

IN2120 Information Security
University of Oslo
Autumn 2018

Lecture 8

Risk Management

Business Continuity Management



UiO, 2018

Audun Jøsang

What is risk?

- ISO31000 Risk Management:
 - **“Risk is the effect of uncertainty on objectives”**
 - No distinction between positive and negative effects of uncertainty
 - This definition is too abstract for most people
 - Also says: **“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*.”**
- Harris, CISSP 7th ed.:
 - **“Risk is the likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact.”** (Glossary p.1285)
- ISO 27005 (Information Security Risk)
 - **“Risk is the potential that a given threat will exploit vulnerabilities of assets and thereby cause harm to the organization.”**

Threats

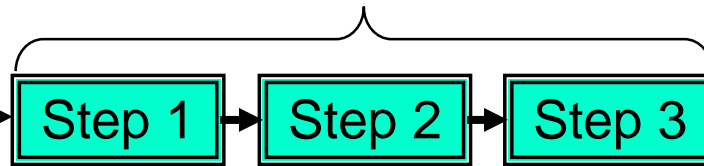
- **Threat Scenario:** A set of discrete steps or procedures, controlled or triggered by one or multiple threat actors, which can negatively affect the victim's information assets. A threat scenario can materialize to become a real incident.
- **Threat Actor:** An active entity which can control or trigger threat scenarios. Threat actors can be intelligent entities with malicious intent, or forces of nature which can be too strong or unpredictable to be effectively prevented.
- When simply using the term “threat”, it must be assumed to mean a “threat scenario”.

Threat actor



controls

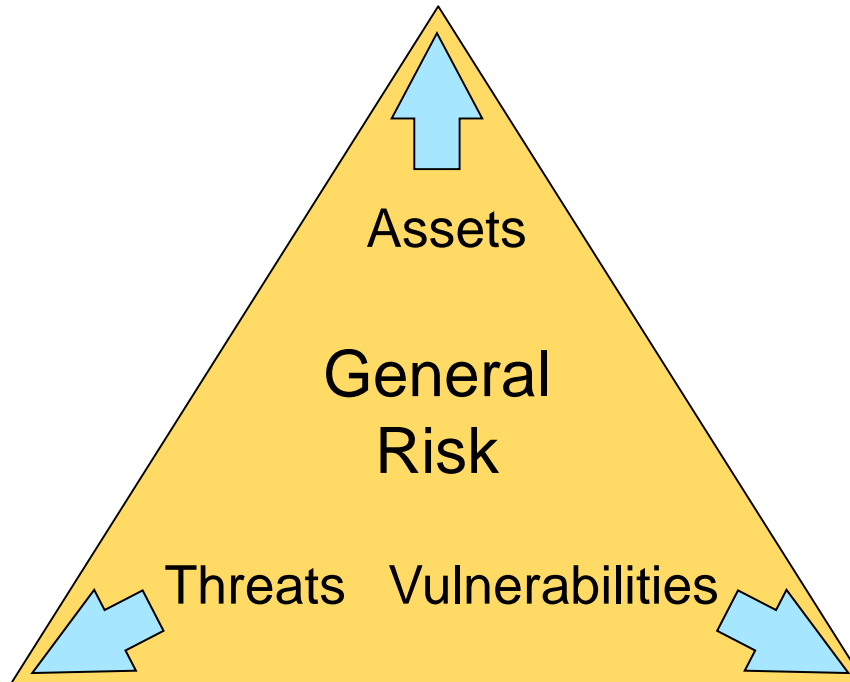
Threat scenario



causes

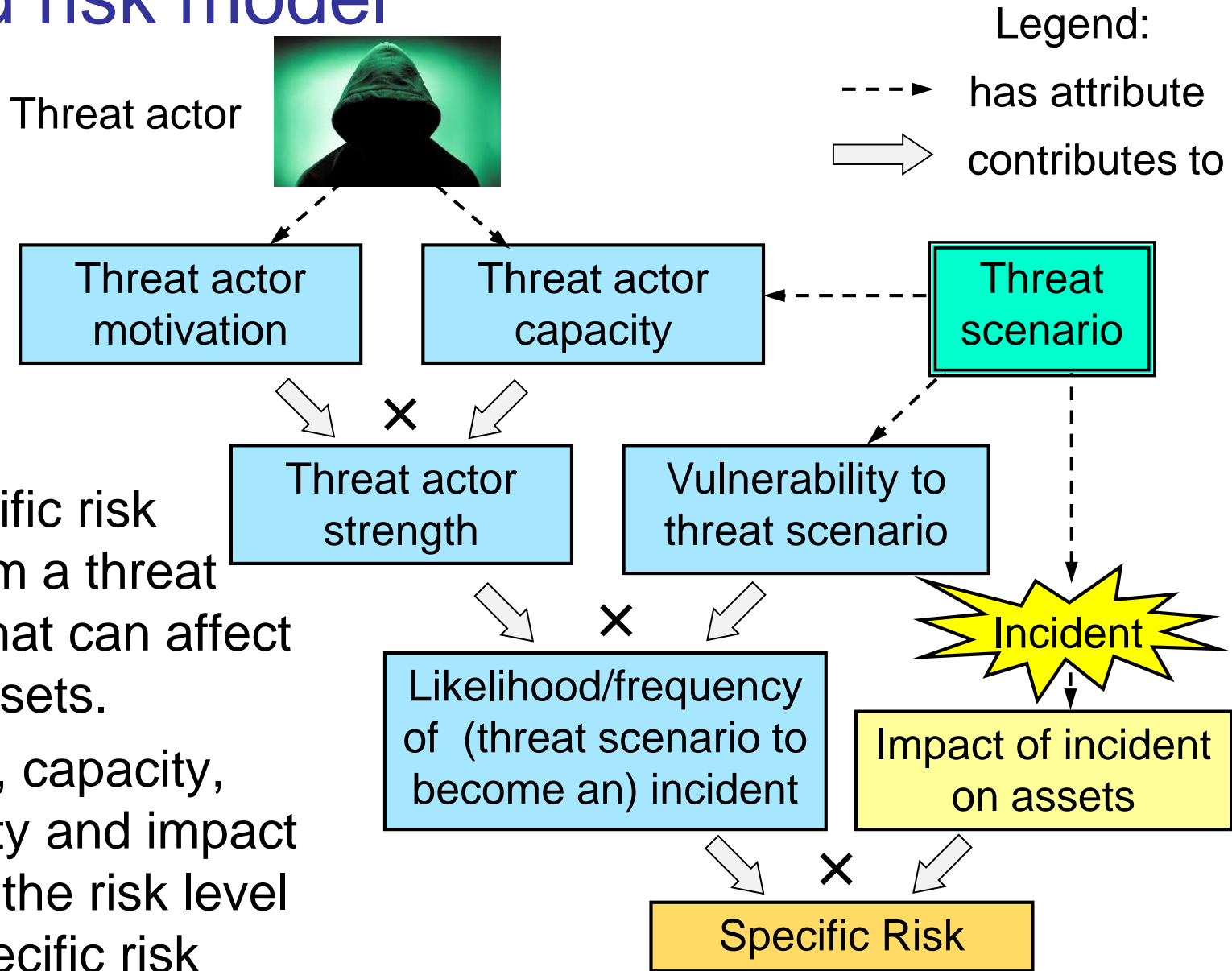


Abstract Risk Model (NSM)



- Models general risk in an abstract way
 - The more assets you have, the more threats you are faced with, and the more vulnerable you are, then the greater the risk.

