

Security analysis – basic notions and ideas

October 28, 2005

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

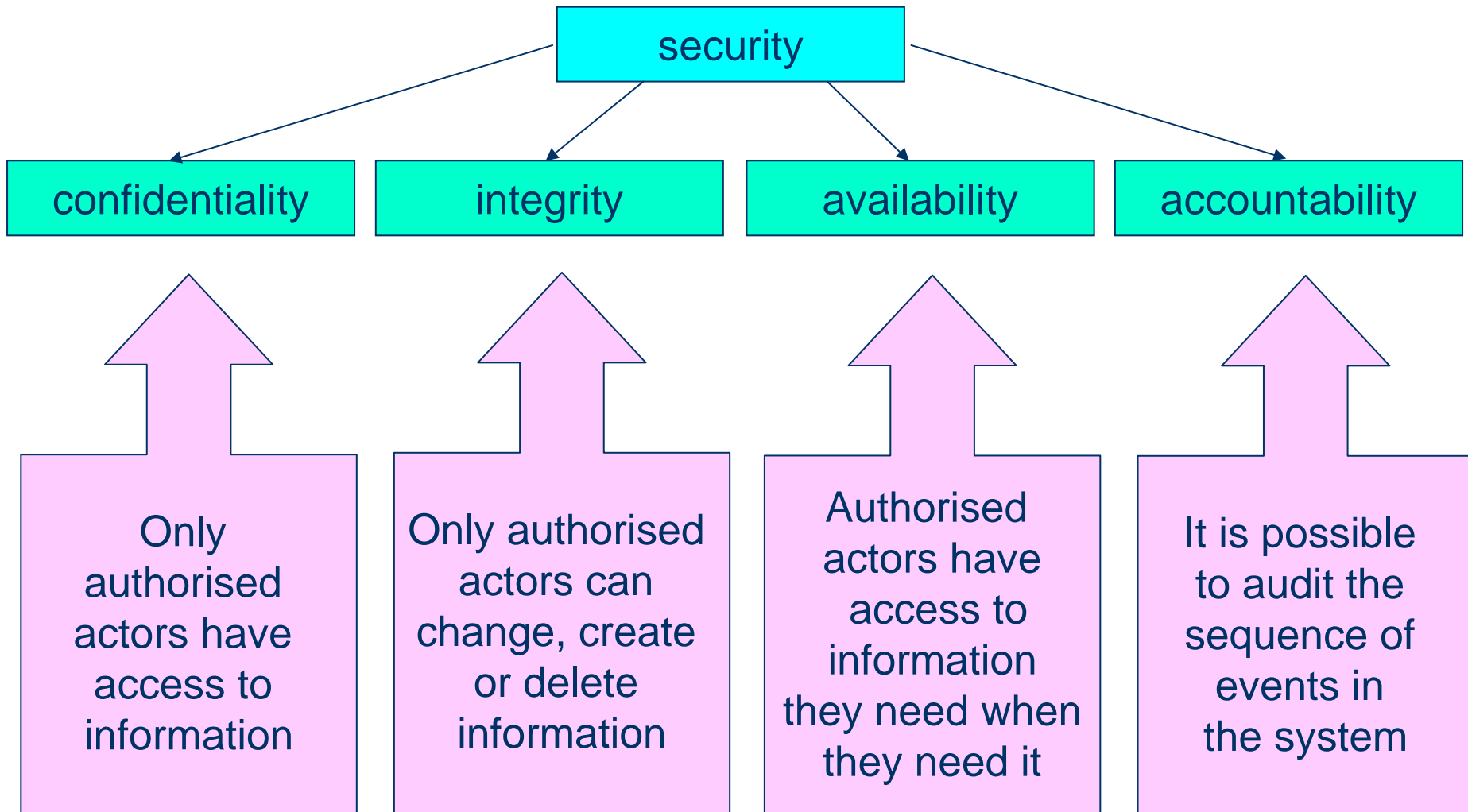
Objectives for the three lectures on security analysis

