

# INF3510 Information Security

## University of Oslo

### Spring 2010

---

## Lecture 12

# Risk Management and Business Continuity Planning



Audun Jøsang

# Outline

---

- Risk Management
  - What is risk?
  - What is risk management?
  - Risk management practice
- Business Continuity Planning
  - Business contingency planning
  - Disaster Recovery

# Documentation

---

- Risk Management guidelines
  - NIST SP800-30 Risk Management Guide for Information Technology Systems
  - AS/NZS 4360 Risk Management
  - ISO/IEC 27002 Section 4
- Business Continuity Planning guidelines
  - NISTSP800-34 Contingency Planning Guide for Information Technology Systems
  - ISO/IEC 27002 Section 14

# What is risk?

---

- “the possibility of damage happening”
  - (Shon Harris, author of CISSP All-in-One Exam Guide)
- “the chance of something happening that will have an impact upon objectives.” ... measured in terms of consequences and likelihood (AS/NZS 4360:2004 Risk Management)
  - **Consequence**: the outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain...
  - **Likelihood**: used as a qualitative description of probability or frequency
- “the net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur”
  - (NIST SP800-30)

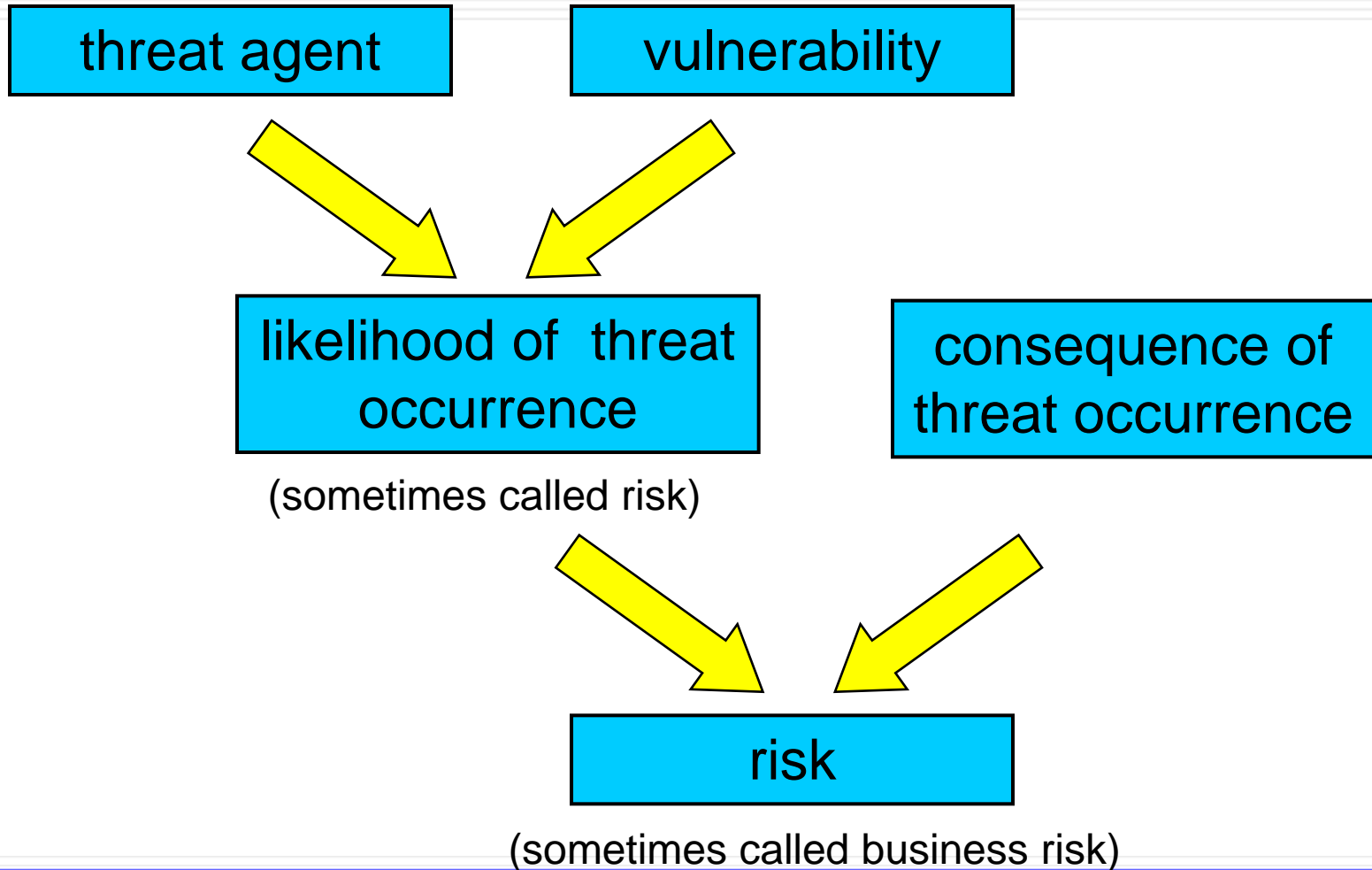
# What is risk?

