Security analysis — basic notions and ideas

October 6, 2006

Ketil Stølen, SINTEF & UiO

Acknowledgements

- The lectures on security analysis is the result of joint work with a number of colleagues at SINTEF; in particular:
  - Folker den Braber
  - Ida Hogganvik
  - Mass Soldal Lund
  - Fredrik Vraalsen

- The initial version of CORAS was jointly developed by the 11 partner in the CORAS project

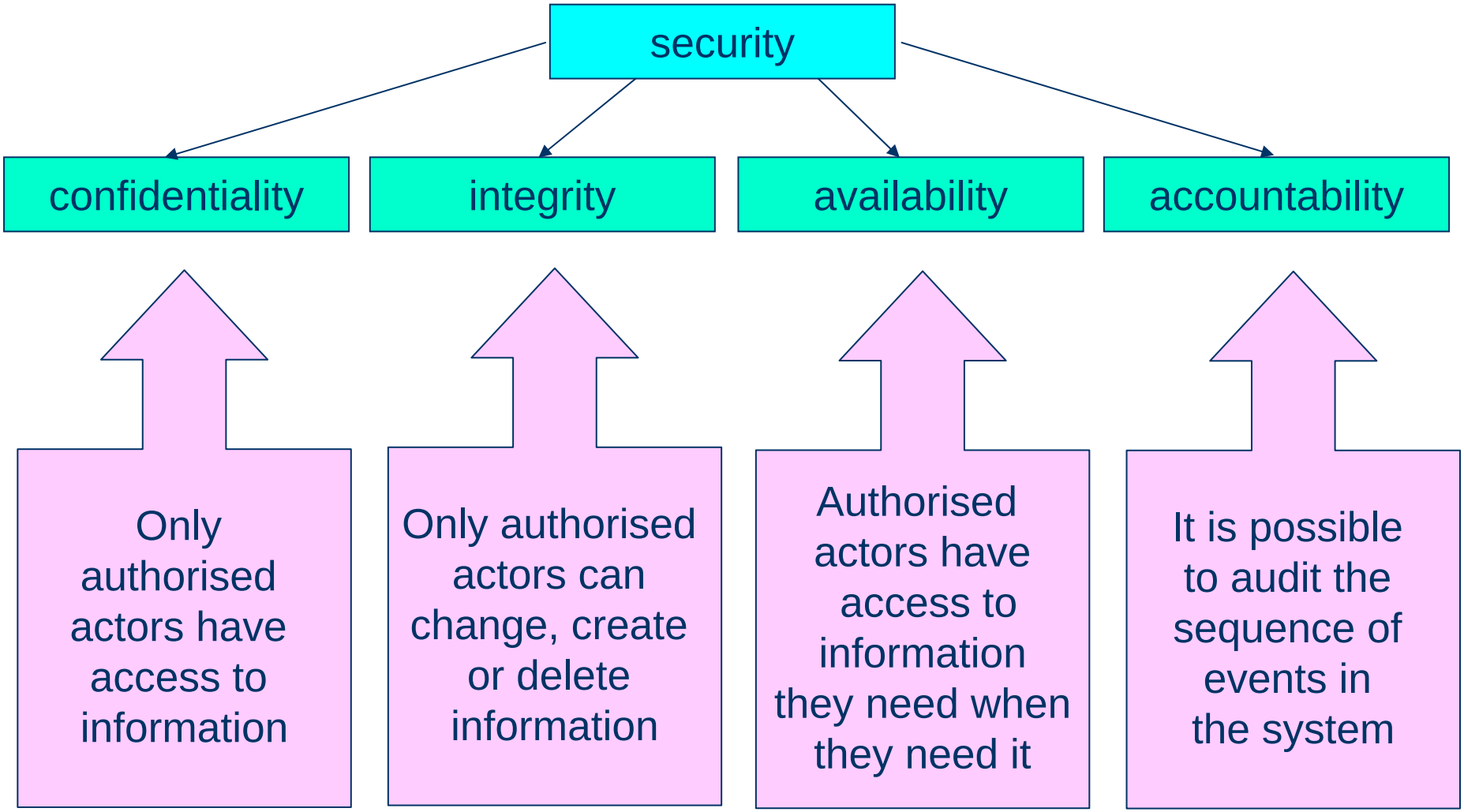
Objectives for the three lectures on security analysis

- Classify security concepts
- Introduce, motivate and explain a basic apparatus for risk management in general and risk analysis in particular
- Relate risk management to system development
- Describe the different processes that risk management involve
- Motivate and illustrate model based security analysis
- Identify relevant standards
- Demonstrate the use of risk analysis techniques

What is security analysis?

