Security analysis — basic notions and ideas

October 09, 2009

Ketil Stølen, SINTEF & UiO

Acknowledgements

- The lectures on security analysis is the result of joint work with a number of current and past colleagues at SINTEF; in particular:
  - Ida Hogganvik, Mass Soldal Lund, Bjørnar Solhaug, Fredrik Vraalsen, Heidi Dahl

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

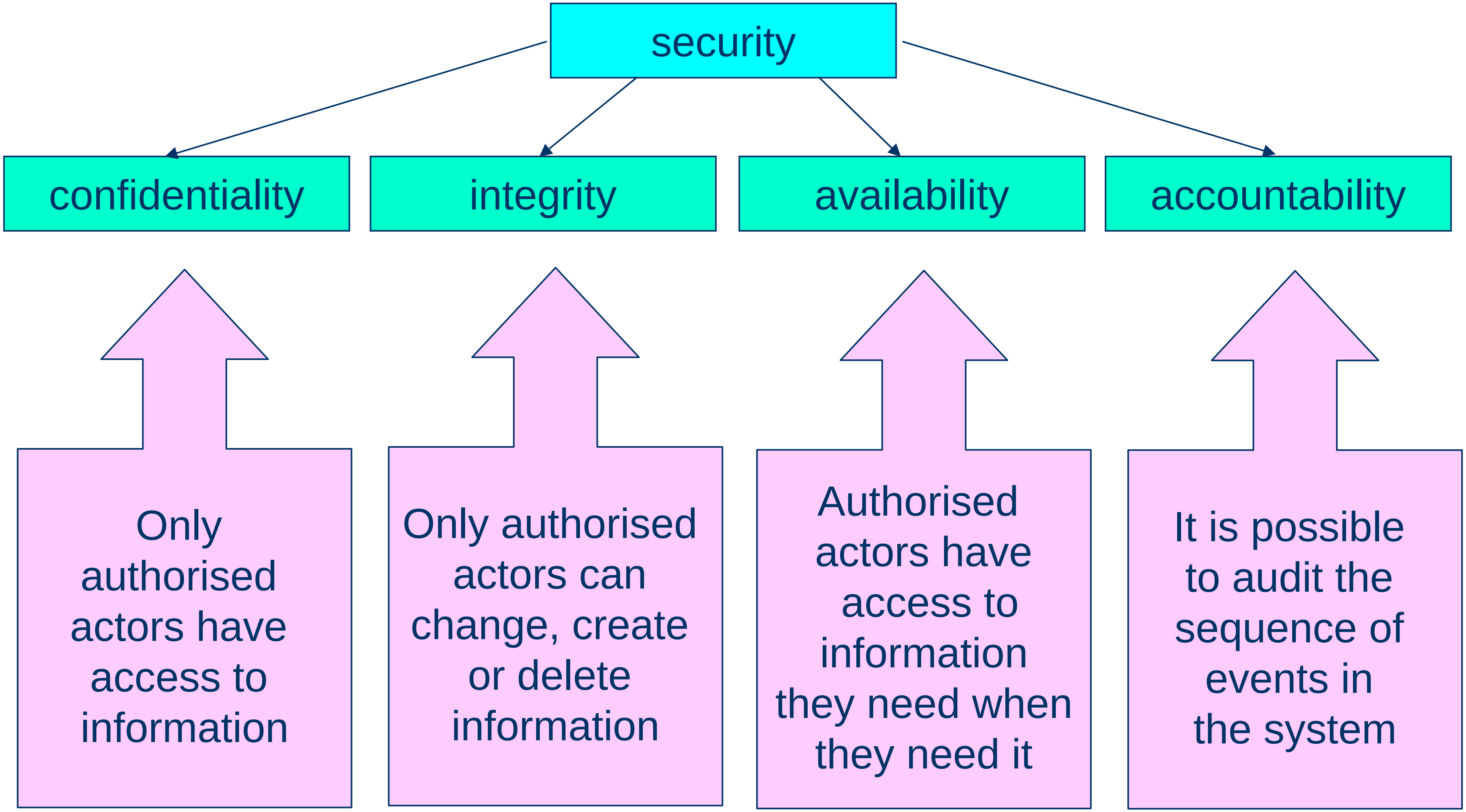
Objectives for the three lectures on security analysis

- 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
- 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?



