INF3510 Information Security
University of Oslo
Spring 2014

Lecture 3

Risk Management

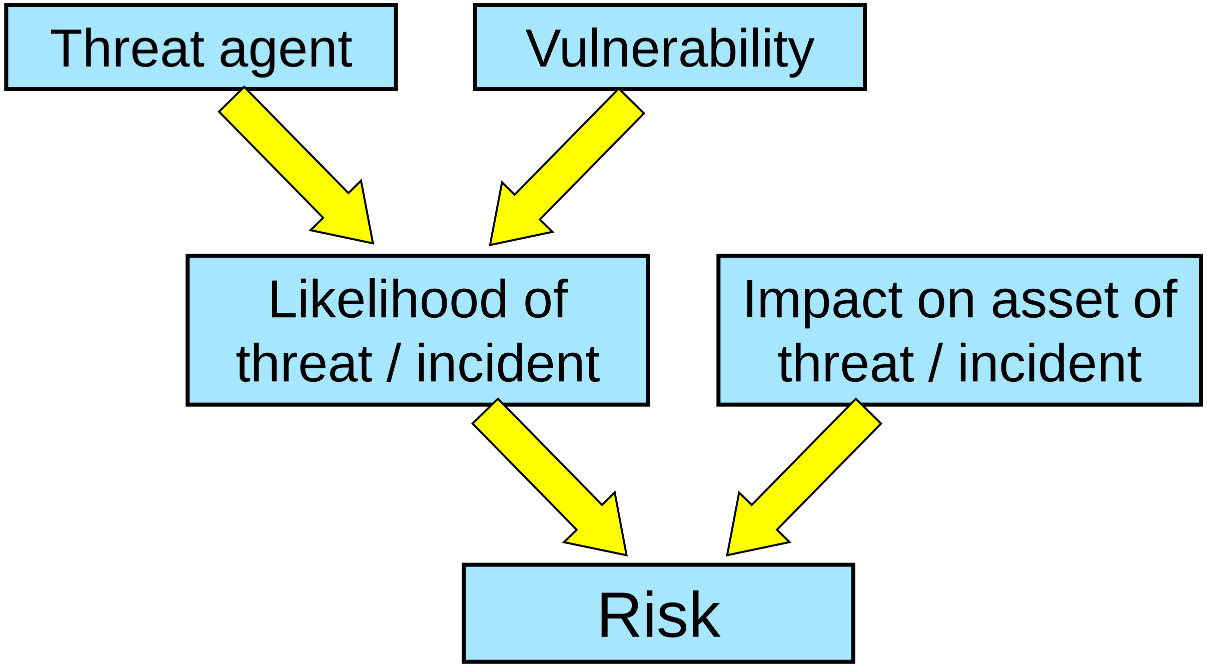
Business Continuity Management

University of Oslo, spring 2014

Audun Jøsang

What is risk ?

