

INF3510 Information Security
University of Oslo
Spring 2012

Lecture 3

Risk Management and
Business Continuity Planning



Audun Jøsang

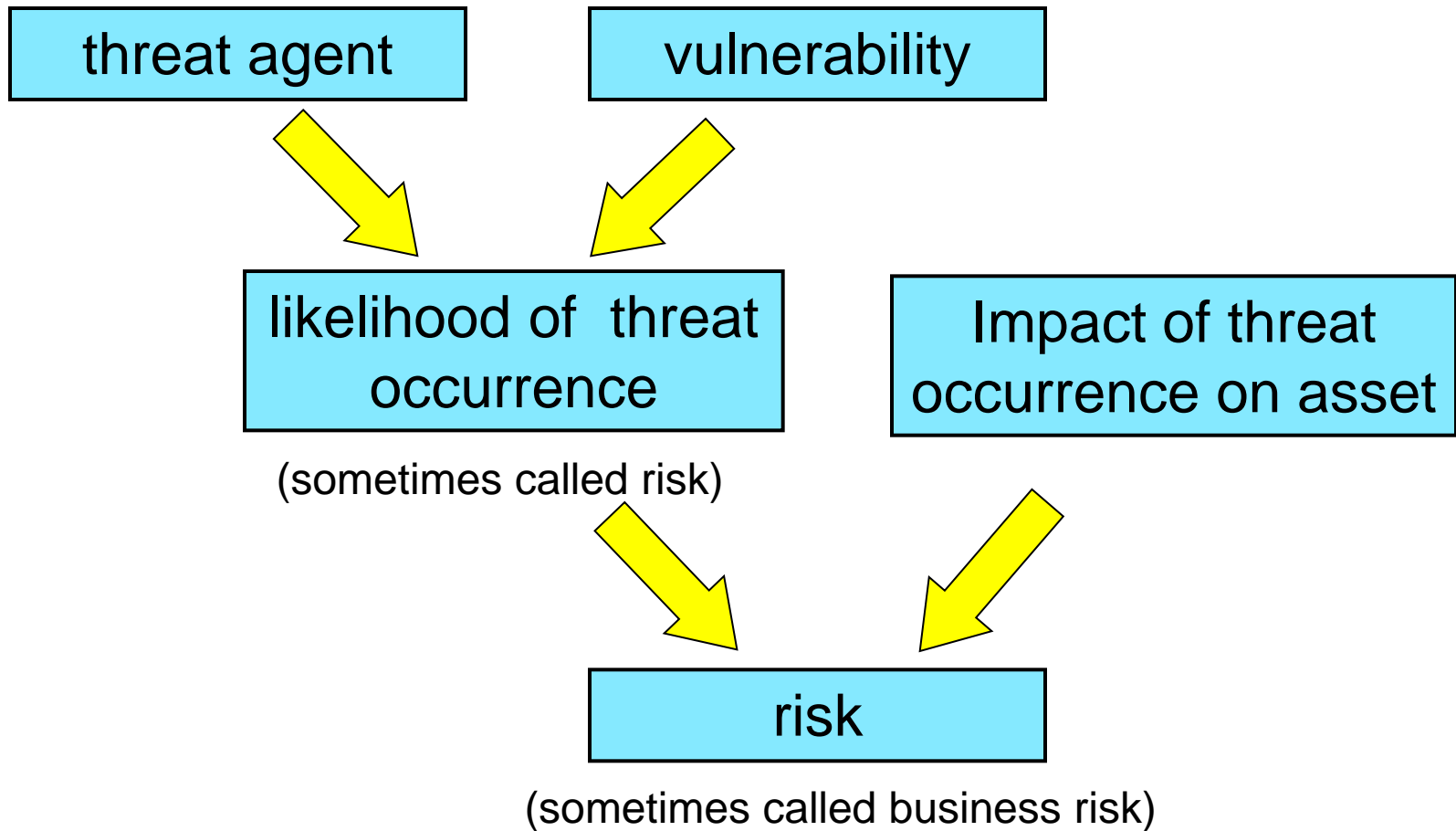
Frameworks for risk management and BCP

- Risk Management standards and guidelines
 - ISO 27005 Information security risk management
 - ISO31000 Risk Management
 - NIST SP800-39 Managing Information Security Risk
 - NIST SP800-30 Guide for Conducting Risk Assessment
 - ISO 27002 Section 4
- Business Continuity Planning guidelines
 - ISO 27031 Guidelines for information and communications technology readiness for business continuity
 - NISTSP800-34 Contingency Planning Guide for Information Technology Systems
 - ISO 27002 Section 14

What is risk?