---

- Not defined explicitly in
  - ISO/IEC 27002 (Risk assessment and risk management defined)
  - ISO/IEC 27001 (Risk acceptance, risk analysis, risk assessment, risk evaluation, risk management and risk treatment defined)but considered as “the combination of the likelihood (probability) of a threat occurrence, and its impact (consequence)”.
- Risk is assessed as a function of three variables:
  1. the probability that there is a threat
  2. the probability that there are any vulnerabilities
  3. the potential impact to the business.
  - The two probabilities are sometimes combined and are also known as likelihood. If any of these variables approaches zero, the overall risk approaches zero.
  - (source: Wikipedia)

# What is risk?

---

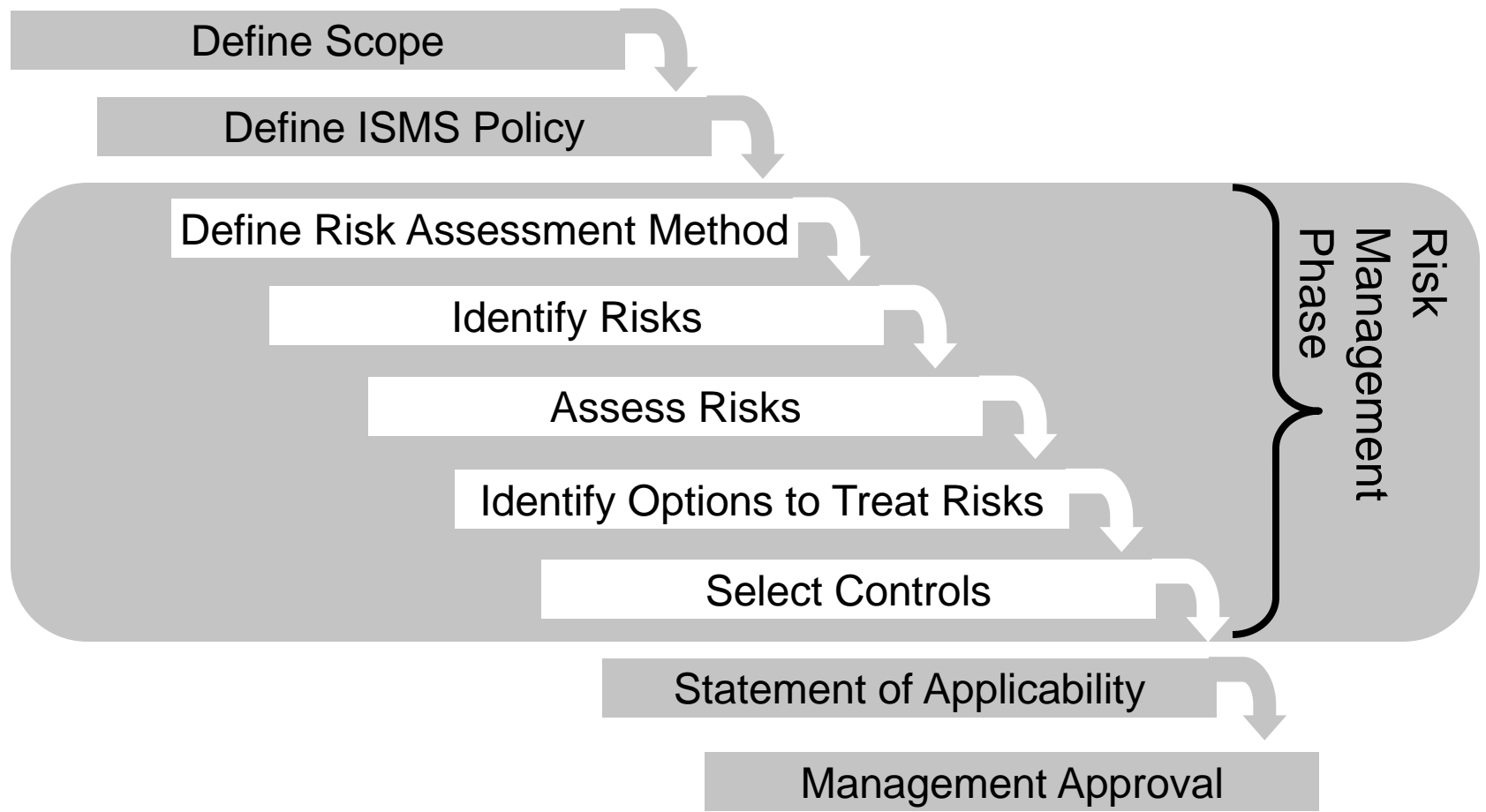


# What is risk management?

---

- “the process of identifying, assessing and reducing the risk to an acceptable level and implementing the right mechanisms to maintain that level of risk”
  - Shon Harris (author of CISSP Exam Guide)
- “the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.”
  - AS/NZS 4360:2004 p4
- “Coordinated activities to direct and control an organisation with regard to risk”
  - ISO/IEC 27002

# Risk Management in the ISMS PDCA: Establish the ISMS (Plan)





# Risk Identification and Control

---

- Risk management: process of identifying and controlling risks facing an organization
- Risk identification: process of examining an organization's current information technology security situation
- Risk control: applying controls to reduce risks to an organization's data and information systems

# An Overview of Risk Management

---

- Know yourself: identify, examine, and understand the information and systems currently in place
- Know the enemy: identify, examine, and understand threats facing the organization
- Responsibility of each community of interest within an organization to manage risks that are encountered