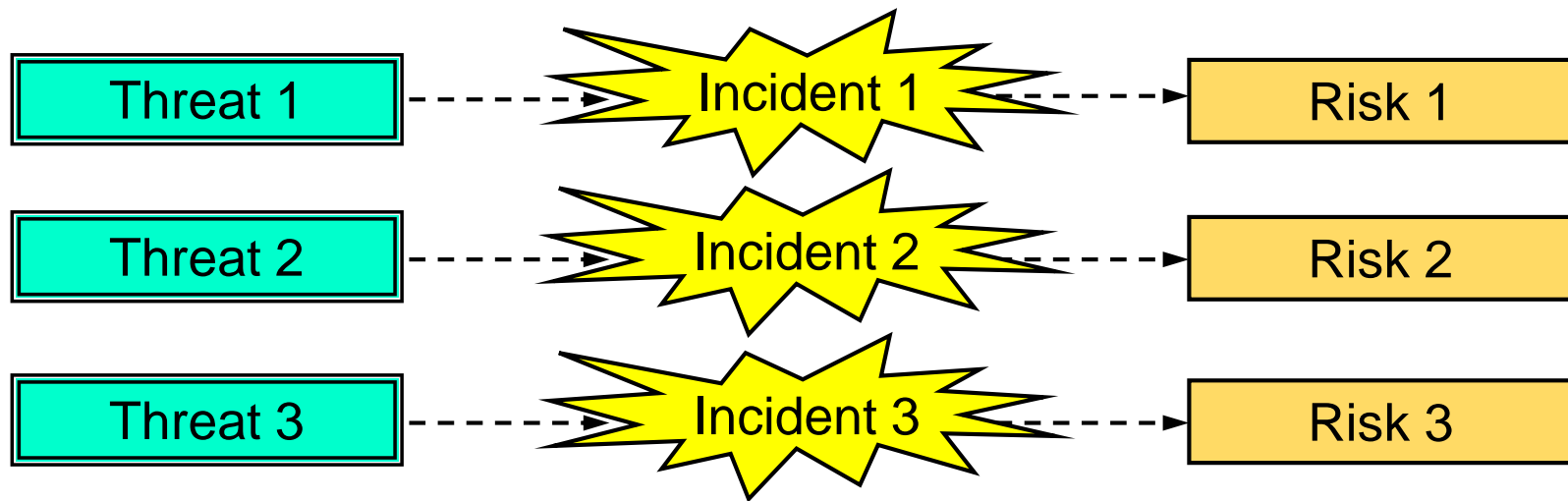
Detailed risk model



- Each specific risk results from a threat scenario that can affect specific assets.
- Motivation, capacity, vulnerability and impact determine the risk level for that specific risk

Many Risks

- Multiple different threats (scenarios) can be identified
- Each threat can potentially cause a (different) incident
- Each potential incident has a risk level
- Multiple threats \Rightarrow Many risks



Identifying specific risks

Threats / incidents

- Password compromise
- SQL injection
- Logical bomb in SW
- Trojan infects clients
- Cryptanalysis of cipher
- Brute force attack
- Social engineering
-

Vulnerabilities

- Weak passwords
- Poor awareness
- No input validation
- Outdated antivirus
- Weak ciphers
- Short crypto keys
- Poor usability
- ...

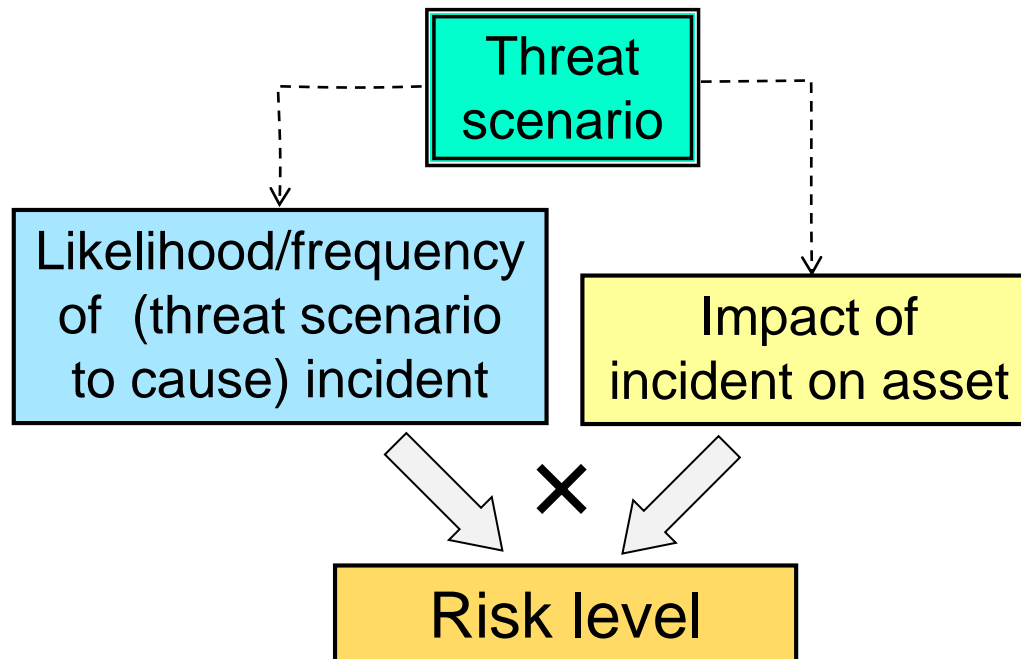
Asset impacts

- Deleted files
- Stolen files
- Corrupted files
- Intercepted traffic
- False transaction
- Process disruption
- Damaged reputation

- The relevant combination of a threat scenario, a corresponding incident and impact represents a single specific risk
- All relevant specific risks should be identified

Practical risk model

- Practical risk analysis typically considers two factors to determine the level of each risk
 1. Likelihood / frequency of each type of incident
 2. Impact on assets (loss) resulting from each type of incident



Risk Management standards

- ISO 27005 Information Security Risk Management
- ISO 31000 Risk Management
- NIST SP800-39 Managing Information Security Risk
- NIST SP800-30 Guide for Conducting Risk Assessment
 - formerly called “Risk Management Guide for Information Technology Systems”
- NS 5831 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikohåndtering
- NS 5832 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikoanalyse

What is risk management?

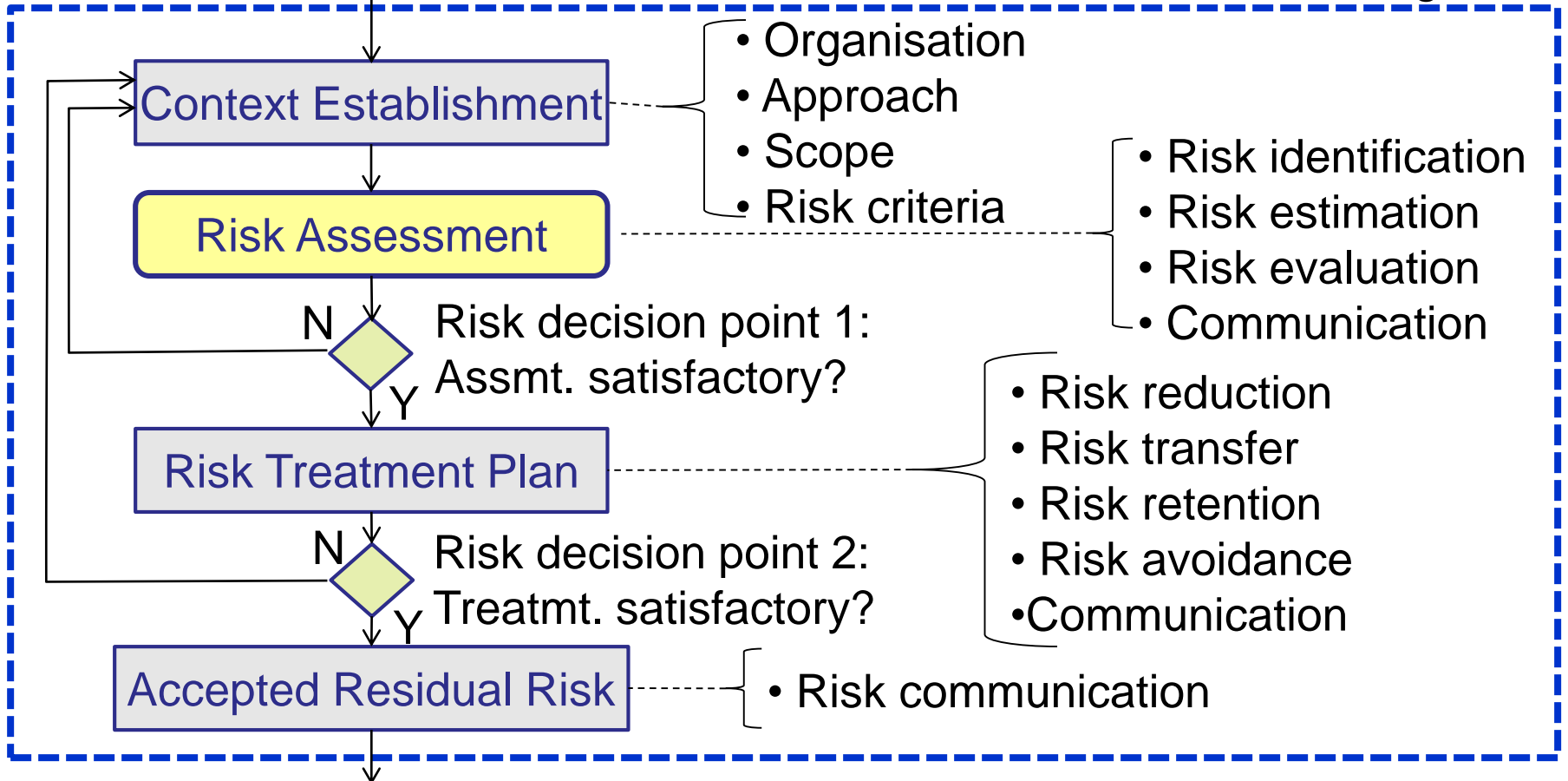
- “IS risk management analyses what can happen and what the possible consequences can be, before deciding what should be done and when, to reduce risk to an acceptable level.”
 - ISO 27005
- “Risk management consists of coordinated activities to direct and control an organization with regard to risk.”
 - ISO31000