- Risk is assessed as a function of three variables:
 1. Strength of threat agent (e.g. incentive & capability to attack)
 2. Presence (severity) of vulnerabilities
 3. Potential impact of threat occurrence to the business.
 - Elements 1) and 2) are typically combined in the form of likelihood of threat occurrence. If any of these variables approaches zero, the overall risk also approaches zero.
- Not defined explicitly in
 - ISO 27001, 27002 or 27005 (but they define “risk assessment” and “risk management”, “risk acceptance”, “risk analysis”, “risk assessment”, “risk evaluation”, “risk management” and “risk treatment”)but is interpreted as “the combination of the likelihood (probability) of a threat occurrence, and its impact (consequence)”.

What is risk?



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.”
 - ISO 31000 , ISO 27002

Problems of measuring risk

Businesses normally wish to measure risk in monetary value, but this is difficult for many reasons:

- Valuation of assets
 - Value of data and in-house software - no market value
 - Value of goodwill and customer confidence
- Likelihood of threats
 - How relevant is past data to the calculation of future probabilities?
 - The nature of future attacks is unpredictable
 - The actions of future attackers are unpredictable
- Measurement of benefit from security measures
 - Problems with the difference of two approximate quantities
 - How does an extra security measure affect a $\sim 10^{-5}$ probability of attack?

Roles involved in risk management

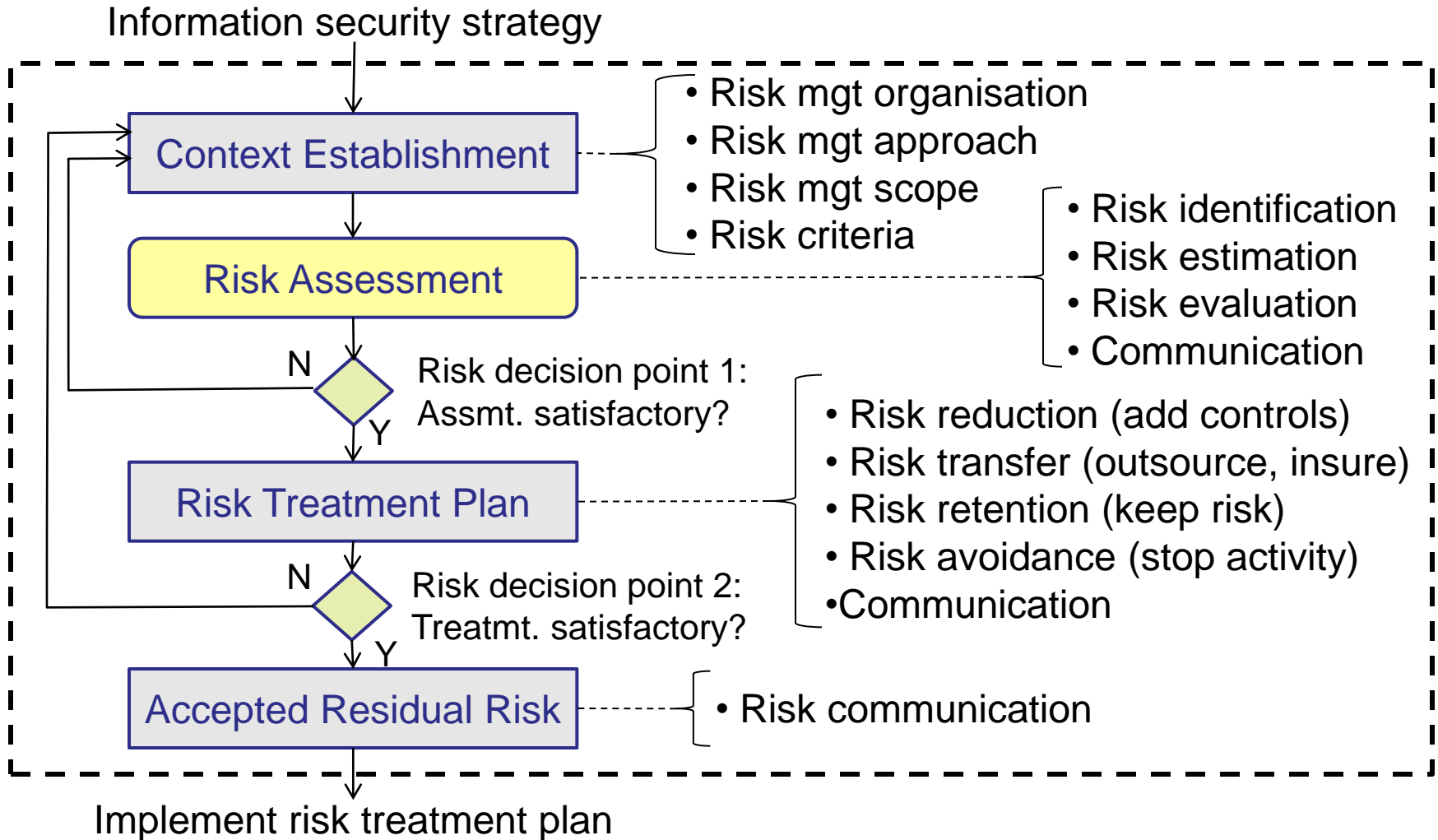
- Management, users, and information technology must all work together
 - Asset owners must participate in developing inventory lists
 - Users and domain experts must assist in identifying threats and vulnerabilities, and in determining likelihoods
 - Risk management experts must guide stakeholders through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