- Security analysis is a specialized form of risk analysis focusing on security risks

What is security?



What is risk analysis?

- Determining what can happen, why and how
- Systematic use of available information to determine the level of risk
- Prioritisation by comparing the level of risk against predetermined criteria
- Selection and implementation of appropriate options for dealing with risk

Note: Security is more than technology

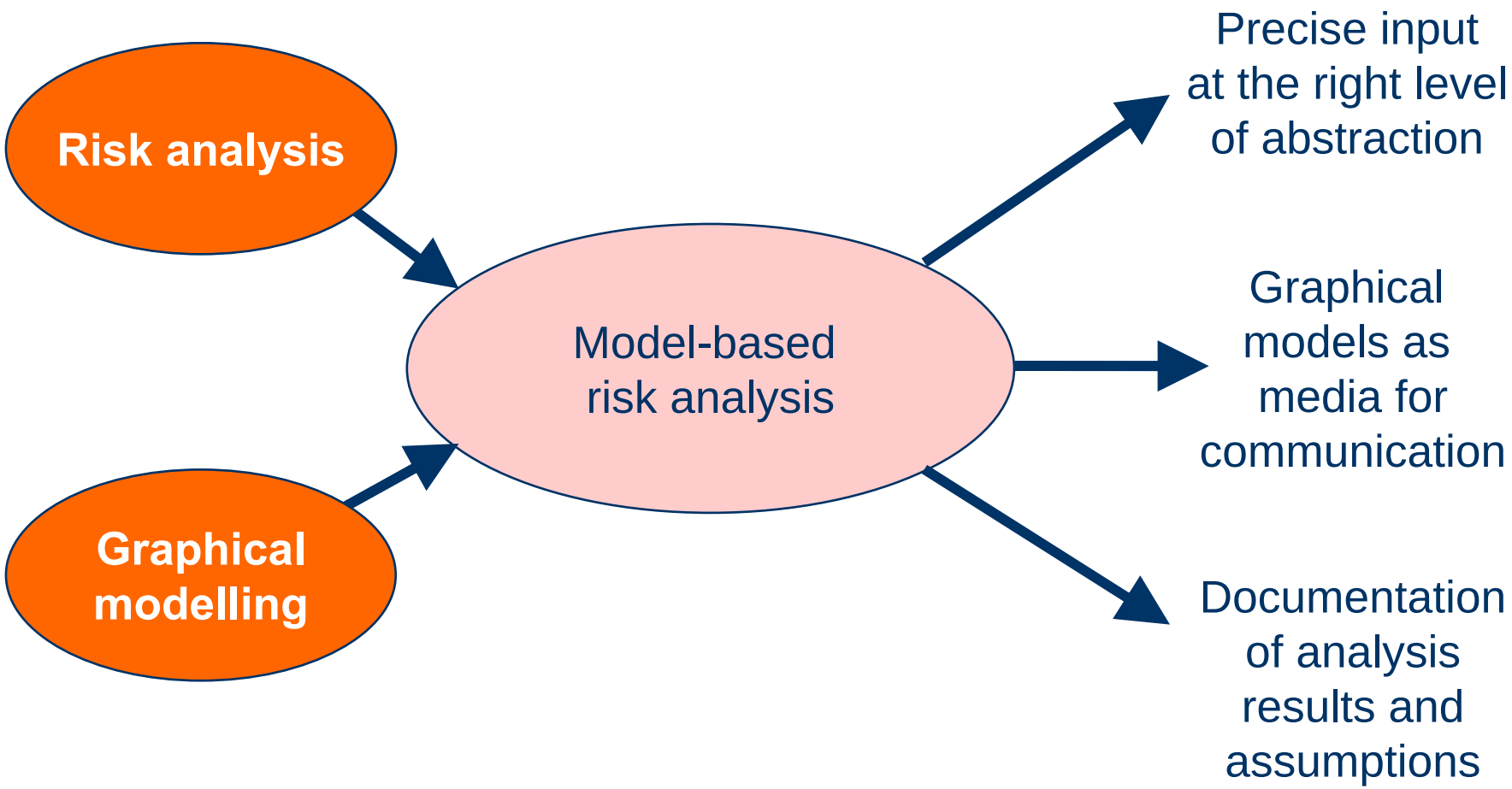
- From a technical standpoint, security solutions are available – but what good is security if no one can use the systems?