Risk management process

ISO 27005

Information security strategy

IS Risk Management



Implement risk treatment plan (security controls)

Risk assessment process

ISO 27005

Context establishment

Risk Assessment

Risk identification

- Identification of assets
- Identification of threats
- Identification of existing controls
- Identification of vulnerabilities
- Identification of consequences

Risk analysis

Risk estimation

- Assess asset values and impacts
- Assess incident likelihood/frequency
- Determine/compute risk levels

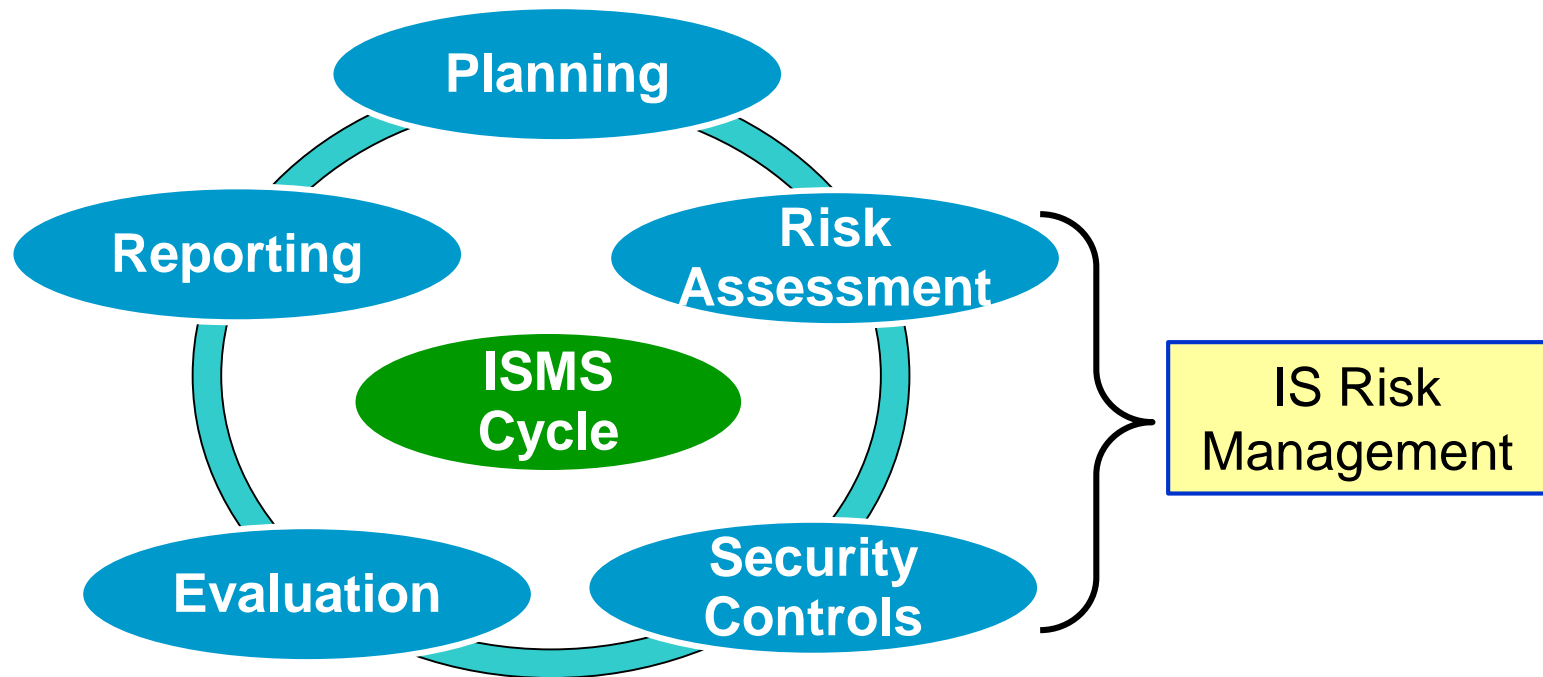
Risk evaluation

- Rank risks
- Compare risks with criteria

Decide whether risk assessment is satisfactory

Risk Management – ISMS integration

- Risk management is an essential element of ISMS
 - Required to identify threats (what can go wrong)
 - Basis for selecting security controls
 - Tool for top management to understand organization’s risk exposure



Basis for assessing risk

- Know the assets: identify and understand the value of information assets and systems.
- Know the threats: identify and understand relevant threat scenarios which can harm information assets and systems.
- Know the losses your organisation want to tolerate.
- Know which stakeholders in the organisation which are responsible for managing the risks that are identified.

Roles involved in risk management

- Management, users, and information technology must all work together
 - Asset owners must participate in developing asset inventory
 - Users and experts must assist in identifying threats and vulnerabilities, and in determining likelihoods of incidents
 - Risk management experts must guide stakeholders through the risk assessment process
 - Security experts must assist in selecting security controls
 - Management must review the risk management process and approve risk management strategy (security controls)

Problems of measuring risk

Businesses normally wish to measure risk in money, but almost impossible to do this

- Valuation of assets
 - Value of data, hard to assess
 - Value of goodwill and customer confidence, very vague
- Likelihood of incidents
 - Past events not always relevant for future probabilities
 - The nature of future attacks is unpredictable
 - The actions of future attackers are unpredictable
- Measurement of benefit from security control
 - Problems with the difference of two approximate quantities
 - Estimation of past and present risk

Asset Valuation and Prioritization

- Questions help develop criteria for asset valuation
- Which information asset:
 - is most critical to organization's success?
 - generates the most revenue/profitability?
 - would be most expensive to replace or protect?
 - would be the embarrassing or cause liability if revealed?
- Prioritization
 - Create weighting for each category
 - Calculate relative importance of each asset
 - List the assets in order of importance using a weighted factor analysis worksheet

