Gjensidige

Auditing Cyber

Gaute Brynildsen, CAE.

23.5.2024

About me and Gjensidige

- More than 17 years in internal audit
- Operational experience in IT
- Certified CIA, CISA, CRISC, CCSP, GIAC GSNA , CCSK, Azure Fundamentals, APMG CISA og CRISC trainer
- MBA
- Earlier president of ISACA Norway Chapter and board member of CSA

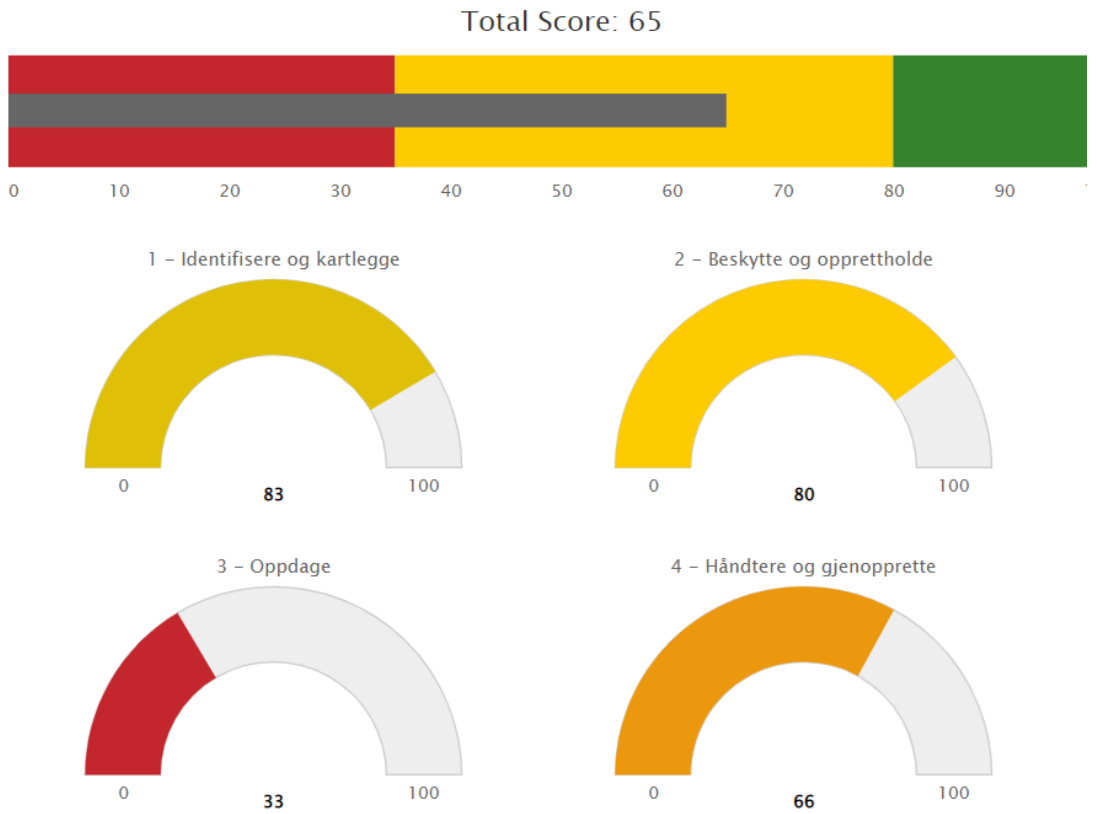
- Gjensidige is the largest insurance company in Norway with operations in Denmark, Sweden, Estonia, Latvia and Lithuania.
- 9 persons in group audit