- Security requires more than technical understanding
- Security problems are often of non-technical origin
- A sound security evaluation requires a uniform description of the system as a whole
  - how it is used, the surrounding organisation, etc.

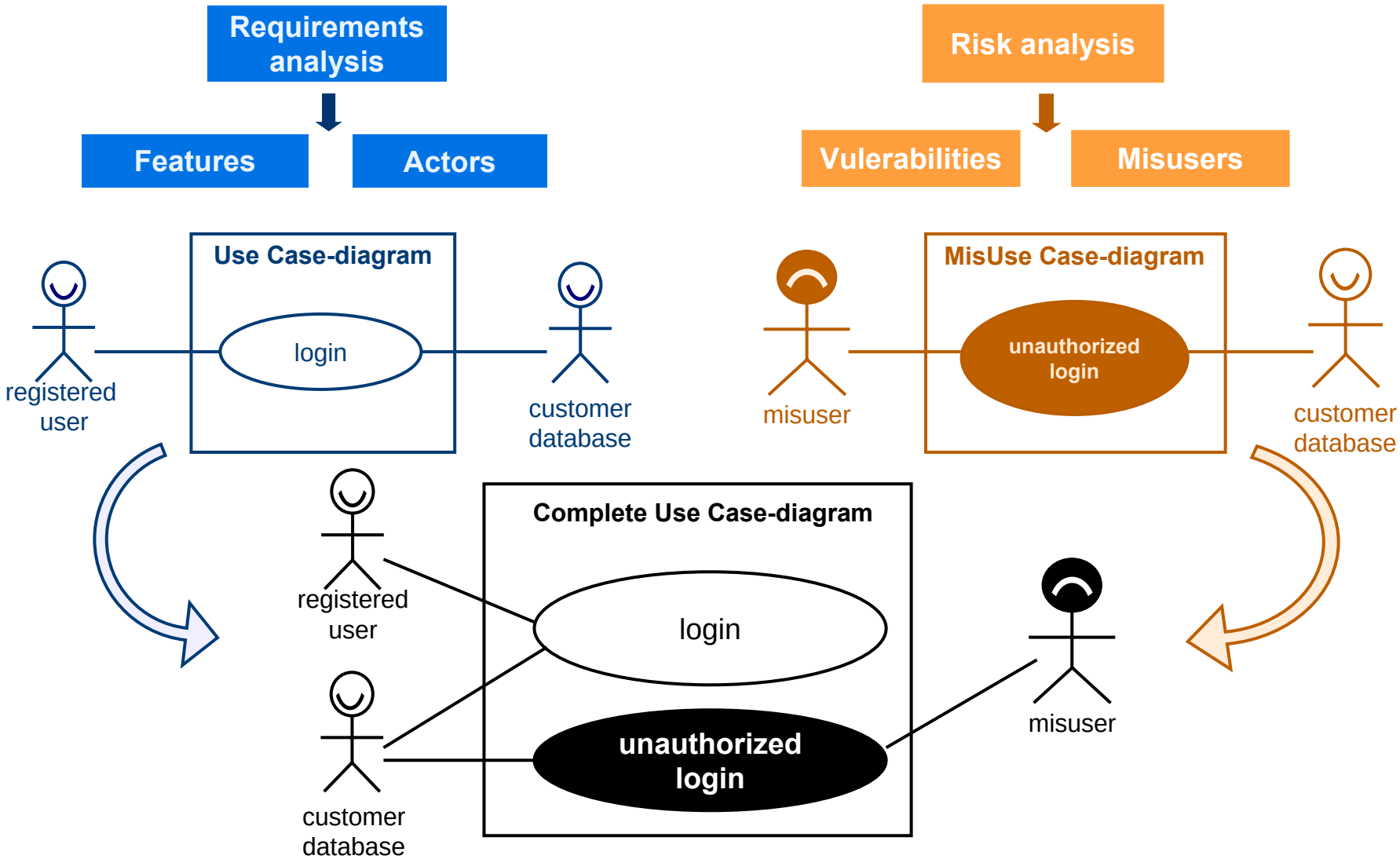
Security – part of system development

- Security is traditionally added as an “afterthought”
  - Solutions often reactive rather than proactive
  - Security issues often solved in isolation
  - Costly redesign
  - Security not completely integrated
- Requirements analysis and risk analysis are two sides of the same coin and should be integrated
  - Focus on desired and undesired behaviour, respectively

