The Augusta Group

A Path Towards December 2023

Preparing for New SEC Cyber Disclosure

August 31st 11:00 – 12:30 EST

The Augusta Group

Supporting the audit community understand the SEC final rule, definitions and compliance requirements

Agenda

- Learning Objectives.
- Unpacking the new rule.
- Considerations – Legal and Ethical.
- Complying to the final rule.
- The Assessment and reporting of material cyber risk and incidents.
- Opportunities for internal audit.
- Closing remarks.

Author: Rachel V Rose, Andy Watkin-Child
LI: www.linkedin.com/in/rachel-v-r-95759824/
LI: www.linkedin.com/in/andywatkinchild/
LI: www.linkedin.com/in/rachel-v-r-95759824/)
email: rvrose@rvrose.com, andy@augustagrp.com , ted@chathamtech.com

The Augusta Group

Andy Watkin-Child

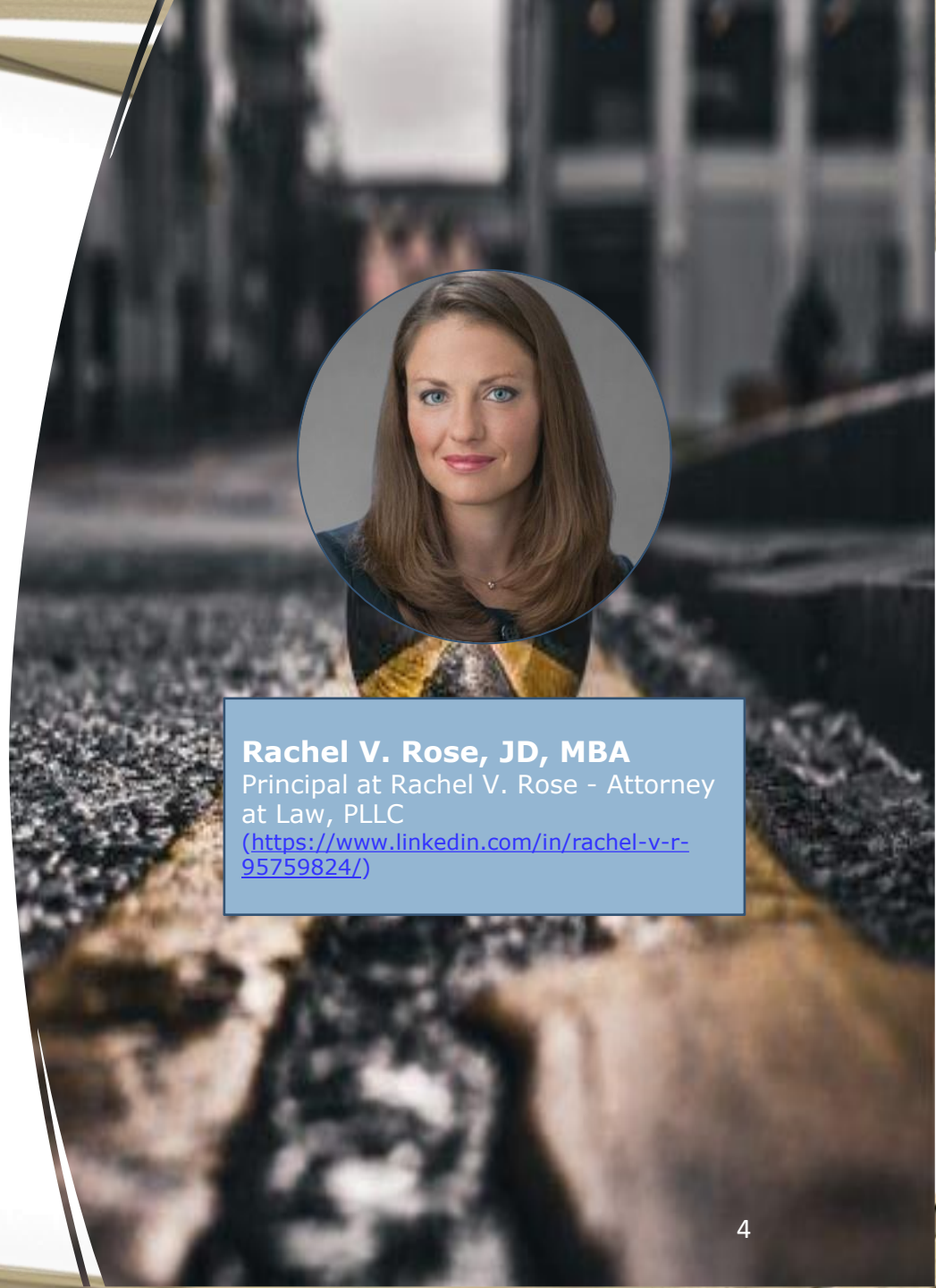
Andy Watkin-Child is a 20-year veteran of cybersecurity, risk management, and technology. He has held international leadership positions in the first and second lines of defense for cybersecurity, cyber-risk management, operational risk, and technology within engineering/manufacturing, financial services, and publishing/media companies with balance sheets of more than €1 trillion. He is an experienced member of management boards, global risk leadership teams, and cybersecurity, operational risk, and GDPR committees. Watkin-Child is the Founding Partner of Parava Security Solutions, supporting organizations in delivering cyber-risk management and cyber regulatory programs. He is also the founding partner of the Augusta Group, a U.S advisory company focused on the harmonisation of cyber risk management between the U.S, UK and Europe.

