Security Risk Assessment I

Ketil Stølen

SINTEF

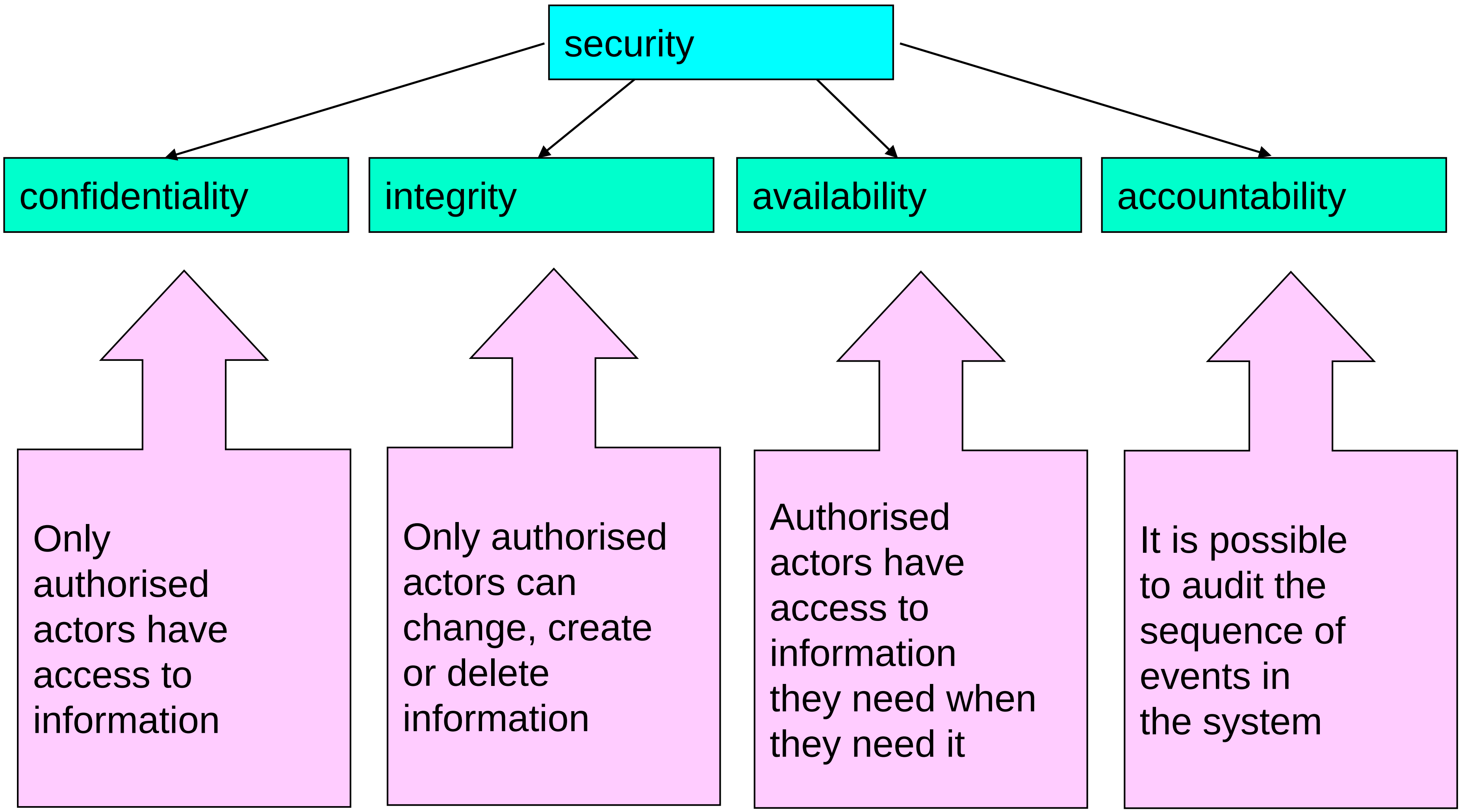
Overview of today

- What is security?
- What is risk?
- What is risk management?
- What is the relationship to cyber security?
- What is CORAS?

What is Security Risk Assessment?

- Security risk assessment is a specialized form of risk assessment 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

Security is more than Technology

- What good is security if no one can use the systems?
- Requires more than technical understanding
- Incidents often of non-technical origin
- Requires uniform description of the whole
  - how it is used, the surrounding organisation, etc.

Security should not be an "afterthought"

- Security issues solved in isolation
- Costly redesign
- Security not completely integrated

What is Risk?

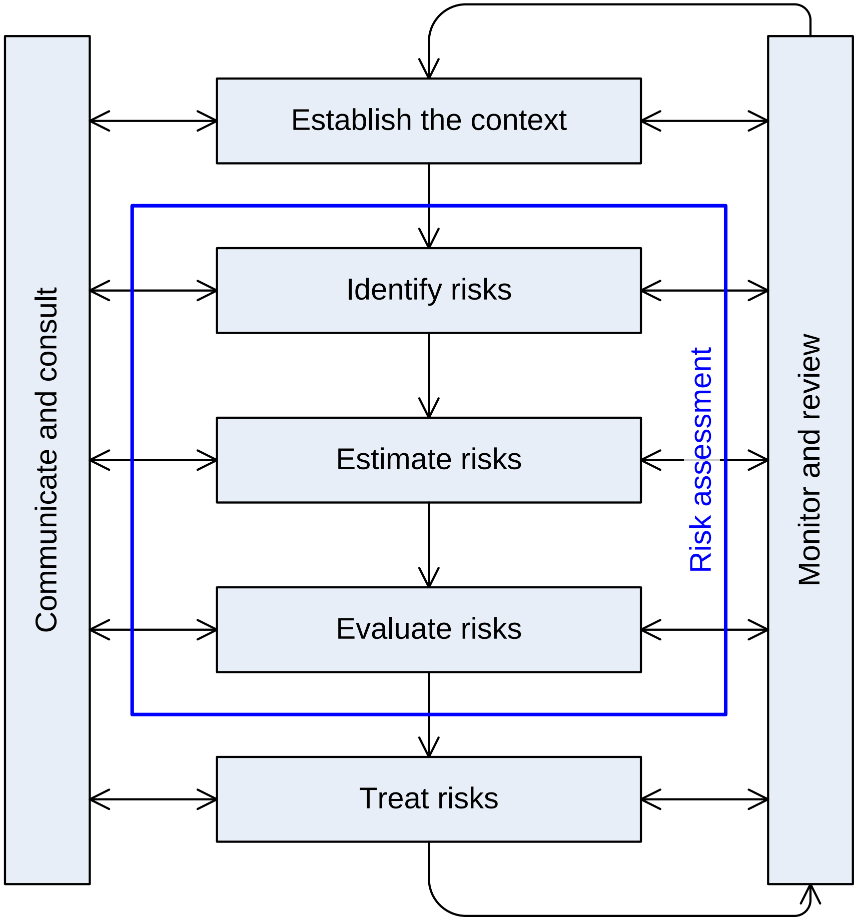
- Many kinds of risk
  - Contractual risk
  - Economic risk
  - Operational risk
  - Environmental risk
  - Health risk
  - Political risk
  - Legal risk
  - Security risk

