Cybersecurity, Cyber Risk Management, Oversight and Assurance

Agenda

- Introductions.
- Why cybersecurity is an issue?
- **Part 1** - Introduction to cybersecurity risk management.
- **Part 2** - Building an organisation for cybersecurity risk management.
- **Part 3** - Cybersecurity practices - What you should be good at.
- Questions

"Skate to where the puck is going to be, not where it has been".

- Wayne Gretzky hockey player

Aim to address where we will be, not where we are

The Augusta Group

Cybersecurity Risk Management

Introductions

The Augusta Group

Ted Dziekanowski

Security professional, cybersecurity educator, trainer advisor

https://www.linkedin.com/in/tdziekanowski/

Ted is a veteran of cybersecurity with over 40 years' experience of the design, delivery, oversight and assurance of cybersecurity and risk management systems. Ted's area of expertise is the management of risk in Information Technology developed over the years. He is an experienced systems Auditor and Integrator giving him a unique insight as to the challenges associated with developing an e-GRC program that satisfies the compliance requirements faced by organizations of all types and sizes.

He is an internationally recognised cybersecurity, risk management and Information system auditor. A highly respected security trainer, authorized to train ISACA CISA, CISM, CRISC, ISC2 CAP, CCSP, and CISSP. He holds DoD secret clearance and has taught causes for a broad range of public and private sector. (available on request)

The Augusta Group

Andy Watkin-Child CSyP, MSyI, CEng, MIMechE, AMAE

Security professional, risk advisor, CISO, Counsel appointed cyber expert

https://www.linkedin.com/in/andywatkinchild/

- A technology, risk and security executive with over 20 years experience as Group VP cyber risk, Chief Information Security Officer (CISO), Head of IT and European head of cyber and risk.
- Andy has built and led global 1st and 2nd Line of Defence cybersecurity and risk management functions, for international organisations including Grupo Santander, Mizuho Corporate Bank, Penguin Random House and Rolls-Royce plc.
- Andy holds Royal Chartered Security Professional (CSyP) and Chartered Engineer (CEng).
- Member of the Register of Chartered Security Professionals (recognised by CPNI).
- Andy is member of the Board of the Security Institute (MSyI).
- Practicing Associate of the Academy of Experts (TAE).
- Counsel appointed cybersecurity and risk expert and witness (BA and Marriott).
- A freemen of the Worshipful Company of Security Professionals (WCoSP) 109th City of London Livery Company.
- Founding Partner of Parava Security Solutions and the Augusta Group.
- Founding member of the CMMC AB Standards Working group.

The Augusta Group

Cybersecurity Risk Management

Why Cybersecurity is an issue

The Augusta Group

Cyber is a complex risk

- The enterprise-wide use of data, information and digital transformation makes cyber a significant risk for all organisations.
- Cyber is not a technical risk, it is a business risk.
- Recent cases have highlighted the issues organisation and CISO face with cybersecurity compliance. Resulting civil and criminal prosecution.
- Cybersecurity is evolving to cybersecurity risk management.
- U.S and EU regulators are focusing on cyber regulation. With the U.S DoD cyber security program a compliance requirement since 2017.
- U.S regulators implemented cyber enforcement regimes in 2021. The first 2 cases concluded in 2022.
- Boards have often treated cybersecurity as a risk that will not impact them. Treating it as a risk that always happens to someone else.

Placing cybersecurity and risk management professionals requires an understanding of the challenges clients face. Challenges and complexities they themselves may not yet be aware.

