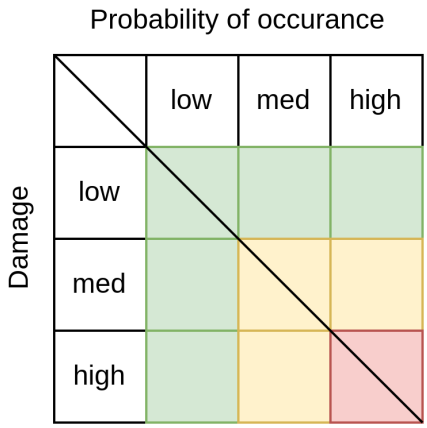
Solutions: Sheet 11

1. Information Security Risk Management

(a) What is an information security (IS) risk? How can the value of a risk be estimated?

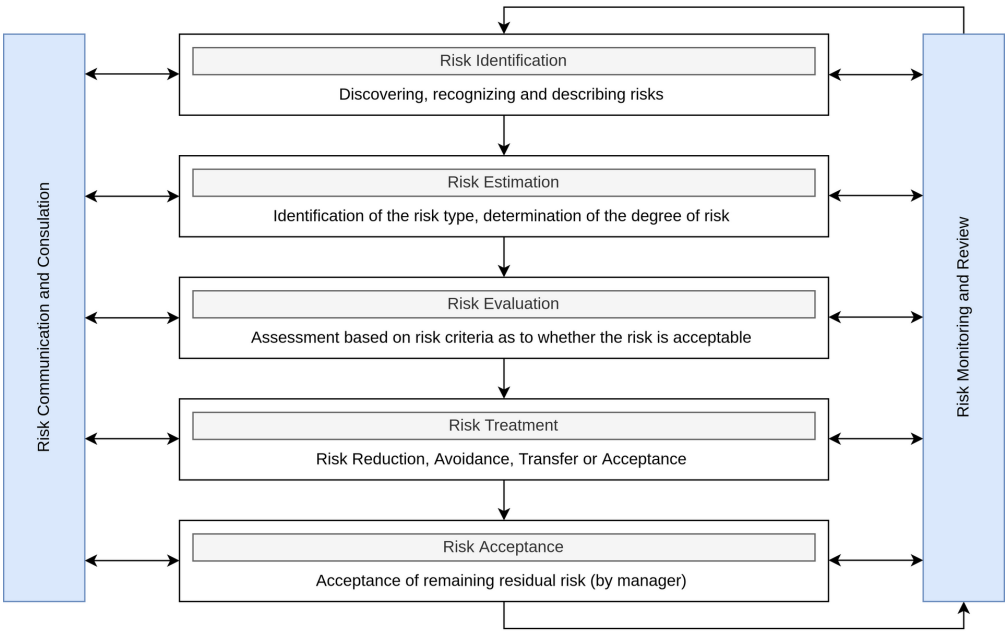
- A risk is a potential impact that can have a either positive or negative impact on a organization or a company
- An information security risk is the probability that a protection goal (confidentiality, integrity, availability, authenticity) will be broken, and the amount of damage resulting therefrom
- The probability of occurance can be estimated by evaluating the means and motivations of an attacker
- The amount of damage can be estimated by evaluating the consequences of an attack
- $\text{risk} = \text{probability} \cdot \text{damage}$



(b) What are the objectives of IS risk management?

- Coordinated management and control of risks $\rightarrow$ effective use of resource to reduce most important risk
- Helps to prioritize measures to be implemented

(c) What are the five steps of the IS risk management cycle according to ISO 27005? Briefly describe each of the steps.



- **Risk Identification:** Disover and describe the risk
- **Risk Estimation:** What does it cost
- **Risk Evalulation:** Do we need to fix the risk?
- **Risk Treatment:** How do we treat the risk
- **Risk Acceptance:** The manager checks if the done steps to reduce the risk are acceptable or more needs to be made (List of all risks is checked)

https://www.iso27001security.com/html/27005.html

(d) Name and describe the four options for *risk treatment*.

https://www.linkedin.com/pulse/discussing-iso-27005-risk-treatment-options-your-27001-phillips

- **Risk Reducation:** Modify the risk in such a way it's reducing (add a technology, procedure or employee training)
- **Risk Avoidance:** The conscious decision not to perform any action that make the risk become present
- **Risk Transfer:** The risk is transferred to someone else (e.g insurance or outsourcing)
- **Risk Acceptance:** The conscious decision to accept the existing risk but not to treat it

2. Information Security Management

(a) Name three standards for Information Security Management Systems (ISMS).

- ISO 27001
- IT-Grundschutz
- NIST Cybersecurity Framework

(b) What are the four areas of measures that should be addressed within an ISMS?

- **Technical:** Technical measure to solve problem
- **Organizational:** Who is responsable for what (Roles)
- **Personnal:** Traing personal
- **Infrastructure:** Phyiscal security of devices, building, etc.

(c) Why should the ISMS be a cyclic process that is constantly repeated?