Andy Watkin-Child CSyP, CEng, AMAE
Cyber risk management advisor, former Group VP Cyber, CISO, Counsel appointed cyber adviser (https://www.linkedin.com/in/andywatkinchild/)

The Augusta Group

Rachel V Rose

Rachel V. Rose advises and represents clients on healthcare, cybersecurity, securities, as well as qui tam compliance, transactional, litigation, and government enforcement matters. She also teaches bioethics as an Affiliated Member with Baylor College of Medicine's Center for Medical Ethics and Health Policy. She has served as a testifying expert and is often quoted in publications. Rachel has held numerous leadership roles with the Federal Bar Association, co-edited the American Health Lawyers Association's Enterprise Risk Management Handbook for Healthcare Entities (2nd Edition), and co-authored two American Bar Association books. She has been named consecutively to the Texas Bar College, the National Women Trial Lawyers Association's Top 25, the National Trial Lawyers Association's Top 100, and The Nation's Top One Percent. In 2023, she was selected for SuperLawyers (healthcare).



Rachel V. Rose, JD, MBA
Principal at Rachel V. Rose - Attorney at Law, PLLC
(https://www.linkedin.com/in/rachel-v-r-95759824/)

The Augusta Group

Michael Downing

Michael Downing is Senior Director for U.S. Advocacy at The IIA. Previously, as Deputy Assistant Secretary for Intergovernmental Affairs at the U.S. Department of Labor (DOL), he liaised with state and local governments during the outset of the COVID-19 pandemic and helped coordinate implementation of certain CARES Act provisions. Downing formerly served as a member of the president's transition team at the U.S. General Services Administration (GSA), where he was later appointed Deputy Chief of Staff and White House Liaison. His earlier senior political and state government positions in Pennsylvania included Deputy Director of Public Liaison to the Governor of Pennsylvania, responsible for coordinating executive nominations and appointments made by the Governor to 400+ boards and commissions.

Michael Downing
(https://www.linkedin.com/in/michael-downing-91a8424a/)

SEC Cybersecurity Disclosures:

Unpacking the new rule

The Augusta Group

Learning objectives

Preparing internal audit for the new SEC final rule

1. The importance of materiality, reasonableness and adequate compliance to the SEC ruling.
2. The evaluation of material cyber risks, required for Form 10-K and Form 20-F disclosures that will be due beginning with annual reports for fiscal years ending on or after December 15, 2023.
3. Material cyber incident disclosures by U.S domestic and International Foreign Issuers (Form 8-K and Form 6-K) due from the 18th December 2023. Disclosures to be submitted 4 business days after a company determines that a material cybersecurity incident has occurred.
4. Adequate compliance to the Final ruling.
5. Legal and fiduciary considerations.
6. The important role Internal Audit has in the oversight, assurance and attestation of material cyber risk and material cyber incident disclosure to the SEC.