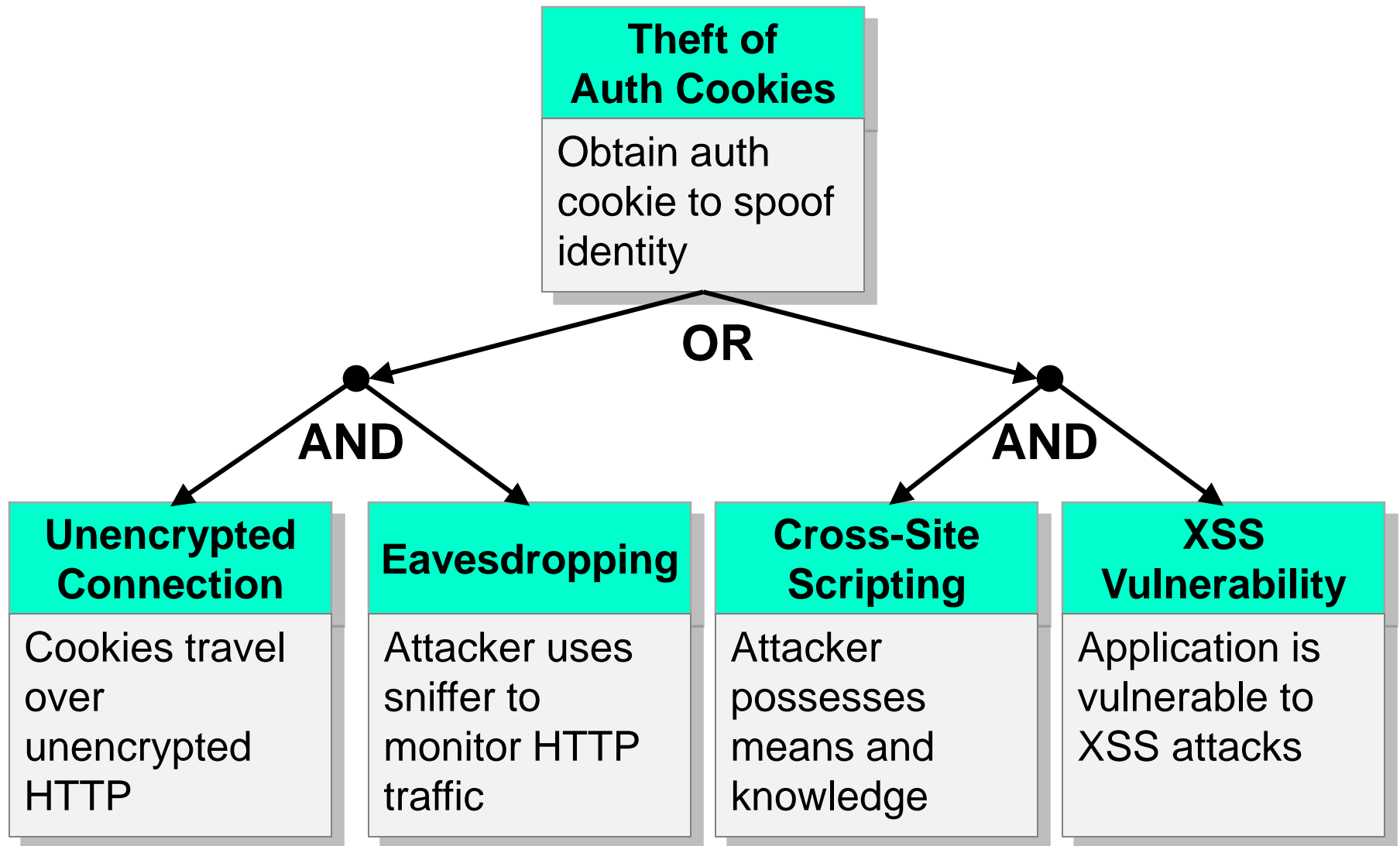
Threat Modelling

- Threat modelling is the process of identifying, analysing and describing relevant threat scenarios.
- Unimportant/irrelevant threat scenarios can be ignored.
- Examine how each relevant threat scenario can be executed against the organization's assets.
- The threat modelling process works best when people with diverse backgrounds within the organization work together in a series of brainstorming sessions.
- Threat modelling is important during system development
 - Used to identify, remove and avoid vulnerabilities when developing software and systems.
- Multiple approaches/methods for threat modelling

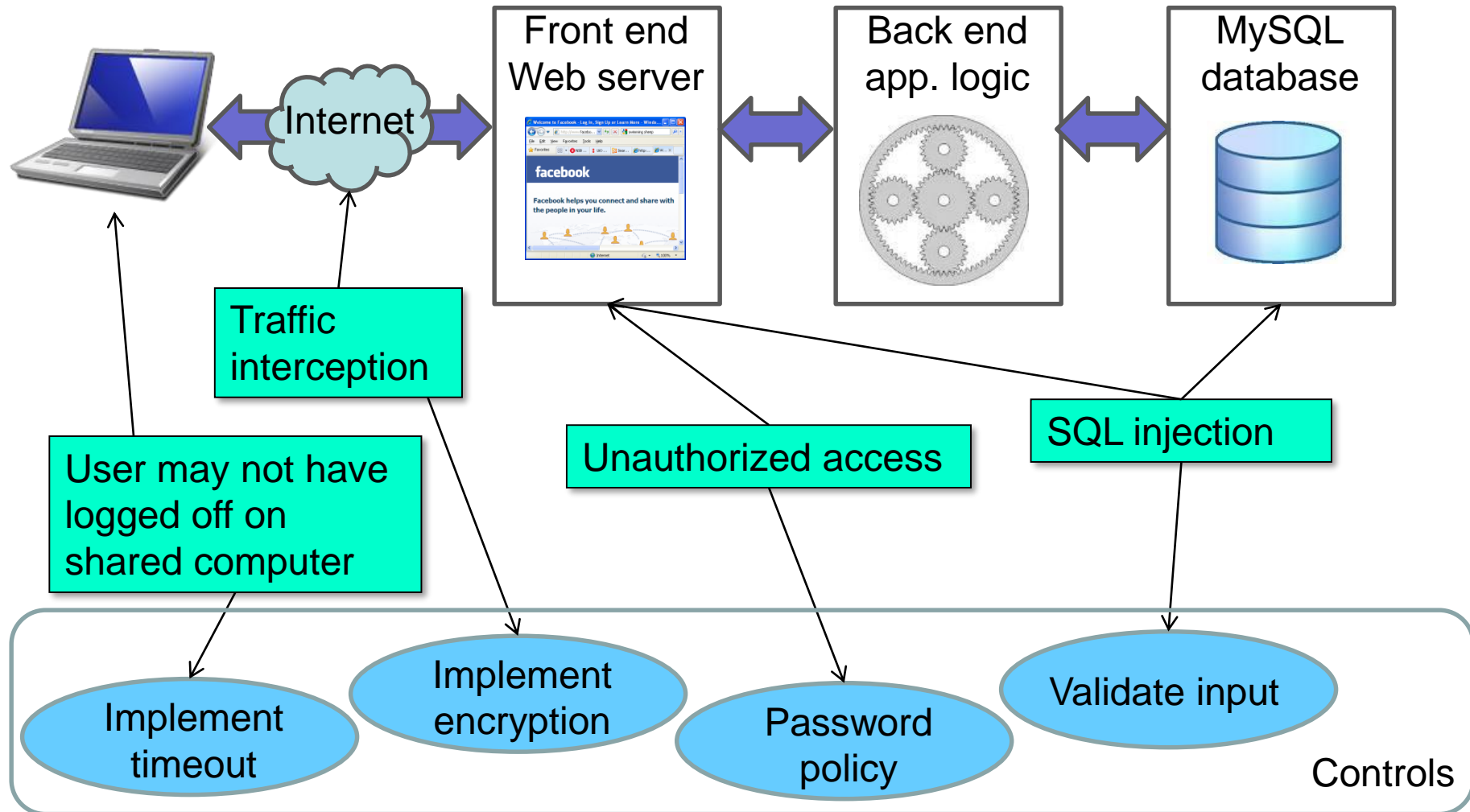
Threat Modelling Methods

- **Attacker-centric**
 - Starts from attackers, evaluates their goals, and how they might achieve them through attack tree. Usually starts from entry points or attacker action.
- **System-centric (aka. SW-, design-, architecture-centric)**
 - Starts from model of system, and attempts to follow model dynamics and logic, looking for types of attacks against each element of the model. This approach is e.g. used for threat modeling in Microsoft's Security Development Lifecycle.
- **Asset-centric**
 - Starts from assets entrusted to a system, such as a collection of sensitive personal information, and attempts to identify how security breaches of CIA properties can happen.