# The Roles of the Communities of Interest

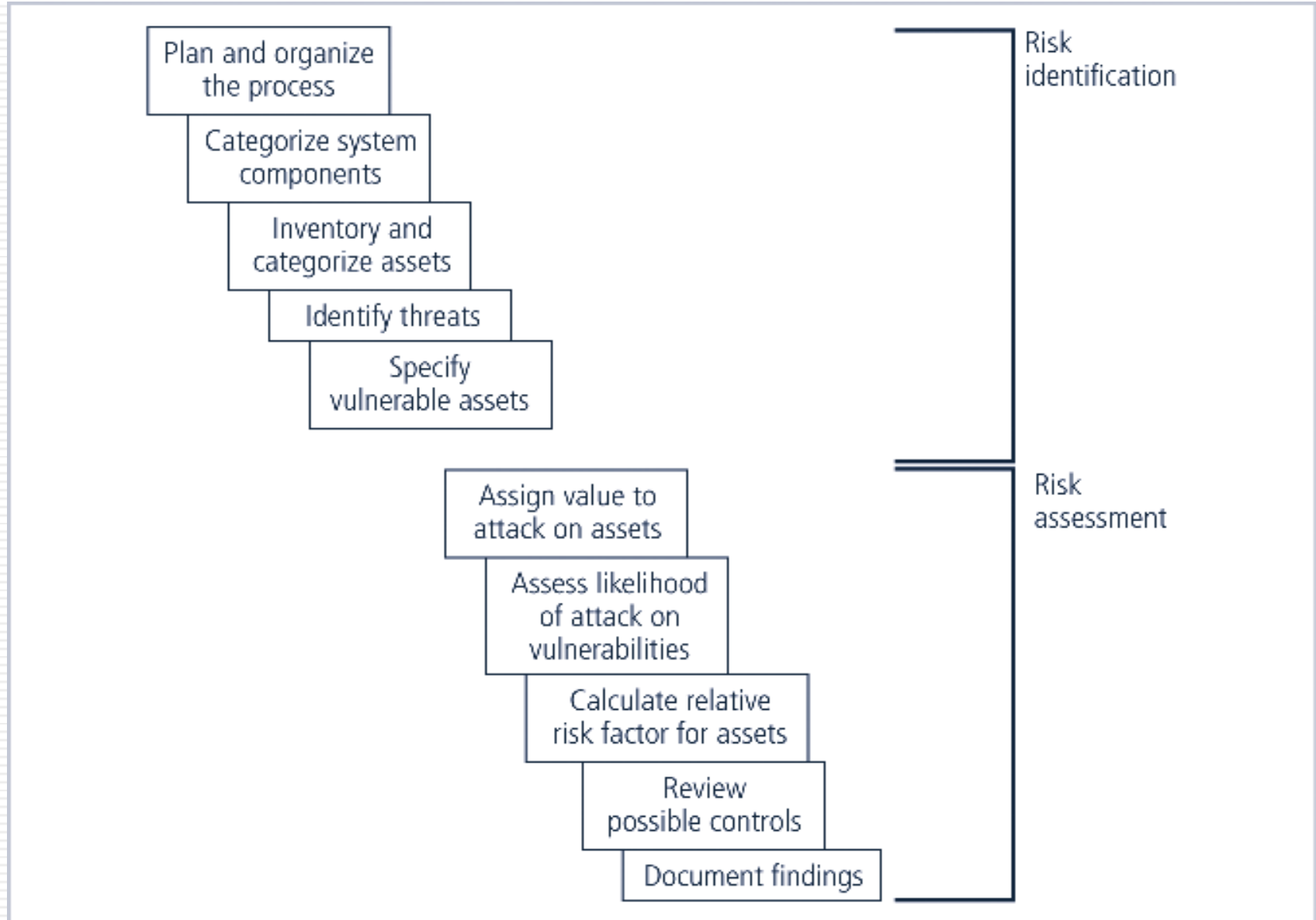
---

- Information security, management and users, and information technology all must work together
  - Assets 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 Identification

---

- Assets are targets of various threats and threat agents
- Risk management involves identifying organization's assets and identifying threats/vulnerabilities
- Risk identification begins with identifying organization's assets and assessing their value



**FIGURE 4-2** Components of Risk Identification

# Asset Identification, Valuation, and Prioritization

---

- Iterative process; begins with identification of assets, including all elements of an organization's system (people, procedures, data and information, software, hardware, networking)
- Assets are then classified and categorized

# People, Procedures, and Data Asset Identification

---

- Human resources, documentation, and data information assets are more difficult to identify
- People with knowledge, experience, and good judgment should be assigned this task
- These assets should be recorded using reliable data-handling process

# People, Procedures, and Data Asset Identification (continued)

---

- Asset attributes for people: position name/number/ID; supervisor; security clearance level; special skills
- Asset attributes for procedures: description; intended purpose; what elements it is tied to; storage location for reference; storage location for update
- Asset attributes for data: classification; owner/creator/manager; data structure size; data structure used; online/offline; location; backup procedures employed



# Hardware, Software, and Network Asset Identification

---

- What information attributes to track depends on:
  - Needs of organization/risk management efforts
  - Management needs of information security/information technology communities
- Asset attributes to be considered are: name; IP address; MAC address; element type; serial number; manufacturer name; model/part number; software version; physical or logical location; controlling entity

# Information Asset Classification

---

- Many organizations have data classification schemes (e.g., confidential, internal, public data)
- Classification of components must be specific to allow determination of priority levels
- Categories must be comprehensive and mutually exclusive

# Information Asset Valuation

---

- 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 most embarrassing or cause greatest liability if revealed?