Definition of Risk from ISO 31000

- **Risk:** Effect of uncertainty on objectives
  - NOTE 1 An effect is a deviation from the expected — positive and/or negative
  - NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process)
  - NOTE 3 Risk is often characterized by reference to potential **events** and **consequences**, or a combination of these
  - NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** of occurrence
  - NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood

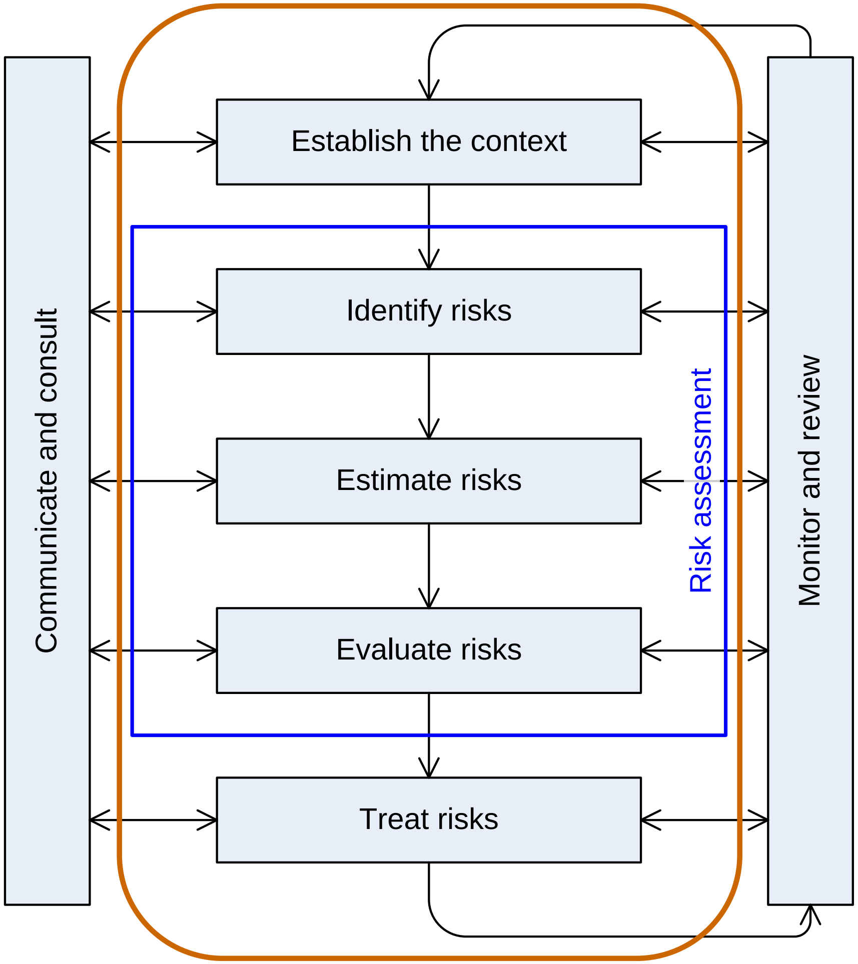
What is Risk Management?

- **Risk management:** Coordinated activities to direct and control an organization with regard to **risk**