The Augusta Group

Cybersecurity Risk Management

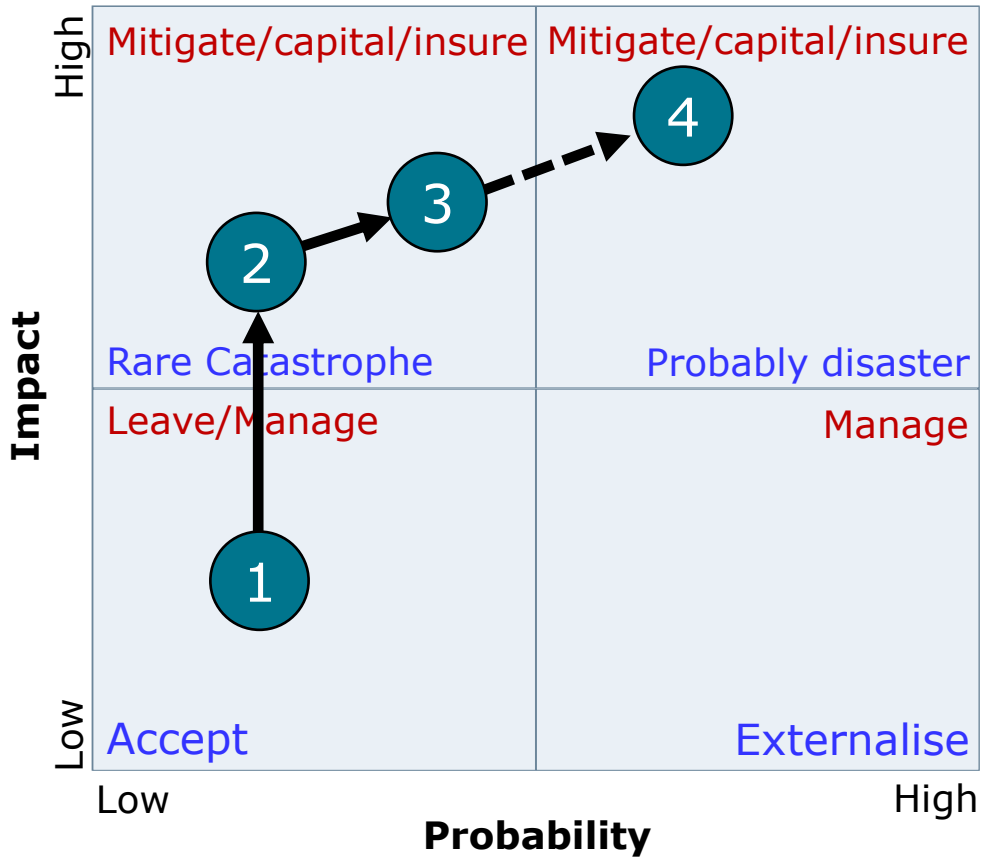
Part 1

Introduction to cybersecurity risk management

The Augusta Group

The impact of cyber attacks

Probability and impact of losses



The Impact of cyber – in general

1. Cyber attacks prior to 2017 were generally relatively low probability and low impact events. Resulting in website compromise and data thefts - **Low complexity, low impact.**
2. From 2017 there attack complexity and severity started to rise with nation state input and ransomware attacks – **Low probability, medium impact.**
3. 2021 - Nation state attackers, proxy's and criminals exploiting tools increasing profitability of Ransomware and data theft. Attack severity, complexity and frequency increases – **Medium Probability, medium-to-high impact.**
4. As the current ransomware attack vector matures and remains profitable it will evolve into a **higher probability, higher impact threat.**