- 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

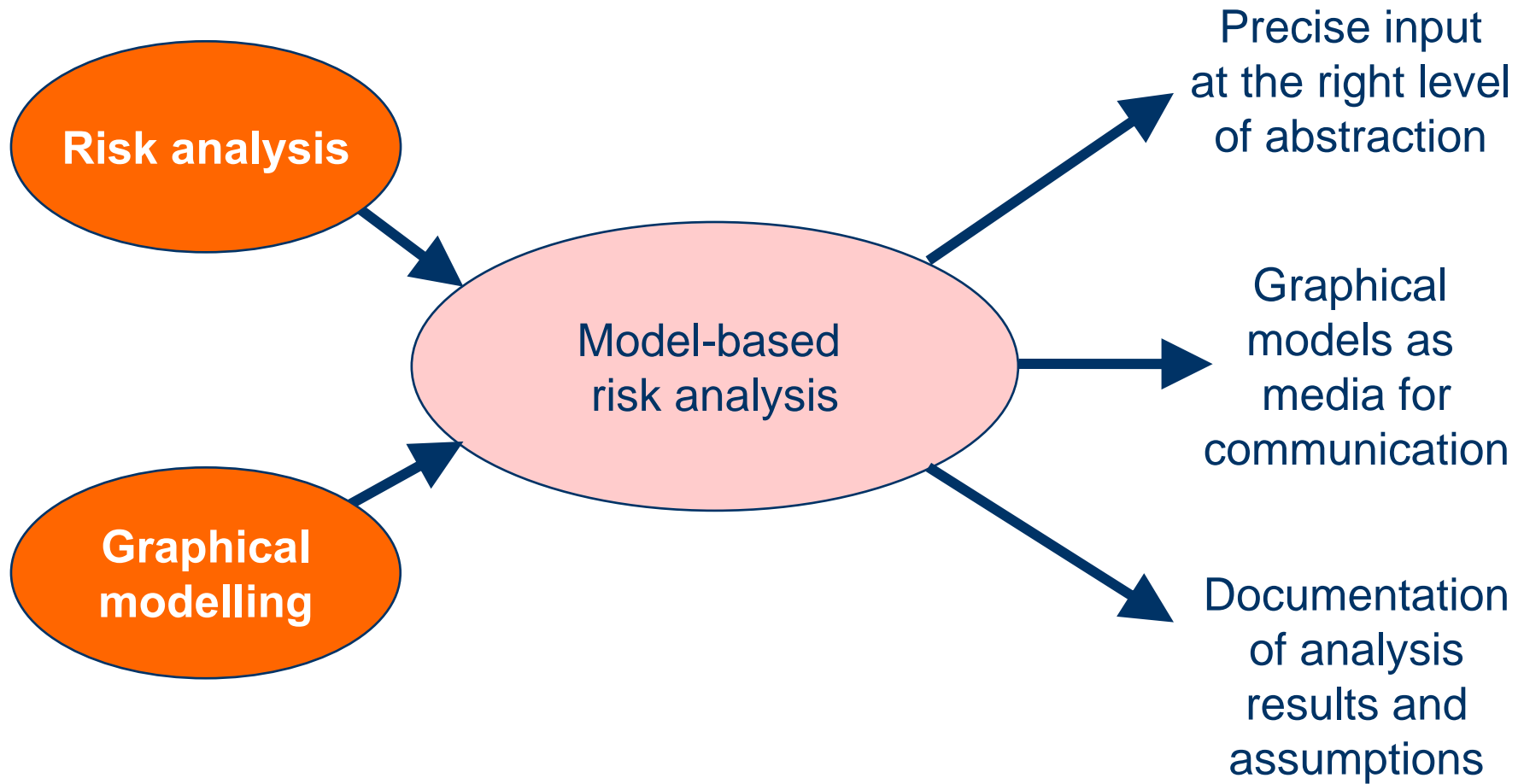
Note: Security is more than technology

- 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.