# Information Asset Prioritization

---

- Create weighting for each category based on the answers to questions
- Calculate relative importance of each asset using weighted factor analysis
- List the assets in order of importance using a weighted factor analysis worksheet

**TABLE 4-2** Example of a Weighted Factor Analysis Worksheet

Information asset	Criteria 1: impact to revenue	Criteria 2: impact to profitability	Criteria 3: public image impact	Weighted score
<i>Criterion Weight (1-100)</i> <i>Must total 100</i>	30	40	30	
EDI Document Set 1— Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2— Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2— Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Notes: EDI: Electronic Data Interchange  
SSL: Secure Sockets Layer

# Data Classification and Management

---

- Variety of classification schemes used by corporate and military organizations
- Information owners responsible for classifying their information assets
- Information classifications must be reviewed periodically
- Most organizations do not need detailed level of classification used by military or federal agencies; however, organizations may need to classify data to provide protection

# Threat Identification

---

- Realistic threats need investigation; 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 requires greatest expenditure to prevent?

**TABLE 4-3** Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

©2003 ACM, Inc., Included here by permission.



# Vulnerability Identification

---

- Specific avenues threat agents can exploit to attack an information asset are called vulnerabilities
- Examine how each 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

# Risk Assessment

---

- Risk assessment evaluates the relative risk for each vulnerability
- Assigns a risk rating or score to each information asset

# Assess risks

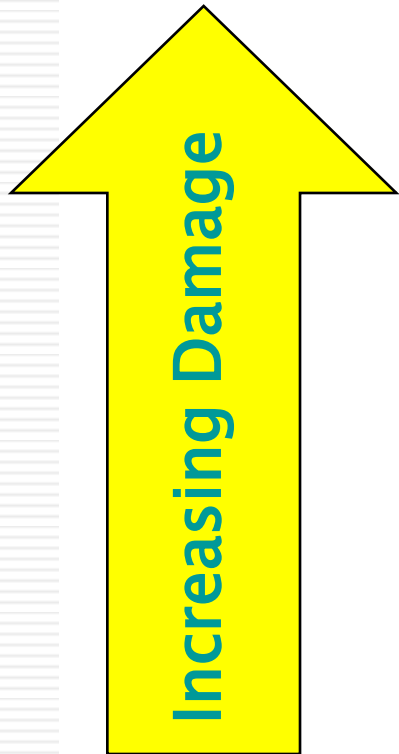
---

## Types of analysis

- **Qualitative**
  - Uses descriptive scales. **Example:**
    - **Consequence:** 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 Risk Analysis Example

## Qualitative Consequence scale

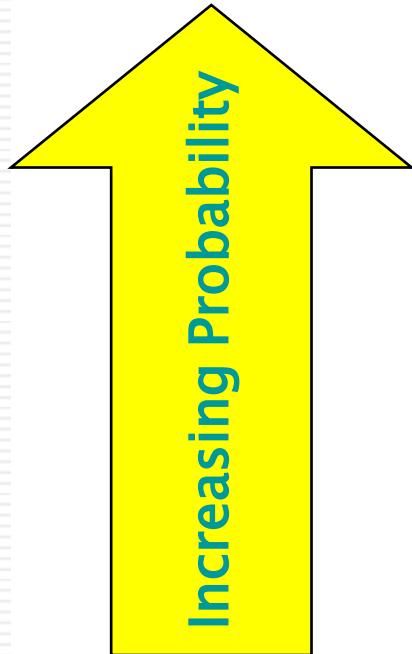


Measure	Description
Major	<b>Major problems</b> would occur and threaten the provision of important processes <b>resulting in significant financial loss.</b>
Moderate	<b>Services would continue</b> , but would <b>need to be reviewed or changed.</b>
Minor	Effectiveness of services would be <b>threatened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

# Qualitative Risk Analysis Example

---

## Qualitative Likelihood scale



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

# Qualitative Risk Analysis Example

**Qualitative Level of Risk** example: Match consequences to likelihoods to determine levels of risk

## Consequence

	Insignificant	Minor	Moderate	Major
High	M	H	E	E
Medium	M	M	H	E
Low	L	M	M	H
Unlikely	L	L	M	M

Legend

**E: extreme risk**; immediate action required

**H: high risk**; senior management attention needed

**M: moderate risk**; management responsibility must be specified

**L: low risk**; manage by routine procedures

# Quantitative Risk Analysis 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 Analysis 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

# Set Priorities

---

## Risk register

Risk Description	Risk Assessment		Existing controls	Impact Rating	Likelihood Rating	Level of Risk	Risk priority
	Threat	Probability					
<b>Router Compromise</b>	Intrusion, Disruption	Many times per year	Password Only	<b>MODERATE</b>	<b>HIGH</b>	<b>HIGH</b>	<b>?</b>
<b>Physical Destruction of Data Centre</b>	Operations Disrupted for one month	Once in 25 Years	None (Not addressed in BCP)	<b>MAJOR</b>	<b>LOW</b>	<b>HIGH</b>	<b>?</b>

Source: Mark Ames' (Suncorp) seminar on Managed Risk- Effective Security

# AS/NZS 4360: Treat risks

---

Identifying options for risk treatment with **positive** outcomes

- Options include:
  - **Actively seek** an opportunity
  - **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

# AS/NZS 4360: Treat risks

---

Identifying options for risk treatment with **negative** outcomes

- Options include:
  - **Avoid** the risk
  - **Reducing** the likelihood of negative outcome by changing
    - the likelihood of the risk
    - the consequences
  - **Sharing** the risk
  - **Retaining** the risk