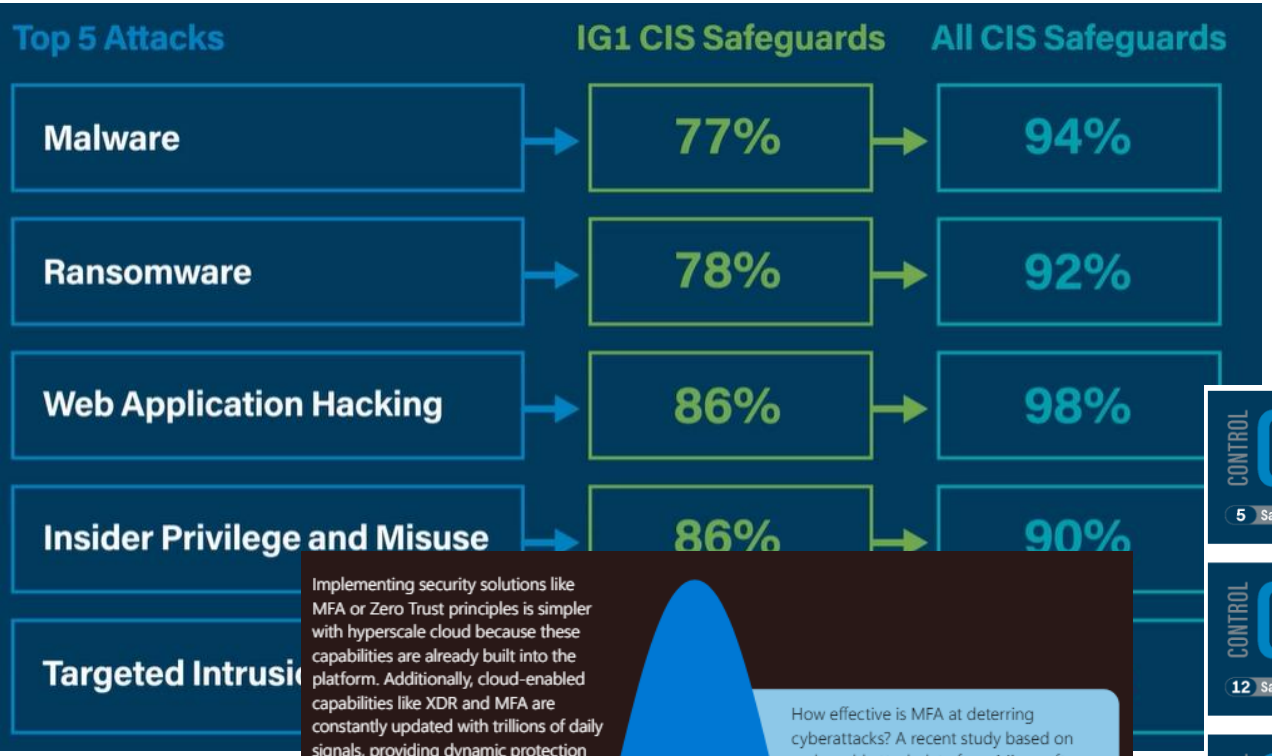
Topics

- Cybersecurity audit fundamentals
- Cybersecurity auditing in your organization
- Vendor and cloud security audits
- Emerging trends and our practices in cybersecurity auditing

Cybersecurity audit fundamentals

- Cybersecurity, big topic and a top risk for a long time
- Scoping can be difficult, go broad or go deep, where?
- What are the main risks for your company? Where is the gold?
- So many standards and controls to choose from, but do you have any regulatory requirements?
  - EBA and EIOPA
- Most successful attacks were possible due to missing or weaknesses in some common controls.