- Motivation
- Capacity



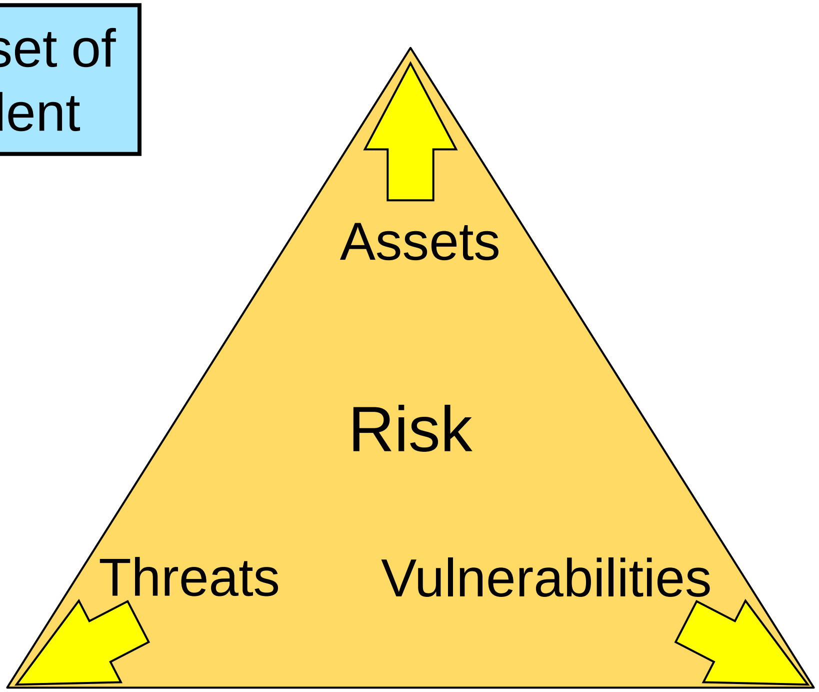
Threat agent

Vulnerability

Likelihood of threat / incident

Impact on asset of threat / incident

Risk



Assets

Risk

Threats

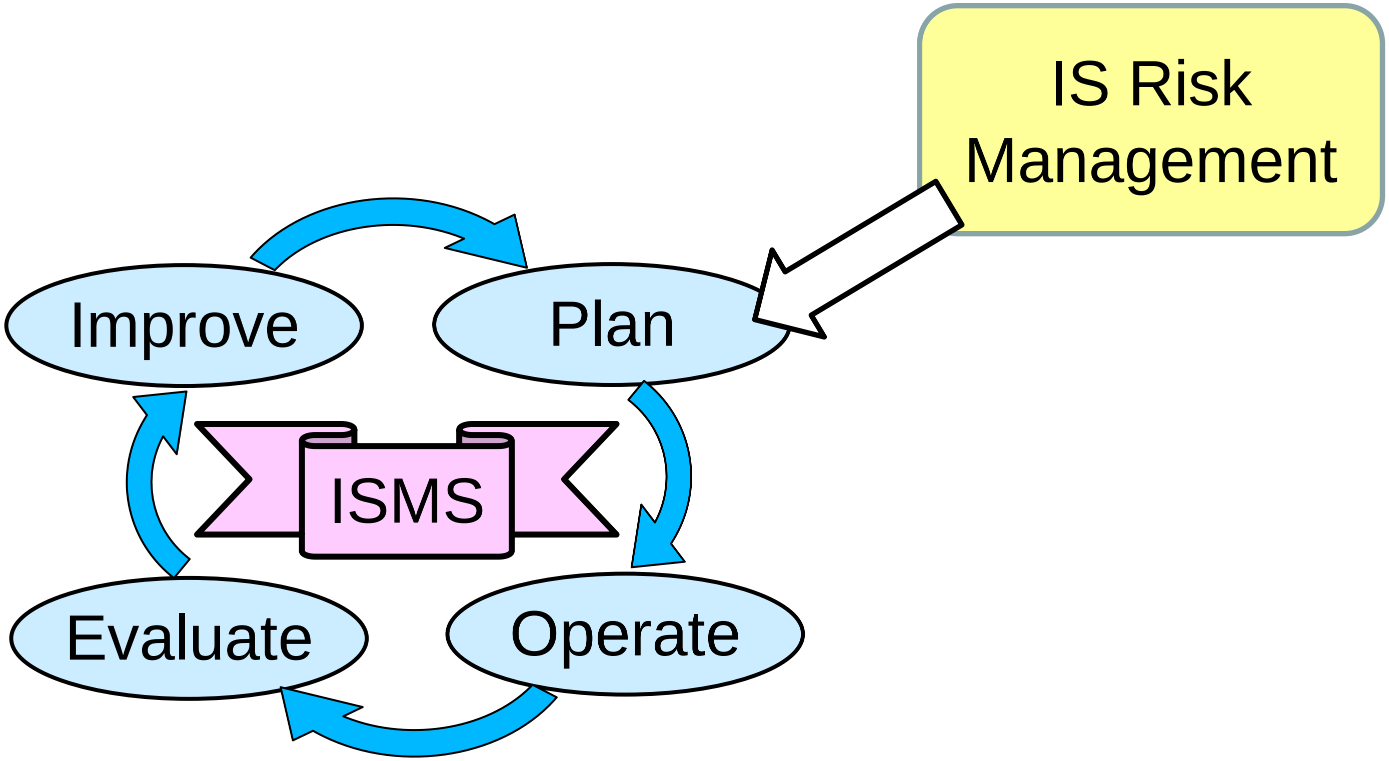
Vulnerabilities

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 – ISMS integration



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

Basis for assessing risk

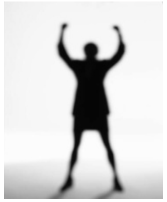
- Know the assets: identify, examine, and understand the information and systems currently in place
- Know the enemy: identify, examine, and understand threats facing the organization
- Know the losses your organisation can tolerate.
- Know responsibility of each stakeholders within an organization to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

Proportionality principle

How much should I spend on securing ?

? Why ?

How much should I spend on securing my reputation ?



- The Proportionality Principle:
  - Apply a set of controls (physical, technical and administrative controls) that match the perceived risk to, and value of, an organisation’s information assets

Problems of measuring risk

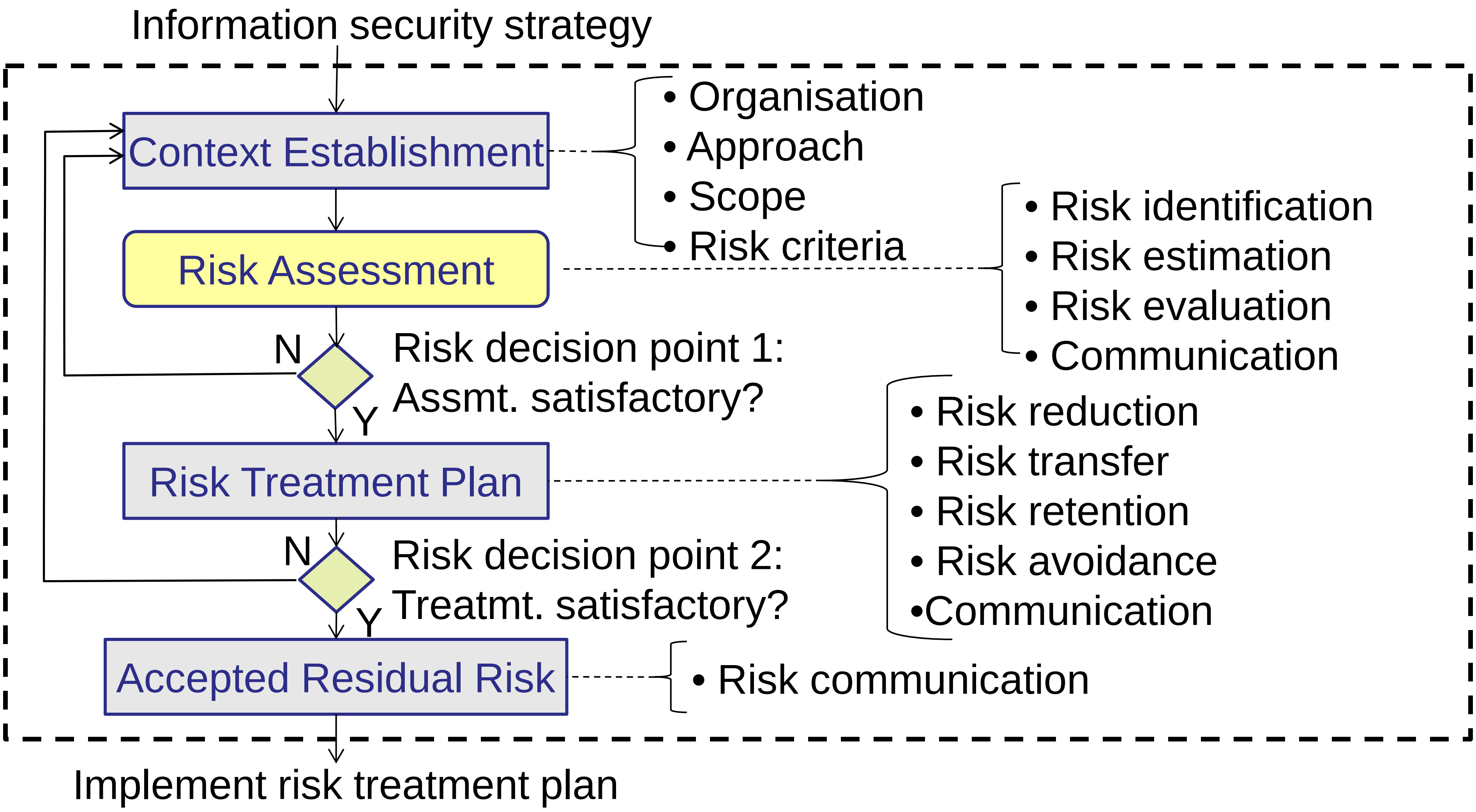
Businesses normally wish to measure risk in money, but almost impossible to do this