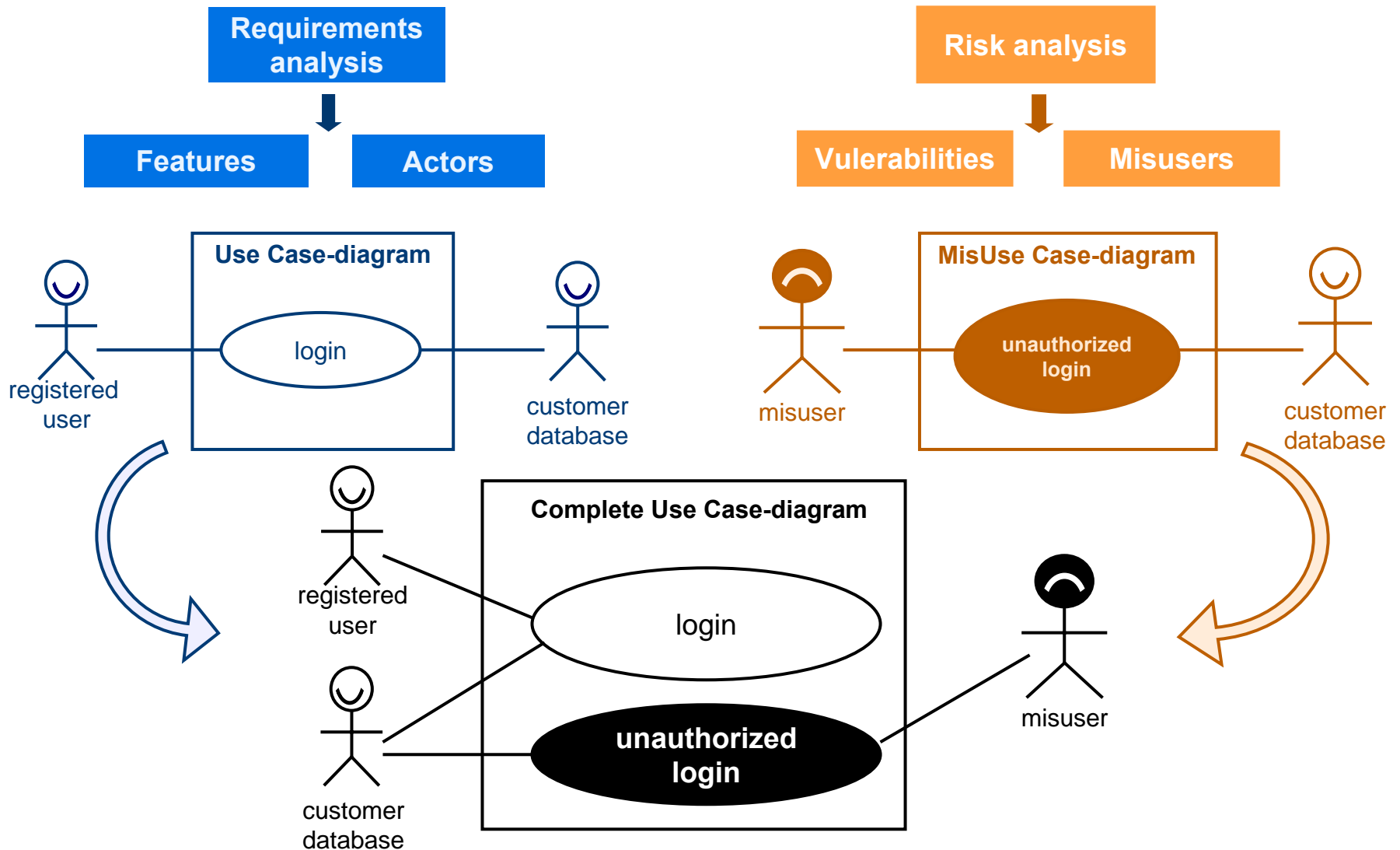
Security – part of system development

- 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



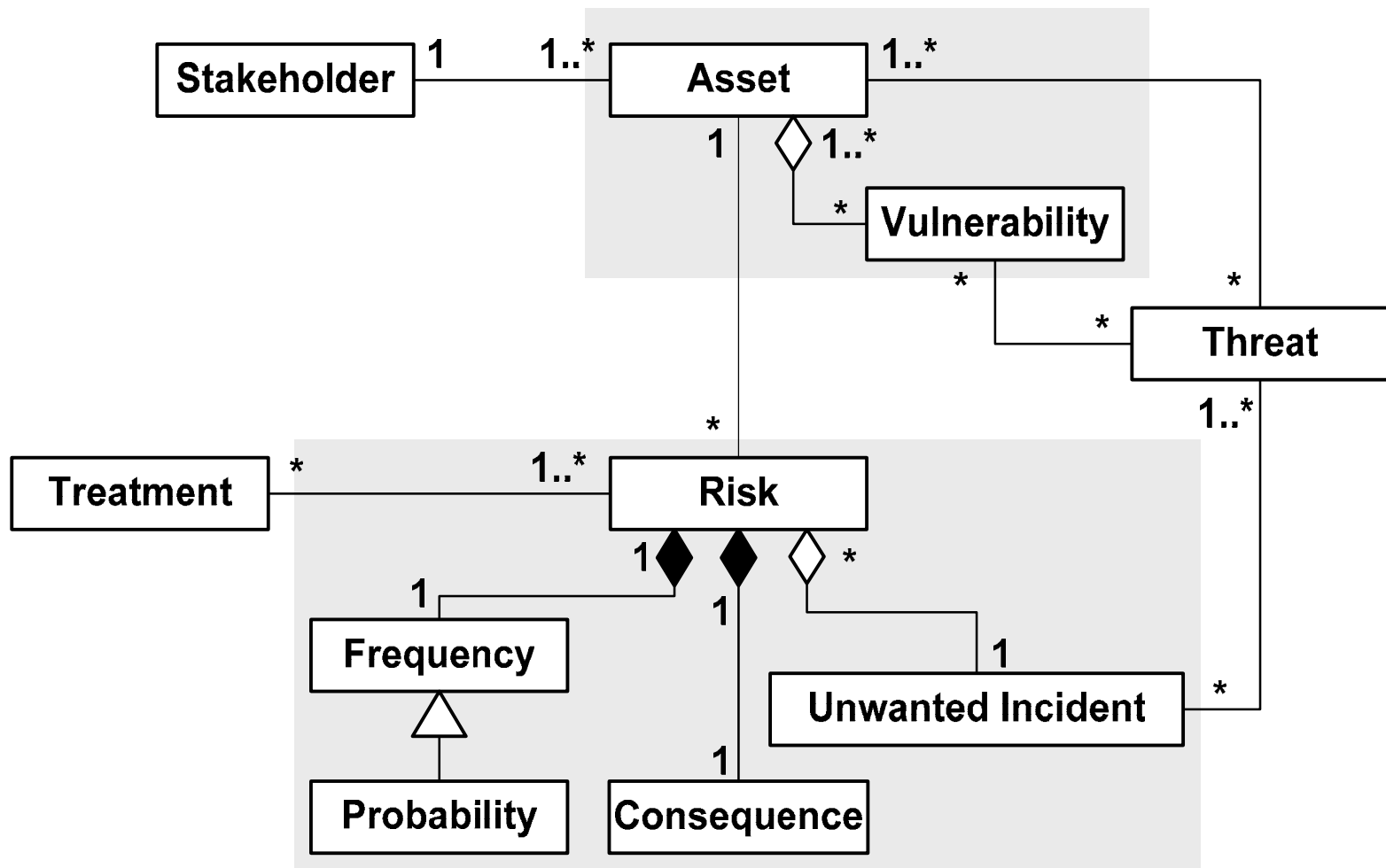
Terminology exercise

- Useful for you, for me and for further research
- We will present the correct answers later in the lecture
- Filled in forms will be copied and handed back during the lecture
- Furthermore:
 - This is anonymous
 - You have to remember your number to get your form back
 - IMPORTANT TO GUESS IF YOU DON'T KNOW THE ANSWER