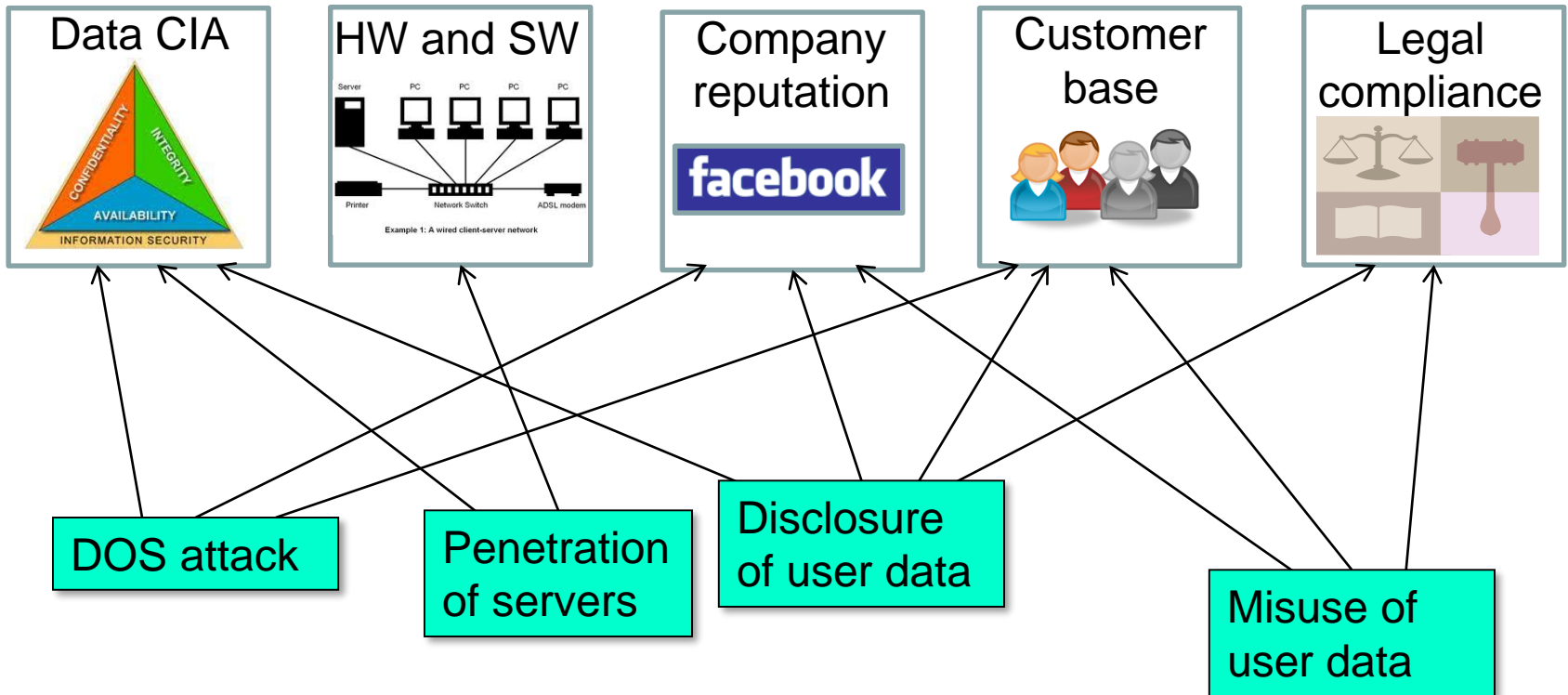
Attacker Centric: Threat Tree Example



System-centric threat modelling example



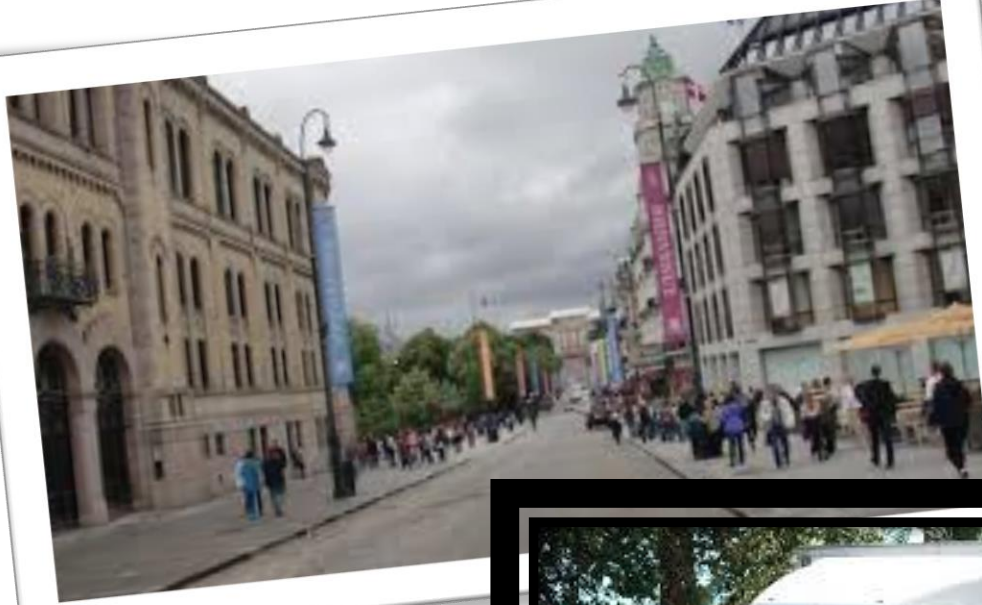
Asset-centric threat modelling example



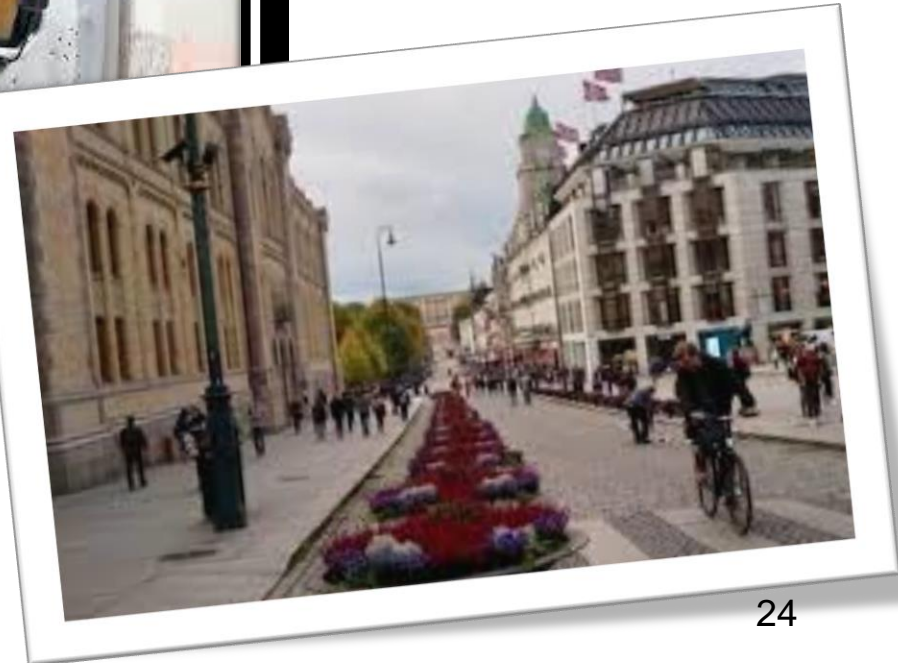
Vulnerability Identification

- Vulnerabilities are specific opportunities that threat actors can exploit to attack systems and information assets.
- Generic vulnerability identification
 - To identify a vulnerability is the same as to determine how to block a specific threat scenario.
 - Removing a vulnerability is the same as blocking a threat.
 - A vulnerability is **the absence of blocks** against a threat.
 - Blocking a threat (i.e. removing a vulnerability) is typically done with a security control.
- Tool-based and checklist-based vulnerability identification
 - **Vulnerability scanners** are automated tools to detect known vulnerabilities in networks and systems, e.g. Wireshark
 - **Check lists of vulnerabilities** are used by teams when doing risk assessment and removing vulnerabilities, e.g. OWASP Top 10.

No vulnerability
without a threat



New threat
appears in 2016



Vulnerability removed and
threat blocked

Feilbetegnelsen “ROS-analyse”

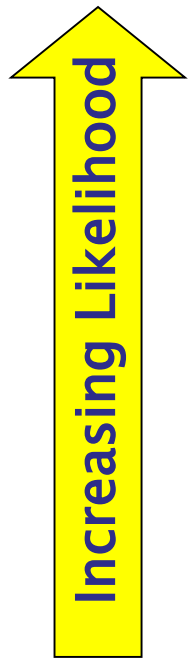
- ROS-analyse = Risiko- og sårbarhetsanalyse
- ROS-analyse fokuserer på å identifisere sårbarheter, som typisk gjør at man mister fokus på trusler.
- Begrepet ROS-analyse brukes ofte på norsk, og er faktisk et særnorsk begrep.
- Det snakkes det aldri om “risk and vulnerability analysis” som eget begrep i engelsk faglitteratur.
- Engelsk faglitteratur bruker “threat and risk analysis”, som på norsk kan oversettes til **TOR-analyse**.
- TOR-analyse er en bedre betegnelse enn ROS-analyse.

Estimating risk levels

Types of analysis

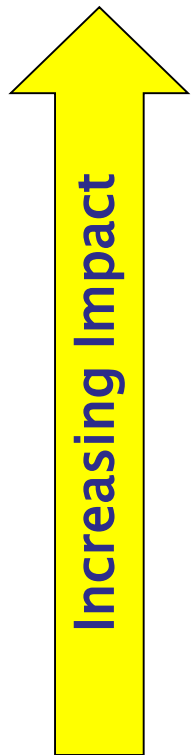
- **Qualitative**
 - Uses descriptive scales. **Example:**
 - **Impact level:** Minor, moderate, major, catastrophic
 - **Likelihood:** Rare, unlikely, possible, likely, almost certain
- **Relative / Semi-quantitative**
 - Relative numerical values assigned to qualitative scales
 - Gives relatively good distribution of risk levels
- **Quantitative**
 - Use numerical values for both consequence (e.g. \$\$\$) and likelihood (e.g. probability value)

Qualitative likelihood scale



Likelihood	Description
High	Is expected to occur in most conditions (1 or more times per year).
Medium	The event will probably happen in most conditions (every 2 years).
Low	The event should happen at some time (every 5 years).
Unlikely	The event could happen at some time (every 10 years).

Qualitative impact level scale



Impact	Description
Major	Major problems would occur and threaten the provision of important processes resulting in significant financial loss.
Moderate	Services would continue , but would need to be reviewed or changed.
Minor	Effectiveness of services would be threatened but dealt with.
Insignificant	Dealt with as a part of routine operations.