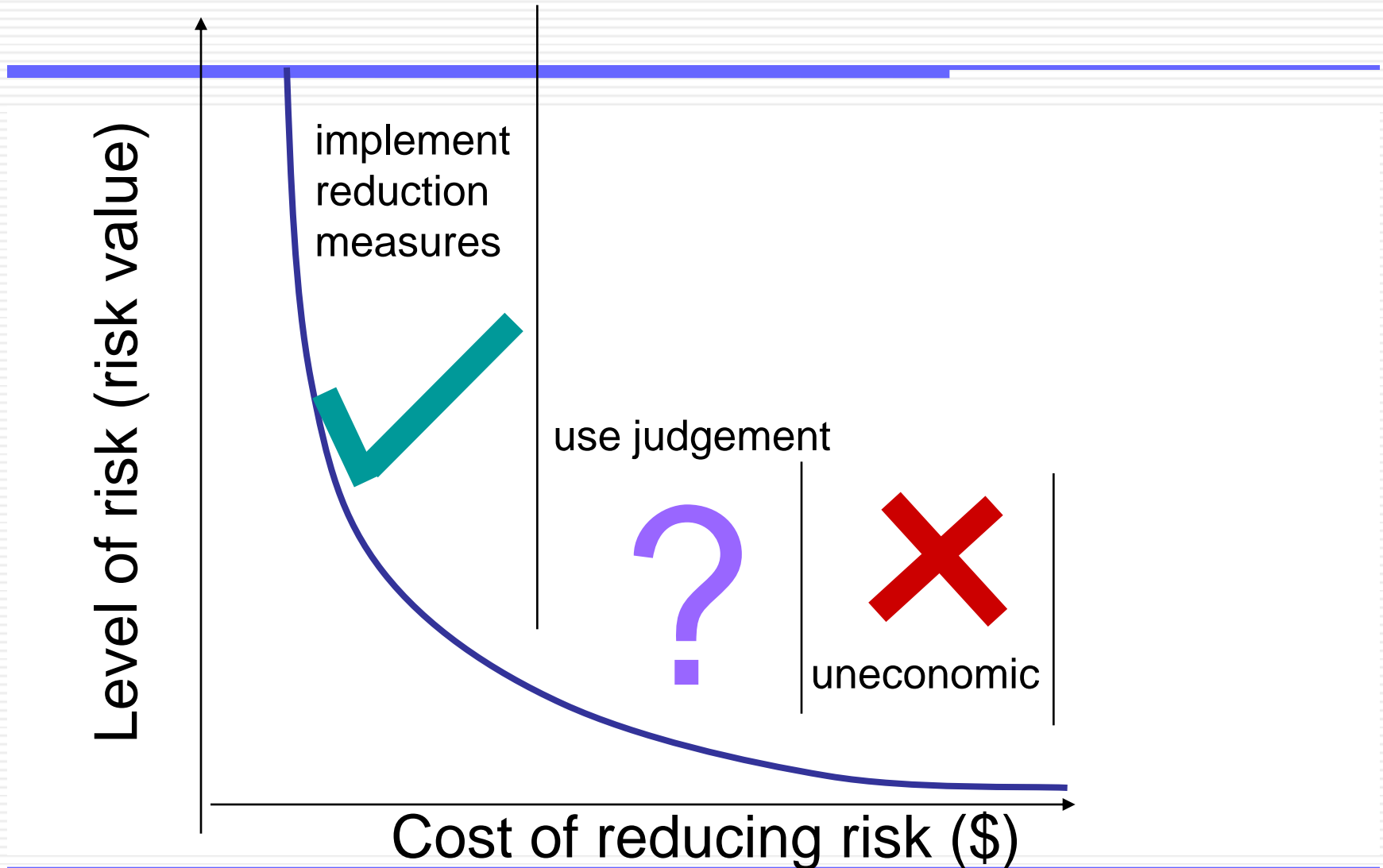
# AS/NZS 4360: Treat risks

---

## Assessing risk treatment options

- Assess based on the extent of risk reduction, and any additional benefits obtained
  - High risk levels may be acceptable if beneficial opportunities arise as a result of taking the risk
- Balance cost of implementing treatment option and benefits derived (proportionality principle)
  - Large risk reductions for low expenditure should be implemented

# Risk treatment prioritising



# Identify Possible Controls

---

- For each threat and associated vulnerabilities that have residual risk, create preliminary list of control ideas
- Residual risk is risk that remains to information asset even after existing control has been applied

# Access Controls

---

- Specifically address admission of a user into a trusted area of organization
- Access controls can be:
  - Mandatory access controls (MAC): give users and data owners limited control over access to information
  - Nondiscretionary controls: managed by central authority in organization; can be role-based or task-based
  - Discretionary access controls (DAC): implemented at discretion or option of data user



# 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 Control Strategies

---

- Once ranked vulnerability risk worksheet complete, must choose one of four strategies to control each risk:
  - Apply safeguards (avoidance)
  - Transfer the risk (transference)
  - Reduce impact (mitigation)
  - Understand consequences and accept risk (acceptance)

# Avoidance

---

- Attempts to prevent exploitation of the vulnerability
- Preferred approach; accomplished through countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards
- Three common methods of risk avoidance:
  - Application of policy
  - Training and education
  - Applying technology

# Transference

---

- Control approach that attempts to shift risk to other assets, processes, or organizations
- If lacking, organization should hire individuals/firms that provide security management and administration expertise
- Organization may then transfer risk associated with management of complex systems to another organization experienced in dealing with those risks