CIS 18 Critical security controls

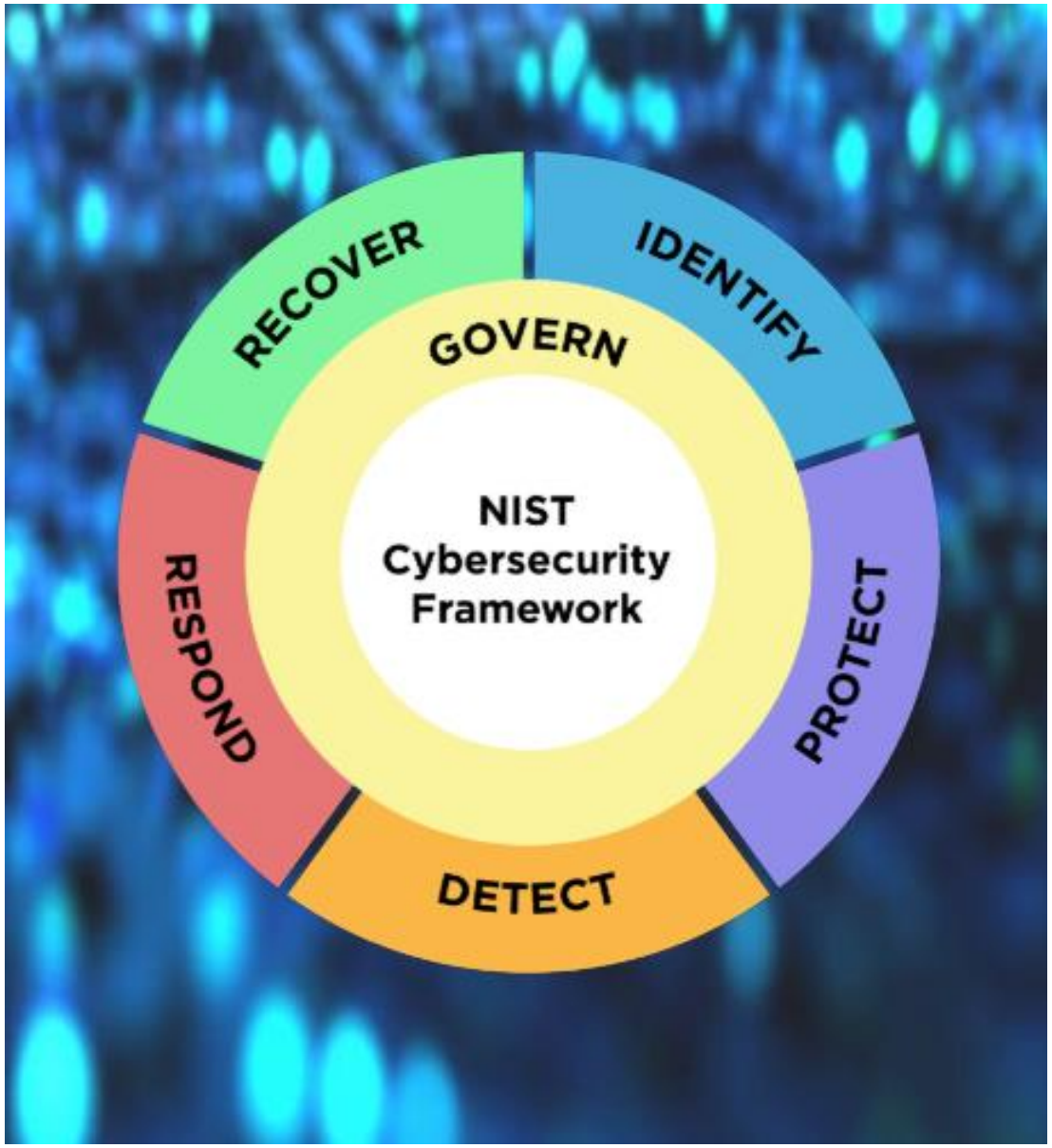
Competence and tools

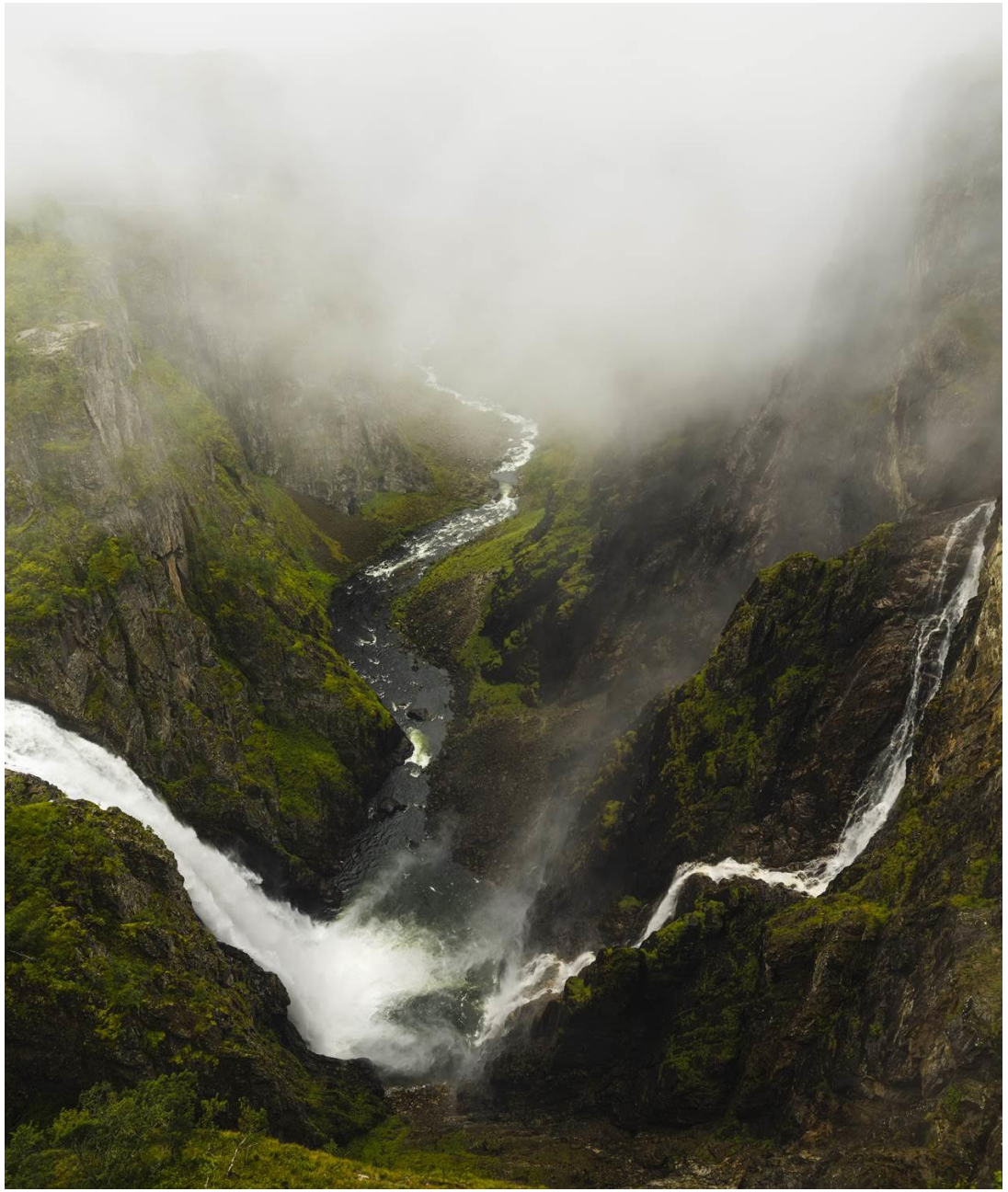
- Even if you don't have IT knowledge you can do a lot of good asking some key questions
- But for testing you need the right competence and tools
  - Maybe you have IT auditors
  - Could you use someone from the organization
  - Consultants
  - Pooled audits
- Some tools
  - https://www.shodan.io/
  - https://dmarcian.com/domain-checker/
  - ChatGPT 4o
  - PowerShell
  - Microsoft Defender for Cloud
  - etc

Auditing cyber in your organization

It all starts in your company

- What is the second line doing?
- What has the external auditor done?
- Any penetration tests or incidents?
- What reports do the board of directors and the group management get?
- What governing documents are relevant for cyber? Risk appetite?
- Who is responsible for what?
- Who would attack you, where and how?
- What are the most important assets of the company?
- How much of IT is done inhouse and how much is outsourced?





