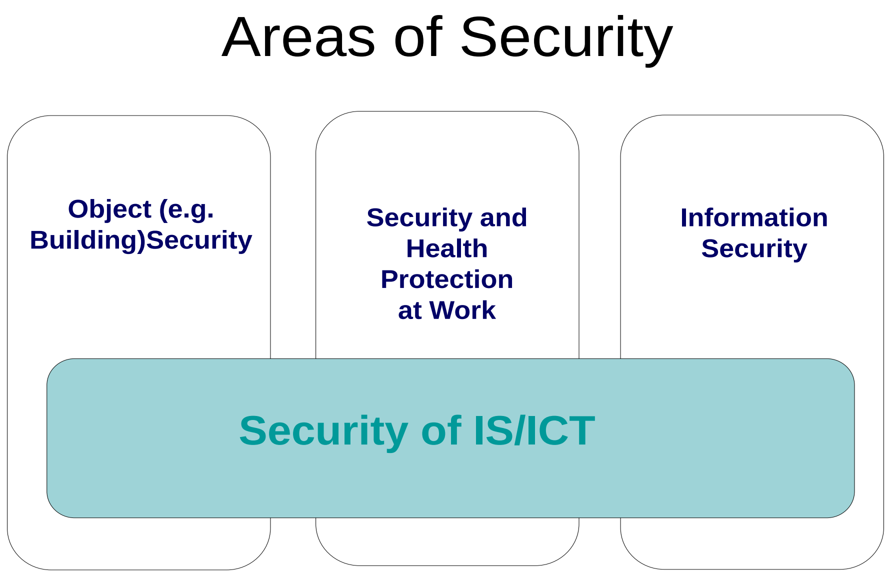
Safety of information systems

Lecturer: Roman Danel

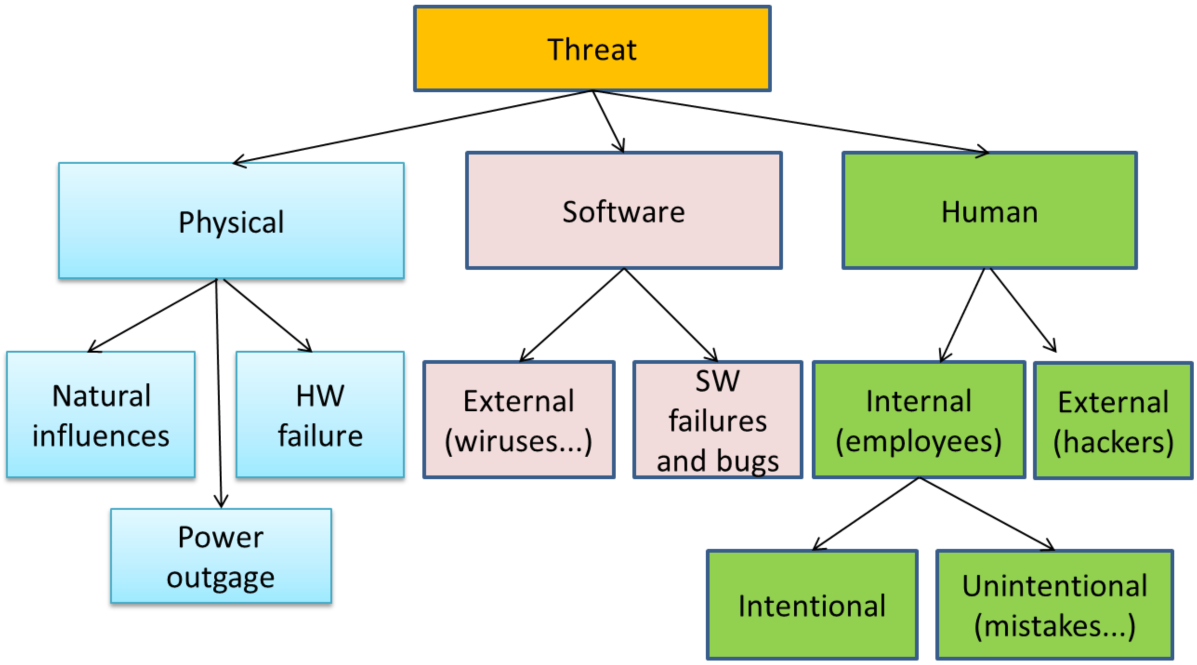
Risk analysis, threats category

The term "security" is a broad concept. In principle, we can divide it into the three areas:


Areas of Security
Object (e.g. Building)Security
Security and Health Protection at Work
Information Security
Security of IS/ICT

The following text is going to treat security as "Information Security".