The Augusta Group

Unpacking the New Rule

Materiality, adequacy, and the role of a reasonable investor

1. Materiality, adequacy, and the role of a reasonable investor
2. Governance, material risk, incident and reporting requirements
   - ➢ What, how, and the challenges with compliance and disclosure
     - • Governance
     - • Material cyber risks
     - • Material cyber incident
3. Legal and ethical considerations

The Augusta Group

Materiality, Adequacy and a Reasonable Investor

Definitions a covered entity should consider

Materiality, Adequacy and the Role of a Reasonable Investor

- **Materiality:** The Material impact of a cyber incident on a registrant is central to the determination of whether to notify the SEC (Form 8-K) of the incident. Materiality is a key qualified in determining whether any risk from cybersecurity threats (including as a result of any previous cybersecurity incidents) has affected or a 'reasonably' likely to affect a registrant.
- **Reasonable:** Information is material if there is a substantial likelihood that a 'reasonable' investor would consider it important. Materiality determinations must be made 'without unreasonable delay' and registrants are required to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes and risks.
- **Adequate:** Registrants are to provide investors with 'adequate' information to gain an 'adequate' understanding of the impact of a cyber incident and make decisions on incident 'materiality'. The registrant is required to provide up-to-date disclosures on their preparations for 'adequate cyber security risk management'.

The Augusta Group

Governance and Reporting Requirements

What, How, and the Challenges with Compliance and Disclosure

Governance

17 CFR 229.106(c)(1) (Regulation S-K "Item 106(c)(1)"). (P.68)
"[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."

and registrants

17 CFR 229.106(c)(2) (Regulation S-K "Item 106(c)(2)"). (P.69)
- must "[d]escribe management's role in assessing and managing the registrant's material risks from cybersecurity threats."

requiring 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."

The Augusta Group

Governance and Reporting Requirements

What, How, and the Challenges with Compliance and Disclosure

Risk Management and Strategy

The SEC is adopting 17 CFR 229.106(b)(1) (Regulation S-K "Item 106(b)(1)"). Requiring 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." (P.61)

and registrants

The SEC is adopting 17 CFR 229.106(b)(2) (Regulation S-K "Item 106(b)(2)")16. Requiring 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." (P.63)

The Augusta Group

Governance and Reporting Requirements

What, How, and the Challenges with Compliance and Disclosure

Incident disclosure

'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.' (P.29)

and

'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.' (P.185)