- 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

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

Risk management process
ISO 27005



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

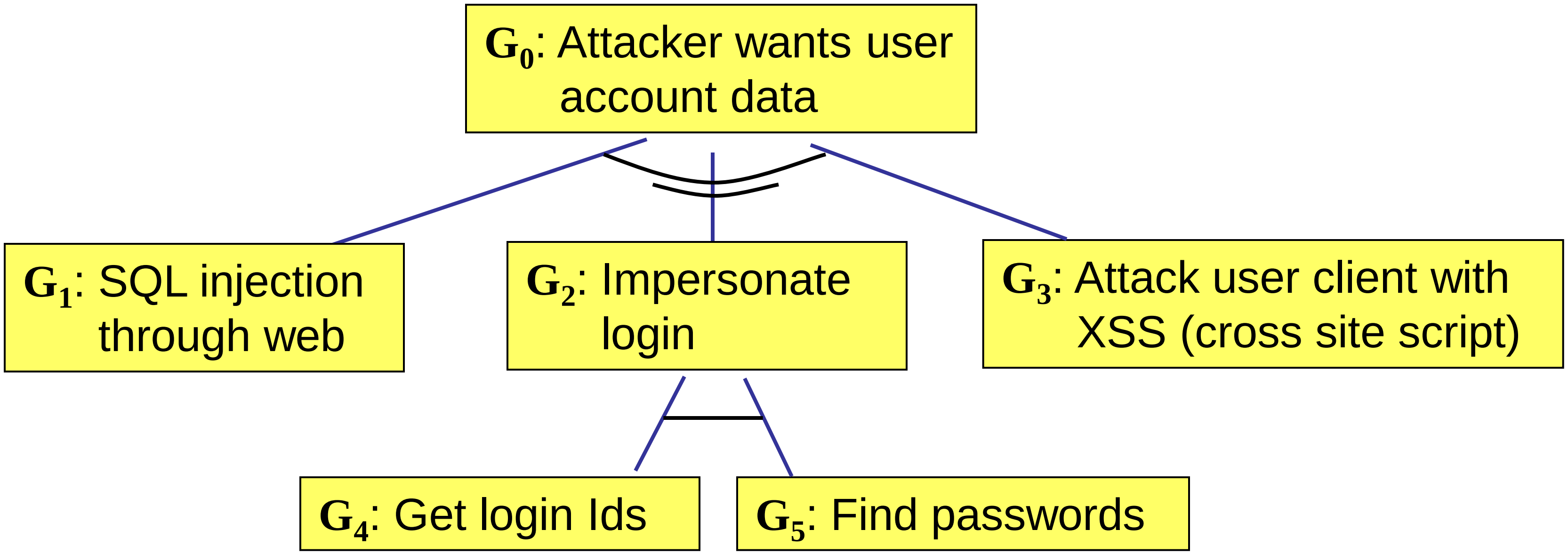
Threat identification

- Realistic threats need to be described; unimportant threats are set aside
- 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 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


G0: Attacker wants user account data
G1: SQL injection through web
G2: Impersonate login
G3: Attack user client with XSS (cross site script)
G4: Get login Ids
G5: Find passwords

Legend:

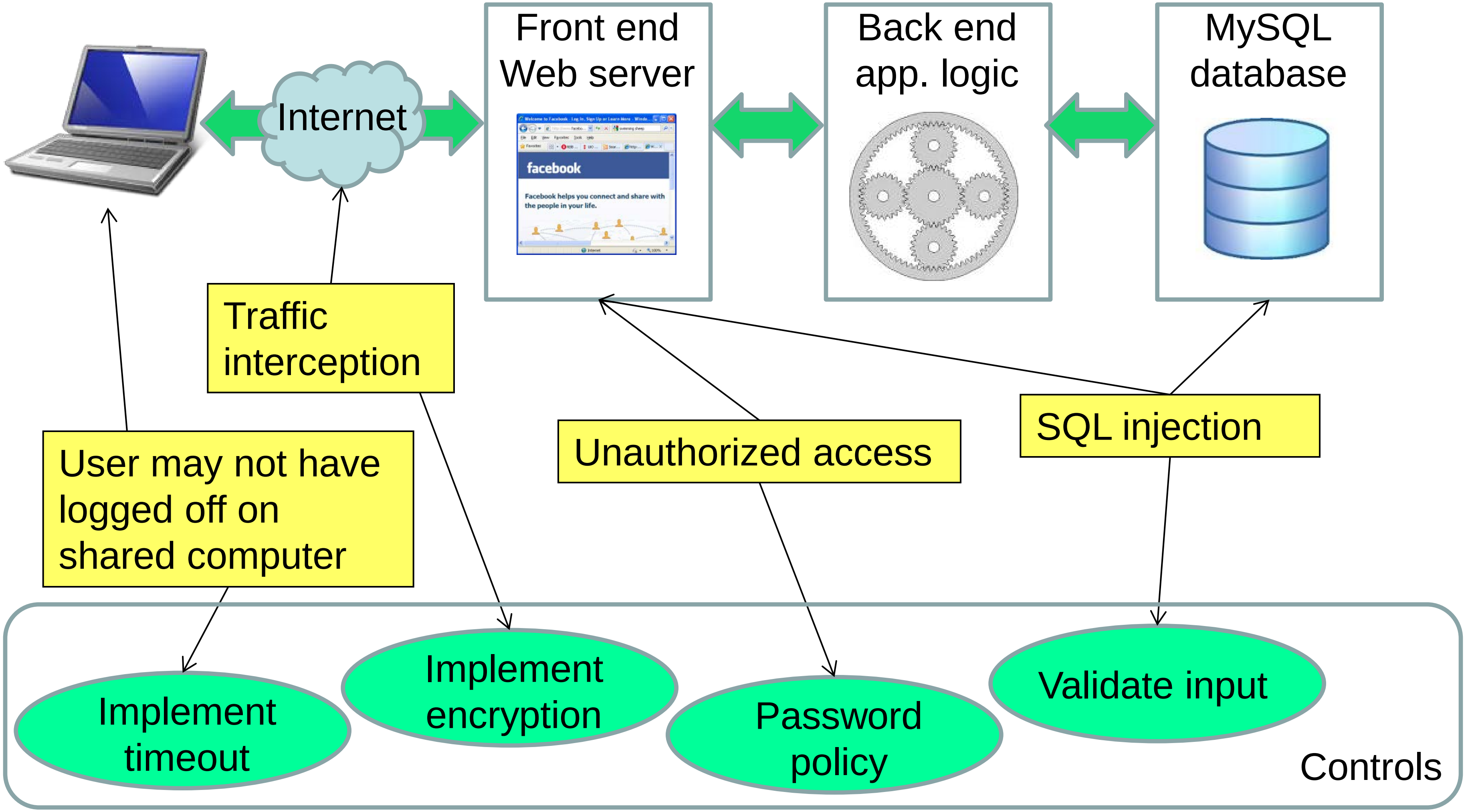
G_0: Main goal

—— AND (conjunctive)
all subgoals needed

≫ OR (disjunctive)
any subgoal needed

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

System-centric threat modelling example



Internet

Front end Web server

facebook
Facebook helps you connect and share with the people in your life.