security

confidentiality

integrity

availability

accountability

Only authorised actors have access to information

Only authorised actors can change, create or delete information

Authorised actors have access to information they need when they need it

It is possible to audit the sequence of events in the system

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

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

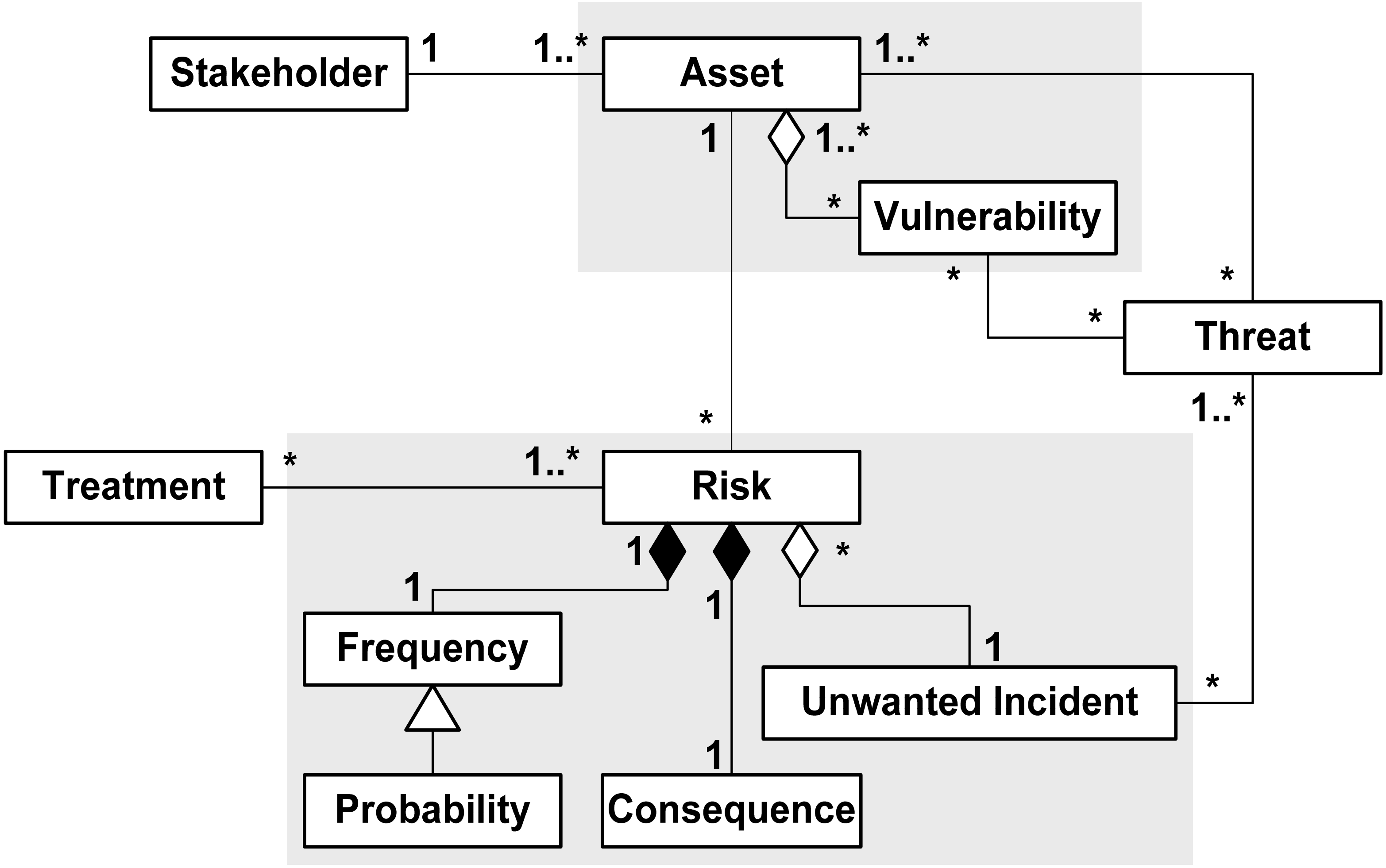
In what way is “security” related to

- safety
- reliability
- dependability
- maintainability
- data protection
- privacy
- trustworthy
- trust
- public key infrastructure based on trusted third party
- authentication and authorization

Oversettelse av terminologi

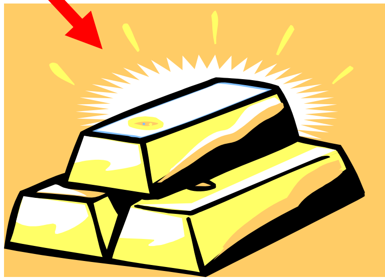
asset	aktivum (noe med verdi)
threat	trussel
unwanted incident	uønsket hendelse
risk	risiko
vulnerability	sårbarhet
consequence	konsekvens
probability	sannsynlighet
frequency	frekvens/hyppighet
treatment	behandling