Model-based risk analysis



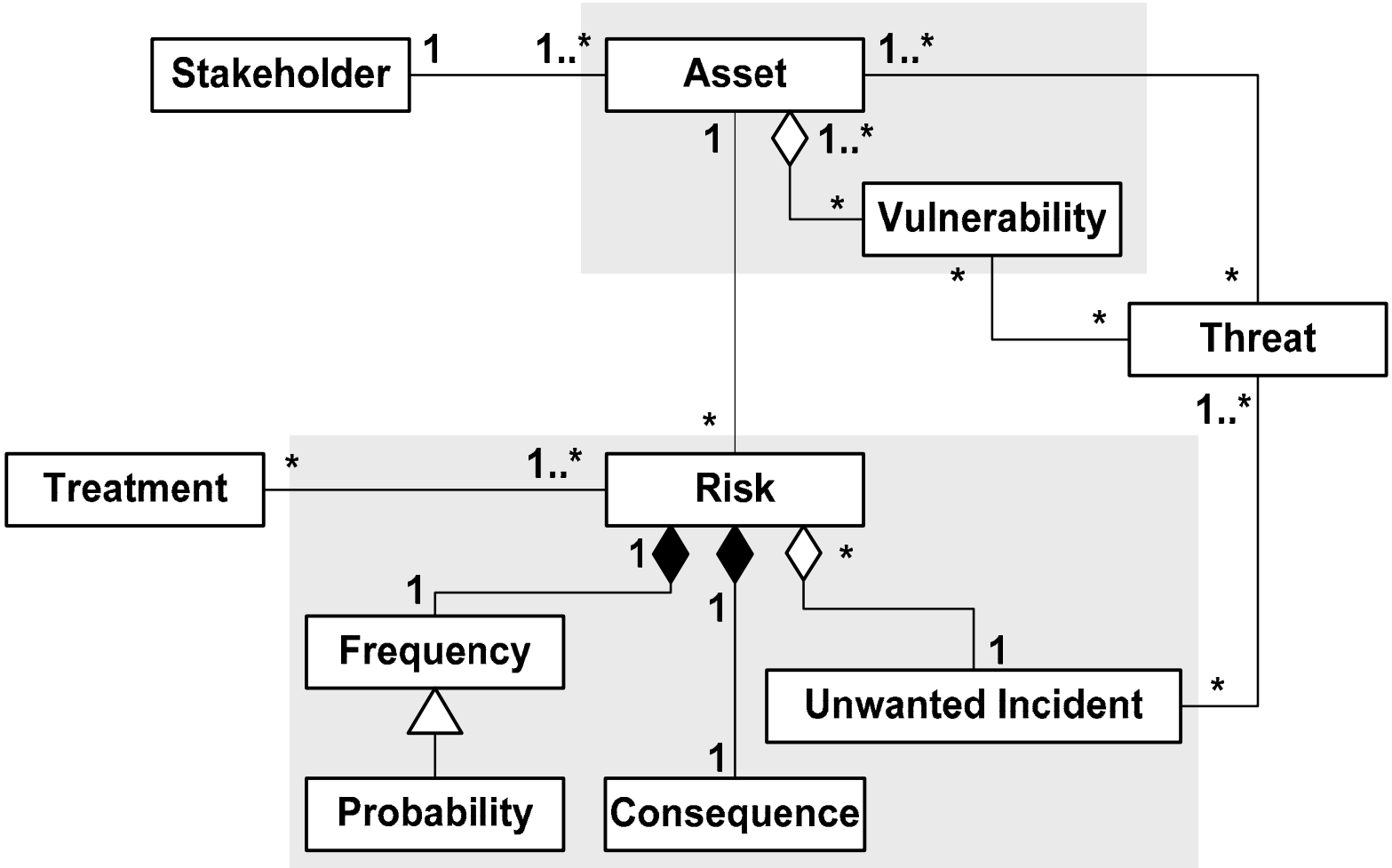
Model-based risk analysis



Oversettelse av terminologi

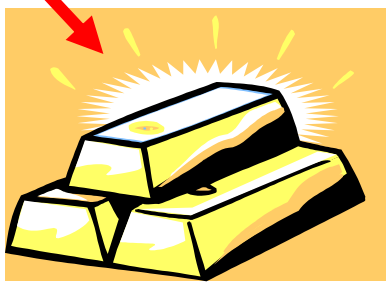
asset	aktivum/aktiva (noe med verdi)
threat	trussel
unwanted incident	uønsket hendelse
risk	risiko
vulnerability	sårbarhet
consequence	konsekvens
probability	sannsynlighet
frequency	frekvens/hyppighet
treatment	behandling

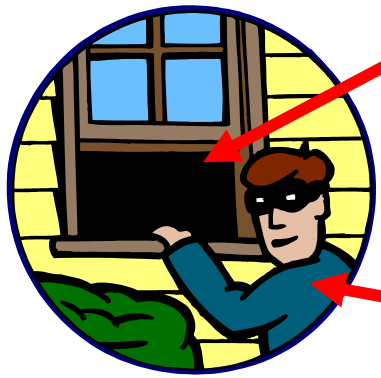
Conceptual model for risk analysis



Terms

asset, something of value