Vendor/cloud audits

- Supply chain/third party risks are high on the agenda
- Regulatory requirements increasing
- Several known attacks came via a third party
- For several companies the amount of third parties have increased

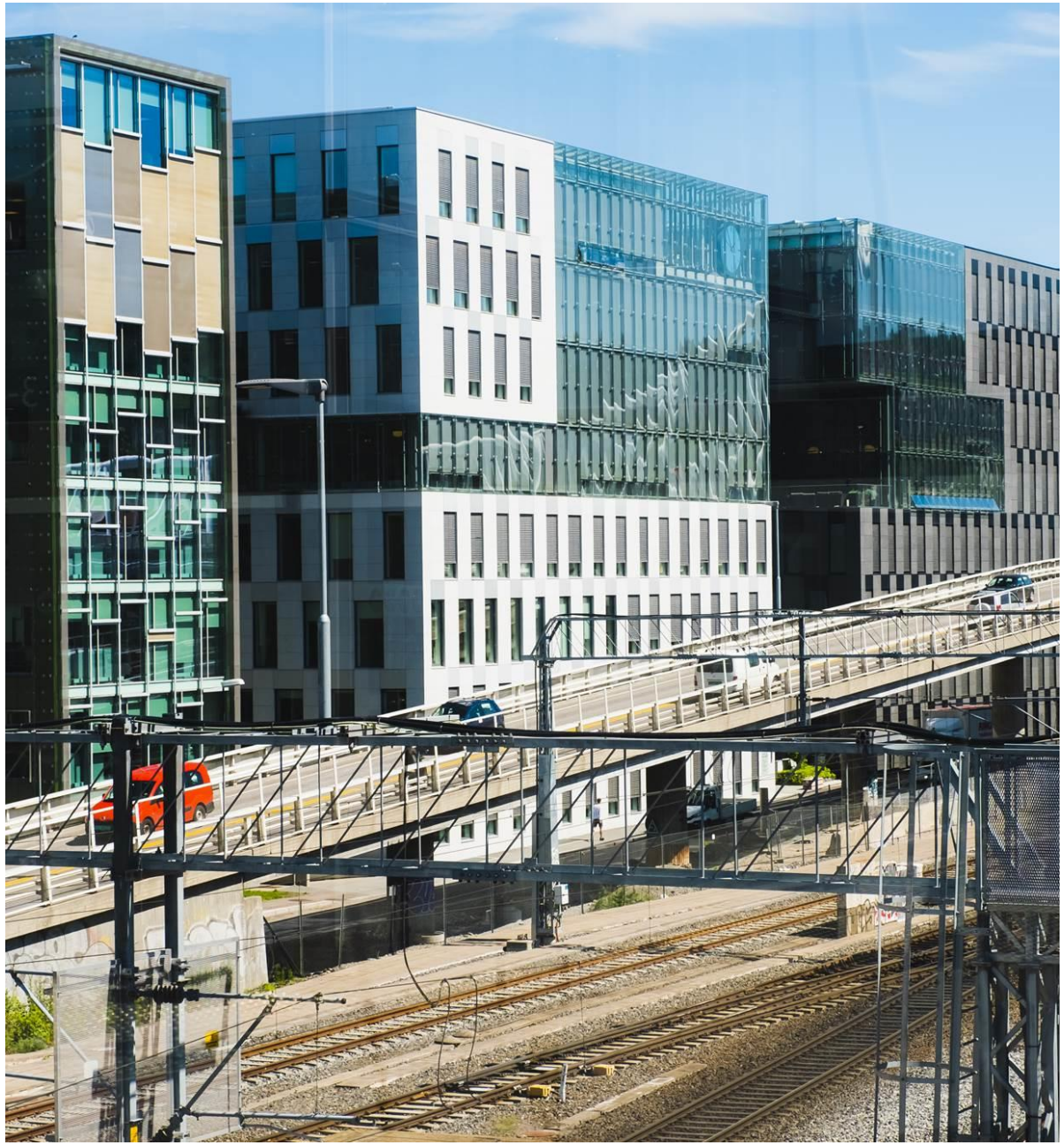
- Audit rights in the contract, use the rights
- Audit statements like SOC reports, use them and understand their scope. Also certifications.
- What is the second line doing or IT security?
- What meeting places are there and what reporting is in place?
- Consider pooled audits