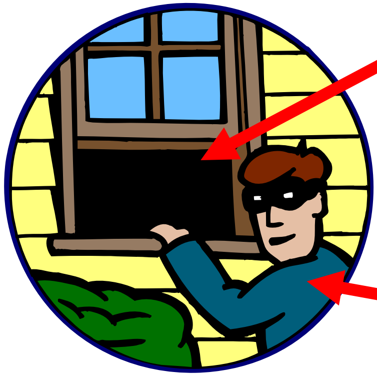
Conceptual model for risk analysis



Terms

asset, something of value





vulnerability

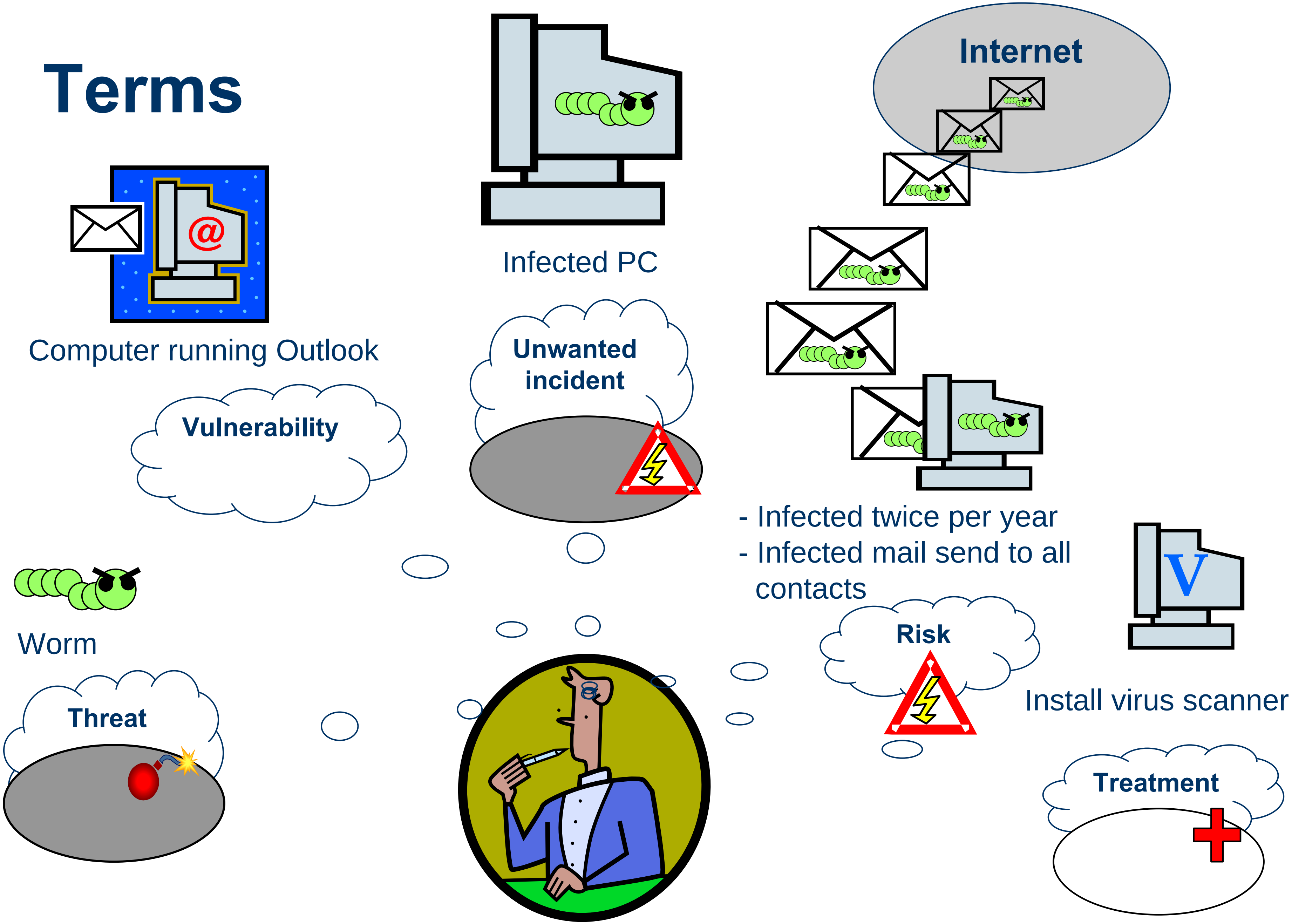
threat

reduced security risk

Risk with respect to security

need to introduce security mechanisms

Terms



Computer running Outlook

Infected PC

Internet

Vulnerability

Unwanted incident