The Augusta Group

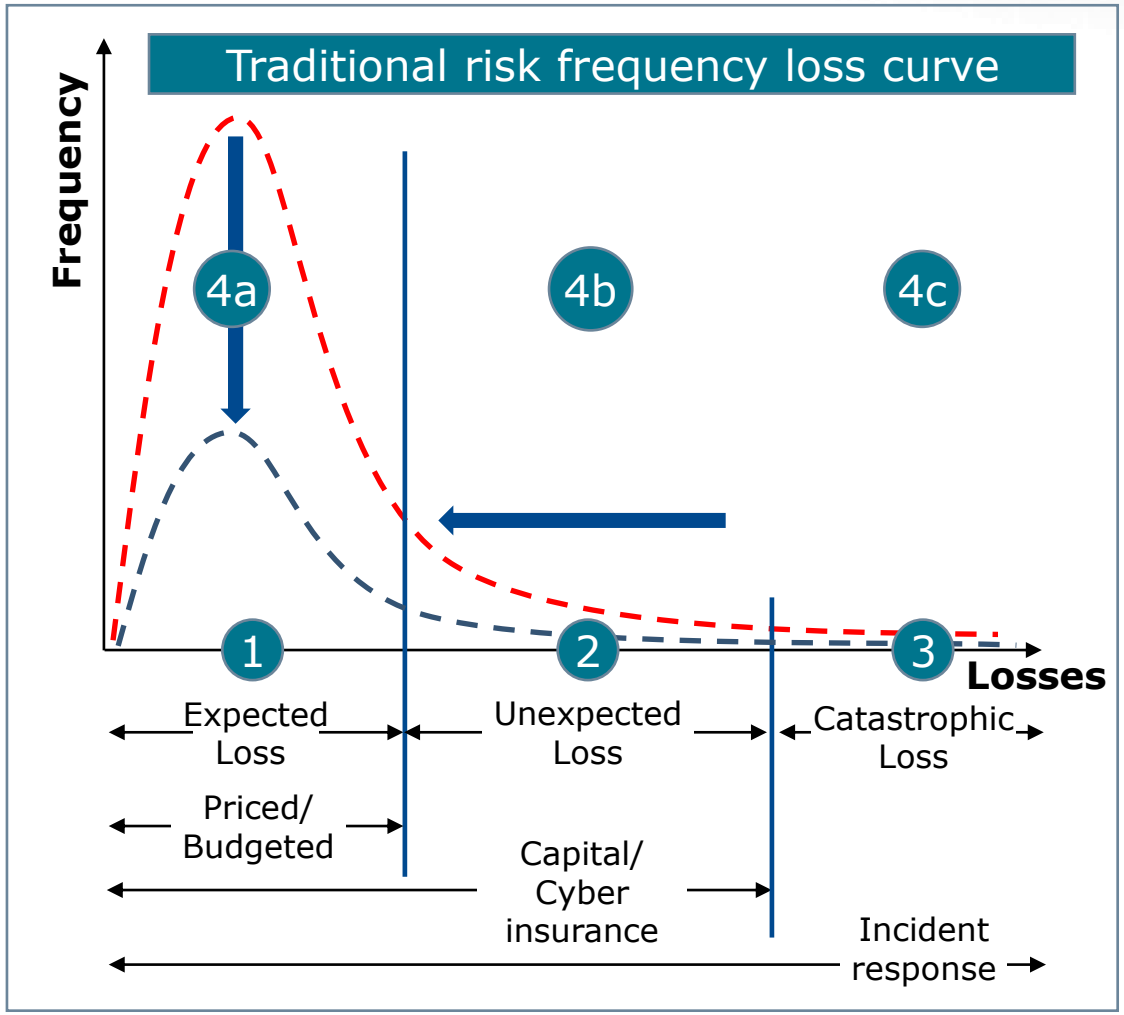
Cyber risk management in 1 slide

The purpose of a cyber risk management

The cybersecurity program is critical for managing cyber security risks.

1. Organisations have cybersecurity losses they expect to incur – **Expected losses, priced and budgeted.**
2. Organisations incur losses that they do not predict. **Unexpected losses, capital and insured.**
3. Organisation can be impacted by events outside their control that are. **Catastrophic Loss, Incident response.**
4. A cybersecurity program reduces the impact of expected losses (4a), improves management of unexpected losses (4b) and reduces the impact of catastrophic losses (4C).

Frequency - Loss



The Augusta Group

Challenges and Opportunities

Regulation/ Legislation

- Current DFARS 252.204 – 7012, 7019 and 7020 regulations mandate NIST 800 – 171 compliance.
- SEC Proposal.
- EU NIS – 2.0, EU DORA, EU Cyber Resilience Act
- Cyber is moving 'left of bang', it is a regulatory compliance and legal issue.