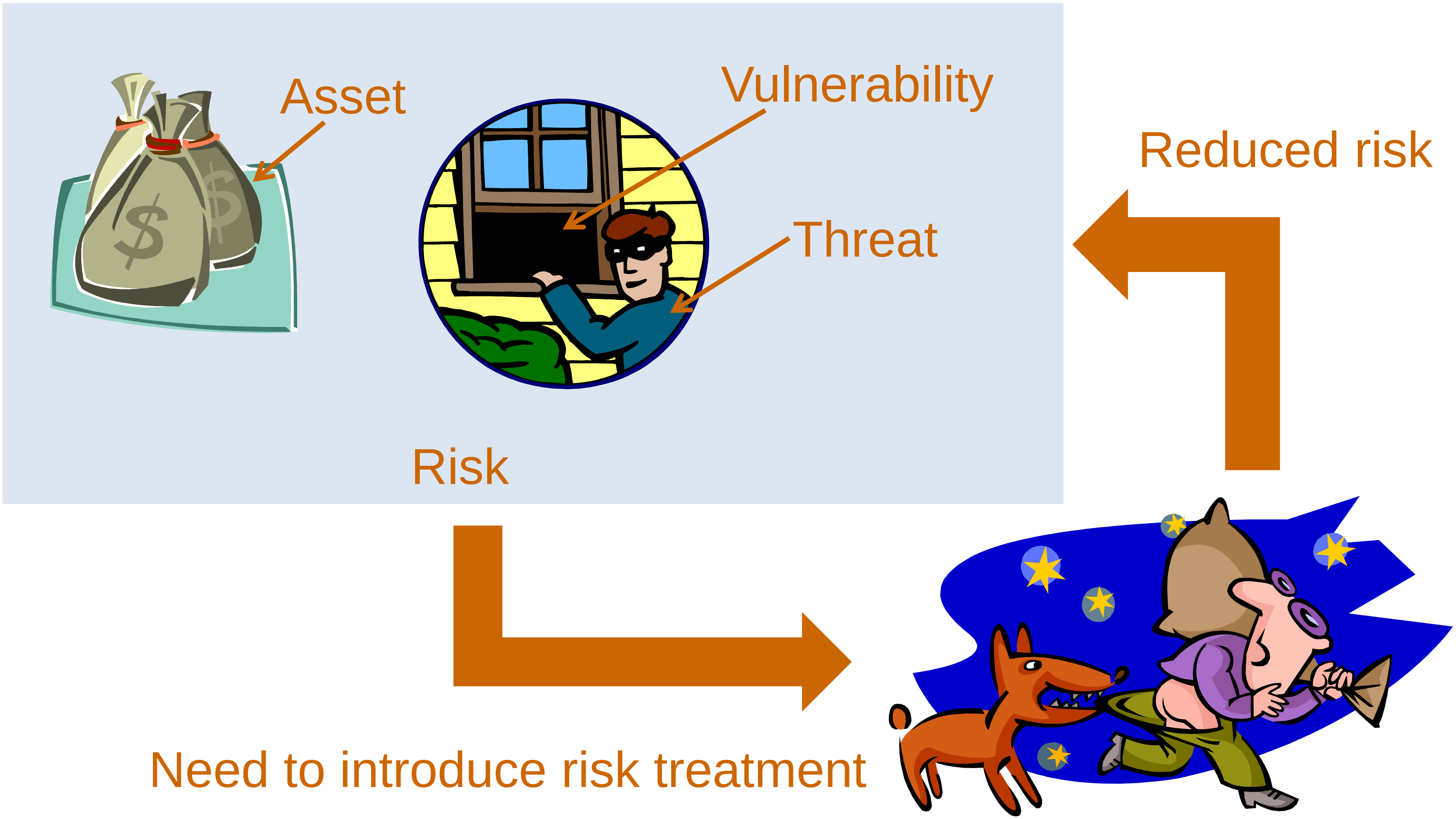


Risk Assessment Involves

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



Terms



Asset

Vulnerability

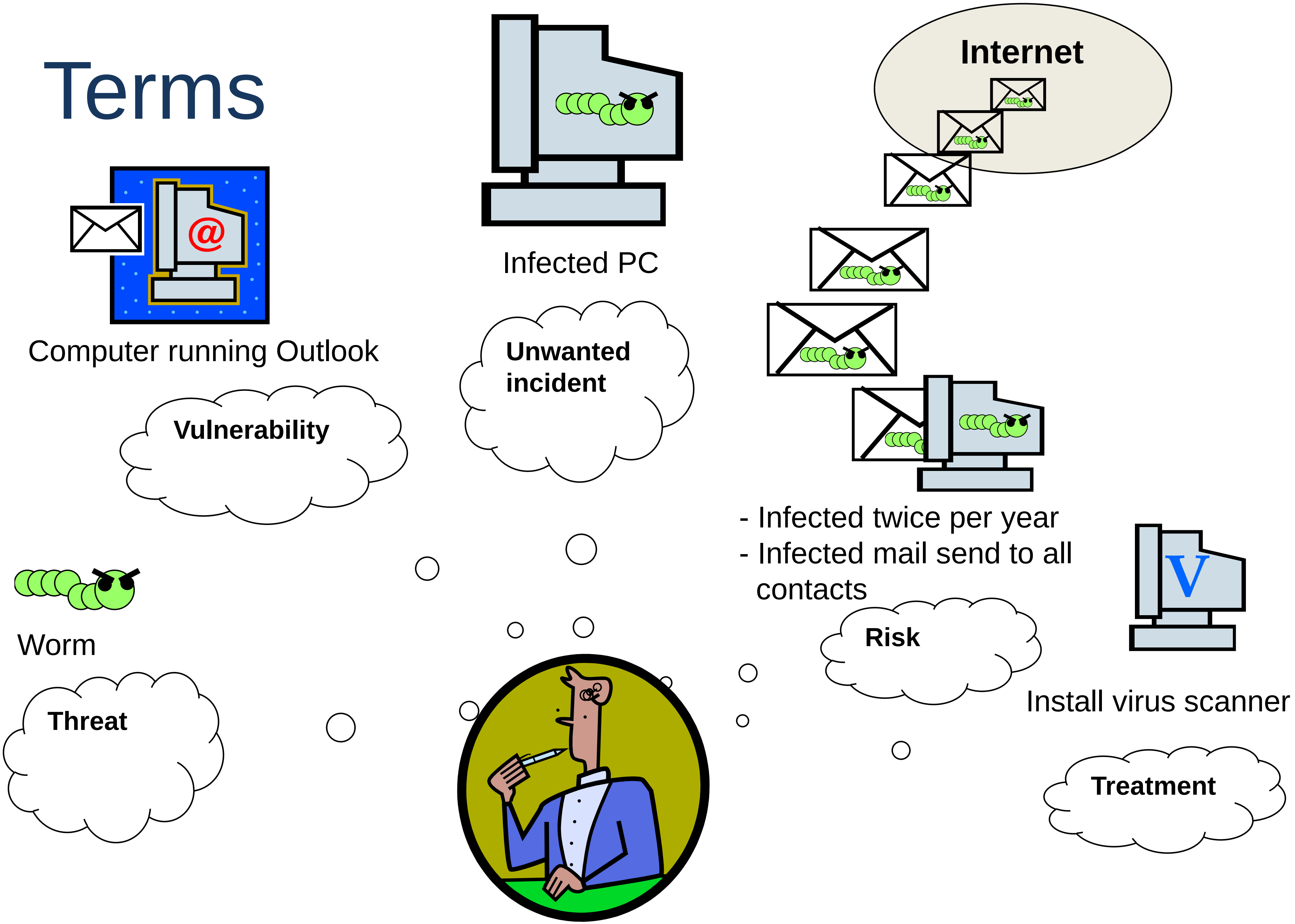
Threat

Risk

Reduced risk

Need to introduce risk treatment

Terms



Computer running Outlook

Vulnerability

Worm

Threat

Infected PC

Unwanted incident

Internet

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

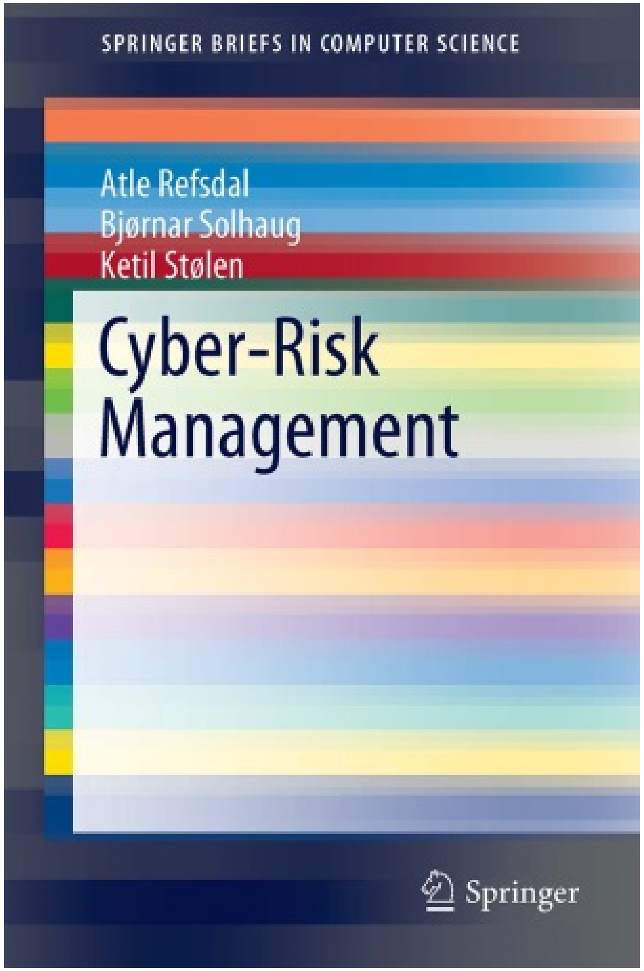
Risk

Install virus scanner

Treatment

Cyberspace, Cybersecurity and Cyber-risk

What is new with "cyber"?



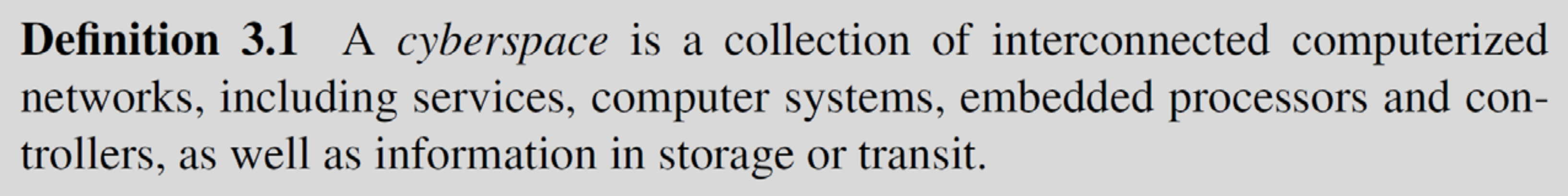