ISMS (information Security Management System) PDCA cycle and Risk management

ISMS Phase	Risk management elements
Plan	Risk management process
Do	Implement risk treatment plan
Check	Monitor and review risk environment
Act	Maintain and improve risk management process

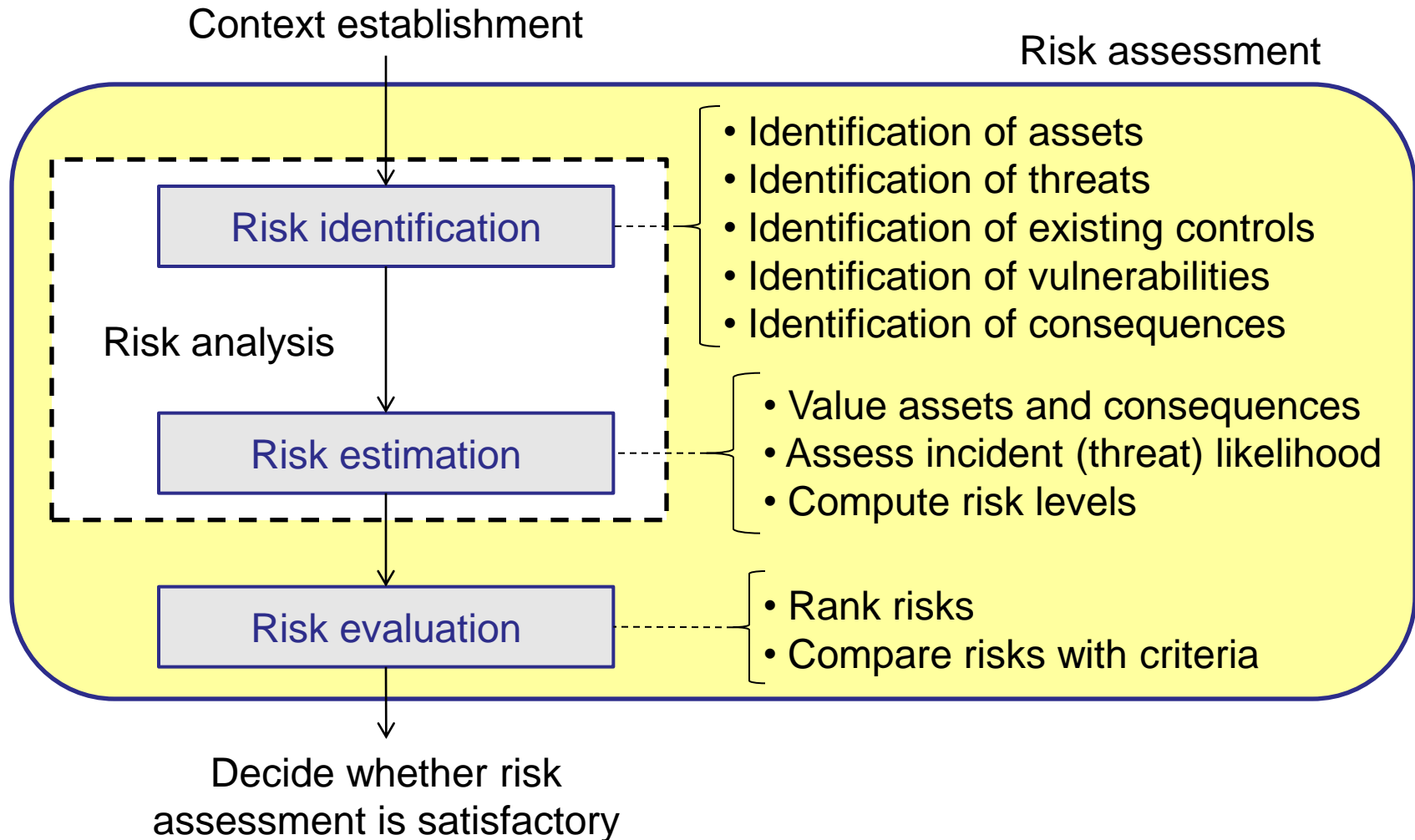
Risk management process

ISO 27005



Risk assessment process

ISO 27005



Risk Identification

- Assets are targets of various threat agents
- Risk management involves identifying organization's assets and identifying possible incidents caused by threat agents exploiting vulnerabilities
- Risk identification begins with identifying organization's assets and assessing their value