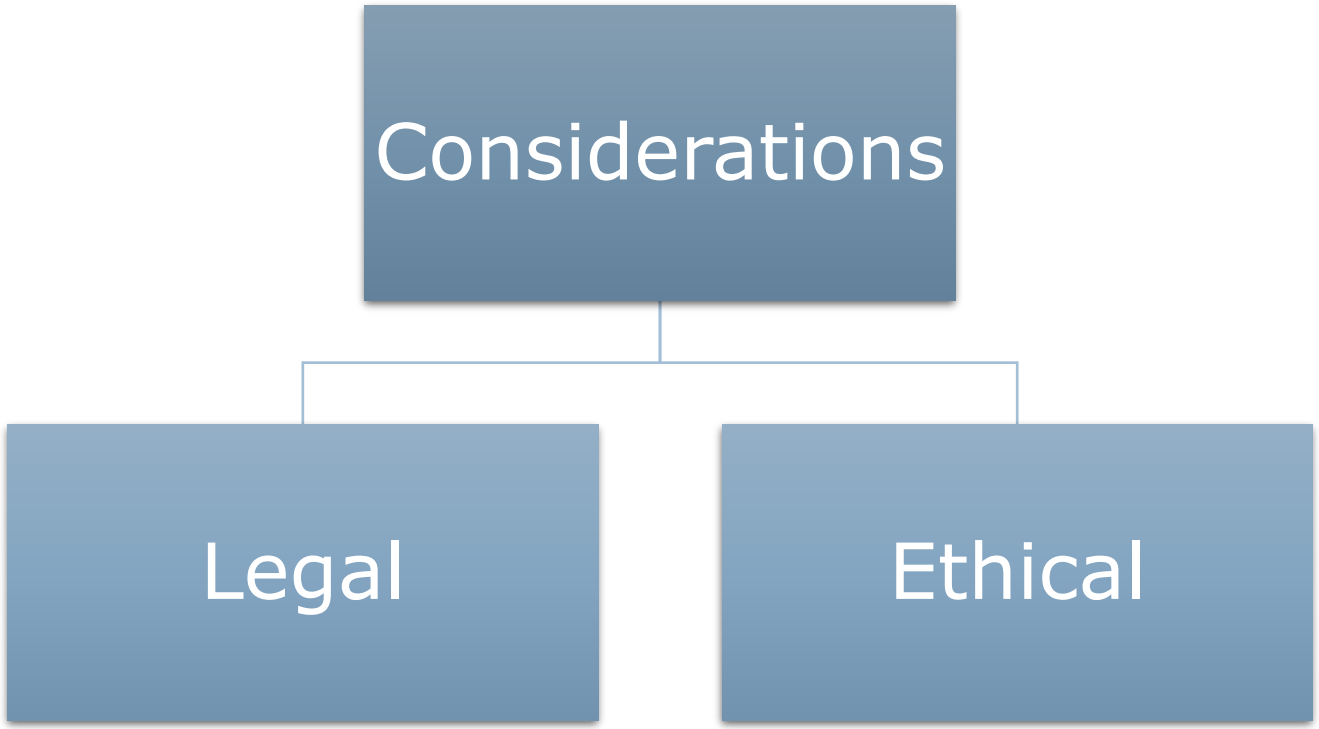
and for Periodic Reporting

'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.' (P.50)

The Augusta Group

Legal and Ethical Considerations

What, How, and the Challenges with Compliance and Disclosure



The Augusta Group

Complying with the final rule

The Augusta Group

Complying to the Final Rule

Preparing interna audit for the new SEC final rule

Complying to the Final Rule

1. Understand the final ruling, its effect on the registrant and the SEC compliance drivers, including the legal and ethical considerations.
2. Define materiality, reasonableness and adequacy for the organisation
3. Develop a Governance framework.
4. Evaluate the current cybersecurity risk management program and close gaps.
5. Evaluate the current cybersecurity framework profile and security program.
6. Material cyber incident evaluation and disclosure.