The basic division of security threats (Risks Analysis):



Risks Analysis

- What happens when information is not protected?
- How information security could be violated?
- How likely is it to happen?

What should be protected?

- Technical Resources - against technical defect, theft, ...
- Communication paths - avoid monitoring data to be transferred ...
- Software
- Data – damage, theft

What is an aim of information security?

- Ensuring confidentiality of data
- Ensuring data integrity
- Ensuring data availability

Methodologies and Tools for Risk Analysis

CRAMM - CCTA Risk Analysis and Management Method (1985)

- According BS7799

- Current version – 5

- Complexly covers all phases of risk management, from the actual analysis of risks all the way to the proposal ofcountermeasures, including the generation of outputs for security documentation (emergency and continuity assurance planning). CRAMM also helps to prove the efficiency of the cost expended on risk management, security and emergency planning. It contains a unique broad library of security countermeasures.

Risk IT

Connected with methodology CoBit for IT/ICT management. Provides guidance to help executives and management ask the key questions, make better, more informed risk-adjusted decisions and guide their enterprises so risk is managed effectively.

RiskPAC

Automated risk analysis program can detect and help eliminate vulnerabilities in data security.

Octave-S - Operationally Critical Threat, Asset and Vulnerability Evaluation

Octave is a security framework for determining risk level and planning defences against cyber assaults. The framework defines a methodology to help organizations minimize exposure to likely threats, determine the likely consequences of an attack and deal with attacks that succeed.

OCTAVE defines three phases:

- Phase 1: Build Asset-Based Threat Profiles
- Phase 2: Identify Infrastructure Vulnerabilities
- Phase 3: Develop Security Strategy and Plans

OCTAVE was developed in 2001 at Carnegie Mellon University (CMU), for the United States Department of Defense. The framework has gone through several evolutionary phases since that time, but the basic principles and goals have remained the same. Two versions exist: OCTAVE-S, a simplified methodology for smaller organizations that have flat hierarchical structures, and OCTAVE Allegro, a more comprehensive version for large organizations or those with multilevel structures.

Marion - Methodology of Analysis of Computer Risks Directed by Levels

Marion is origin from France (Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau).

It is based on a methodology of audit, which, as its name indicates, allows for estimating the level of IT security risks of a company through balanced questionnaires giving indicators in the form of notes on various subjects relative to security. The objective of the method is to obtain a vision of the company with regard to a level considered "correct", and on the other hand with regard to companies having already answered the same questionnaire. The level of security is estimated according to 27 indicators distributed in 6 large subjects, each of them assigns a grade between 0 and 4. The level 3 is the level to be reached to ensure a security considered as correct. At the conclusion of this analysis, a more detailed analysis of risk is carried out to identify the risks (threats and vulnerabilities) that face the company.

ISO 27001

ISO 27001 is a standard designation for information security management system in an organization. ISO 27001 belongs to the family of ISO 27000 and it is part of the international standards issued by the International Organization for Standardization (ISO). ISO 27001 has replaced a standard BS 7799 and became an international standard for information security management systems.

ISO 27001 is the main standard of the whole family ISO 27000 and provides a comprehensive approach to information security in the organization. It includes data from all assets, paper documents, and information and communication technologies to knowledge. It also includes staff qualification development and technical protection against computer fraud.

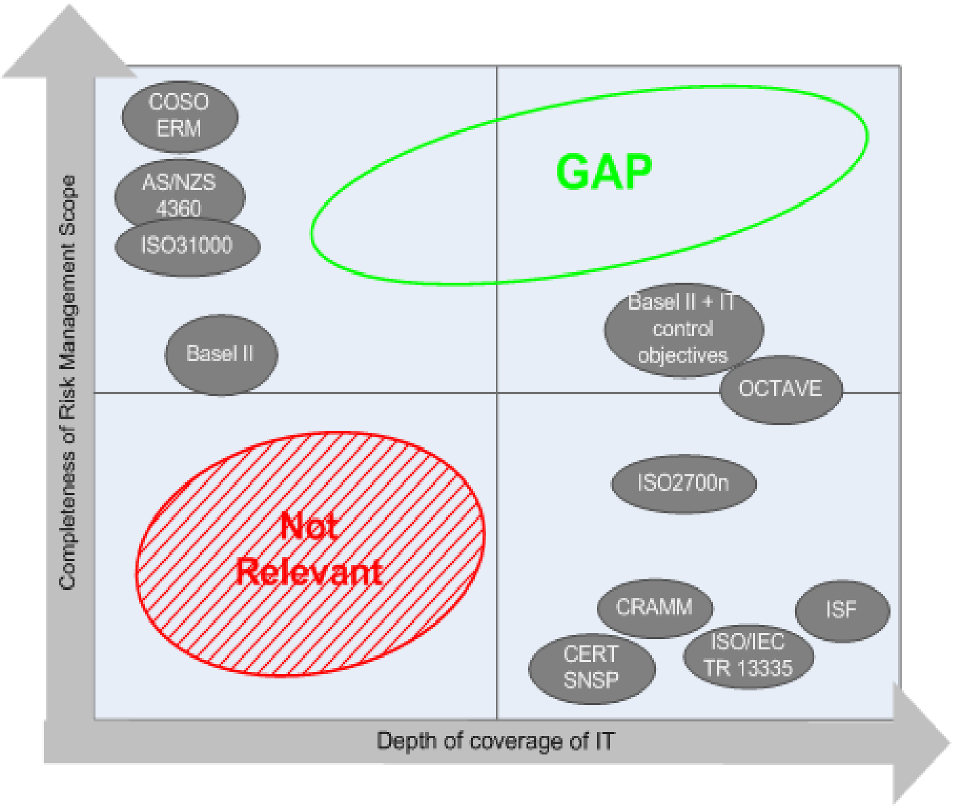
Principles of information protection according to ISO 27001 are based on three principles of information security:

- **Confidentiality** - which means that information is accessible only to those who are allowed (who have authorized access)
- **Integrity** - which means that there is accuracy and completeness of the information
- **Availability** - which means that authorized users have access to information when they need it

ISO 27001 is in accordance with other management systems like ISO 9001. It involves a continuous process of improving the entire information security management system using integrated PDCA model.

Terms from Risk analysis

- **ARO** (Annualized Rate of Occurrence) - probability of occurrence of threat per year
- **SLE** (Single Loss Exposure) - loss at one occurrence of the threat
- **ALE** (Annualized Loss Expectancy) **-** expected damage and recovery costs



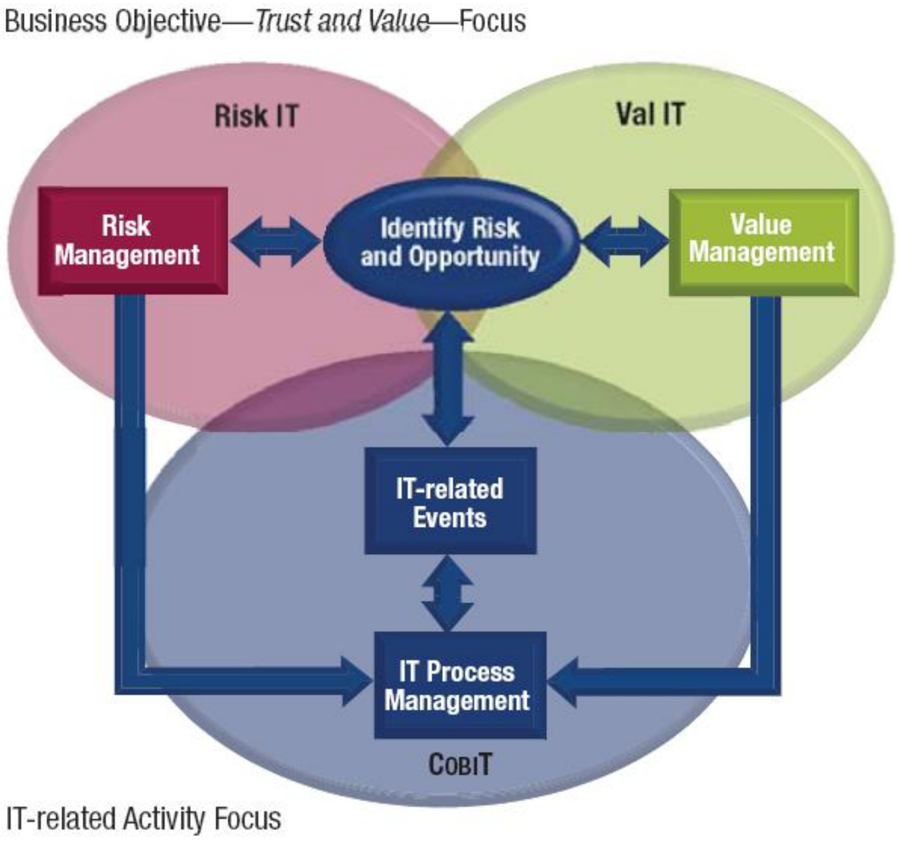

Business Objective—*Trust and Value*—Focus
Risk IT
Val IT
Risk Management
Identify Risk and Opportunity
Value Management
IT-related Events
IT Process Management
COBIT
IT-related Activity Focus

Figure 1 - Risk IT structure (compatibility with Cobit)

[Source: www.isaca.org]