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

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

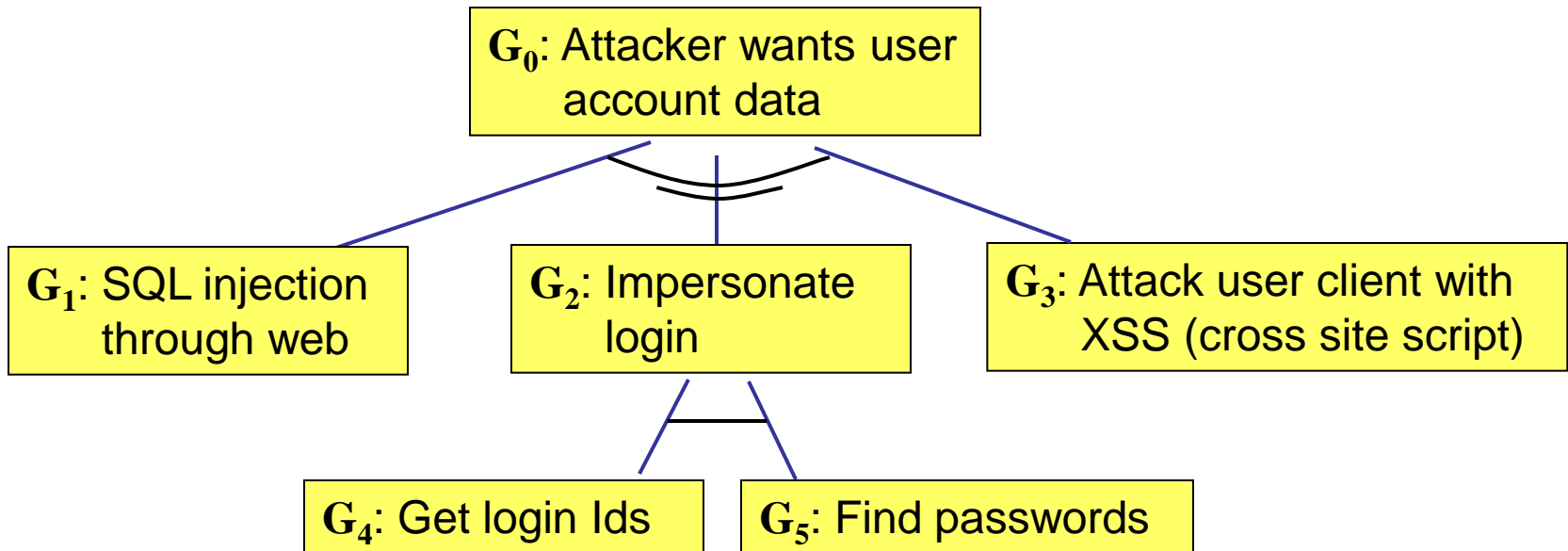
Data Classification and Management

- 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 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:

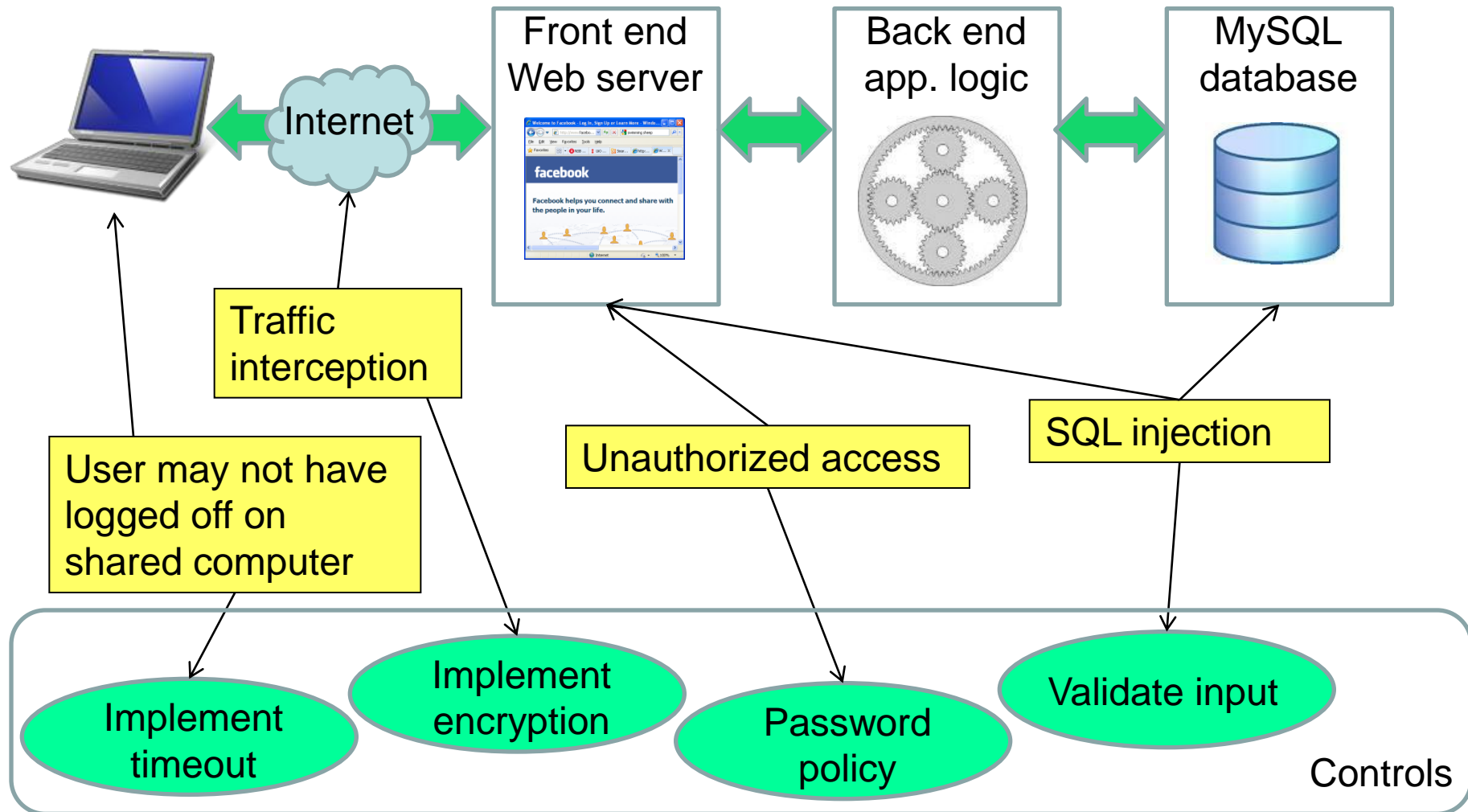
G_0 : Main goal

— AND (conjunctive)
all subgoals needed

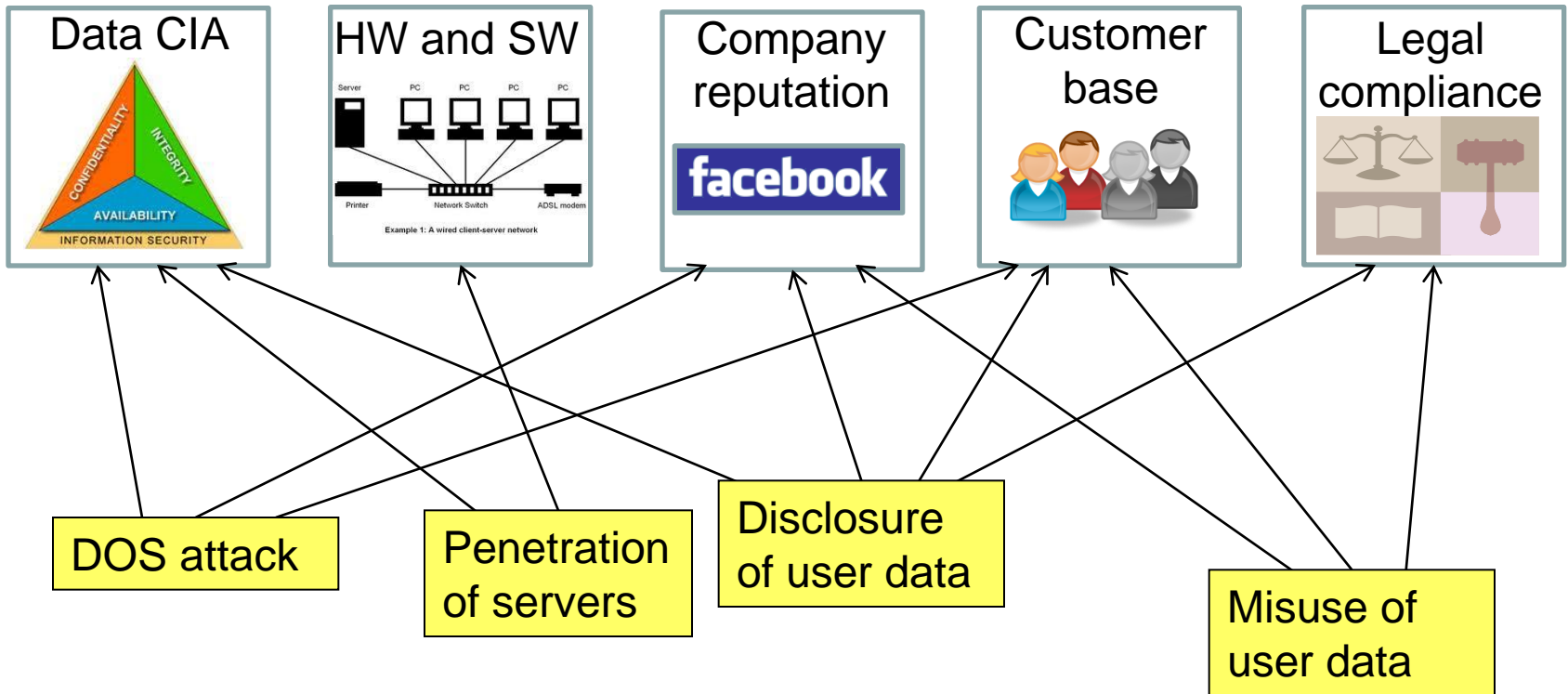
≅ OR (disjunctive)
any subgoal needed

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



Incident / threat identification

- Realistic incidents / threats need consideration; unimportant incidents / threats are set aside
- Questions help to identify threats:
 - Which incidents/threats can affect assets?
 - Which incidents/threats represent the most danger to information and assets?
 - How much would it cost to recover from attack?
 - Which incidents/ threat are most expensive to prevent?