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

Worm

Threat

Risk

Install virus scanner

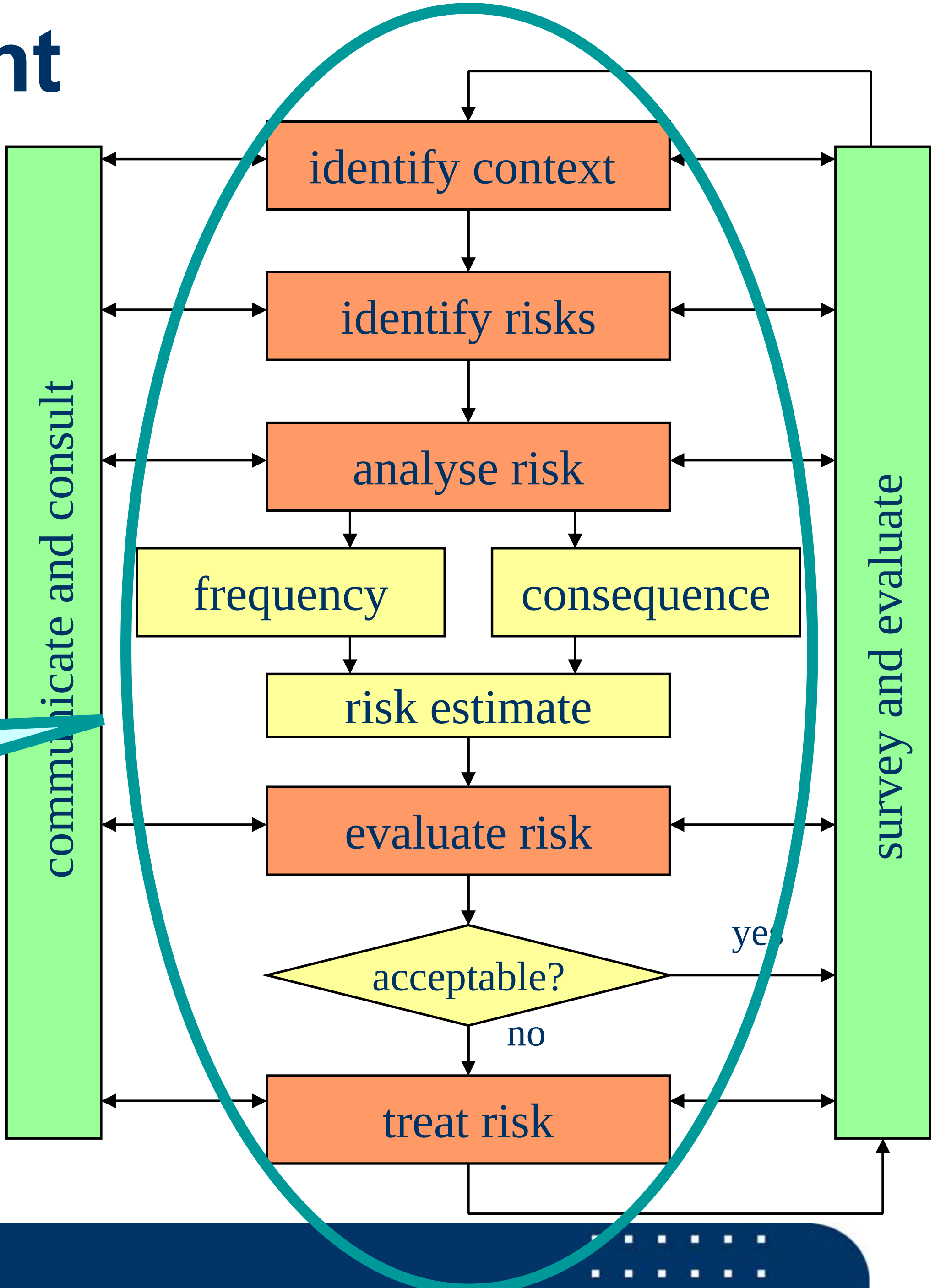
Treatment

Risk management

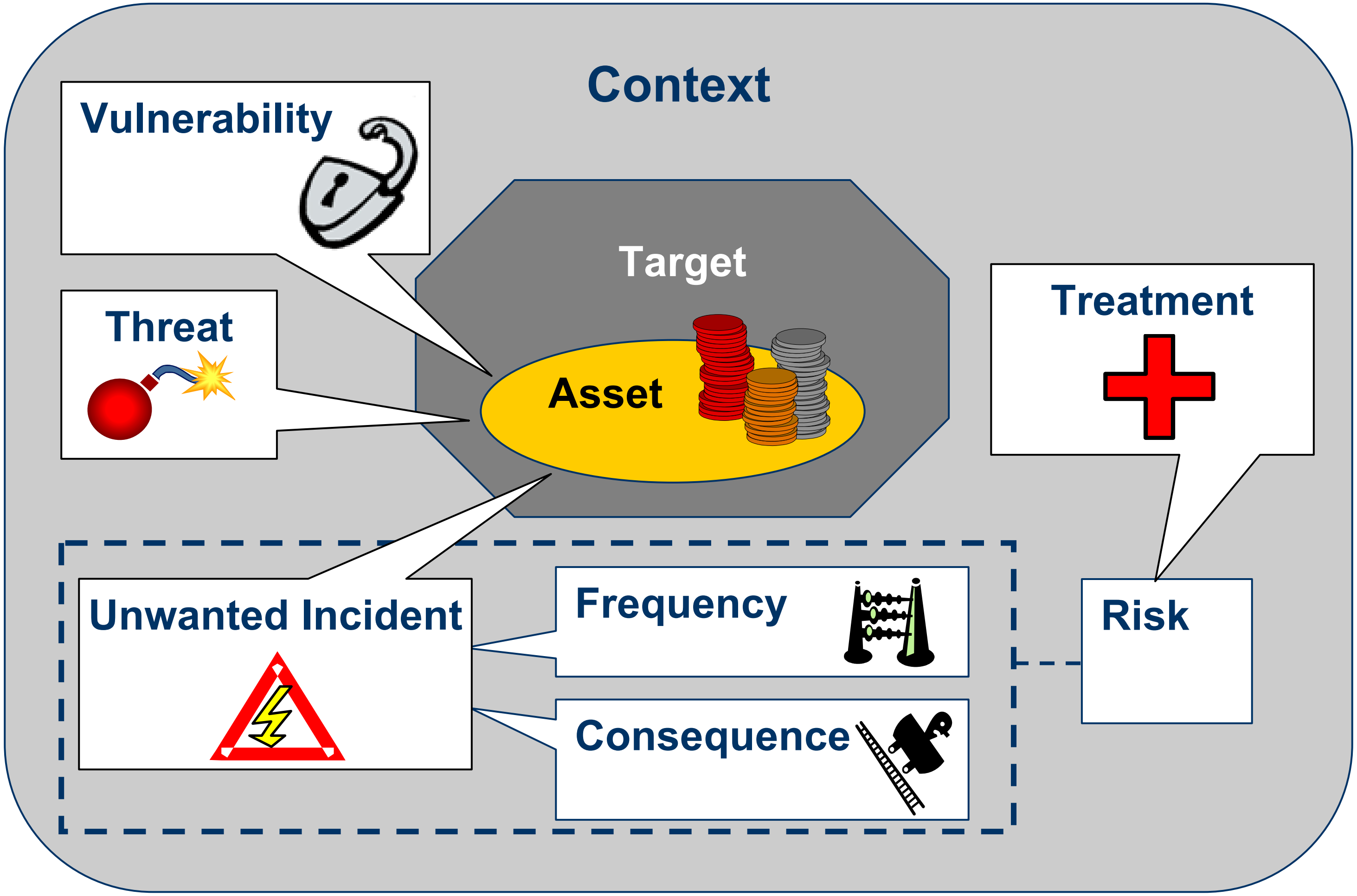
Risk management is the culture, processes and structures that are directed towards
realizing potential opportunities whilst managing adverse effects