Oversettelse av terminologi

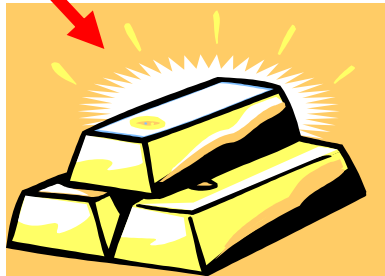
asset	aktivum/aktiva (noe med verdi)
threat	trussel
unwanted incident	uønsket hendelse
risk	risiko
vulnerability	sårbarhet
consequence	konsekvens
probability	sannsynlighet
frequency	frekvens/hyppighet
treatment	behandling

Conceptual model for risk analysis

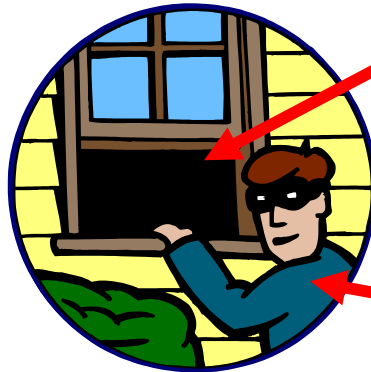


Terms

asset, something of value



vulnerability



threat

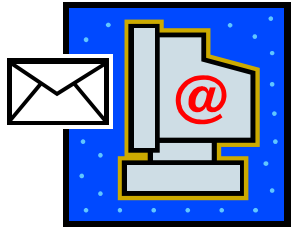
reduced security risk

Risk with respect to security

need to introduce security mechanisms

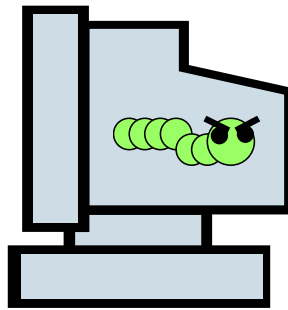


Terms



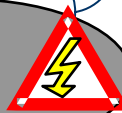
Computer running Outlook

Vulnerability



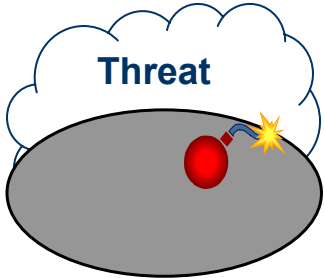
Infected PC

Unwanted incident



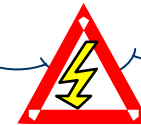
Worm

Threat

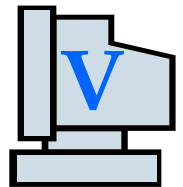


- Infected twice per year
- Infected mail send to all contacts

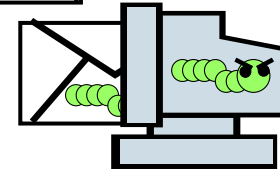
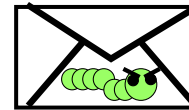
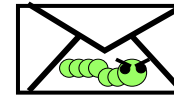
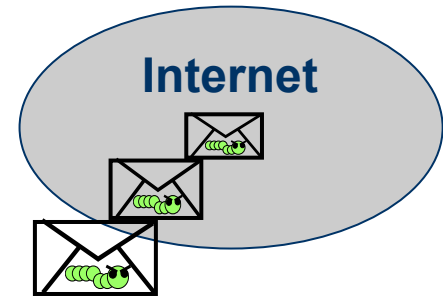
Risk