Back end app. logic

MySQL database

Traffic interception

User may not have logged off on shared computer

Unauthorized access

SQL injection

Implement timeout

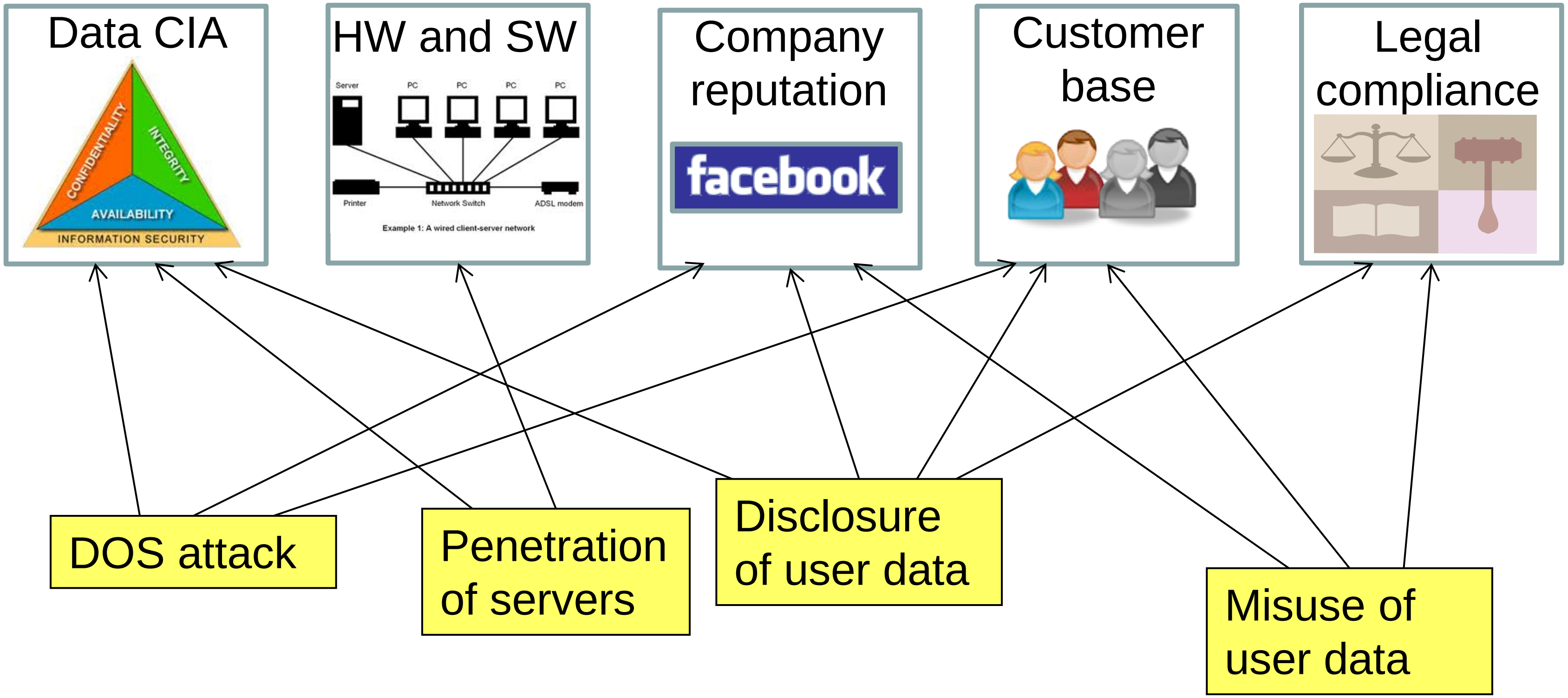
Implement encryption

Password policy

Validate input

Controls

Asset-centric threat modelling example



Data CIA

HW and SW

Company reputation

Customer base

Legal compliance

DOS attack

Penetration of servers

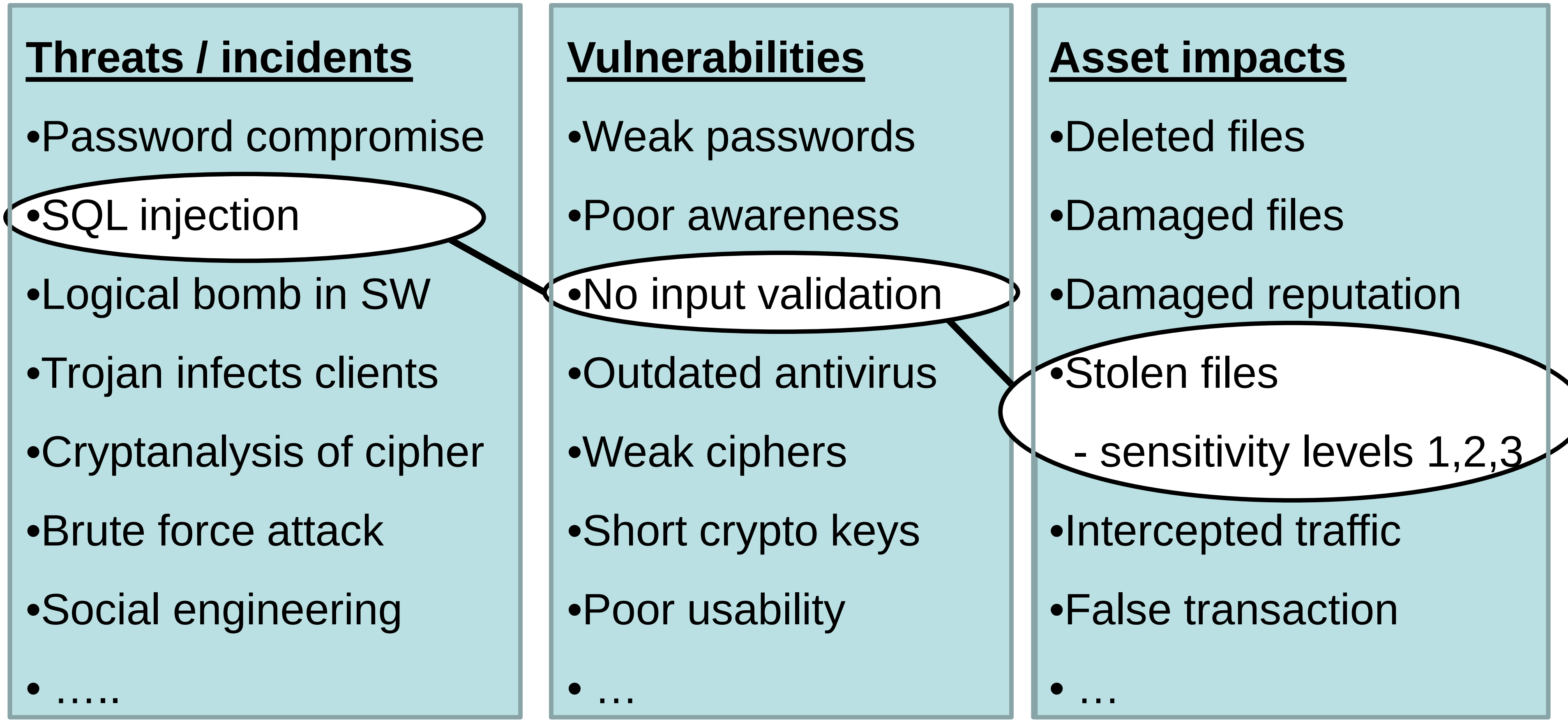
Disclosure of user data

Misuse of user data

Vulnerability Identification

- Specific avenues threat agents can exploit to attack an information asset are called vulnerabilities
- Examine how each incident/threat could be perpetrated and list organization’s assets and vulnerabilities
- 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

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
- Damaged files
- Damaged reputation
- Stolen files
  - sensitivity levels 1,2,3
- Intercepted traffic
- False transaction
- …

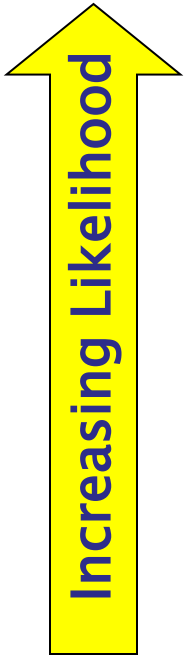
- A valid combinations of threat, vulnerability and asset impact represents a single specific risk
- All relevant specific risks should be identified

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)

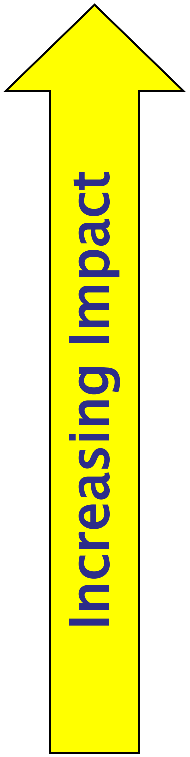
Qualitative likelihood scale



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

