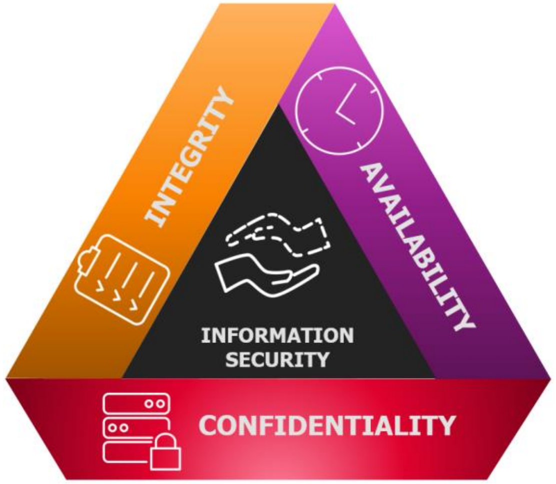
Information security: Business risk or IT risk?

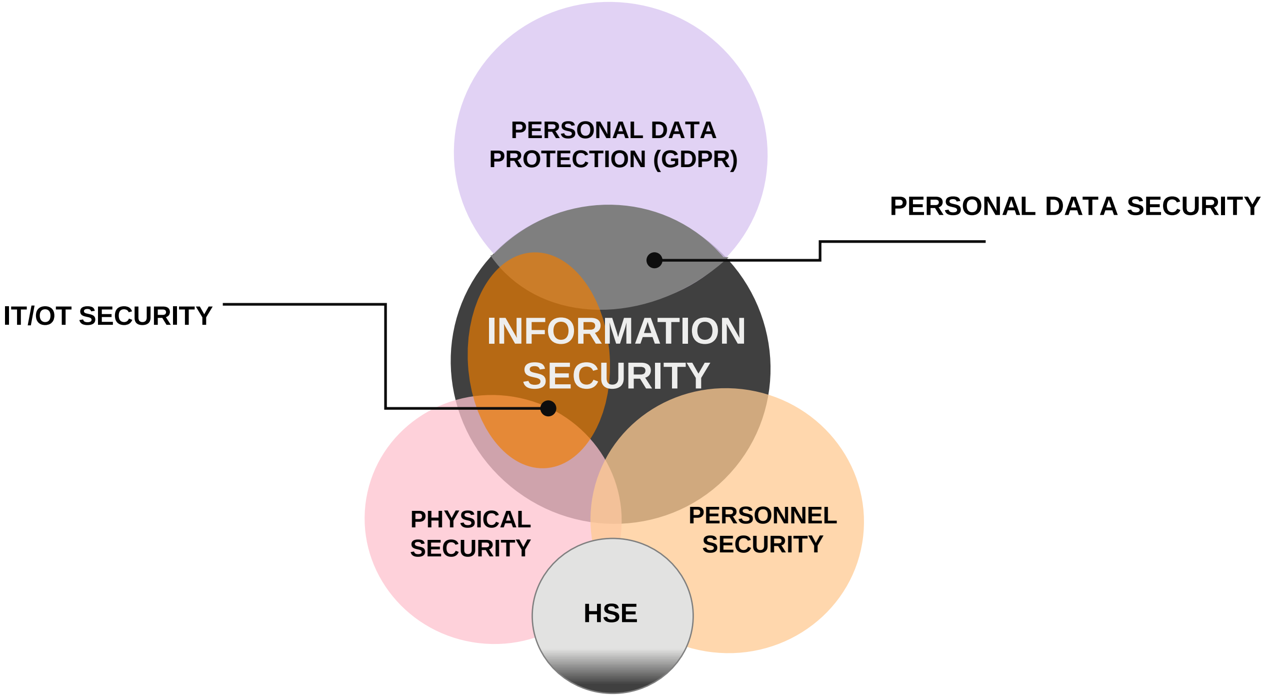
Andreas Grefsrud
Consulting Director, Sopra Steria

What is information security

- It is about safeguarding your **information and data** against compromise of confidentiality, integrity and availability