SPRINGER BRIEFS IN COMPUTER SCIENCE

Atle Refsdal
Bjørnar Solhaug
Ketil Stølen

Cyber-Risk Management

Springer

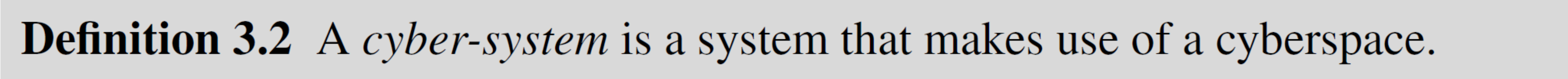
Cyberspace



Definition 3.1 A *cyberspace* is a collection of interconnected computerized networks, including services, computer systems, embedded processors and controllers, as well as information in storage or transit.

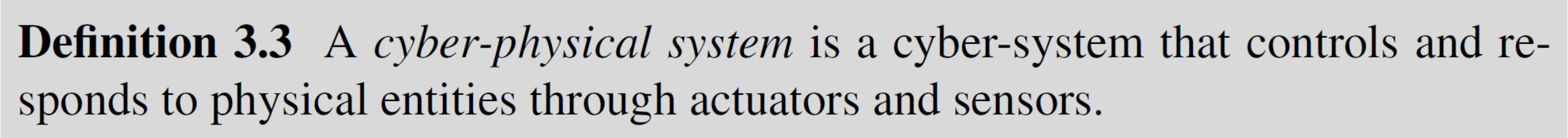
The term cyberspace first appeared in science fiction
(**novel by William Gibson**)

Cyber-system



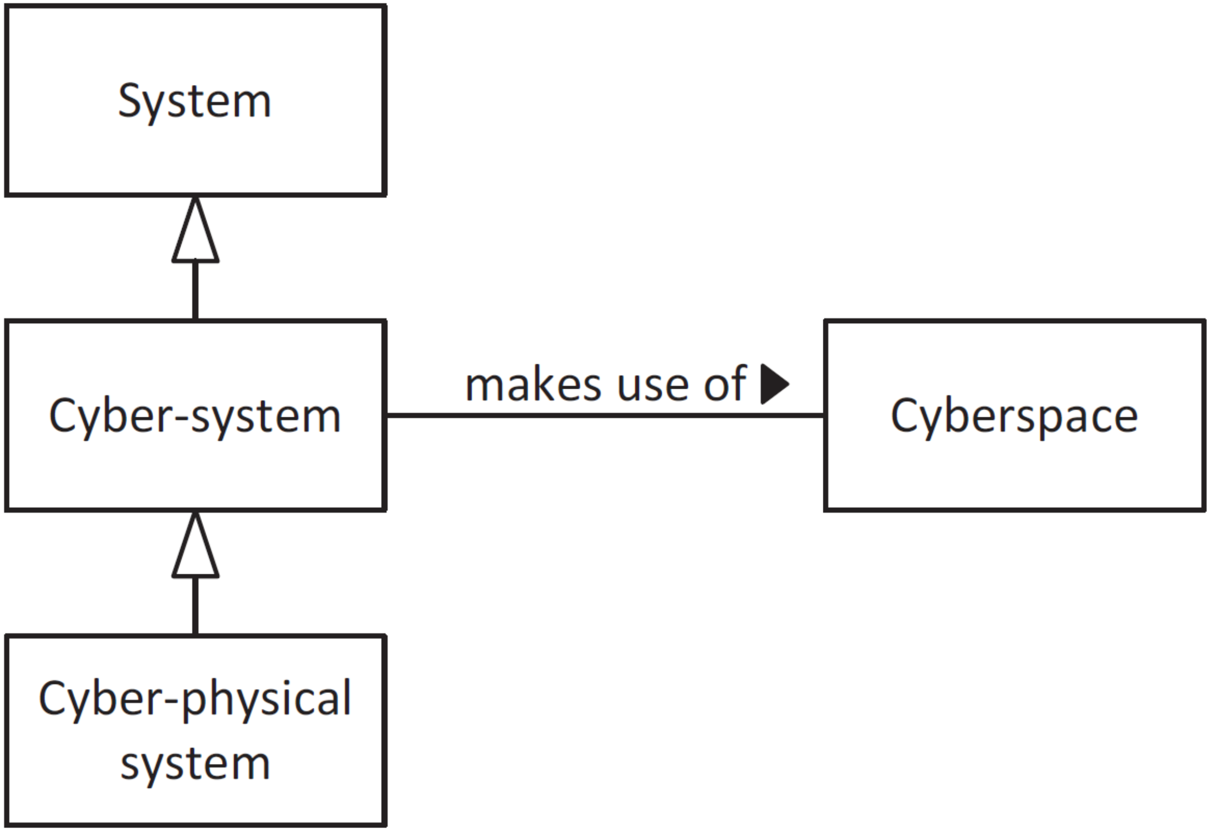
Definition 3.2 A *cyber-system* is a system that makes use of a cyberspace.