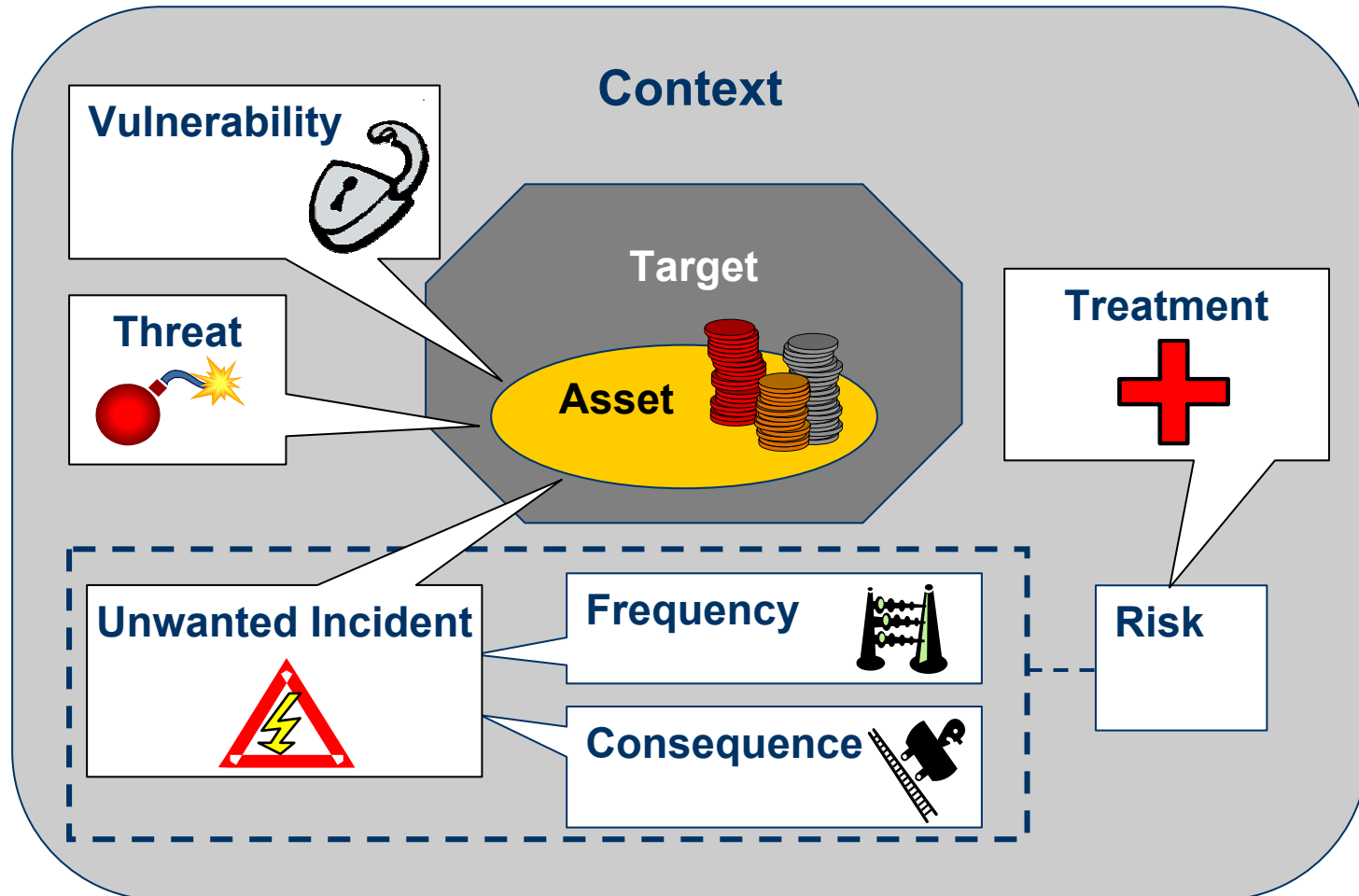
Install virus scanner



Treatment



Elements of risk analysis



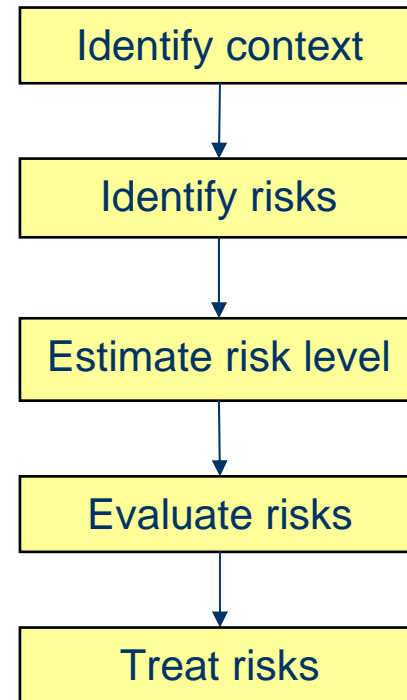
CORAS background



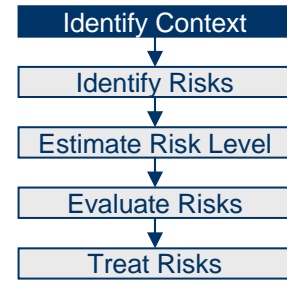
- Research and technological development project under the Information Society Technologies (IST) Programme
- January 2001 -> July 2003
- 11 partners from 4 European countries
- Goal: Develop an improved methodology for precise, unambiguous, and efficient risk analysis of security critical IT systems

CORAS methodology

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

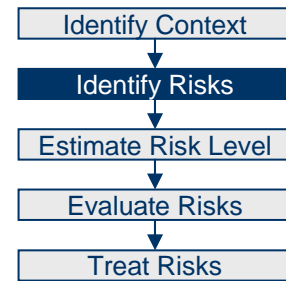


Context identification



- 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



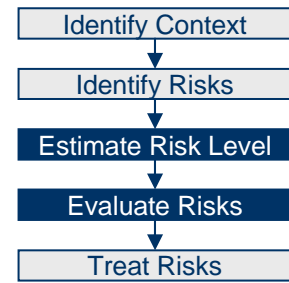