Our focus:

Risk Analysis

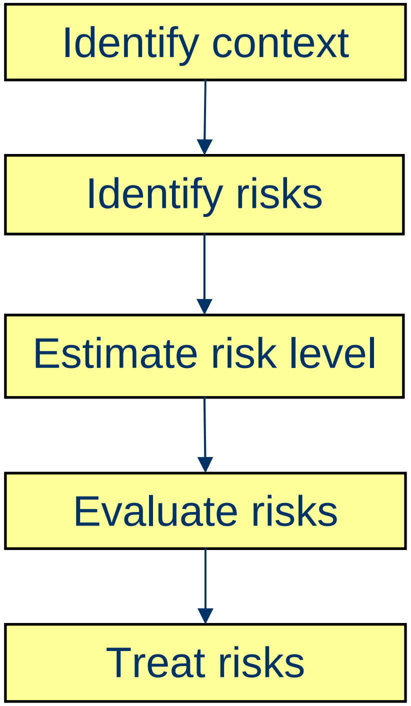


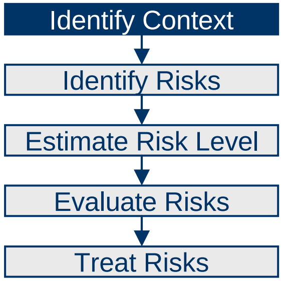
Elements of risk analysis



The CORAS process

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

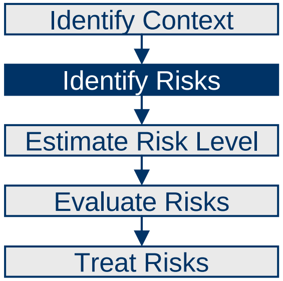




Context identification

- 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 evaluation criteria
  - There will always be risks, but what losses can the client tolerate?
  - Similar to requirements in system development

Risk identification


Identify Context

Identify Risks

Estimate Risk Level

Evaluate Risks

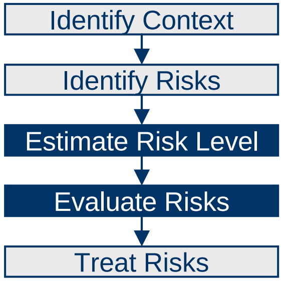
Treat Risks

- 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

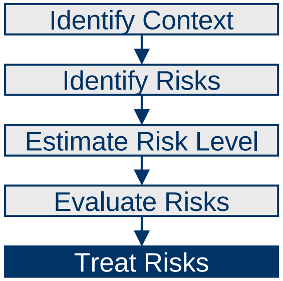
- Is equipment properly physically protected against unauthorised access to data or loss of data?
- Are power supplies handled in a manner that prevents loss of data and ensures availability?
- …