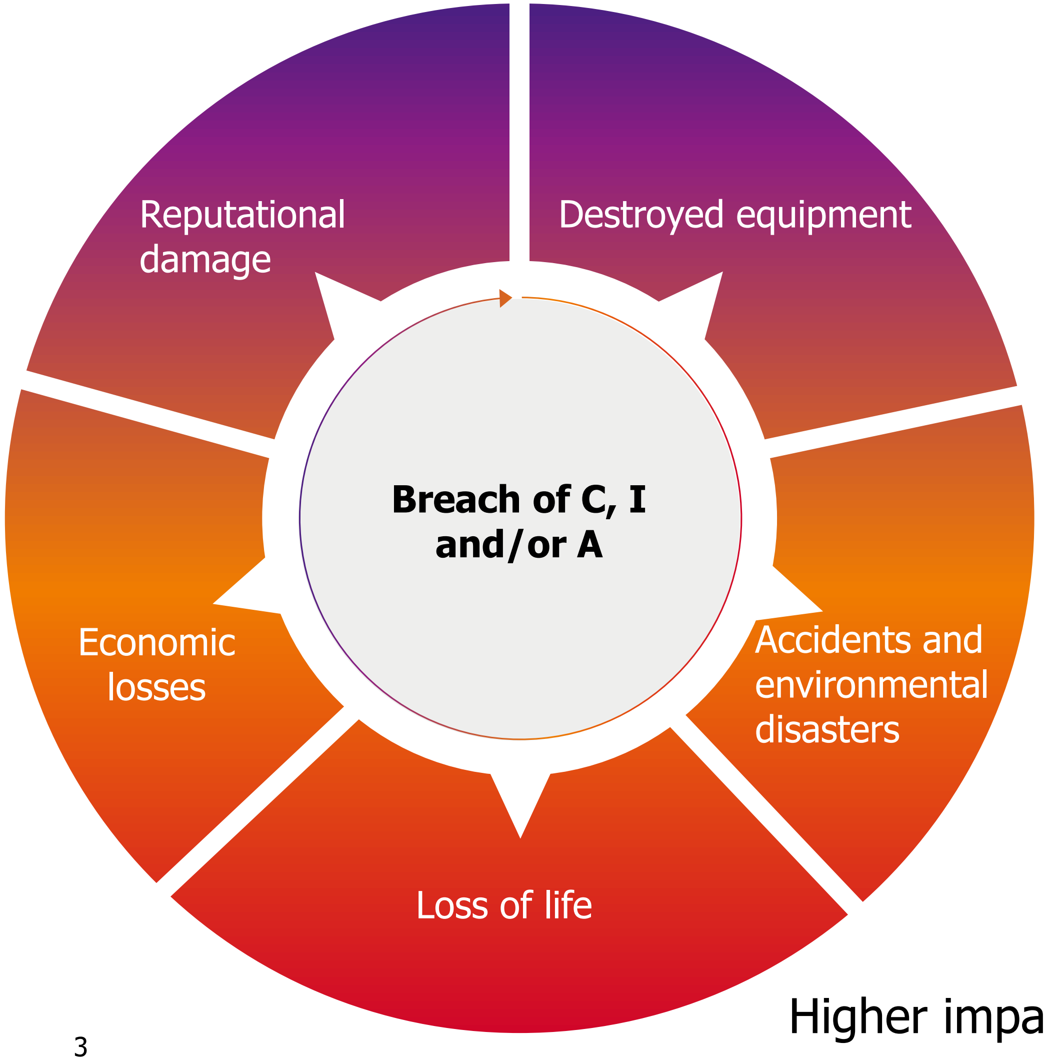
→ **They are ASSETS**





Information and data assets

Information and data underpins the core business of the company. If breach of CIA, you can face



If you are responsible for the results in your business unit, you are also responsible for what goes wrong