# Mitigation

---

- Attempts to reduce impact of vulnerability exploitation through planning and preparation
- Approach includes three types of plans:
  - Incident response plan (IRP)
  - Disaster recovery plan (DRP)
  - Business continuity plan (BCP)

# Mitigation (continued)

---

- DRP is most common mitigation procedure
- The actions to take while incident is in progress is defined in IRP
- BCP encompasses continuation of business activities if catastrophic event occurs

# Acceptance

---

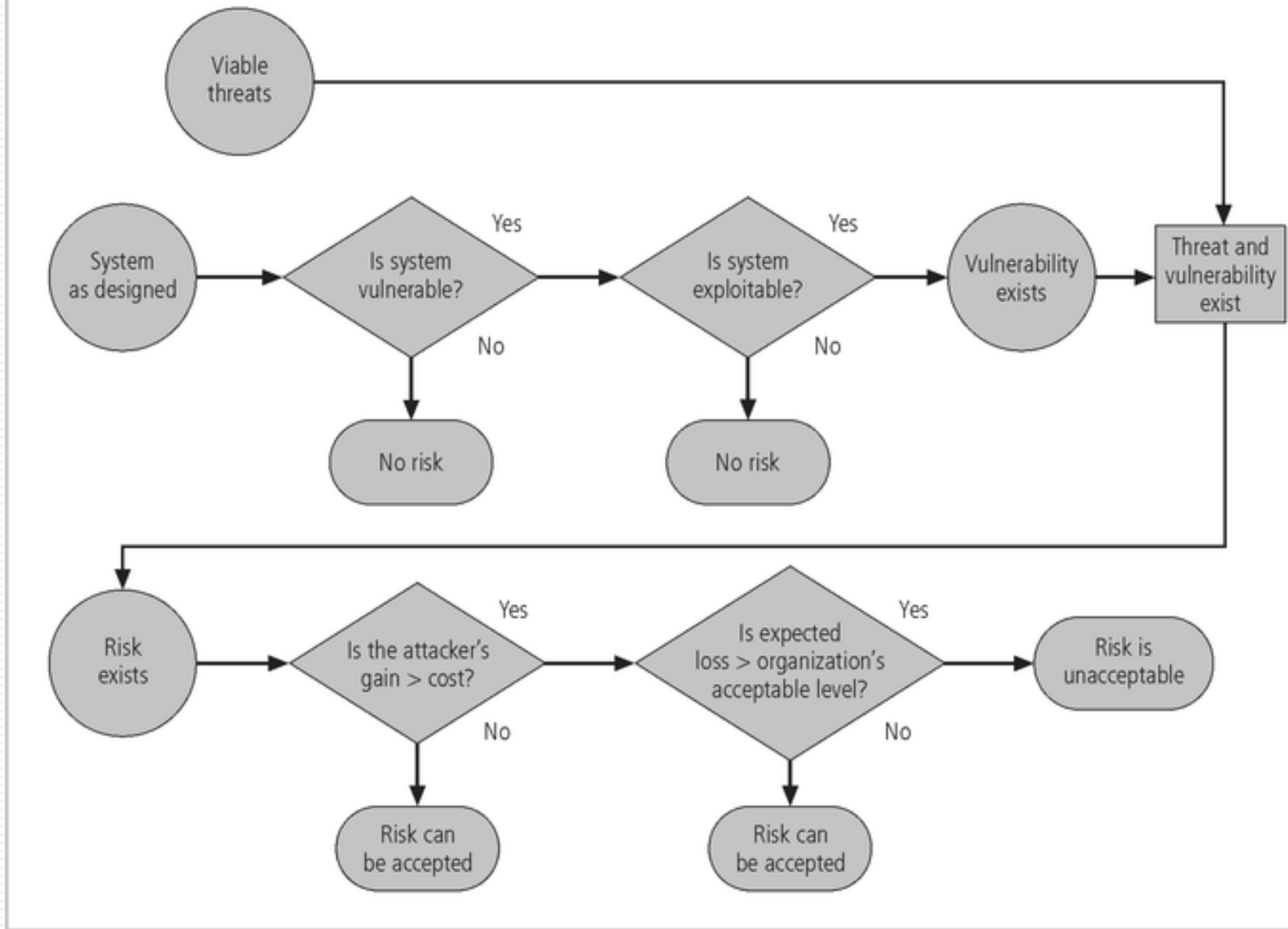
- Doing nothing to protect a vulnerability and accepting the outcome of its exploitation
- Valid only when the particular function, service, information, or asset does not justify cost of protection
- Risk appetite describes the degree to which organization is willing to accept risk as trade-off to the expense of applying controls

# Selecting a Risk Control Strategy

---

- Level of threat and value of asset play major role in selection of strategy
- Rules of thumb on strategy selection can be applied:
  - When a vulnerability exists
  - When a vulnerability can be exploited
  - When attacker's cost is less than potential gain
  - When potential loss is substantial





**FIGURE 5-2** Risk Handling Decision Points<sup>7</sup>

# Feasibility Studies

---

- Before deciding on strategy, all information about economic/non-economic consequences of vulnerability of information asset must be explored
- A number of ways exist to determine advantage of a specific control

# Cost Benefit Analysis (CBA)

---

- Most common approach for deciding on information security controls is economic feasibility of implementation
- CBA is begun by evaluating worth of assets to be protected and the loss in value if those assets are compromised
- The formal process to document this is called cost benefit analysis or economic feasibility study