Legal

- Legal risk is high
- Boards are being held accountable for cyber security risk management.
- CISOs face criminal convictions.
- US Regulators have developed cyber compliance regimes that are being tested in court.
- U.S DoD regulations have been in place for 5 years.

Implementation

- UK and EU do not legislate cyber security. cybersecurity and cyber-risk standards fall short of US standards.
- UK and EU defensive cybersecurity maturity is low.
- Cyber standards we low across the UK and EU.
- Organisations are not equipped to deliver cyber regulations.

Opportunities

- Cybersecurity is a U.S national security priority.
- Implementation of cybersecurity and cyber risk management is an economic differentiator for organisations.
- Re-Skilling the cyber workforce.

Cybersecurity moving ‘left of bang’

Today the predominant cybersecurity model is, ‘right of bang’

- The focus is on incident management and remediation.
- Cybersecurity support is requested at the time of an incident, or ahead of regulatory enforcement actions.

Cyber regulation and enforcement is driving cyber ‘left of bang’

- Cyber security compliance requires active management of cybersecurity risks. Organisations will have to demonstrate their governance, oversight, assurance and reporting of cybersecurity ‘left of bang’.
- Boards will be required to confirm their cybersecurity risk management experience and knowledge.
- Organisations will be required to report cyber incidents between 2 hours and 3 days.

Aim for where the puck will be, not where it is

The Augusta Group

Managing cybersecurity risk

Part 2

Building an organisation for cybersecurity risk management

A critical risk for the board to manage

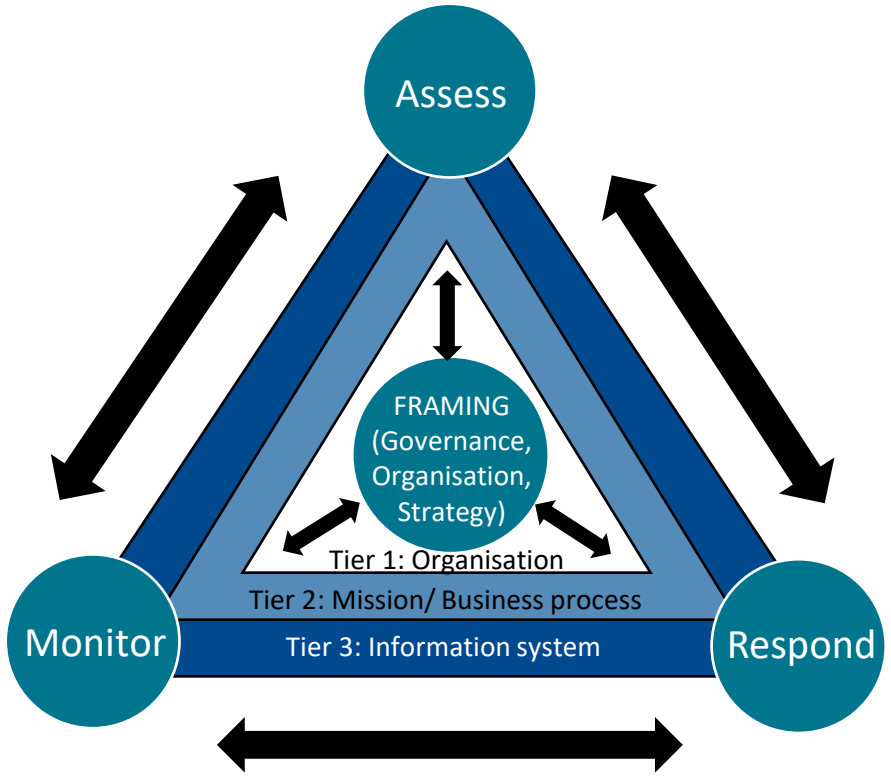
The Augusta Group

Cybersecurity risk management

Combining Risk Management Processes and Organisational Design

Cybersecurity risk management processes are aligned to the three organisational tiers so that appropriate ownership, governance and reporting of cyber security risks can take place.