vulnerability

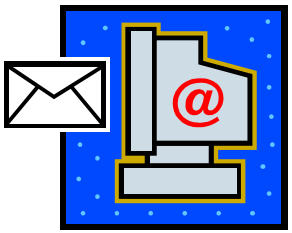
threat

reduced security risk

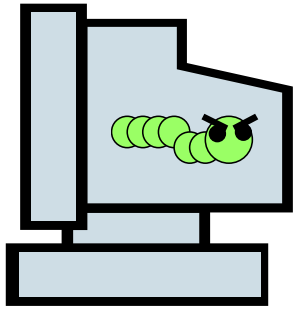
Risk with respect to security

need to introduce security mechanisms

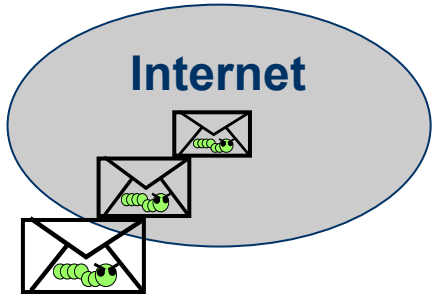
Terms

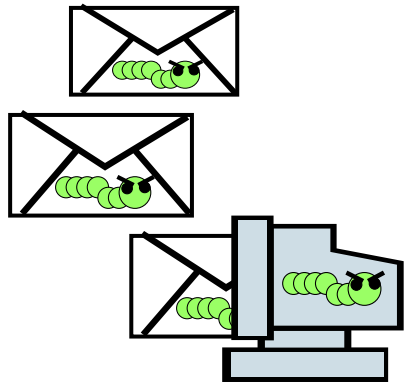


Computer running Outlook



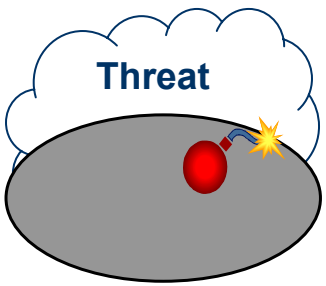
Infected PC

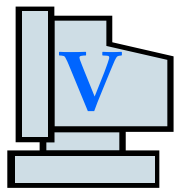




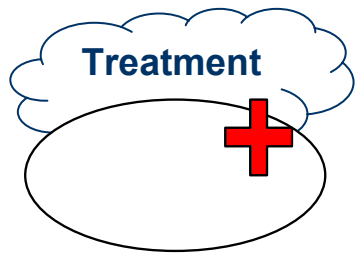
- Infected twice per year
- Infected mail send to all contacts