IN OTHER WORDS, THE BUSINESS UNITS ARE SPONSIBLE FOR THEIR OWN STUFF

Ultimately, it is the CEO on behalf of the board that is accountable

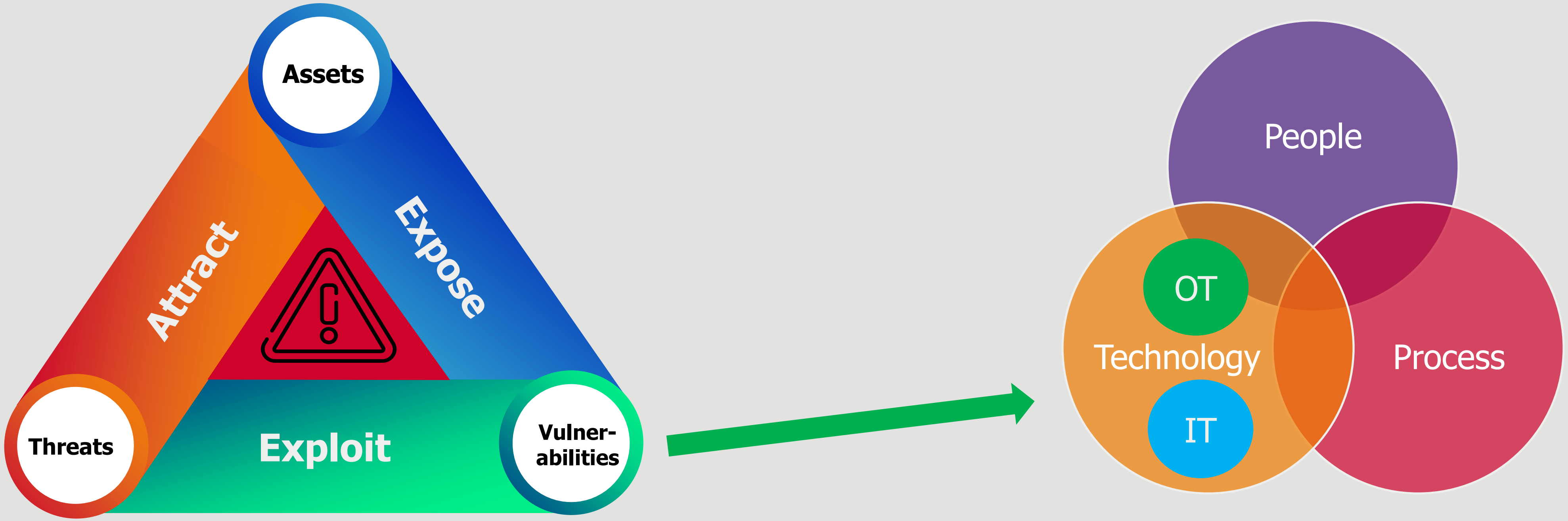
Higher impact means higher asset value

Business impact of information security breach

Who carry the costs should something like this happen:

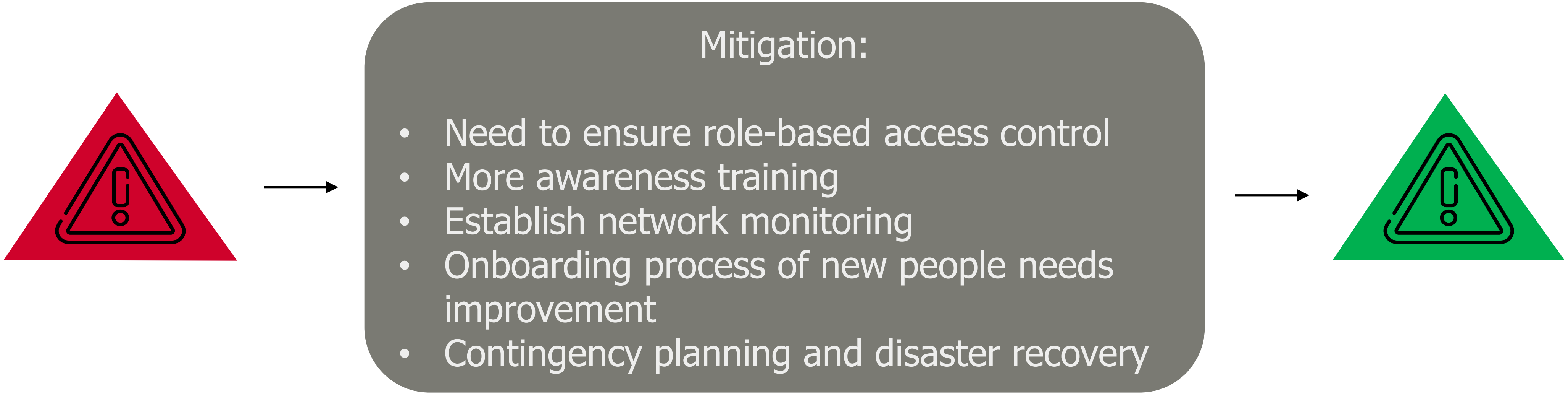
Risk

The risk triangle



A risk-based approach is needed

Purpose is to reduce identified vulnerabilities.