Feeding risk and control effectiveness information from *Tier 3, information systems and Tier 2 Mission and Business Processes* to management and the executive board at *Tier 1 Organisation*



The Augusta Group

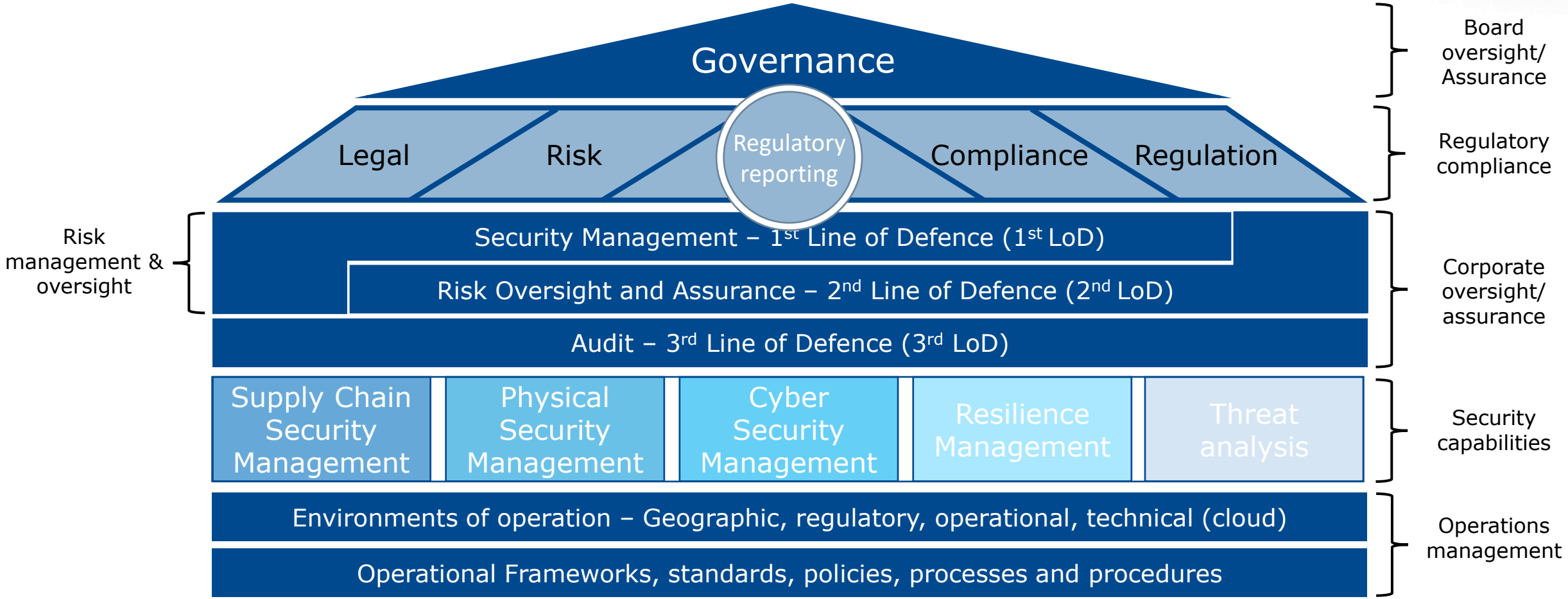
Cybersecurity risk management

Governance
&
Target Operating Model

The Augusta Group

Cyber-Risk - Target Operating Model

Creating 3 Lines of Defence for the oversight and assurance of cybersecurity risk



The Augusta Group

Cybersecurity risk management

Managing cybersecurity risk requires an appropriate cybersecurity risk management framework