# Cost Benefit Analysis (CBA)

## (continued)

---

- Items that affect cost of a control or safeguard include: cost of development or acquisition; training fees; implementation cost; service costs; cost of maintenance
- Benefit is the value an organization realizes by using controls to prevent losses associated with a vulnerability
- Asset valuation is process of assigning financial value or worth to each information asset; there are many components to asset valuation

# Cost Benefit Analysis (CBA)

## (continued)

---

- Once value of assets is estimated, potential loss from exploitation of vulnerability is studied
- Process result is estimate of potential loss per risk
- Expected loss per risk stated in the following equation:  
Annualized loss expectancy (ALE) equals  
Single loss expectancy (SLE) TIMES  
Annualized rate of occurrence (ARO)
- SLE is equal to asset value times exposure factor (EF)

# The Cost Benefit Analysis (CBA) Formula

---

- CBA determines if alternative being evaluated is worth cost incurred to control vulnerability
- CBA most easily calculated using ALE from earlier assessments, before implementation of proposed control:

$$\text{CBA} = \text{ALE}(\text{prior}) - \text{ALE}(\text{post}) - \text{ACS}$$

- ALE(prior) is annualized loss expectancy of risk before implementation of control
- ALE(post) is estimated ALE based on control being in place for a period of time
- ACS is the annualized cost of the safeguard

# Evaluation, Assessment, and Maintenance of Risk Controls

---

- Selection and implementation of control strategy is not end of process
- Strategy and accompanying controls must be monitored/reevaluated on ongoing basis to determine effectiveness and to calculate more accurately the estimated residual risk
- Process continues as long as organization continues to function

# Business Continuity Planning

---



# Business continuity management

---

- Establishes a strategic and operational framework to implement, proactively, an organization's resilience to disruption, interruption or loss in conducting its business.
- Defines 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
- Typically, BC management involves an analysis of critical business processes and continuity needs
- May also include a significant focus on disaster prevention

# 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

# Business continuity management

---

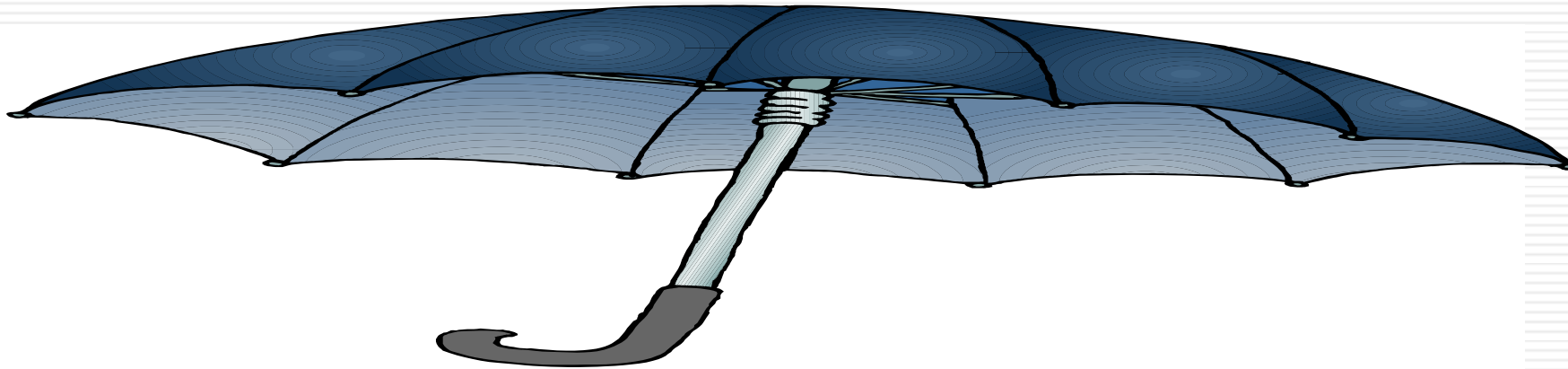
- How common is BCM in ‘the real world’?
- 2006 CCSS extract: Most commonly reported categories of computer security policies and procedures 2006 (2005, 2004):
  - Media backup procedures - 95% (96%, 95%)
  - User access management - 93% (97%, 94%)
  - External network access control procedures - 78% (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 management



