INF3510 Information Security
University of Oslo
Spring 2017

Lecture 5

Risk Management

Business Continuity Management

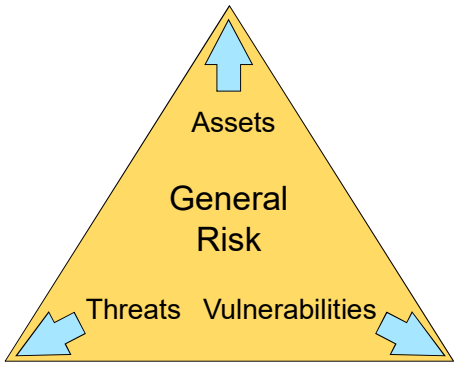
UiO, 2018

Audun Jøsang

What is risk?

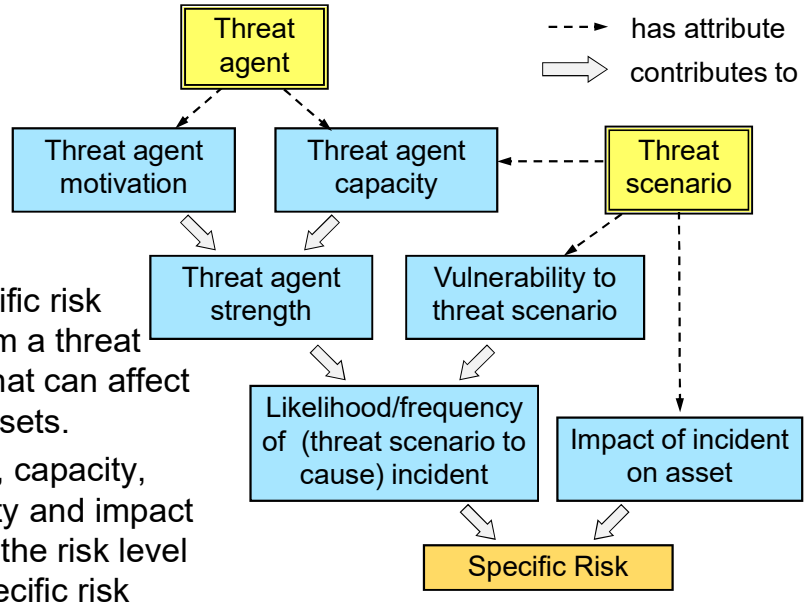
- ISO31000 Risk Management:
  - **"Risk is the effect of uncertainty on objectives"**
  - No distinction between positive and negative effects of uncertainty
  - This definition is too abstract for most people
  - Also says: **"Risk is often expressed in terms of a combination of the *consequences of 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."**

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.