Qualitative risk estimation - example

- Define risk matrix with risk levels according to requirements
 - Number of qualitative levels of likelihood, impact and risk
- Use the risk matrix as a look-up table for each threat scenario

Qualitative impact levels

Qualitative likelihood	Risk levels	Insignificant	Minor	Moderate	Major
	High	M	H	VH	E
	Medium	L	M	H	VH
	Low	VL	L	M	H
	Unlikely	N	VL	L	M

Legend

E: extreme risk; Risk must be handled with priority

(V)H: (very) high risk; Risk must be handled

M: moderate risk; Risk to be handled according to budget

(V)L: (very) low risk; Risk with low priority, handle if there is opportunity


N: Negligible risk; To be ignored

Relative / Semi-quantitative risk estimation

Example

Relative / Semi-quantitative risk levels: Product of likelihood & impact level

Relative Impact levels

Relative risk levels 	(0) Nil	(1) Insign.	(3) Minor	(5) Moderate	(9) Major
(10) High	0	10	30	50	90
(4) Medium	0	4	12	20	36
(2) Low	0	2	6	10	18
(1) Unlikely	0	1	3	5	9
(0) Never	0	0	0	0	0

Relative / semi-quantitative risk estimation can give a better distribution of risk levels than with purely qualitative models.

Quantitative risk estimation example

Example quantitative risk analysis method

- Quantitative parameters
 - Asset Value (AV)
 - Estimated total value of asset
 - Exposure Factor (EF)
 - Percentage of asset loss caused by threat occurrence
 - Single Loss Expectancy (SLE)
 - $SLE = AV \times EF$
 - Annualized Rate of Occurrence (ARO)
 - Estimated frequency a threat will occur within a year
 - Annualised Loss Expectancy (ALE)
 - $ALE = SLE \times ARO$

Quantitative risk estimation example

Example quantitative risk analysis

- Risk description
 - Asset: Public image (and trust)
 - Threat: Defacing web site through intrusion
 - Impact: Loss of image
- Parameter estimates
 - $AV(\text{public image}) = \$1,000,000$
 - $EF(\text{public image affected by defacing}) = 0.05$
 - $SLE = AV \times EF = \$50,000$
 - $ARO(\text{defacing}) = 2$
 - $ALE = SLE \times ARO = \$100,000$
- Justifies spending up to \$100,000 p.a. on controls

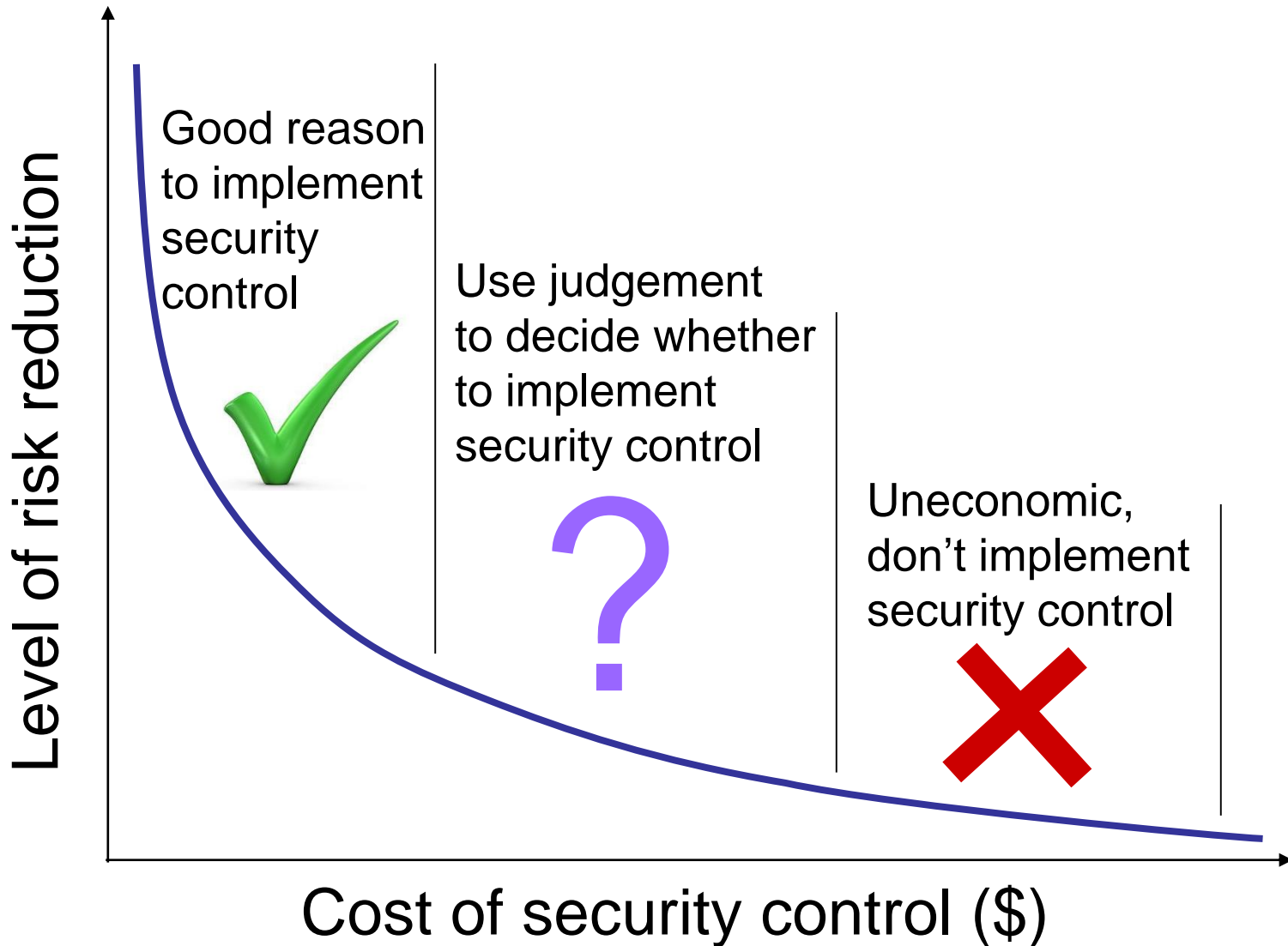
Risk listing and ranking

Threat scenario:	Existing controls & vulnerabilities:	Asset impact:	Impact level:	Likelihood description:	Likelihood:	Risk level:
Compromise of user password	No control or enforcement of password strength	Deleted files, breach of confidentiality and integrity	MODE RATE	Will happen to 1 of 50 users every year	MEDIUM	HIGH
Virus infection on clients	Virus filter disabled on many clients	Compromise of clients	MODE RATE	Will happen to 1 in 100 clients every year	HIGH	EXTREME
Web server hacking and defacing	IDS, firewall, daily patching, but zero day exploits exist	Reputation	MINOR	Could happen once every year	MEDIUM	MODE RATE
Logical bomb planted by insider	No review of source code that goes into production.	Breach of integrity or loss of data	MAJOR	Could happen once every 10 years	UNLIKELY	MODE RATE

Risk Control Strategies

- After completing the risk assessment, the security team must choose one of four strategies to control each risk:
 1. Reduce risk by implementing security controls
 2. Share/transfer risk (outsource activity that causes risk, or buy insurance)
 3. Retain risk (understand and tolerate potential consequences)
 4. Avoid risk (stop activity that causes risk)