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


Identify Context

Identify Risks

Estimate Risk Level

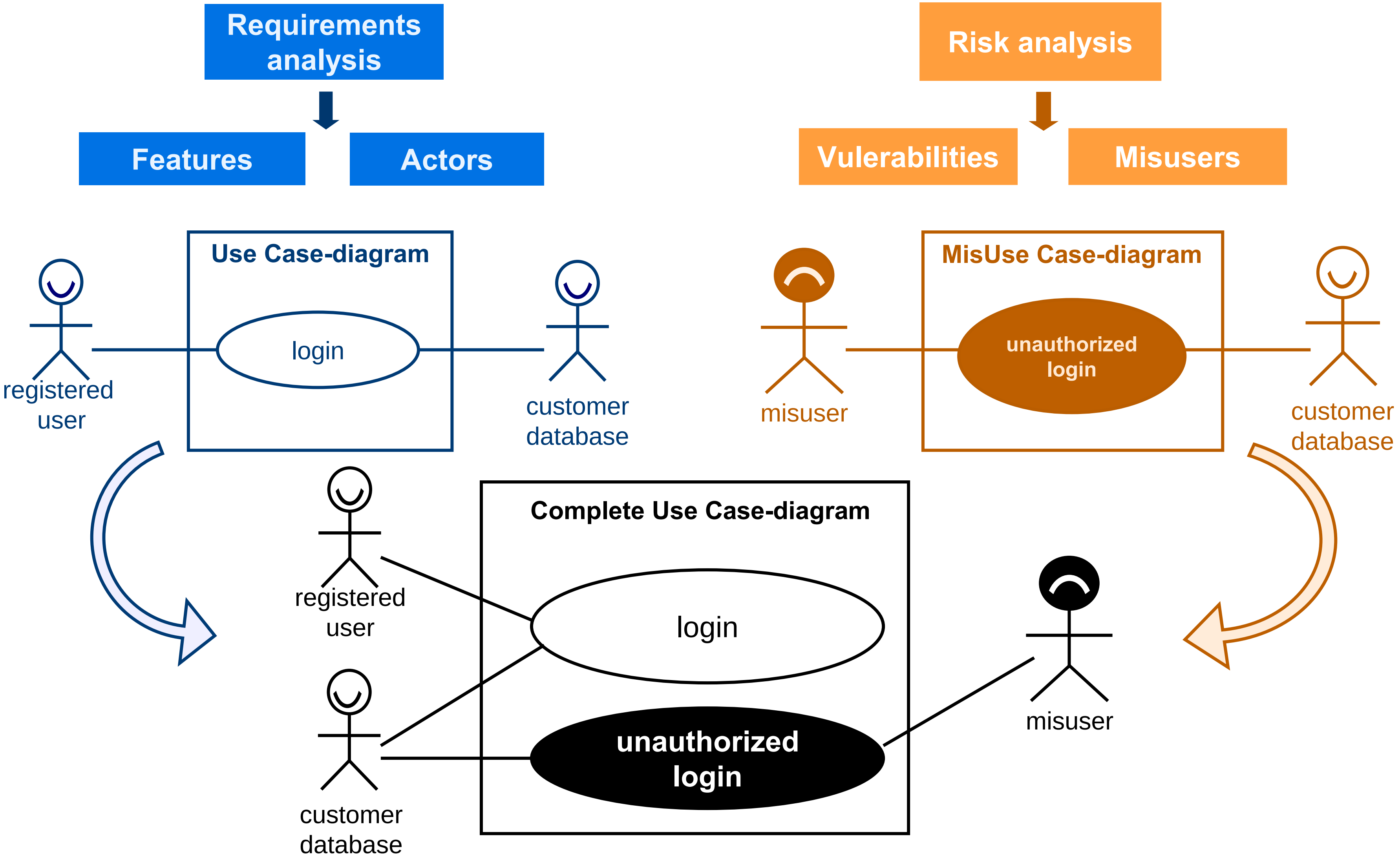
Evaluate Risks

Treat Risks

Risk treatment

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

Model-based risk analysis



Requirements analysis

Features

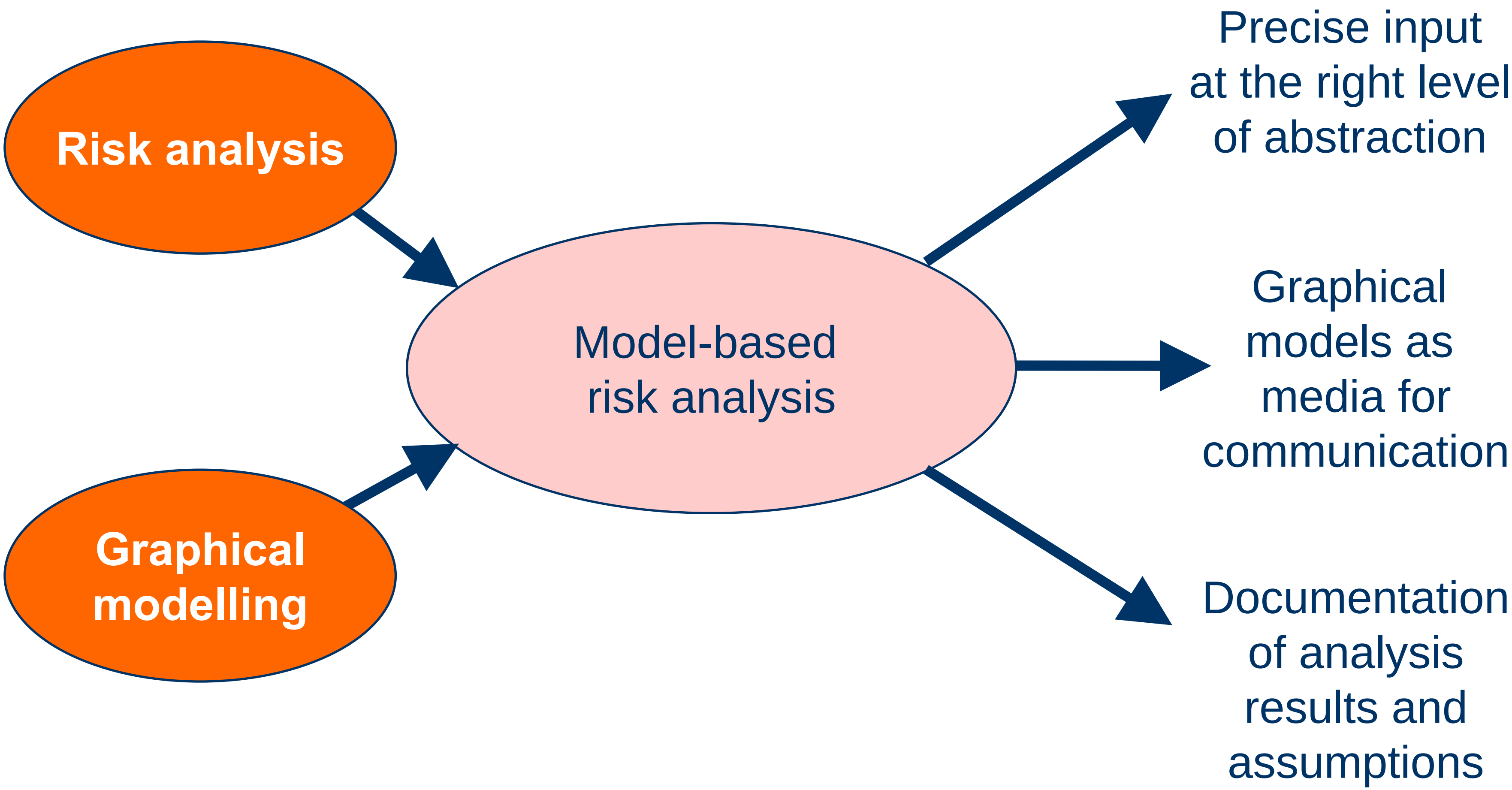