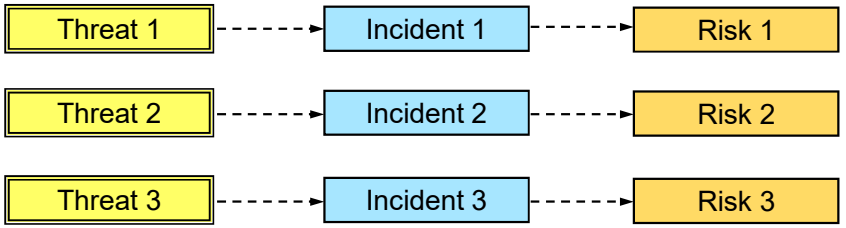
Detailed risk model



- 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

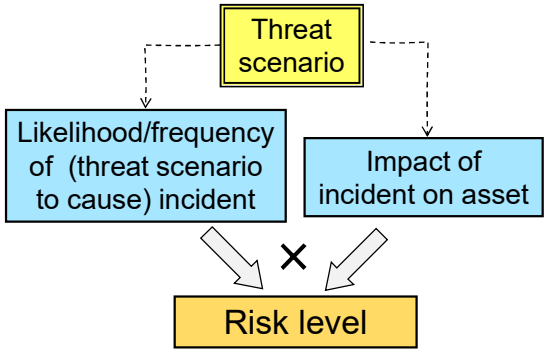
Many Risks

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



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



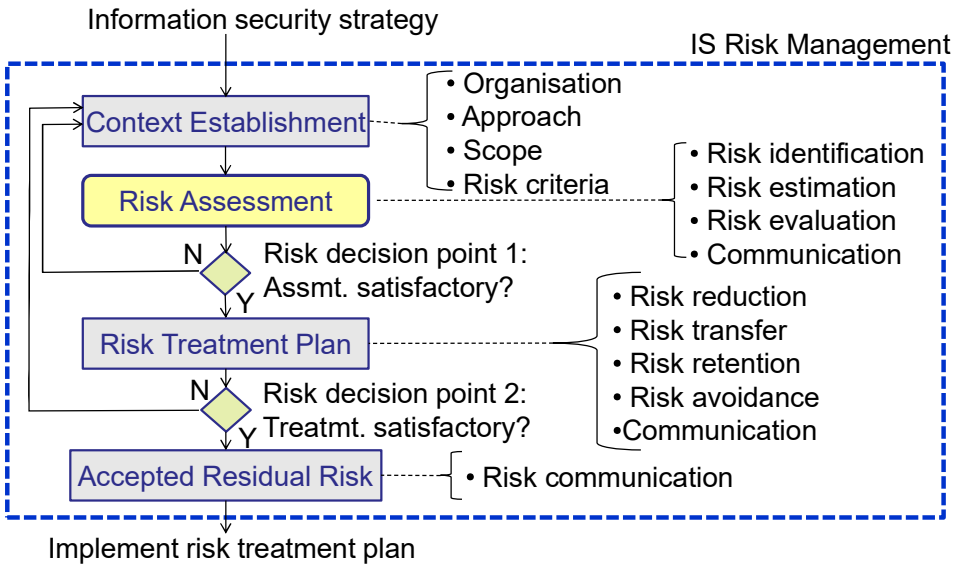
Risk Management standards

- 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

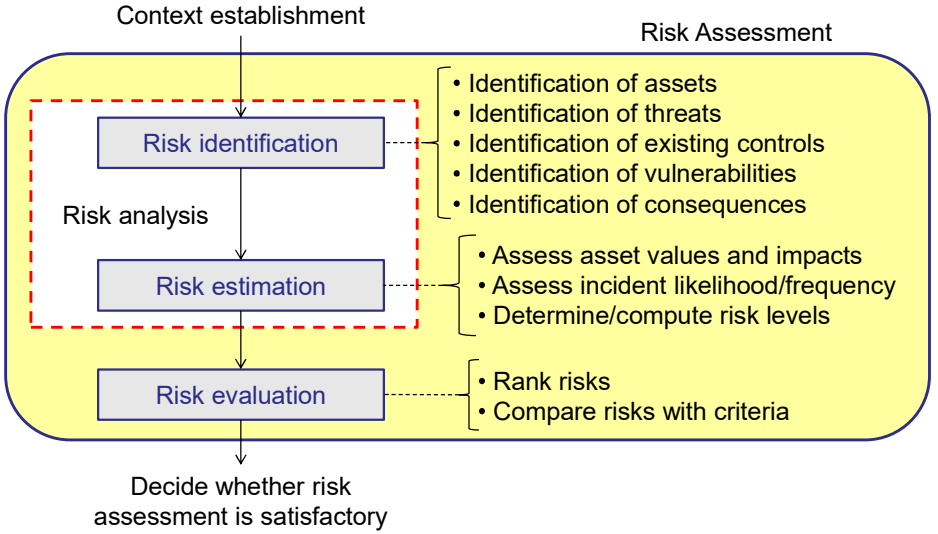
What is risk management?