Economy of security controls



Business Continuity Management

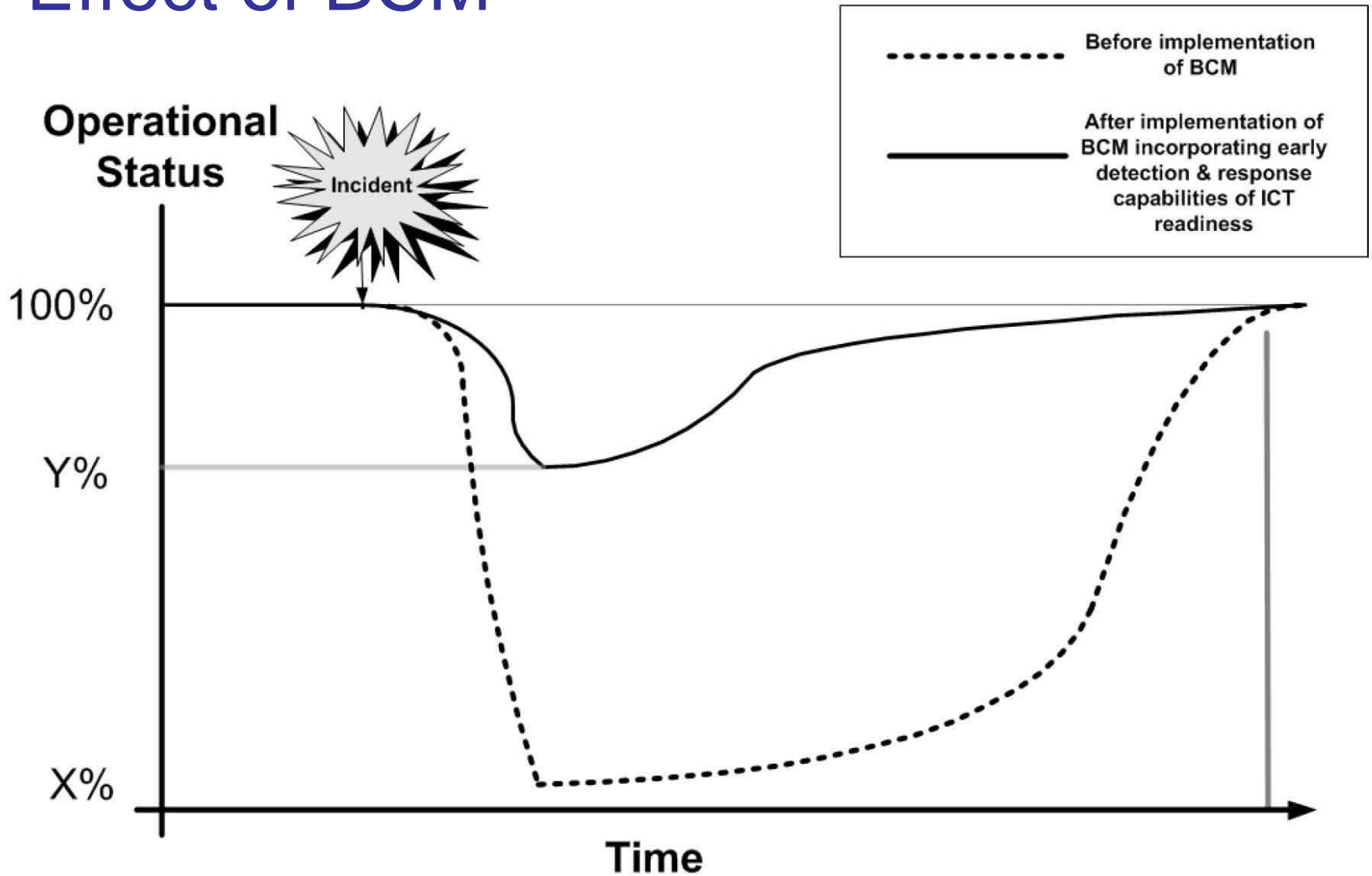
Outline

- Business Continuity Planning
- Business Impact Analysis

Business Continuity Management

- Procedures for the recovery of an organization's facilities in case of major incidents and disasters, so that the organization will be able to either maintain or quickly resume mission-critical functions
- BCM standards
 - ISO 27031 Guidelines for ICT readiness for business continuity
 - NISTSP800-34 Contingency Planning Guide for Federal Information Systems

Effect of BCM



How common is BCM in 'the real world'?

- 2006 CCSS extract: Most commonly reported categories of computer security policies and procedures 2006 (2005, 2004):
 - Media backup procedures - 95% (96%, 95%)
 - User access management - 93% (97%, 94%)
 - External network access control procedures - 78% (83%, 79%)
 - Documented operating procedures - 76% (80%, 83%)
 - User responsibilities policies - 72% (82%, 78%)
 - Controls against malicious software - 66% (75%, 72%)
 - Monitoring system access and use - 64% (72%, 68%)
 - Change control procedures - 60% (82%, 75%)
 - Clock synchronisation policy – 59% (59%, 43%)
 - Decommissioning equipment procedures – 59% (65%, 40%)
 - System audit policy – 58% (71%, 58%)
 - **Business continuity management – 54% (73%, 58%)**
 - Incident management procedures - 51% (67%, 64%)

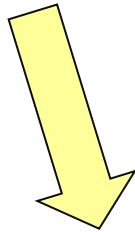
Business continuity management

- The range of incidents and disasters to be considered include:
 - Acts of nature, **for example:**
 - Excessive weather conditions
 - Earthquake
 - Flood
 - Fire
 - Human acts (inadvertent or deliberate), **for example:**
 - Hacker activity
 - Mistakes by operating staff
 - Theft
 - Fraud
 - Vandalism
 - Terrorism

Business Continuity Plan (BCP)

From:

Getting control over the crisis



To:

Back in business

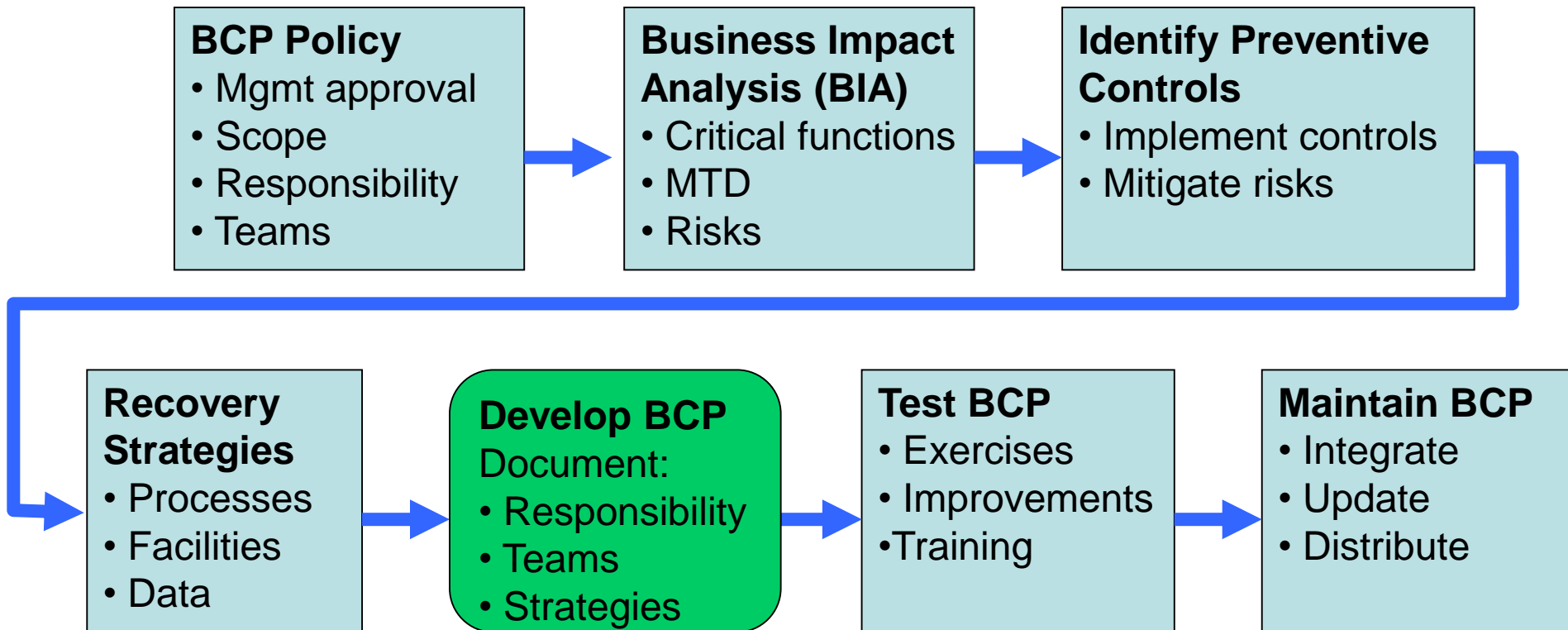


- The business continuity plan describes:
 - a sequence of actions
 - and the parties responsible for carrying them out
 - in response to disasters
 - in order to restore normal business operations as quickly as possible