		Impact level			
	Risk level	(0) Insignificant	(1) Minor	(2) Moderate	(3) Major
Likelihood	(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

Impact level

Risk Level Likelihood	(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

Evaluate risks

- Compare
  - the level of risk found during risk analysis with
  - the established risk criteria
  - NOTE: Consider analysis and criteria on same basis - qualitative or quantitative
- Output: prioritized list of risks for further action
  - Risks in low or acceptable risk categories, may be accepted without further treatment

Risk listing and ranking

Incident / Threat	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	LOW	LOW
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 ranking complexity

Incident / Threat	Existing controls & vulnerabilities	Asset impact	Impact level	Likelihood description	Likelihood	Risk level
Router Compromise	Password only	Intrusion and disruption	MODE RATE	Many times per year	HIGH	HIGH
Physical Destruction of Data Centre	None (not addressed in BCP)	Operations Disrupted for one month	MAJOR	Could happen once in 25 years	LOW	HIGH

- Not easy to prioritize risks of same level but with different impact levels and likelihood

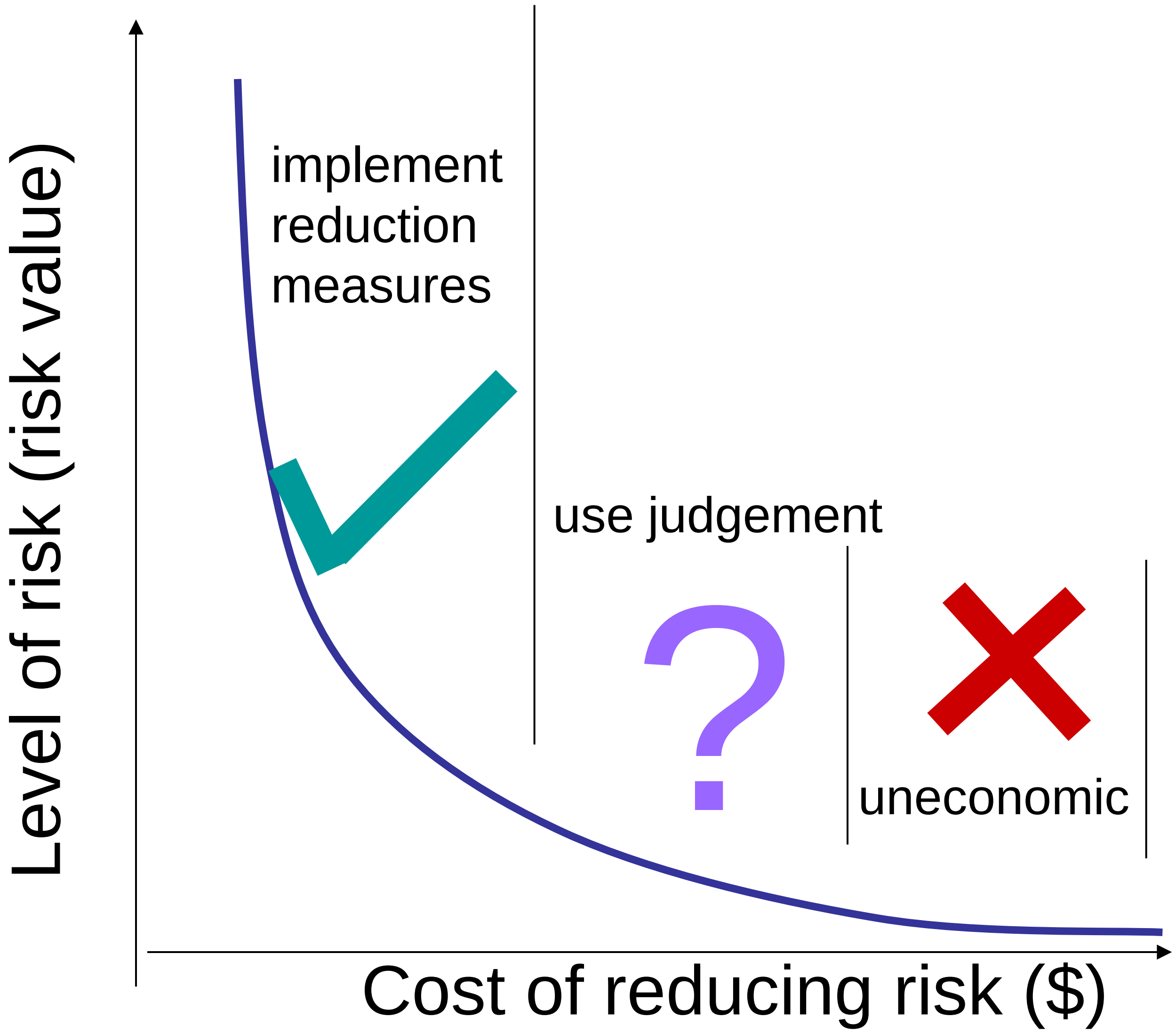
Documenting the results of risk assessment