- "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 , ISO/IEC 27002

Risk management process
ISO 27005

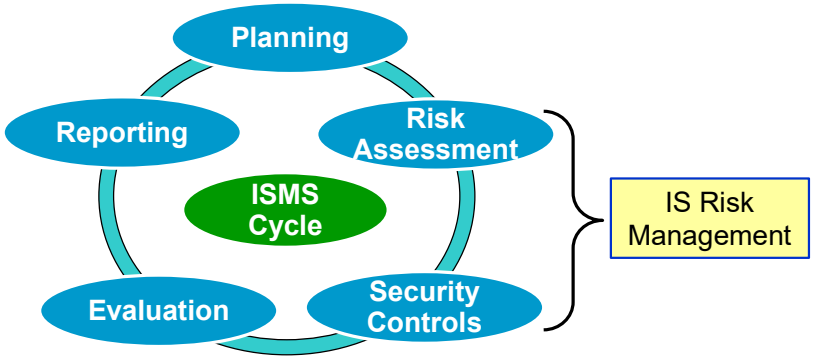


Risk assessment process
ISO 27005



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, examine, and understand the information and systems currently in place
- Know the enemy: identify, examine, and understand threats facing the organization
- Know the losses your organisation can tolerate.
- Know responsibility of each stakeholders within an organization to manage risks that are encountered

Roles involved in risk management

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

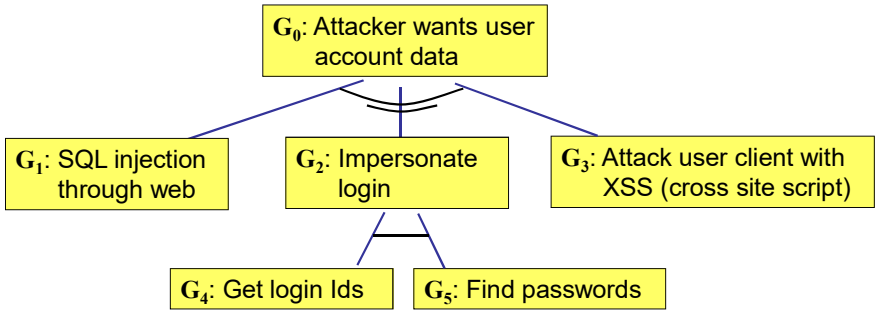
Threat scenario identification

- Realistic threat scenarios need to be described; unimportant threats can be ignored
- Threat assessment:
  - Which threats present danger to assets?
  - Which threats represent the most danger to information?
  - How much would it cost to recover from attack?
  - Which threat are most expensive to prevent?
- Threat assessment is important during system development
  - Used to discover and avoid vulnerabilities in software and systems.

Threat Scenario Modelling

- 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.

