory Investigations, Fines, Impact, Reputation	▶ Review incident disclosure controls and procedures ▶ Assess materiality determination process ▶ Evaluate the timeliness of disclosure	**Form 8-K** (U.S.) **Form 6-K** (Foreign Private Issuers)

Reconceiving the role of the Second Line of Defense



Source: IANs, 2021

CONTACT US ▶

About BDO USA

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

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

For more information, please visit: www.bdo.com.

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