Emerging trends and our experiences

- The quick rise of AI
- Increasing complexity, vendors/cloud

Audit areas

- Cloud audit
- Core system project audits
- Security in the development process DevSecOps
- Basic security controls
- Securing critical assets
- SaaS vendor
- Traditional basic operations vendor
- Detect and respond audit
- Disaster recovery audit



The threats and incidents – some resources I like

- DNB Bank – Digital threats
- Verizon Data breach investigations report
- Microsoft Digital defense report
- 2023 Annual Report | Recorded Future

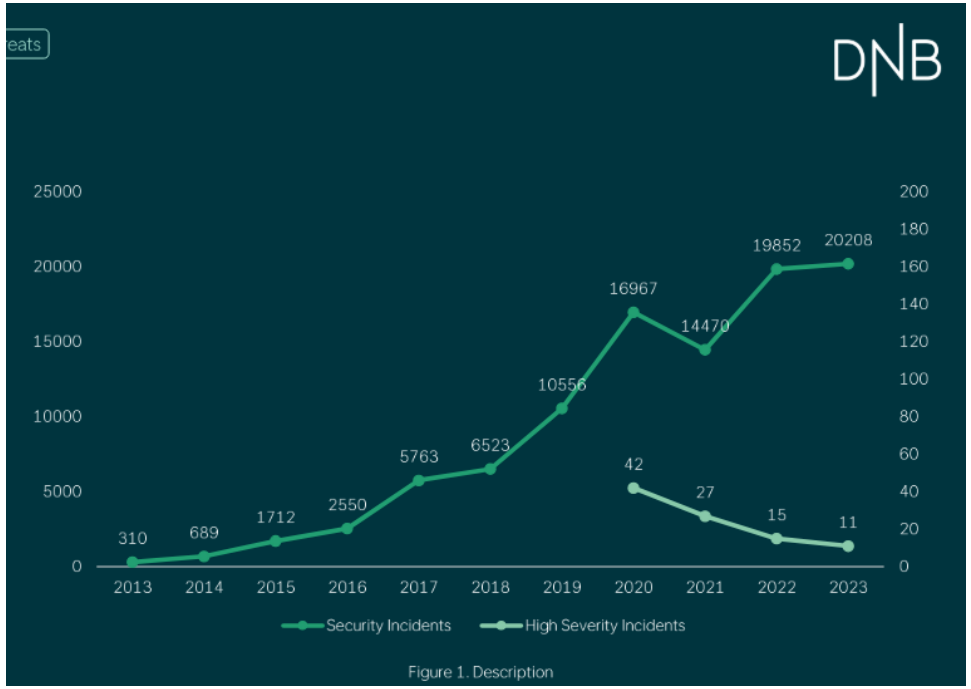


Figure 1. Description

Verizon

Microsoft

Common problems

- Language problems between IT and business
- Ownership of risks (Process, data, systems)
- Missing quantification of risks and business impact analysis
- Overview of assets and prioritization, shadow IT and shadow AI
- Legacy vs Cloud
- Understanding of perimeter
- Understanding of dependencies and core processes
- Single point of failure
- Backups
- Business continuity/disaster recovery
- Building security culture
- Control of privileged access
- Hardening
- Patching to limited
- Locking screens

Thanks