Worm

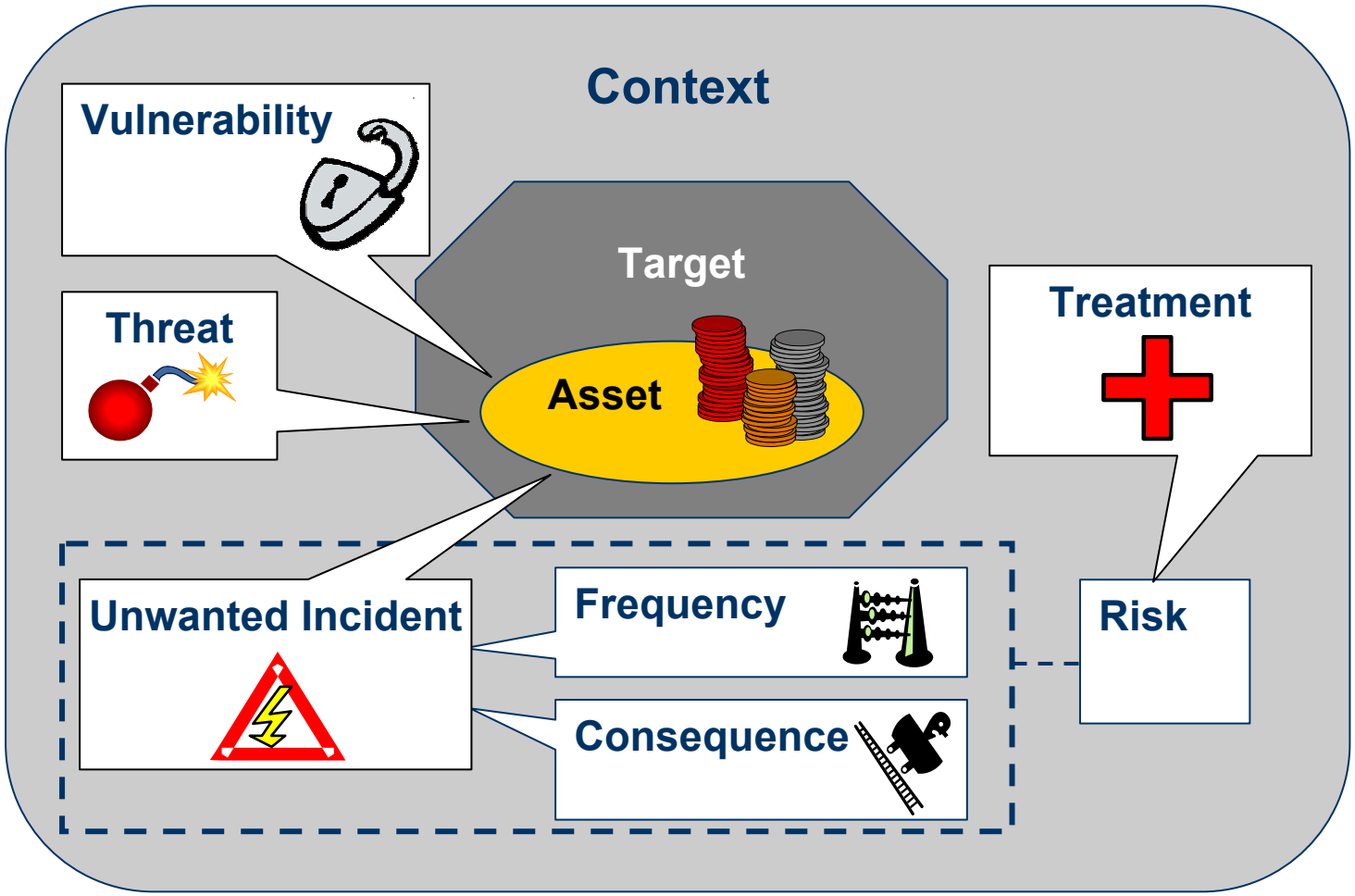




Install virus scanner



Elements of risk analysis



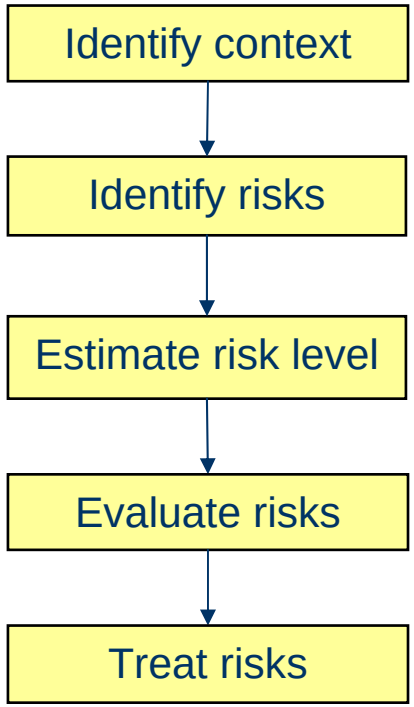
CORAS background

- Research and technological development project under the Information Society Technologies (IST) Programme
- January 2001 -> July 2003
- 11 partners from 4 European countries

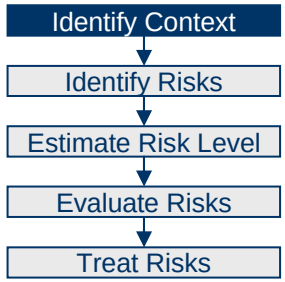
- Goal: Develop an improved methodology for precise, unambiguous, and efficient risk analysis of security critical IT systems

CORAS methodology

- Risk management process based on AS/NZS 4360
- Provides *process* and *guidelines* for risk analysis

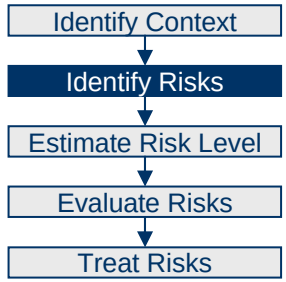


Context identification



- Characterise target of analysis
  - What is the focus and scope of the analysis?
- Identify and value assets
  - Asset-driven risk analysis process
  - Business oriented, e.g. availability of services generating revenue
- Specify risk acceptance criteria
  - There will always be risks, but what losses can the client tolerate?
  - Similar to requirements in system development