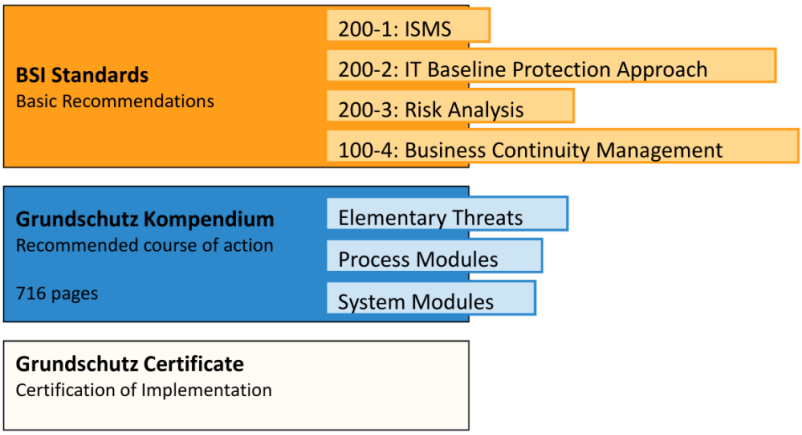
- A cyclic process aims for constant improvement
- New components/products added will may cause new vulnerabilities
- The threat landscapes changes
- Change of technologies (technologies that hasnt been there before)

(d) Name and briefly explain at least five of the 14 control domains of ISO 27001.

- 14 domains of ISO 27001 provide the best practices for an information security management system (ISMS)
- **Access Control:** Ensure restricted access to employee, so they only see and use information which are assinged to their roles
- **Cryptography:** Use encryption for important data to ensure data integrity and confidentiality
- **Physical and Environmental Security:** Prevents unpermitted physical access and or damage to the environmental equipment of an organisation
- **Communication Security:** Protect the communcation of an orgainzation
- **Compliance:** Identify laws and regulations that apply in order to understand legal requirements

(e) Who develops the IT-Grundschutz? What is the target group? What are the three main components of the IT-Grundschutz?

- Developed by Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Made to protect companies and public authorities
- The three main components of the IT-Grundschutz are *BSI Standards*, *Grundschutz Kompendium*, *Grundschutz Certificate*
- **BSI Standards:** Procedures to ensure the secue setup of a system (basic recomendations)
- **Grundschutz Kompendium:** Catalogue of acitons to be applied in case of a threat
- **Grundschutz Certificate:** You can be certified according to BSI standard



3. IT Security Management according to BSI IT-Grundschutz

You are engaged by a startup company to analyze and evaluate the IT security of an existing network (see figure 3). Fundamental errors seem to have occurred when planning the network setup. Your task is to create a minimal IT security concept with the help of the BSI IT-Grundschutz (see slides in Chapter “Security Management”). As shown in the following (not to be taken too seriously) example, give at least four suggestions with the information on IT component(s), protection requirements, threat, risks (naming the protection goals violated) and measures such that the startup company can resolve possible security problems in a meaningful way. Provide at least one example of possible attacks and problematic technologies that cannot be prevented when you implement your measures. Be creative in analyzing the network because the example network may have complex problems.

Example:

- IT component(s): employee notebooks
  - Protection requirement: normal
  - Threat: overheating
  - Risks: total failure of the device, protection goals violated: availability
  - Measures: air conditioning of the room

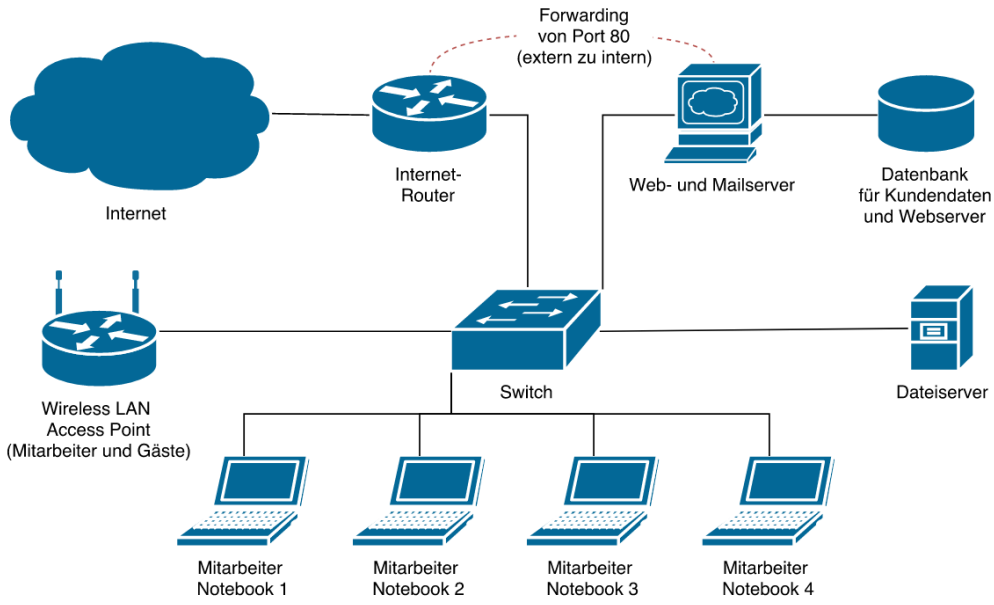


Figure 1: Network Diagram of Startup Company

- **IT component:** Dateiserver
  - **Protection requirement:** High
  - **Threat:** Unauthorized access
  - **Risks:** Modification or loss to stored data
  - **Protection goal violated:** Integrity, confidentiality
  - **Measures:** Adding a backup server and use hash or digital signatures (integrity). Make sure not everybody can access everything using access control (confidentiality).