Assessing cybersecurity risks

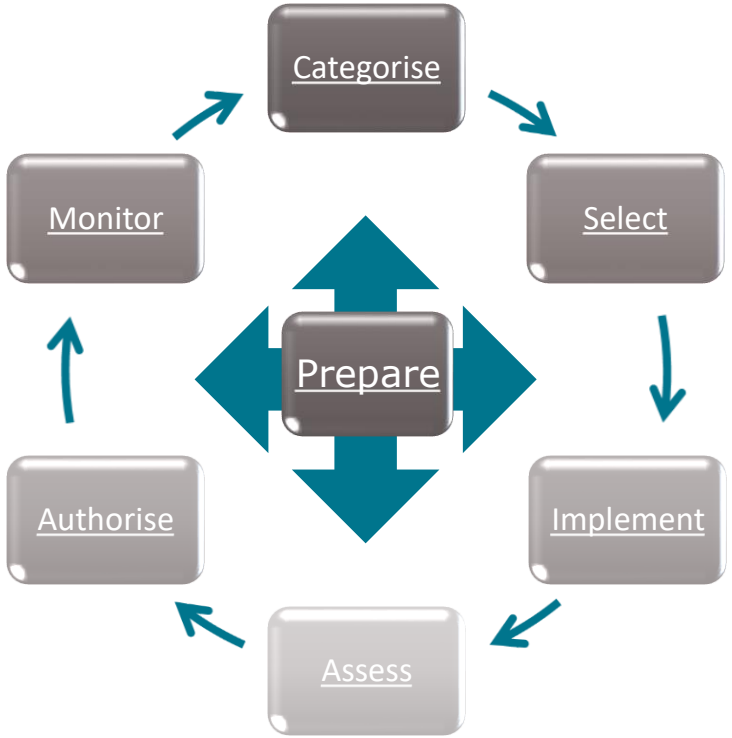
The Augusta Group

Cybersecurity risk management

Cybersecurity Risk Management Framework (RMF) structure and steps

Seven steps in the RMF. Includes a preparatory step (Prepare) to ensure that organizations are ready to execute the process and six main steps. All seven steps are essential for the successful execution of an RMF.

- Prepare to execute the RMF from an organization - and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
- Categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
- Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.



The Augusta Group

Building a risk management program

Governance (GV) – Risk Management (GV.RM)

Cybersecurity risk management framework steps and structure

- Implement the controls and describe how the controls are employed within the system and its environment of operation.
- Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
- Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