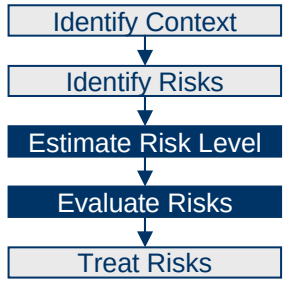
Risk identification



- Identify threats to assets through structured brainstorming
  - Hazard and Operability analysis (HazOp)
  - Involving system owners, users, developers, domain experts, risk analysis experts, etc. (typically 5-7 people)
- Identify vulnerabilities of assets
  - Questionnaires and checklists

Equipment physical security
- Is equipment properly physically protected against unauthorised access to data or loss of data?
- Are power supplies handled in a manner that prevents loss of data and ensures availability?
- …

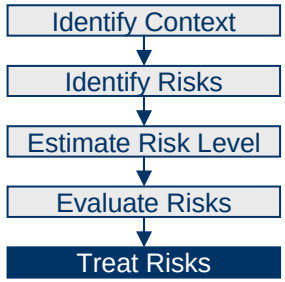
Risk evaluation



- We cannot completely eliminate all risks
- Determine which risks need treatment
  - We need to know how serious they are so we can prioritise

- Risk level is determined based on analysis of the frequency and consequence of the unwanted incident
  - Quantitative values: e.g., loss of 1M€, 25% chance per year
  - Qualitative values: e.g., high, medium, low

Risk treatment



- Identify treatments for unaccepted risks
- Evaluate and prioritise different treatments