Actors

Risk analysis

Vulerabilities

Misusers

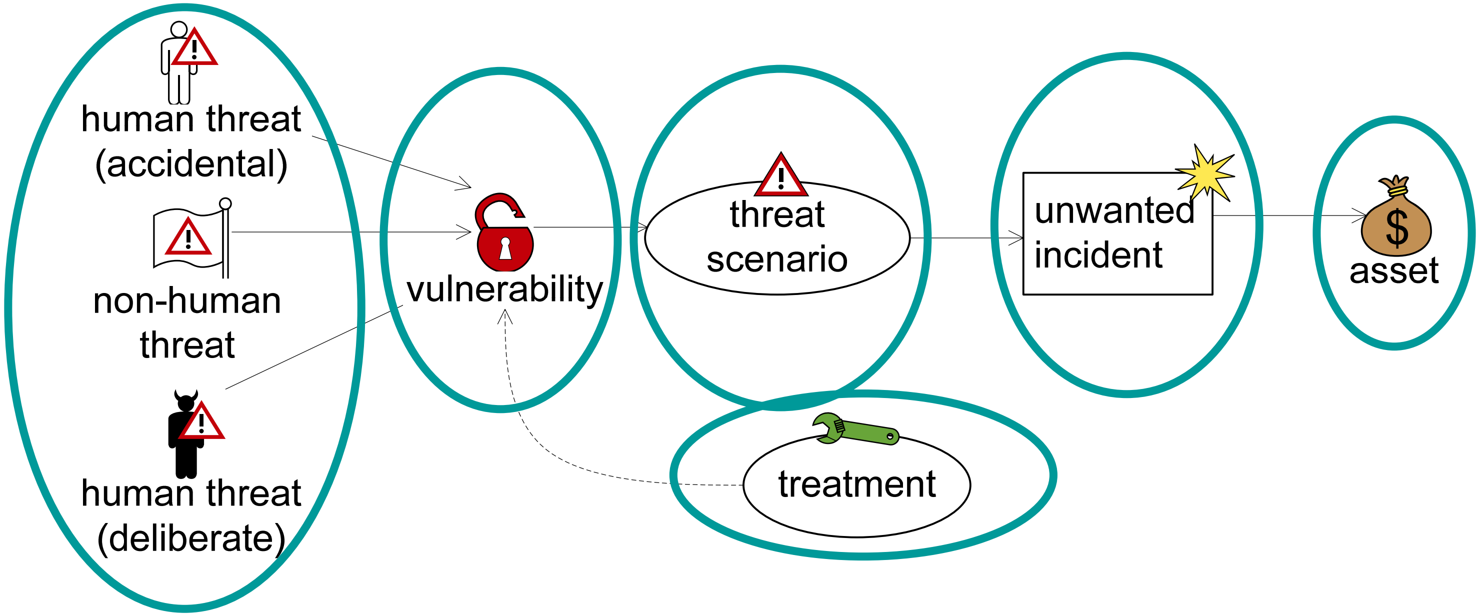
Model-based risk analysis


Risk analysis
Graphical modelling
Model-based risk analysis
Precise input at the right level of abstraction
Graphical models as media for communication
Documentation of analysis results and assumptions

What is CORAS?