**BUSINESS CONTINUTITY PLAN**

**INCIDENT RESPONSE**

**RISK MGMT**

**DISASTER RECOVERY**

**HEALTH & SAFETY**

**ENVIRONMENT PROTECTION**

**EMERGENCY MGMT**

**SECURITY**

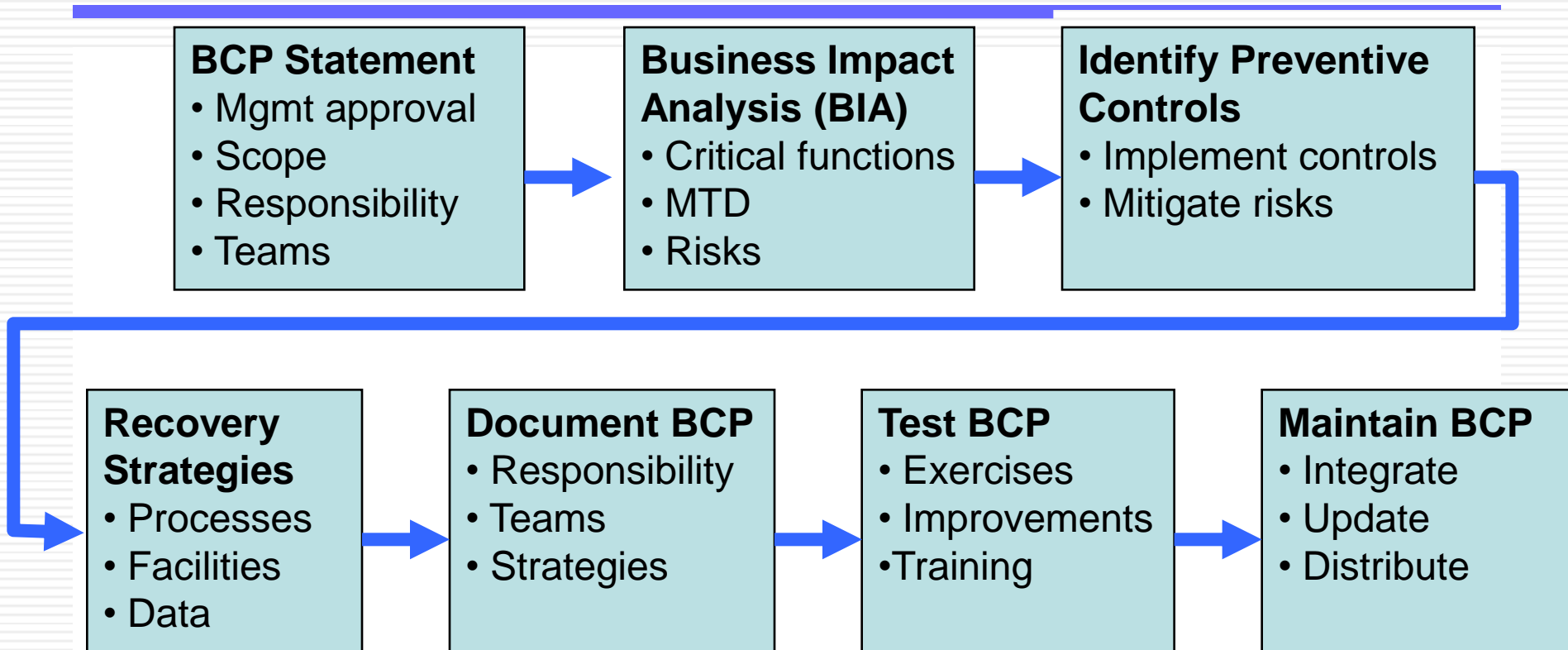
**CRISIS COMMUNICATIONS & P.R.**

# Business Continuity Plan (BCP)



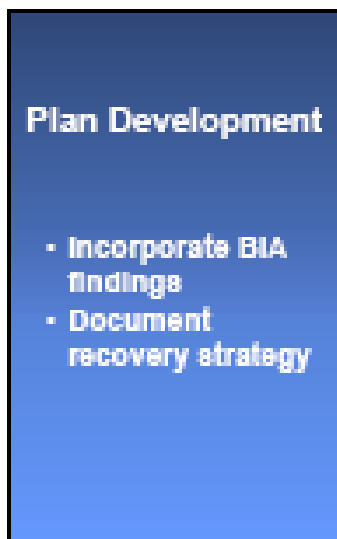
- The business continuity plan describes:
  - a sequence of actions
  - and the parties responsible for carrying them out
  - in response to disasters
  - in order to restore normal business operations as quickly as possible

# BCP Development



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

## Development



### 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

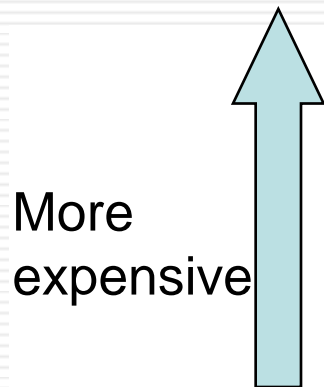
# BCP Development - BIA

---

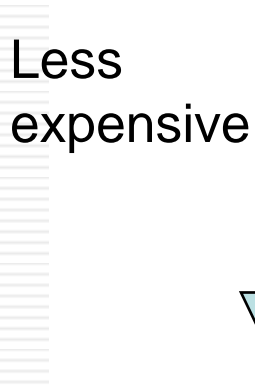
- The MTD (Maximum Tolerable Downtime) is defined for each function in the event of disaster.
- Example:
  - Non-essential = 30 days
  - Normal = 7 days
  - Important = 72 hours
  - Urgent = 24 hours
  - Critical = minutes to hours

# BCP Development - Alternative Sites

---



- 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

# BCP 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

# BCP Recovery Phase Plans

---

- 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



# BCP 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

# ISO/IEC 27002 Section 14

---

- **Objective:** *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.*
- *A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets reduce the disruption caused by disasters and security failures ... to an acceptable level through a combination of preventative and recovery controls.*

# ISO/IEC 27002 Section 14

---

- There should be a managed process in place for developing and maintaining business continuity throughout the organisation. ...key elements of BCM include:
  - Understanding the risks in terms of likelihood and impact
  - Understanding the impact interruptions have on business
  - Considering the purchase of suitable insurance
  - Identifying additional preventive and mitigating controls
  - Formulating and documenting business continuity plans
  - Regular testing and updating of the plans and processes
  - Ensuring BCM is incorporated in organization's processes and structure

---

End of Lecture