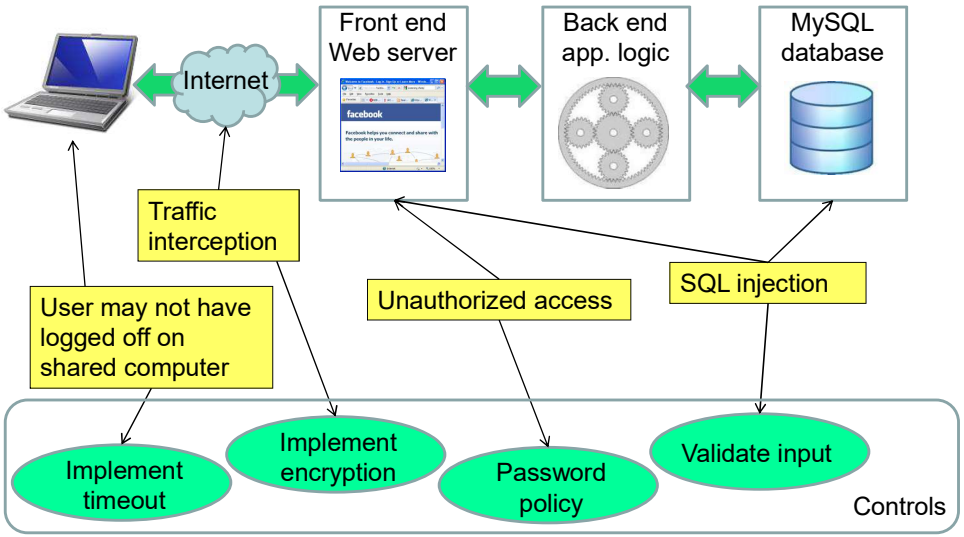
Attacker-centric attack tree example



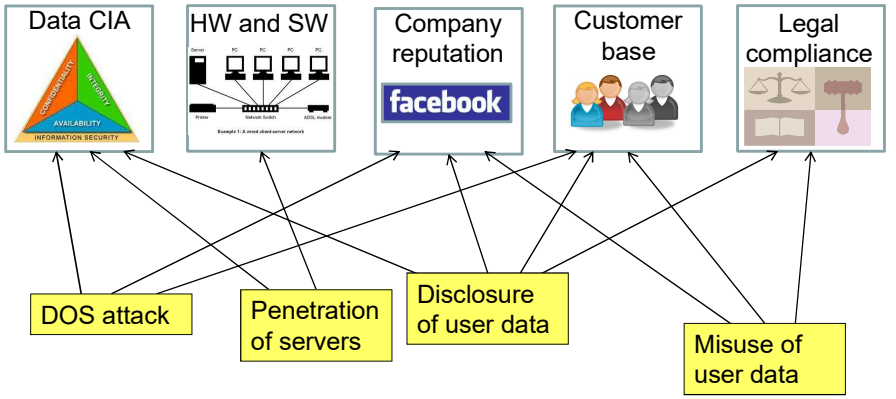
Legend:
G_0: Main goal — AND (conjunctive) all subgoals needed — OR (disjunctive) any subgoal needed

Probability of attack success: $p(G_0) = 1-(1-p(G_1))\cdot(1-(p(G_4)p(G_5)))\cdot(1-p(G_3))$

System-centric threat modelling example



Asset-centric threat modelling example



Vulnerability Identification

- Specific avenues threat agents can exploit to attack an information asset are called vulnerabilities
- Examines how each threat could be perpetrated against the organization's assets
- Process works best when people with diverse backgrounds within organization work iteratively in a series of brainstorming sessions
- At end of risk identification process, list of assets and their vulnerabilities is achieved
- Vulnerabilities discovered during system development can be fixed and avoided in production system.

Identifying specific risks

Threats / incidents	Vulnerabilities	Asset impacts
•Password compromise	•Weak passwords	•Deleted files
•SQL injection	•Poor awareness	•Damaged files
•Logical bomb in SW	•No input validation	•Damaged reputation
•Trojan infects clients	•Outdated antivirus	•Stolen files
•Cryptanalysis of cipher	•Weak ciphers	- sensitivity levels 1,2,3
•Brute force attack	•Short crypto keys	•Intercepted traffic
•Social engineering	•Poor usability	•False transaction
• …..	• …	• …

- A valid combinations of threat, vulnerability and asset impact represents a single specific risk
- All relevant specific risks should be identified

Estimating risk levels

Types of analysis

- **Qualitative**
  - Uses descriptive scales. Example:
    - Impact level: Minor, moderate, major, catastrophic
    - Likelihood: Rare, unlikely, possible, likely, almost certain
- **Semi-quantitative**
  - Qualitative scales assigned numerical values
  - Can be used in formulae for prioritization (with caution)
- **Quantitative**
  - Use numerical values for both consequence (e.g. $$$) and likelihood (e.g. probability value)

Qualitative likelihood scale

Increasing Likelihood

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

Increasing Impact

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

Qualitative risk levels: Add likelihood & impact level

Likelihood \ Impact level	(0) Insignificant	(1) Minor	(2) Moderate	(3) Major
(3) High	(3) M	(4) H	(5) VH	(6) E
(2) Medium	(2) L	(3) M	(4) H	(5) VH
(1) Low	(1) VL	(2) L	(3) M	(4) H
(0) Unlikely	(0) N	(1) VL	(2) L	(3) M

Legend
E: extreme risk; immediate action required
(V)H: (very) high risk; senior management attention needed
M: moderate risk; management responsibility must be specified
(V)L: (very) low risk; manage by routine procedures
N: Negligible risk; To be ignored

Semi-quantitative risk estimation - example

Semi-quantitative risk levels: Multiply likelihood & impact level

Risk Level / Likelihood \ Impact level	(0) Nil	(1) Insign.	(2) Minor	(3) Moderate	(4) Major
(4) High	(0) Nil	(4) M	(8) H	(12) VH	(16) E
(3) Medium	(0) Nil	(3) L	(6) M+	(9) H+	(12) VH
(2) Low	(0) Nil	(2) VL	(4) M	(6) M+	(8) H
(1) Unlikely	(0) Nil	(1) Neg	(2) VL	(3) L	(4) M
(0) Never	(0) Nil	(0) Nil	(0) Nil	(0) Nil	(0) Nil