- Final summary comprised in ranked vulnerability risk worksheet

- Worksheet details asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor

- Ranked vulnerability risk worksheet is initial working document for next step in risk management process: assessing and controlling risk

Risk treatment economy



Risk Control Strategies

- Once ranked vulnerability risk worksheet complete, must choose one of four strategies to control each risk:
  - Reduce/mitigate risk (security and mitigation controls)
  - Share/transfer risk (outsource activity that causes risk, or insure)
  - Retain risk (understand tolerate potential consequences)
  - Avoid risk (stop activity that causes risk)

Treating risk from the positive dimension

- Identify options for risk treatment by seeking opportunities that might increase positive outcomes without increasing the risk.
- Options include:
  - **Actively seek** an opportunity for creating value and profit
  - **Change the likelihood of opportunity** to enhance the likelihood of beneficial outcome
  - **Change the consequences** to increase the extent of the gains
  - **Sharing** the opportunity
  - **Retain** the residual opportunity

Business Continuity Management

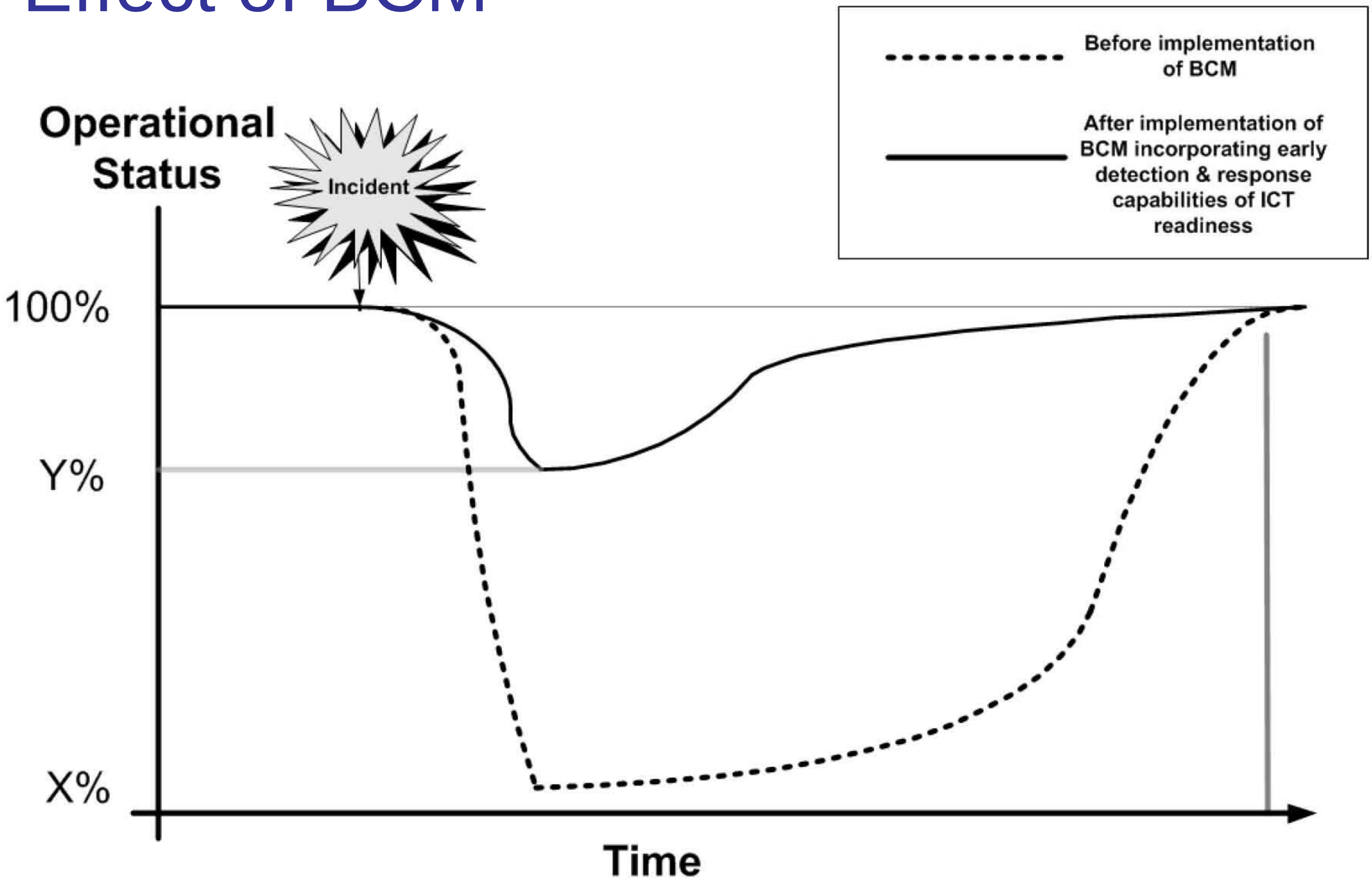
Outline

- 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 communications technology readiness for business continuity
  - NISTSP800-34 Contingency Planning Guide for Information Technology 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:

Dealing with the crisis

To:

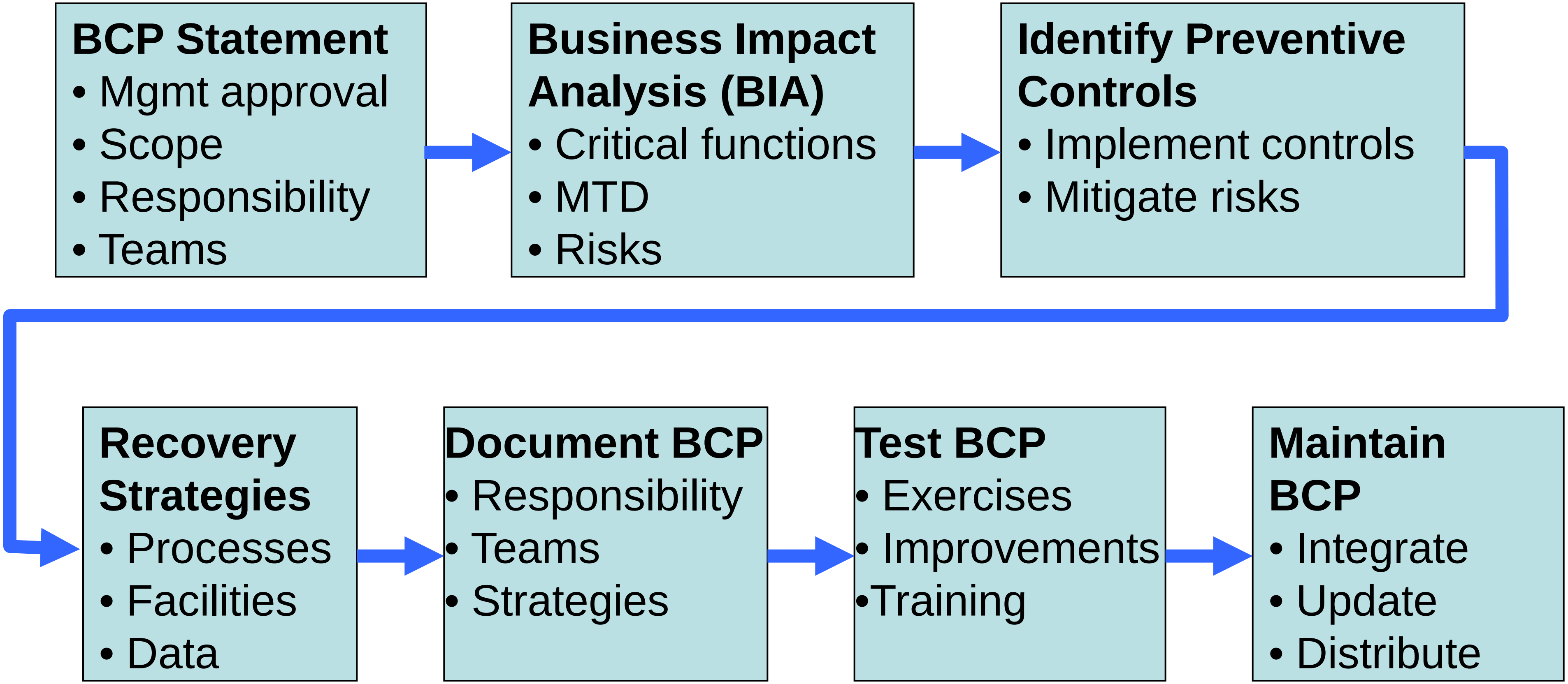
Back in business

- 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
  - Restablishment of business functions after a desaster, possibly in temporary facilities

BCP Development



BCP Statement
- Mgmt approval
- Scope
- Responsibility
- Teams

Business Impact Analysis (BIA)
- Critical functions
- MTD
- Risks

Identify Preventive Controls
- Implement controls
- Mitigate risks

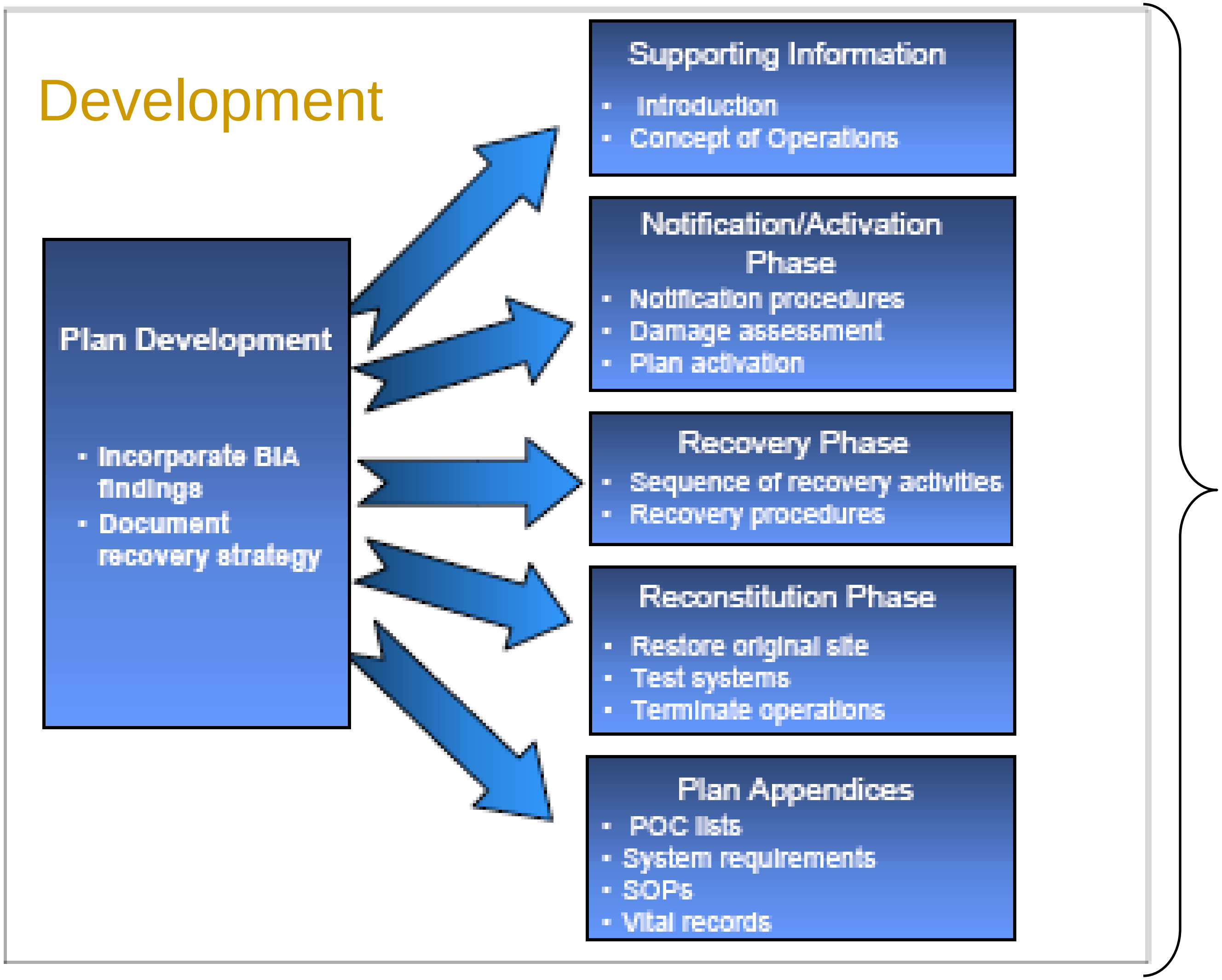
Recovery Strategies
- Processes
- Facilities
- Data