- The CORAS process
  - A process for security risk analysis
- The CORAS language (diagrams)
  - A graphical language that supports the analysis process
  - Basis for communication, documentation and analysis
- The CORAS semantics
  - A schematic translation of any CORAS diagram into English
- The CORAS guideline
  - A guideline for best use of the language within the process
- The CORAS tool
  - A computerized tool supporting the above

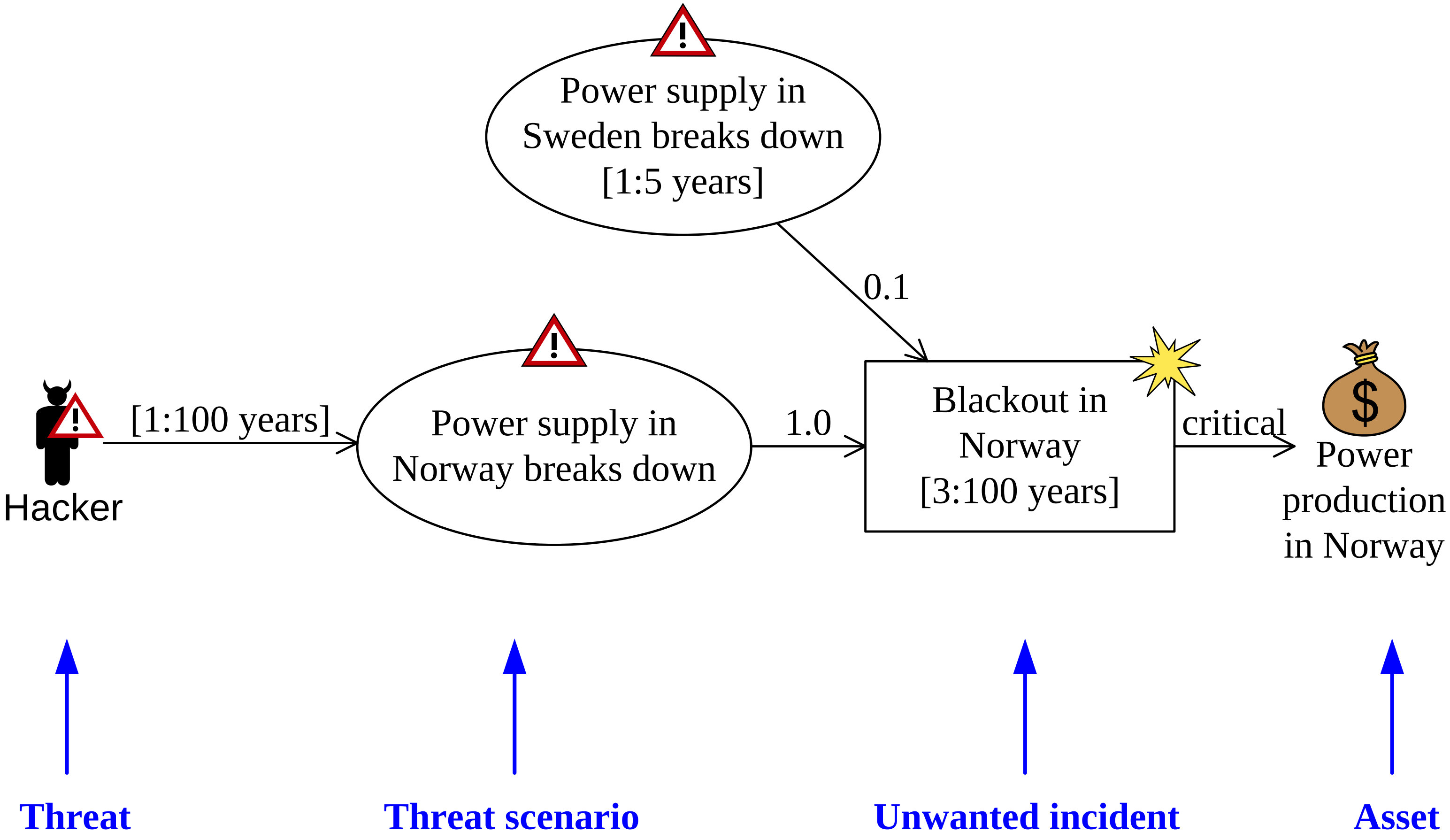
The CORAS language



The CORAS diagrams

- **Asset diagrams**
  Describes the focus of the analysis
- **Threat diagrams**
  Describes scenarios which may cause harm to the assets
- **Risk overview diagrams**
  Summarises the risks presented in threat diagrams
- **Treatment diagrams**
  Adds proposed treatments to threat diagrams
- **Treatment overview diagrams**
  Adds proposed treatments to risk overview diagrams

Threat Diagram



Hacker

[1:100 years]

Power supply in Norway breaks down

Power supply in Sweden breaks down [1:5 years]

0.1

1.0

Blackout in Norway [3:100 years]

critical

Power production in Norway

Threat

Threat scenario

Unwanted incident

Asset

Semantics: Translation into English

- Vertices
  - ”Hacker” is a deliberate threat.
  - Threat scenario ”Power supply in Norway breaks down” occurs with undefined likelihood.
  - Threat scenario ”Power supply in Sweden breaks down” occurs with likelihood ”1:5 years”.
  - Unwanted incident ”Blackout in Norway” occurs with likelihood ”3:100 years”.
  - ”Power production in Norway” is an asset.
- Relations
  - Hacker initiates ”Power supply in Norway breaks down” with likelihood ”1:100” years.
  - ”Power supply in Norway breaks down” leads to ”Blackout in Norway” with conditional likelihood ”1.0”.
  - ”Power supply in Sweden breaks down” leads to ”Blackout in Norway” with conditional likelihood ”0.1”.
  - ”Power supply in Norway breaks down” impacts ”Power production in Norway” with consequence ”critical”.

Next Lecture on Security Analysis

October 30