The Augusta Group

Figure above illustrates the steps in the RMF, NIST SP 800-37R2

Managing cybersecurity risk

Part 3
Cybersecurity practices

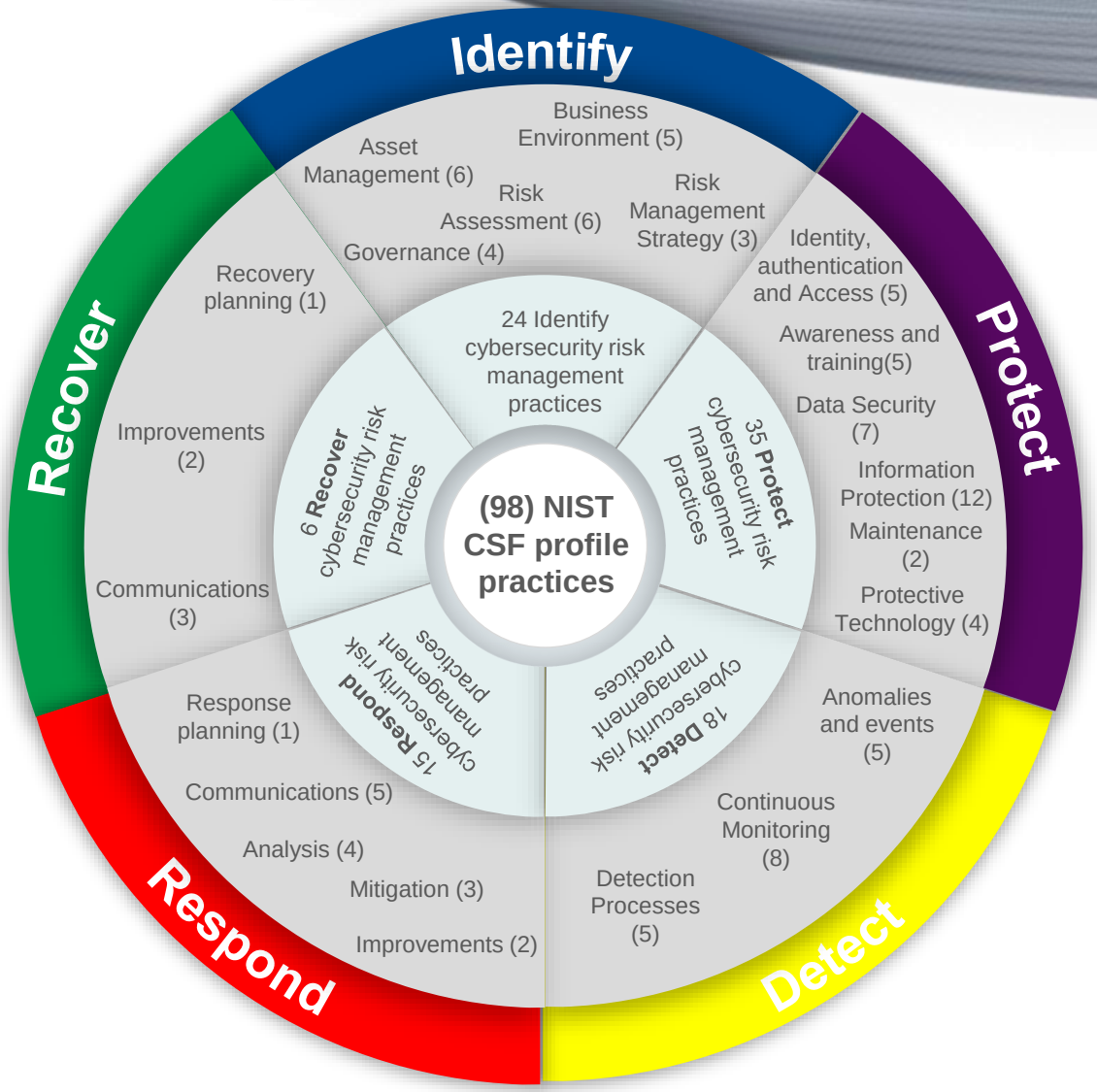
What you need to be good at?

The Augusta Group

Cybersecurity Frameworks Profiles (CSF)

What is a CSF profile?

- A CSF profile aligns control functions, categories, and subcategories with business requirements, risk tolerance, and resources.
- A CSF profile enables organizations to establish a roadmap for reducing cybersecurity risk, aligned with organizational goals, legal/regulatory requirements, industry best practices, and reflects risk management priorities.
- CSF profiles are used to describe the current or desired target state of specific cybersecurity activities.
- CSF profiles support business/mission requirements and aid in communicating risk within an organisation.



The Augusta Group

https://www.nist.gov/cyberframework

Components of a security program

Cybersecurity risk management domains

Managing cybersecurity risk

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

- It is a complex suite of over 19 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 Augusta Group

Conclusion

1. Cybersecurity is a complex enterprise wide risk. The role of the CISO is developing.
2. The cyber issues facing an organisation change as the regulation, location, strategy of an organisation
3. Boards responsibility for cyber risk management is increasing.
4. More companies are moving to the cloud, that is creating additional complexity
5. The regulatory environment for cyber security is developing rapidly and require continual evaluation of regulatory requirements. Regulation can come at any time.
6. To be successful in recruiting cybersecurity talent a basic level of understand of the issues allows a conversation to take place, to identify the ideal person for a given role.
7. The pace of technological change is increasing as is the complexity. Cybersecurity requires constant examination of regulatory issues and technology change.
8. If you do not understand a specific topic, review vendors product and services to understand capabilities.

The Augusta Group

End

The Augusta Group