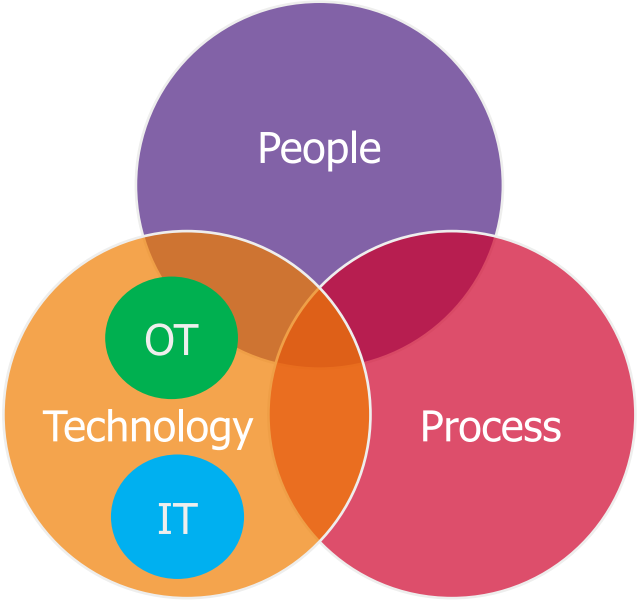
Mitigation:

- Need to ensure role-based access control
- More awareness training
- Establish network monitoring
- Onboarding process of new people needs improvement
- Contingency planning and disaster recovery

But before this makes any sense:

- Some defined level of what is acceptable risk must be defined – (must reflect the risk appetite of the board and the CEO)
- Responsibilities must be delegated, yet there may be different views in the organization about what acceptable risk is.
- It is therefore in the self interest of the board and CEO to have a role that has been given the authority to
  - Define organization-wide security requirements on behalf of the board and the CEO
  - Control and oversee information security implementation and risk management

Going back to this



We often see that such roles are located in the IT-departement, which gives the impression that information security = IT security

A couple of questions that need to be asked:

- Is it an IT cost when something must be done concerning security awareness? **NO**
- Is it IT's responsibility if security processes in a core business unit must change? **NO**
- Is it IT that should drive those changes? **NO**

Would IT be most interested in driving innovation in the IT domain or handling process issues in HR? **DUH**

Could it happen that these activities may be neglected or prioritized lower than deserved? **ABSOLUTELY**

Two situations we want to avoid

Things to consider when organizing your security function

- Your CISO should have unrestricted access to the entire organization
- Having the CISO report to the CIO relegates cybersecurity to an IT security, or technology, function.
- Real story: CIO withheld information from the rest of the C-suite when she felt something reflected negatively on her or the rest of the IT team, while had no problem blaming the CISO when there were impacts to productivity due to security measures or conflicts between security and other IT departments in the company