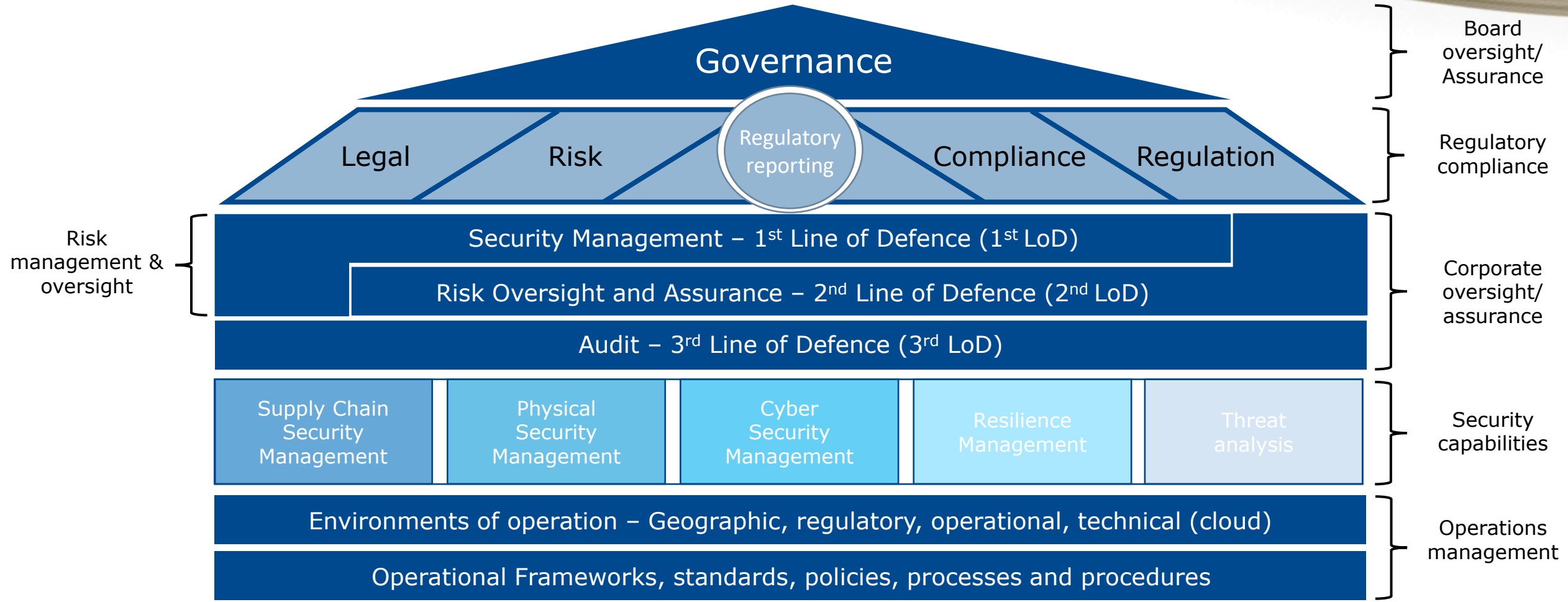
The Augusta Group

Assessment and reporting of Material Cyber Risk and Incidents

The Augusta Group

Cyber Risk Governance

A 3 Line of Defense model for cyber risk compliance



The Augusta Group

Cyber Risk Evaluation

A process to oversight and assure cyber risk management

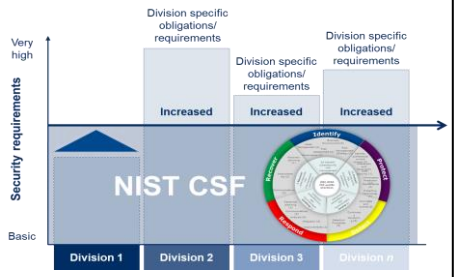
Evaluating Cybersecurity Risks

Governance

Continuous evolution of cyber security risk, oversight, assurance and attestation

- Legal, risk and compliance.
- Risk and cyber standards.
- Cyber threats, vulnerabilities, risk taxonomy.
- Key performance, Risk and Control effectiveness indicators.
- Cyber risk reporting in line with risk appetite. (Regulator)

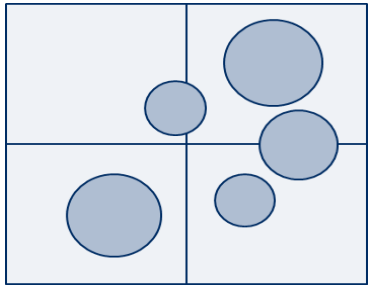
Risk assessment



Continuous cybersecurity risks baseline assessment and reporting.

- Identify cyber threats, vulnerabilities and risks.
- Evaluate inherent risk exposure in line with business strategy, markets and products.
- Evaluate control effectiveness.
- Evaluate residual risk.

Mitigation, evaluation



Risk treatment and mitigation planning

- Prioritize cyber risks.
- Prioritize cyber control effectiveness,
- Develop a risk mitigation program, action plans (POAM) and funding.
- Remediate known risks and re-evaluate residual risk.
- Evaluate and report risk mitigation.

Reporting

Management and regulatory reporting

- Committee reviews of cyber risk management compliance.
- Management committee review of cyber risk management compliance.
- Report material cyber risks and incident to board and/ or subcommittee.

Continuous monitoring, reporting, oversight, assurance and attestation

Cybersecurity Program

Building a program to mitigate cybersecurity risks

Cybersecurity Program

Managing Cybersecurity Risk

A cybersecurity program builds the foundation and continuous improvement of cybersecurity and risk management.

- Cybersecurity standards are a complex suite of security domains.
- That can be based upon a cybersecurity standard or on a risk management framework which incorporates a cybersecurity standard.
- The cybersecurity program implements corporate governance, risk management and manages regulatory compliance.
- Cyber regulatory and enforcement regimes require a cybersecurity and risk program.

The audit program aligned to the risk and cyber programs

What Changes should internal audit consider, preparing for the final rule

The Augusta Group

Internal Audit

Opportunities and Impact of the Final Rule on Internal Audit

- Audit plays a significant role in the oversight and assurance of the SEC Final Ruling,
- Is the audit process described to the regulator as part of the oversight and assurance of material cyber risk and material cyber incidents?
- Is the Audit Committee considered a board sub committee?
- Is the role, knowledge and experience of the Chief Audit Officer described to the SEC as part of regulatory findings?
- How is audit involved in the evaluation of material cyber risk and incidents?
- Is the audit program aligned with material cyber risk and cyber incident activities?

The Augusta Group

Closing Remarks

The Augusta Group