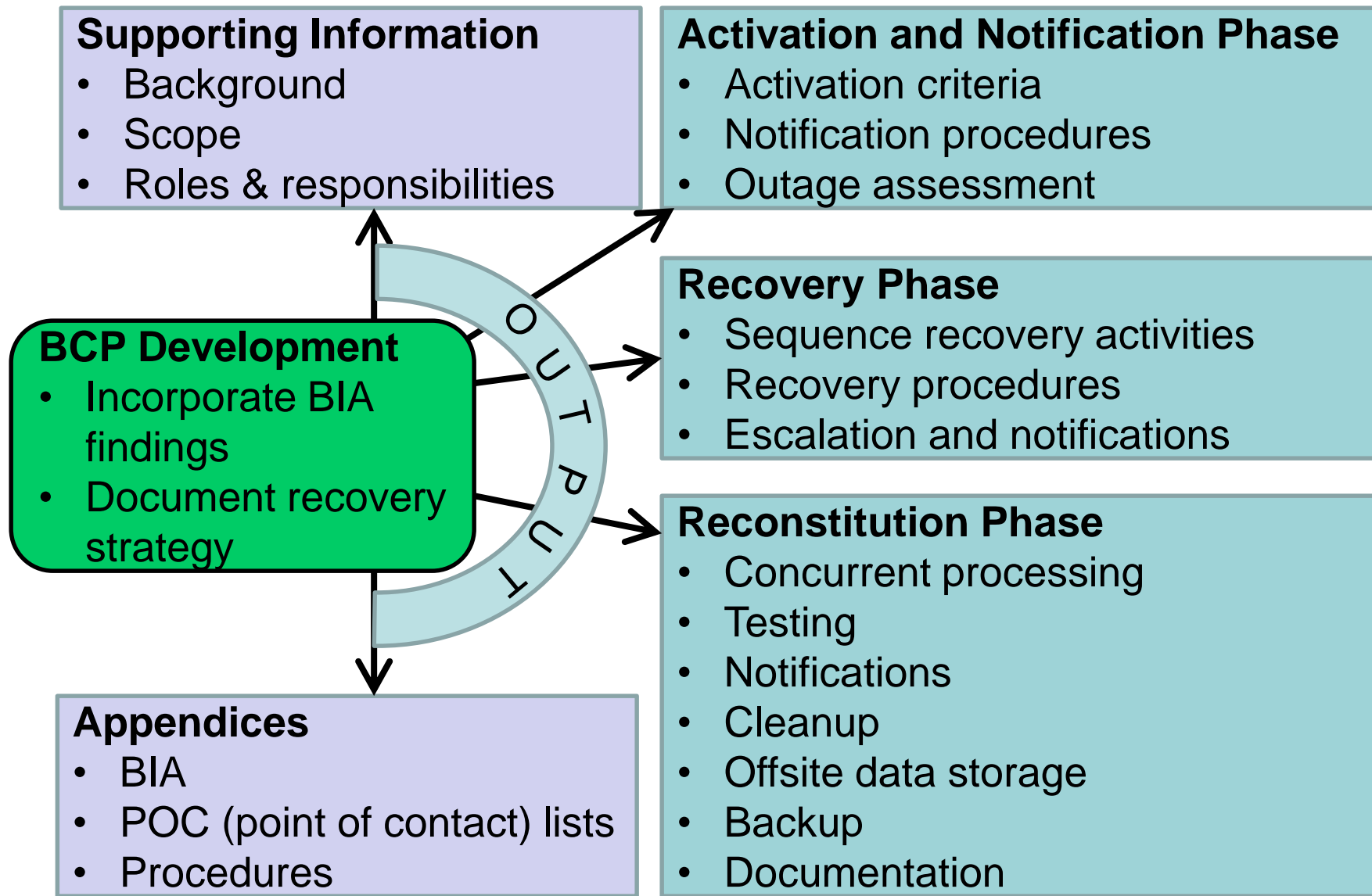
BCP Terminology

- **Business Continuity Plan**
 - Plan for restoring normal business functions after disruption
- **Business Contingency Plan**
 - Same as Business Continuity Plan
 - Contingency means "something unpredictable that can happen"
- **Disaster Recovery**
 - Reestablishment of business functions after a disaster, possibly in temporary facilities
 - Requires a BCP
- **Business Continuity Management**
 - Denotes the management of Business Continuity
 - Includes the establishment of a BCP
 - ICT Readiness for Business Continuity (IRBC) (term used in ISO27031)

BCP Management (same as IRBC)



Source: NIST Special Publication 800-34 rev.1
Contingency Planning Guide for Information Technology Systems (p.13)



BCP Development and Output: NIST SP800-34, rev.1 p.34

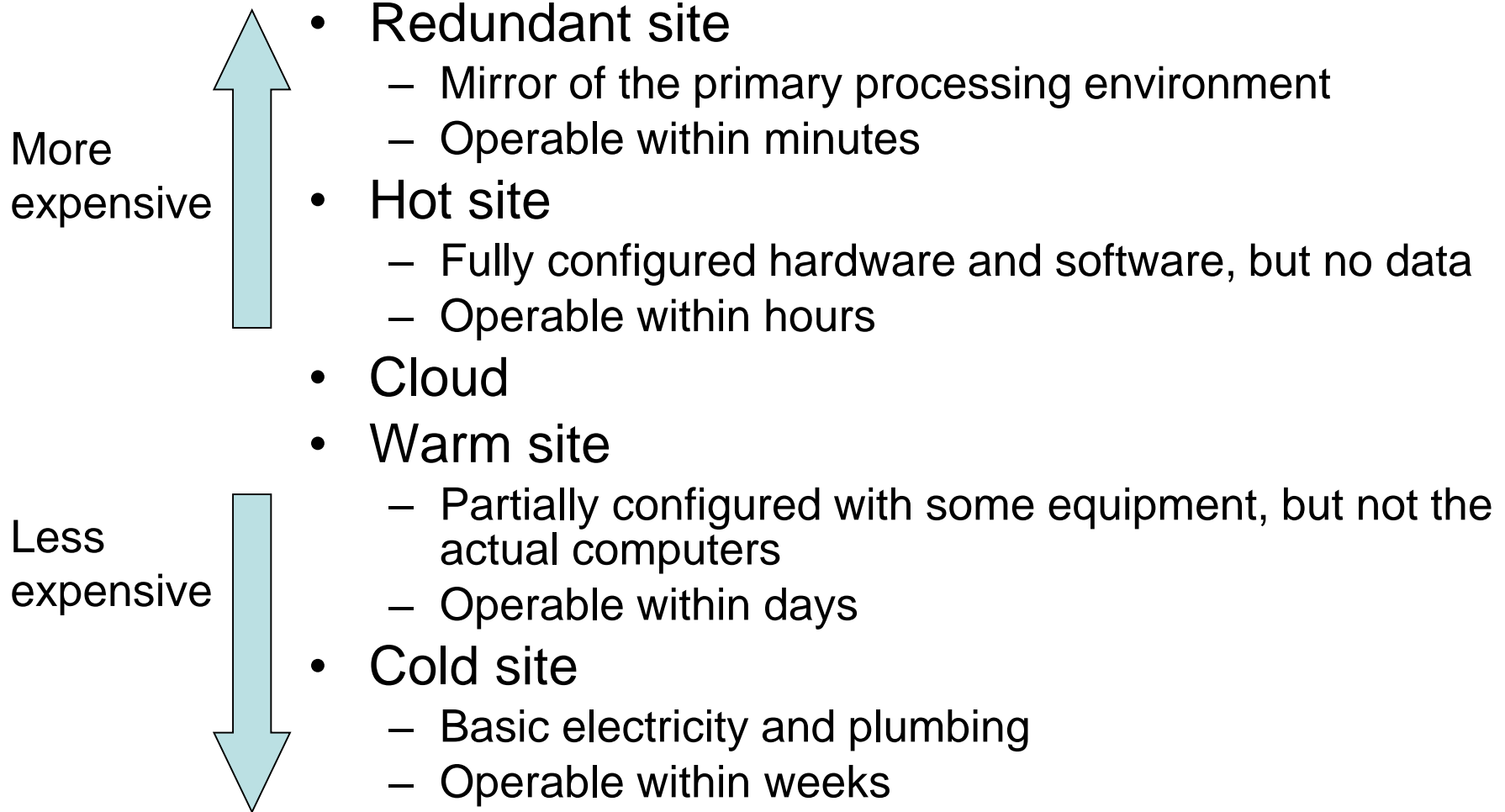
BIA: Business Impact Analysis

- A Business Impact Analysis (BIA) is performed as part of the BCP development to identify the functions that in the event of a disaster or disruption, would cause the greatest financial or operational loss.
- Consider e.g.:
 - IT network support
 - Data processing
 - Accounting
 - Software development
 - Payroll
 - Customer support
 - Order entry
 - Production scheduling
 - Purchasing
 - Communications

BIA (continued)

- The MTD (Maximum Tolerable Downtime) is defined for each function in the event of disaster.
- Example:
 - Non-essential = 30 days
 - Normal = 7 days
 - Important = 72 hours
 - Urgent = 24 hours
 - Critical = minutes to hours

Alternative Sites



Whenever relevant, consider cloud services, which can be relatively low cost

BCP Testing

- Checklist test
 - Copies of the BCP distributed to departments for review
- Structured walk-through test
 - Representatives from each department come together to go through the plan
- Simulation test
 - All staff in operational and support functions come together to practice executing the BCP
- Parallel test
 - Business functions tested at alternative site
- Full interruption test
 - Business functions at primary site halted, and migrated to alternative site in accordance with the BCP

End of Lecture