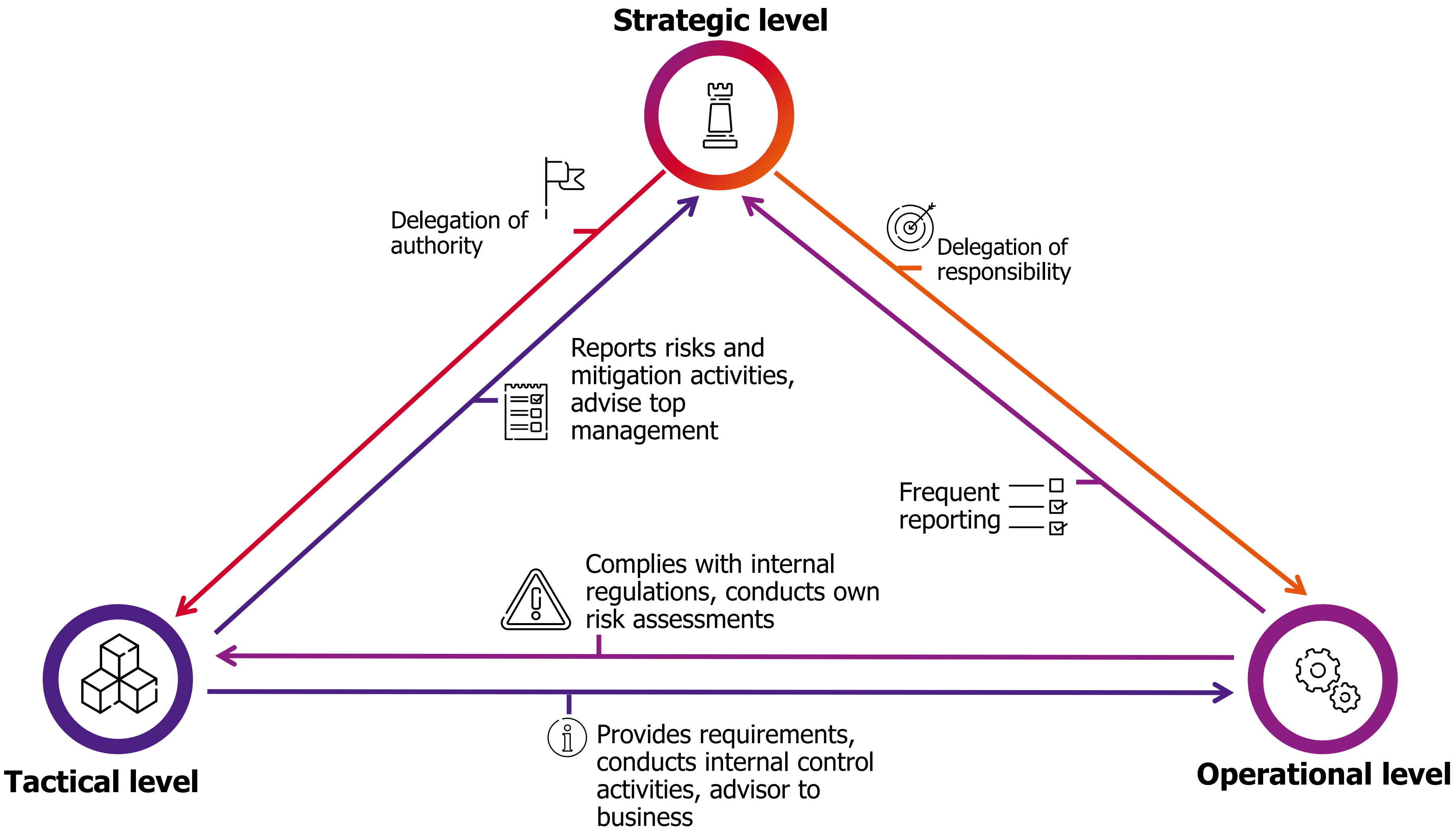
- The IT function and the security function is very much interrelated. But even so:

Move the CISO out of the IT departement

- If the CISO reports higher up the chain of command and has a seat at the C-level table, then cybersecurity is solidly embedded into the overall risk management of the enterprise.

Separation of duties

Principle in a nutshell



Strategic level

Delegation of authority

Delegation of responsibility

Reports risks and mitigation activities, advise top management

Frequent reporting

Complies with internal regulations, conducts own risk assessments

Provides requirements, conducts internal control activities, advisor to business

Tactical level

Operational level

What it means (tactical and operational levels)

Tactical level (CISO)

- **Owns ISMS on management’s behalf**
- **Establish security foundations (requirements and principles)**
- Facilitates and advises BU’s risk assessments
- Conducts «audits» (3rd party pentesting of IT systems if necessary)
- Security awareness program owner
- Collaborate with CERT/CSIRT, communication of threat info internally
- Advising the business and management on security topics, co-ordinates exercises across BU’s
- Reports security posture to top management
- Incident manager

Operational level (IT)

- **Configure IT-systems, applications and infrastructure according to security principles and the requirements of the BU’s**
- Responsible for implementing IT-security risk mitigating actions
- Periodic pentesting
- Continuous monitoring of systems and infrastructure
- Responsible for disaster recovery according to business needs
- Incident handlers, collaboration with SOC

Operational level (BU)

- **Identify and prioritize own information and data assets**
- **Owns BU security risks**
- Contingency planning in own BU
- Responsible for BIA (RTO, RPO, MTO)
- Ensure business processes capture security requirements
- Communication with CISO and IT before new initiatives are implemented
- Owners of exercise results and improvement of plans

Benefits of doing it right

- Information security is not perceived as an IT thing
- Business will take more ownership
- Top management will likely become more informed about the «real» risk picture
- Enables better integration of information security risk management with the enterprise risk management

- The IT security function within the IT department can focus on technical security, and forget the boring governance stuff

- Compliance with laws and regulations
  - IMO resolution MSC 428(98) - information security/ cybersecurity risks must be assessed and be part of the quality management system
  - GDPR (If you organize in the way I've shown, the CISO could potentially also be the Data Protection Officer because conflicts of interest should be eliminated – however, this must be assessed)
  - NIS2 implementation will most likely become much easier

sopra steria