M: moderate; Specify responsibililty
L: low; Manage by routine procedures
VL: very low; Manage by routine
Neg: Negligible; To be ignored
Nil: Nil; No risk exists

E: extreme; Immediate action required
VH: very high; Priority action action
H+: high +; Management attention
H: high; Management attention
M+: moderate +; Specifu responsib

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 × EF
  - Annualized Rate of Occurrence (ARO)
    - Estimated frequency a threat will occur within a year
  - Annualised Loss Expectancy (ALE)
    - ALE = SLE × 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(public image) = $1,000,000
  - EF(public image affected by defacing) = 0.05
  - SLE = AV × EF = $50,000
  - ARO(defacing) = 2
  - ALE = SLE × ARO = $100,000
- Justifies spending up to $100,000 p.a. on controls

Risk listing and ranking

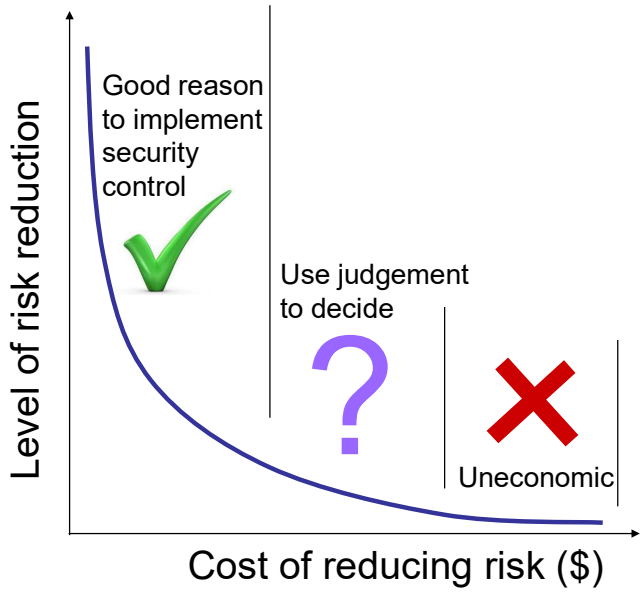
Threat scenario:	Existing controls & vulnerabilities:	Asset impact:	Impact level:	Likelihood description:	Likelihood:	Risk level:
Compromise of user password	No control or enforcement of password strength	Deleted files, breach of confidentiality and integrity	MODERATE	Will happen to 1 of 50 users every year	MEDIUM	HIGH
Virus infection on clients	Virus filter disabled on many clients	Compromise of clients	MODERATE	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	MODERATE
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	MODERATE

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

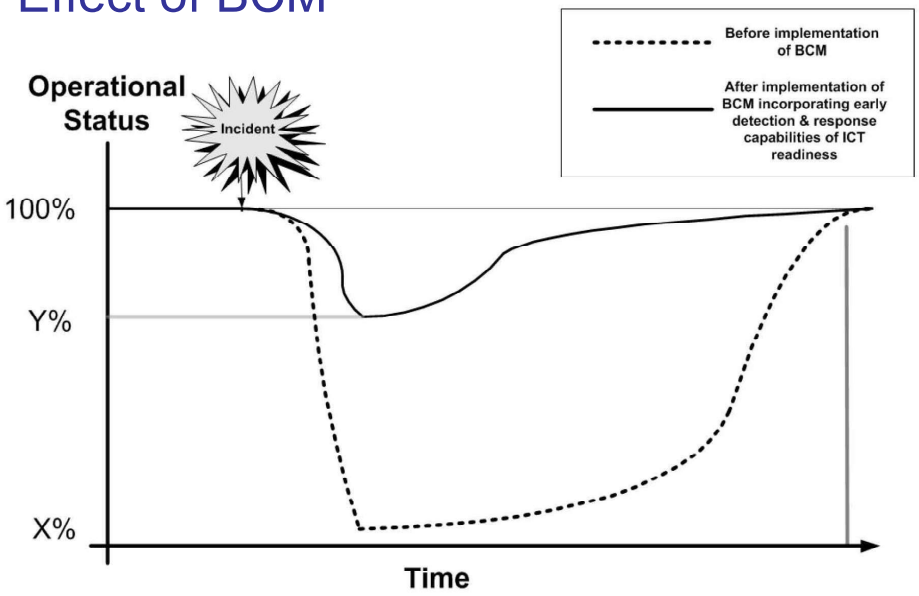
Outline

- Business Continuity Planning
- Disaster Recovery

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 information and communi-cations technology 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:

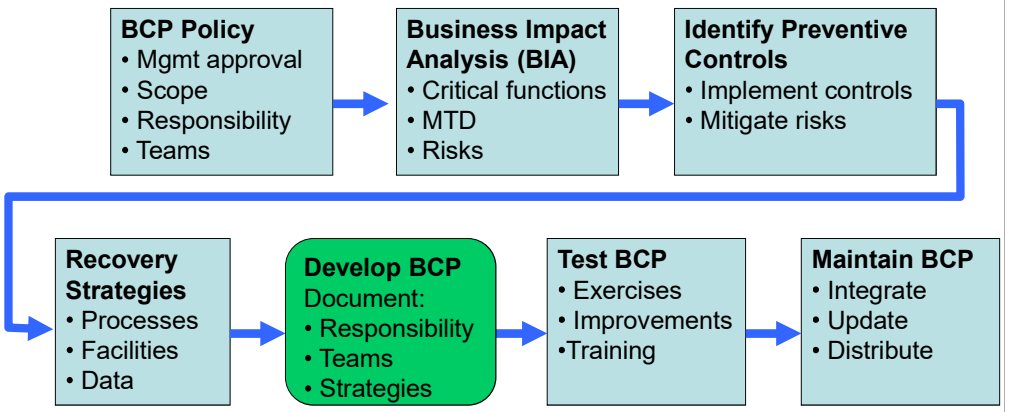
Back in business

- 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

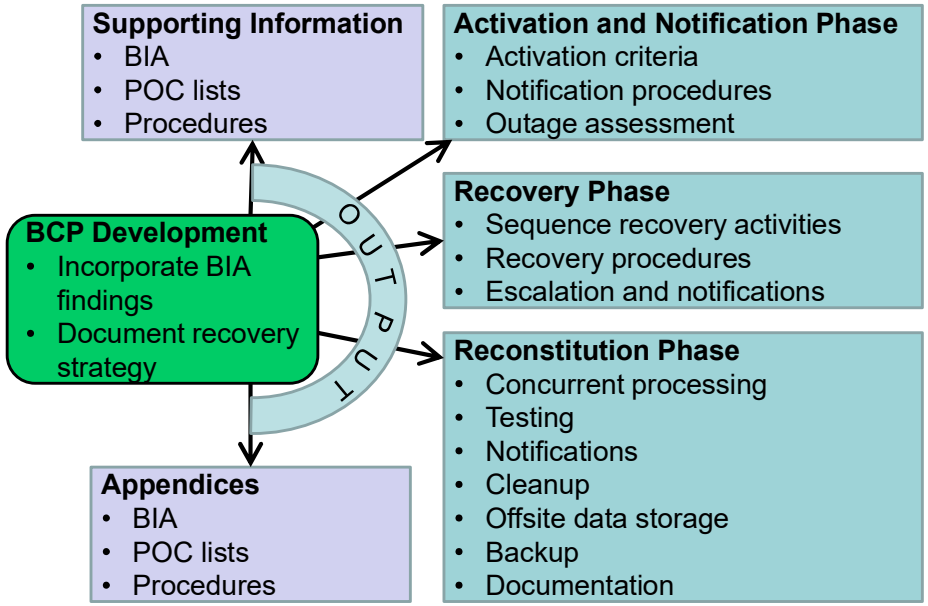
BCP Terminology

- 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

More expensive

- Redundant site
  - Mirror of the primary processing environment
  - Operable within minutes
- Hot site
  - Fully configured hardware and software, but no data
  - Operable within hours
- Cloud
- Warm site
  - Partially configured with some equipment, but not the actual computers
  - Operable within days
- Cold site
  - Basic electricity and plumbing
  - Operable within weeks

Less expensive

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