Cyber-physical system

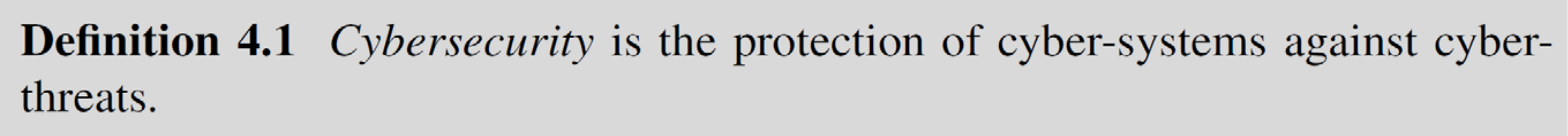


Definition 3.3 A *cyber-physical system* is a cyber-system that controls and responds to physical entities through actuators and sensors.

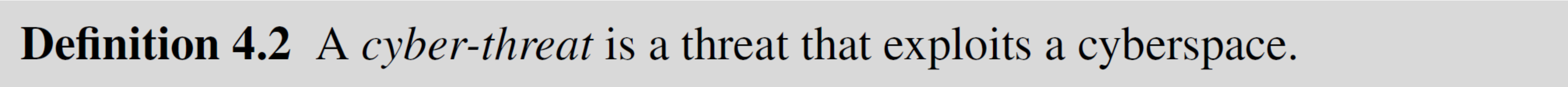
Summary


System
Cyber-system
makes use of ▶
Cyberspace
Cyber-physical system

Cybersecurity

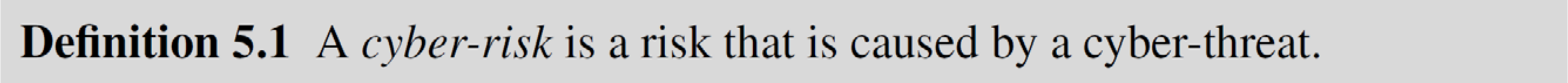


Definition 4.1 *Cybersecurity* is the protection of cyber-systems against cyber-threats.



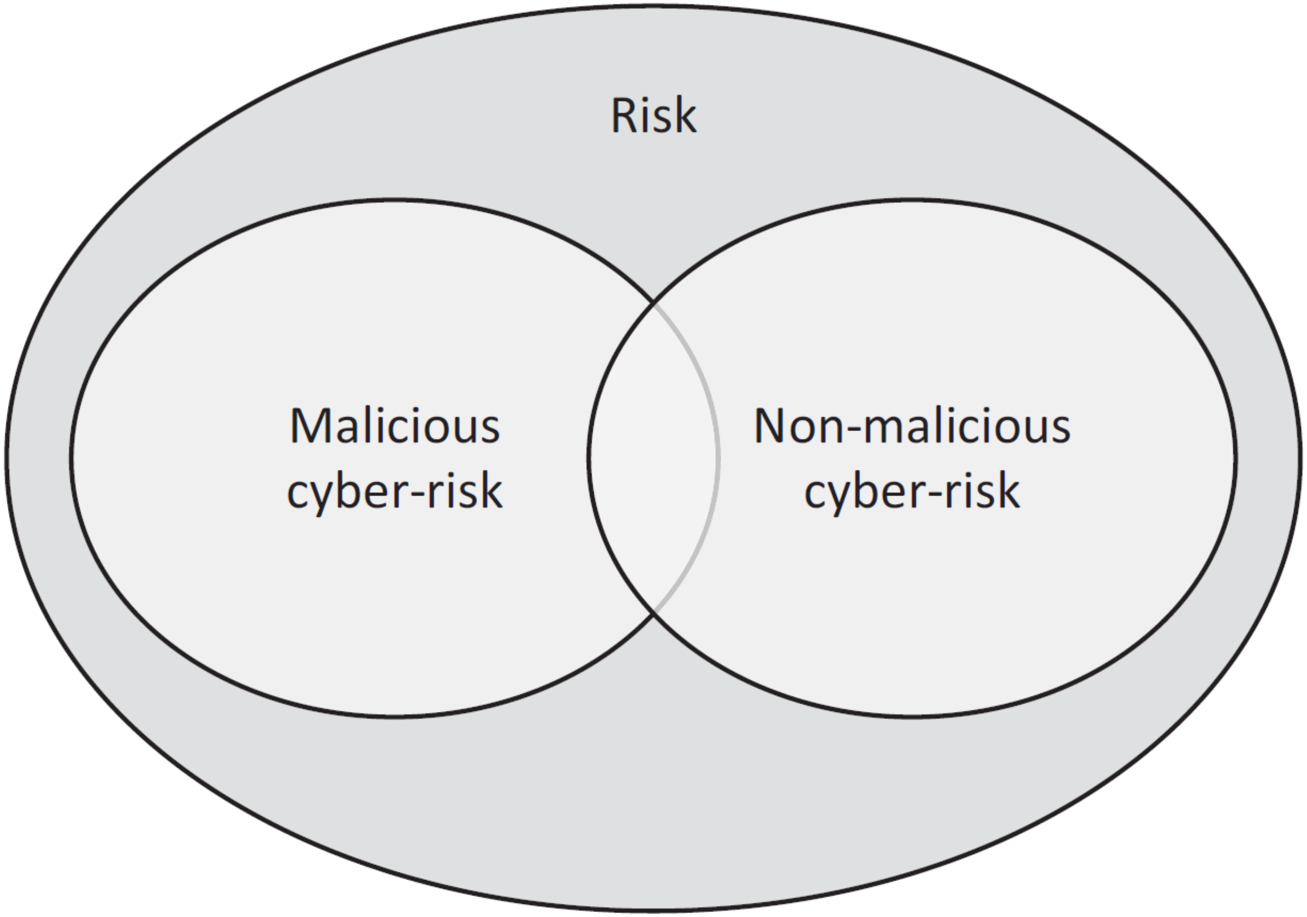
Definition 4.2 A *cyber-threat* is a threat that exploits a cyberspace.