- Identify threats to assets through structured brainstorming
 - Hazard and Operability analysis (HazOp)
 - Involving system owners, users, developers, domain experts, risk analysis experts, etc. (typically 5-7 people)

- 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?
- ...

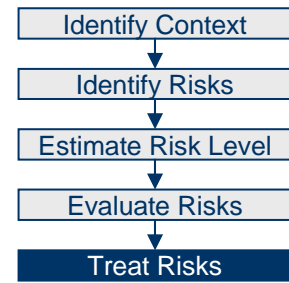
Risk evaluation



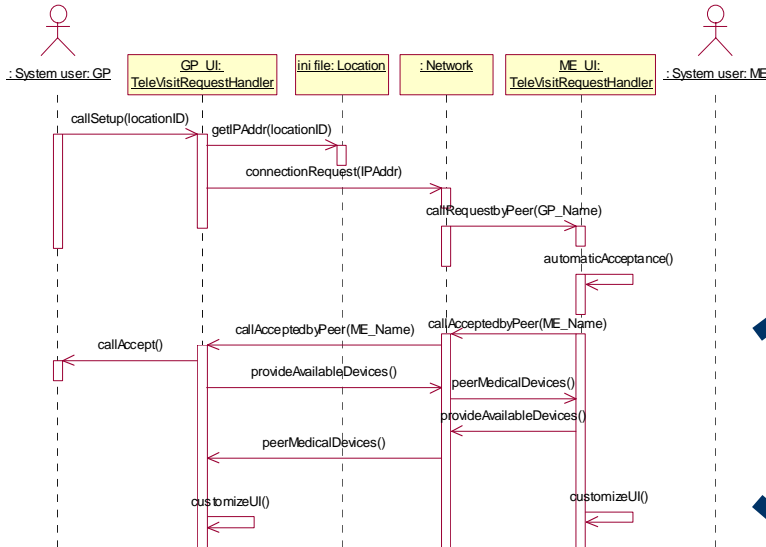
- We cannot completely eliminate all risks
- Determine which risks need treatment
 - We need to know how serious they are so we can prioritise
- Risk level is determined based on analysis of the frequency and consequence of the unwanted incident
 - Quantitative values: e.g., loss of 1M€, 25% chance per year
 - Qualitative values: e.g., high, medium, low