Document BCP
- Responsibility
- Teams
- Strategies

Test BCP
- Exercises
- Improvements
- Training

Maintain BCP
- Integrate
- Update
- Distribute

Source: NIST Special Publication 800-34
Contingency Planning Guide for Information Technology Systems (p.14)



Development

Plan Development

- Incorporate BIA findings
- Document recovery strategy

Supporting Information

- Introduction
- Concept of Operations

Notification/Activation Phase

- Notification procedures
- Damage assessment
- Plan activation

Recovery Phase

- Sequence of recovery activities
- Recovery procedures

Reconstitution Phase

- Restore original site
- Test systems
- Terminate operations

Plan Appendices

- POC lists
- System requirements
- SOPs
- Vital records

Output

BCP Development and Output: NIST SP800-34, p.31

BCP Development - BIA

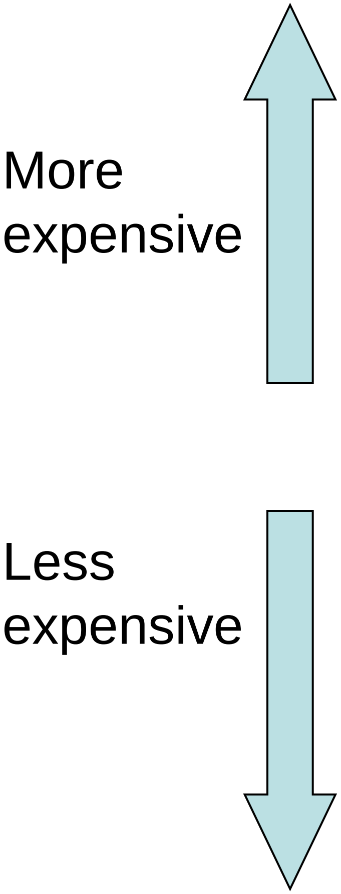
- A Business Impact Analysis (BIA) is performed as part of the BCP development to identify the functions that in the event of a disaster or disruption, would cause the greatest financial or operational loss.
- Consider e.g.:
  - IT network support
  - Data processing
  - Accounting
  - Software development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

Customer support
Order entry
Production scheduling
Purchasing
Communications

BCP Development - BIA

- 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

BCP Development - Alternative Sites



More expensive

Less 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
- Mobile site
- Warm site
  - Partially configured with some equipment, but not the actual computers
  - Operable within days
- Cold site
  - Basic electricity and plumbing
  - Operable within weeks

BCP Development – Strategy Selection

- Analyse alternative disaster recovery strategies
  - Choosing data and software backup facility
  - Choosing alternative site type and contract
  - Human resources
  - Insurance
  - Reciprocal and mutual aid agreements
  - Multiple processing centres
  - Data processing service bureaus

  with respect to BIA, cost, restoration time and practicality

BCP Components

- Supporting information
  - Establish purpose, applicability and scope
  - System description and staff responsibilities
- Notification/Activation Phase
- Recovery Phase
- Reconstruction Phase
- Appendices
  - Contact information
  - SOPs and checklists
  - Equipment and system requirements lists

BCP Phases

- A security incident can vary in magnitude from minor incident to major disaster.
- Different sub-plans needed for different phases in the business continuity process.
  - Plan for activation phase
  - Plans for recovery phase
  - Plan for reconstitution phase

BC Activation Phase Plan

- Actions to take immediately after incident
  - Procedures for contacting recovery teams
  - Assessment of damage to primary site facilities
    - Estimated outage time at primary site
    - Compare with predefined MTD and activation criteria
  - Notify BC management
  - Management declares a disaster if criteria are met
  - Start implementing BCP
- BCP activation responsibility
  - Only one person
  - CEO or other predefined role
  - Succession of responsibility must be predefined

BC Recovery Phase Plan

- Evacuation and safety of personnel
  - Always first priority
- Notifying alternative sites
- Securing home site
- Activation of recovery teams
- Relocation to alternative sites
- Resumption of critical business functions
- Reviewing how the organisation will interface with external parties (customers, partners) from alternative site

BC Reconstitution Phase Plan

- Plan for returning to normal operations at primary site
  - Repairing primary site, or prepare new site
  - Installing hardware and software
  - Testing business functions
  - Migrating business functions stepwise
    - Least critical functions first
    - Most critical functions last
  - Shutting down alternative site
  - Securing and removing sensitive data from alternative site

BCP Appendices

- Include
  - Contact information for key personnel
    - Call tree data
  - Contact information for vendors and alternative site providers
    - Including SLA and reciprocal agreements
  - Checklists for recovery processes
  - Equipment and systems requirement lists
  - Description of and directions to alternative site

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