Cyber-risk



Definition 5.1 A *cyber-risk* is a risk that is caused by a cyber-threat.

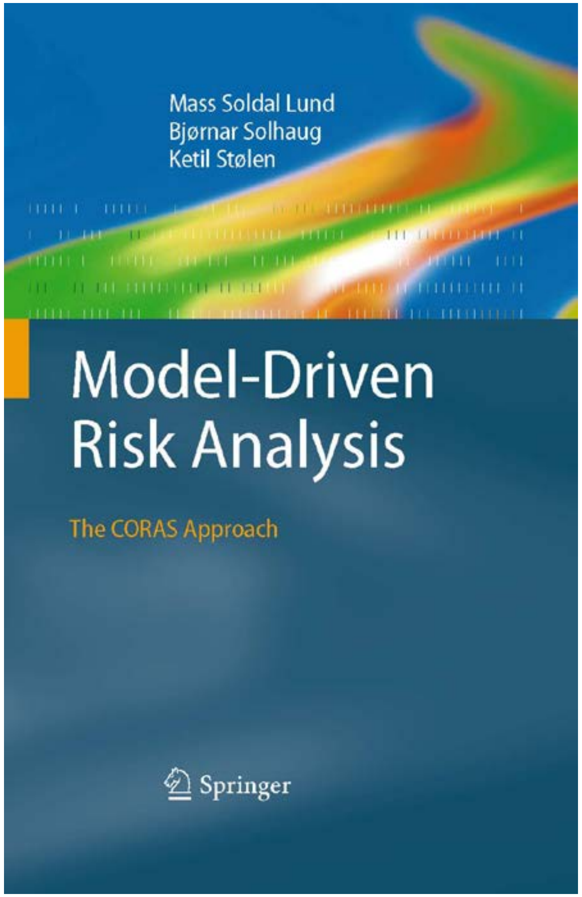
Summary



Security Risk Asessment Using CORAS

Overview

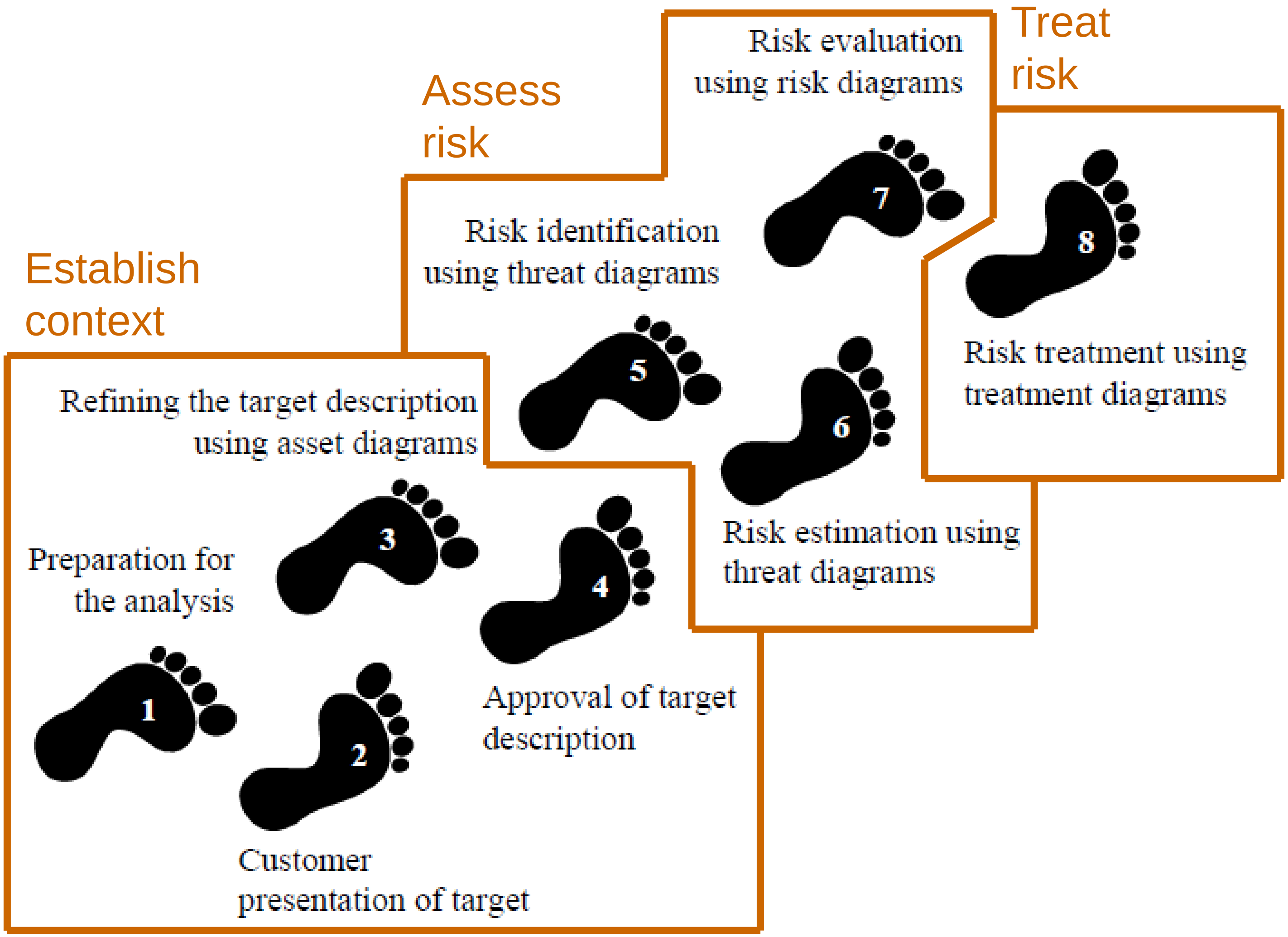
- What is CORAS?
- Main concepts
- Process of eight steps
- Risk modeling
- Semantics
- Calculus
- Tool support
- Further reading



The CORAS Method

- Asset-driven defensive risk analysis method
- Operationalization of ISO 31000 and ISO 27005 risk analysis process in 8 steps
- Detailed guidelines explaining how to conduct each step in practice
- Modeling guidelines for how to use the CORAS language