Risk treatment

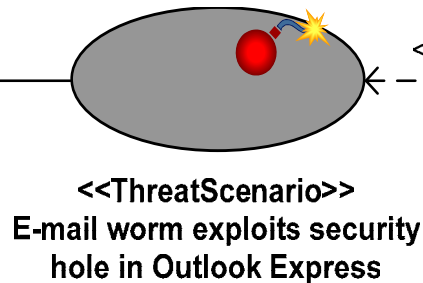
- Identify treatments for unaccepted risks
- Evaluate and prioritise different treatments



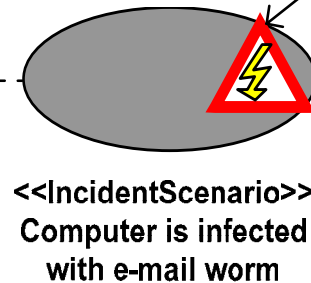
Graphical UML-based modelling



HazOp ID	Asset ID	Guideword	Attribute	Scenario

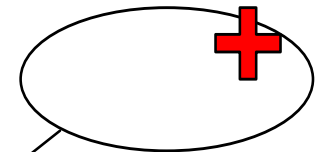


<<include>>



<<Asset>>
System availability

Vulnerability:
- Unpatched Outlook Express



<<Treatment>>
Install virus scanner

<<ReduceFrequency>>

CORAS risk analysis tool

CORAS Risk Analysis Tool

File Edit Window Help

Risk Analysis Project Experience Library CORAS Methodology

- TrustCoM VHC
 - Context identification
 - Risk identification
 - Legal threats**
 - VHC threats
 - Risk analysis
 - Risk evaluation
 - Risk treatment

Filter by viewpoint

Result Info

Type: HazOp Table

Name: Legal threats

Description: Legal threats in the VHC scenario

Concern: Threats

Viewpoint:
 Enterprise
 Information
 Computational
 Engineering
 Technology

Full description:
 Legal threats of the TrustCoM Virtual Hope Community (VHC) scenario in relation to Norwegian data protection law.

Table Legal threats

Asset ID	Item	Threat	Unwanted Incident
legal record	register new user	Registration of new user is processing of personal data, requirements in Section 8 of the personal data act must be observed.	data inspectorate can order cease of unlawful processing, Section 46
legal record		Personal data processed in conflict with any of the provisions of the personal data act (cf. Section 46)	
charity fund		Section 47 In connection with orders pursuant to sections 12, 27, 28 and 46, the Data Inspectorate may impose a coercive fine which will run from the expiry of the time limit set with the order until the order has been complied with.	Coercive fine
charity fund			
legal record		Section 48 (1) a Anyone who wilfully or through gross negligence omits to send notification pursuant to section 48 (1) a, shall be liable to a fine or imprisonment. Check if notification required, is the customer-relationship according to the Personal Data Regulation (legislation not available in English)	

UML Model VHC threats

UML Diagram

File: threat-diagram.png

Browse Save Open in external application

CORAS contact information

- Tool developer: Fredrik Vraalsen
 - E-mail: fredrik.vraalsen@sintef.no
- Folker den Braber
 - E-mail: folker.den.braber@sintef.no
 - Gives the next lecture: November 4
 - Includes case-study and demo
- CORAS webpage: <http://coras.sourceforge.net/>