The 8 Steps of the CORAS Method



Establish context

Preparation for the analysis

Customer presentation of target

Refining the target description using asset diagrams

Approval of target description

Assess risk

Risk identification using threat diagrams

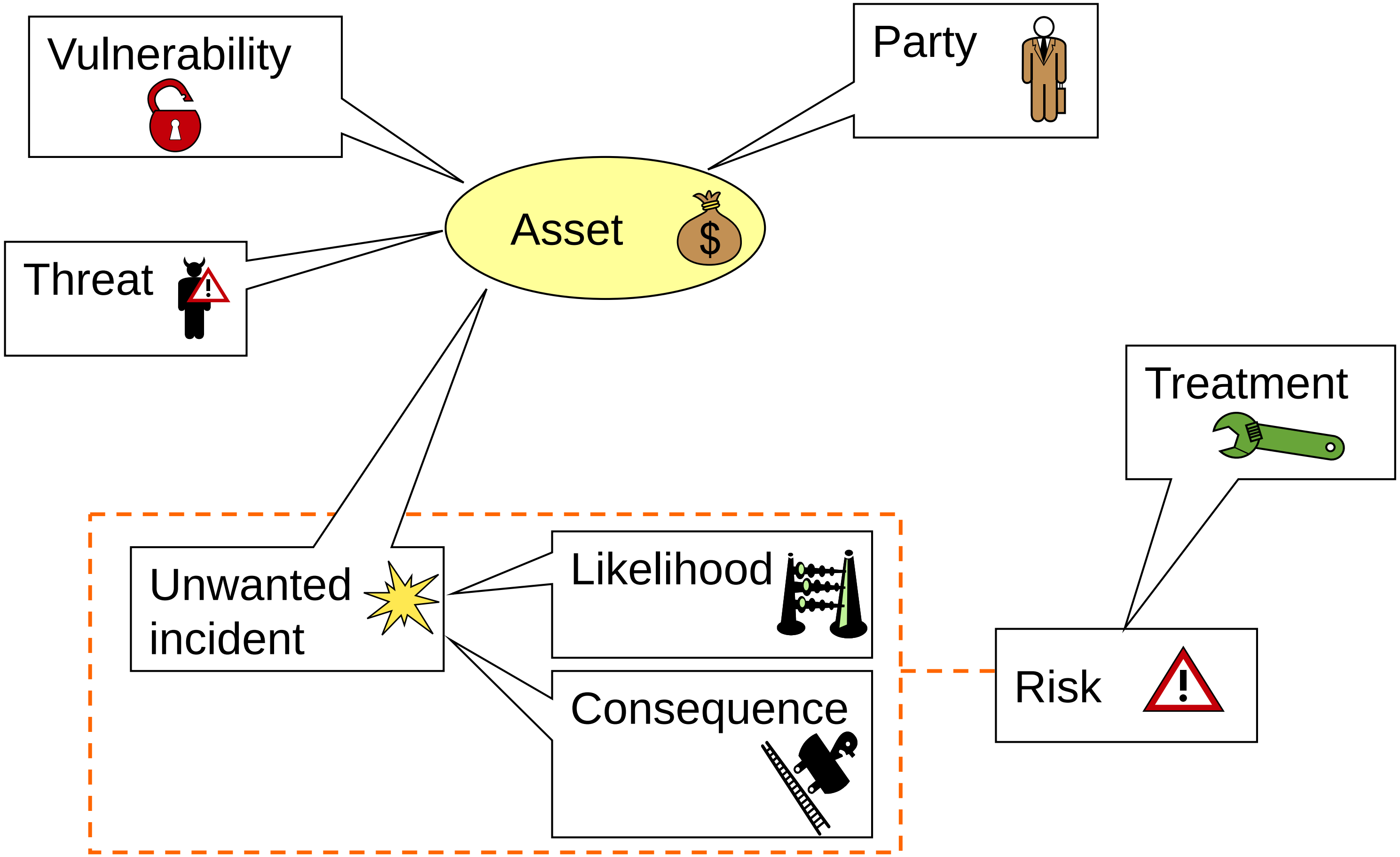
Risk estimation using threat diagrams

Risk evaluation using risk diagrams

Treat risk

Risk treatment using treatment diagrams

Main Concepts



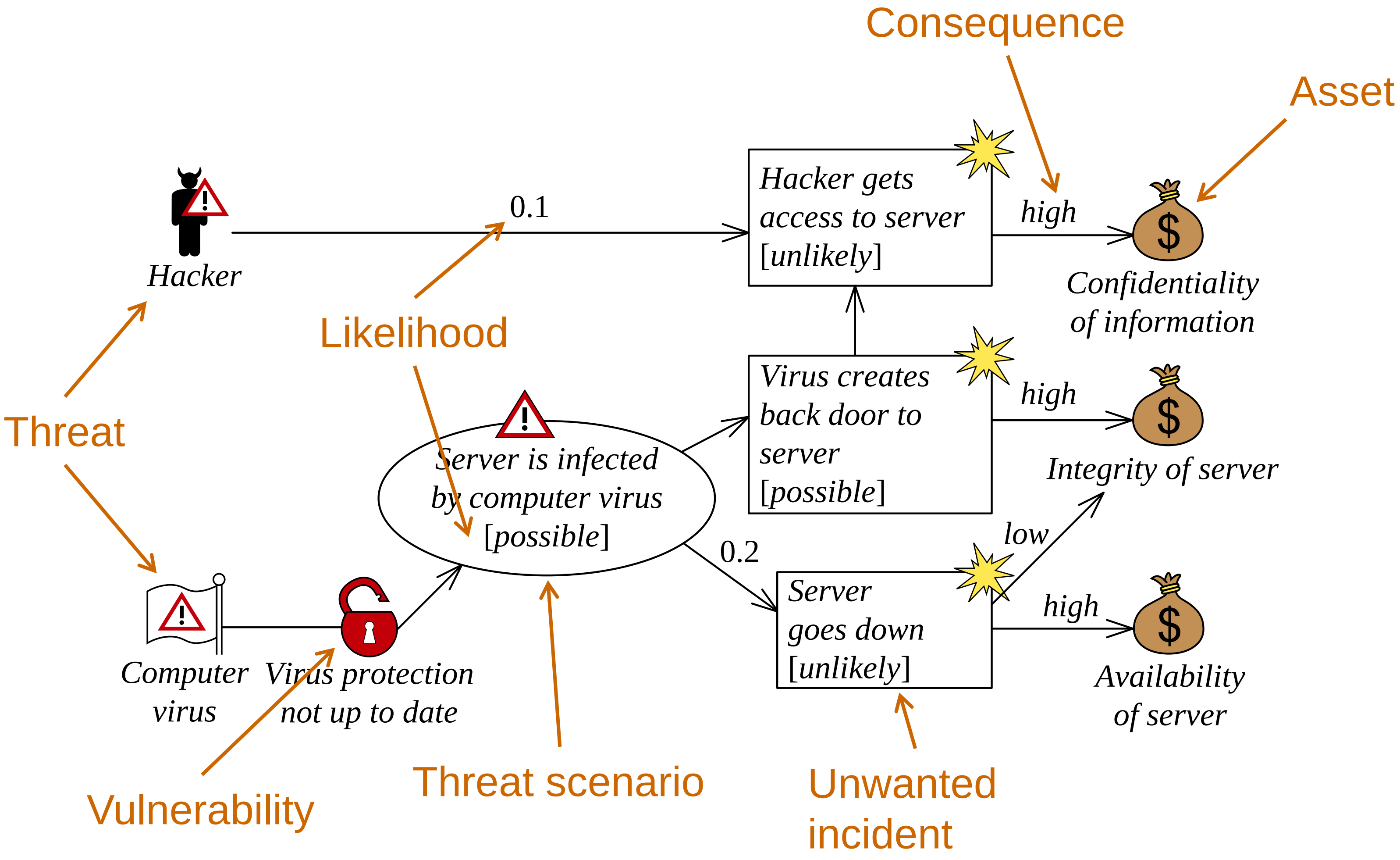
Definitions

- **Asset:** Something to which a party assigns value and hence for which the party requires protection
- **Consequence:** The impact of an unwanted incident on an asset in terms of harm or reduced asset value
- **Likelihood:** The frequency or probability of something to occur
- **Party:** An organization, company, person, group or other body on whose behalf a risk analysis is conducted
- **Risk:** The likelihood of an unwanted incident and its consequence for a specific asset
- **Risk level:** The level or value of a risk as derived from its likelihood and consequence
- **Threat:** A potential cause of an unwanted incident
- **Treatment:** An appropriate measure to reduce risk level
- **Unwanted incident:** An event that harms or reduces the value of an asset
- **Vulnerability:** A weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset

Risk Modeling

- The CORAS language consists of five kinds of diagrams
  - Asset diagrams
  - Threat diagrams
  - Risk diagrams
  - Treatment diagrams
  - Treatment overview diagrams
- Each kind supports concrete steps in the risk analysis process
- In addition there are three kinds of diagrams for specific needs
  - High-level CORAS diagrams
  - Dependent CORAS diagrams
  - Legal CORAS diagrams

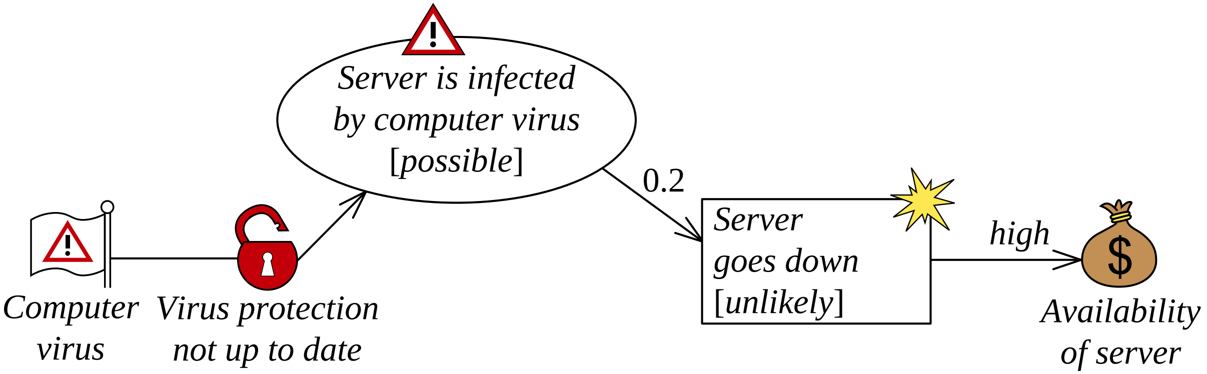
Example: Threat Diagram


Consequence
Asset
Hacker
0.1
Hacker gets access to server [unlikely]
high
Confidentiality of information
Likelihood
Threat
Virus creates back door to server [possible]
high
Integrity of server
Server is infected by computer virus [possible]
low
0.2
Server goes down [unlikely]
high
Availability of server
Computer virus
Virus protection not up to date
Vulnerability
Threat scenario
Unwanted incident

Semantics

- How to interpret and understand a CORAS diagram?
- Users need a precise and unambiguous explanation of the meaning of a given diagram
- Natural language semantics
  - CORAS comes with rules for systematic translation of any diagram into sentences in English
- Formal semantics

Example


Server is infected by computer virus [possible]
0.2
Server goes down [unlikely]
high
Computer virus
Virus protection not up to date
Availability of server

- Elements
  - *Computer virus* **is a non-human threat**.
  - *Virus protection not up to date* **is a vulnerability**.
  - **Threat scenario** *Server is infected by computer virus* **occurs with likelihood** *possible*.
  - **Unwanted incident** *Server goes down* **occurs with likelihood** *unlikely*.
  - *Availability of server* **is an asset**.
- Relations
  - *Computer virus* **exploits vulnerability** *Virus protection not up to date* **to initiate** *Server is infected by computer virus* **with undefined likelihood**.
  - *Server is infected by computer virus* **leads to** *Server goes down* **with conditional likelihood** 0.2.
  - *Server goes down* **impacts** *Availability of server* **with consequence** *high*.

Criticism from System Developers

- The CORAS language is too simplistic
- It is too cumbersome to use graphical icons

Criticism from Risk Analysts

- What’s new with the CORAS language?
- We have been using something similar for years, namely VISIO!

Exercise

- Discuss the statements made by the critics?
- Are they wrong?

Mandatory Reading

- Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen: *Chapter 3 "A Guided Tour of the CORAS Method" in the book "Model-Driven Risk Analysis: The CORAS Approach"*, 2011. Springer. The chapter can be downloaded freely.

- Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen: *Risk Analysis of Changing and Evolving Systems Using CORAS*, 2011. LNCS 6858, Springer. Pages 231-274.