TABLE 4-3 Threats to Information Security

Example threats

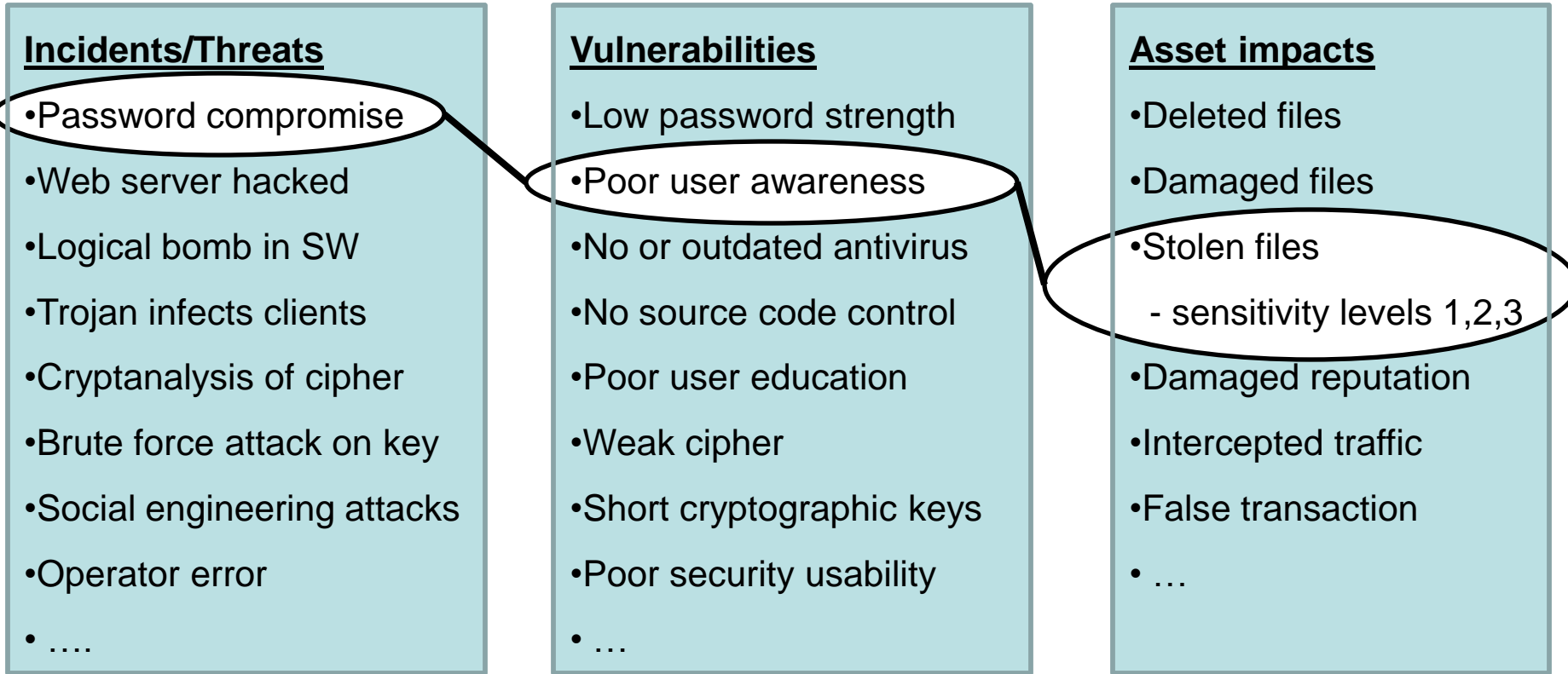
Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
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 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 risks



- Identify valid combinations of incident, vulnerability and asset impact

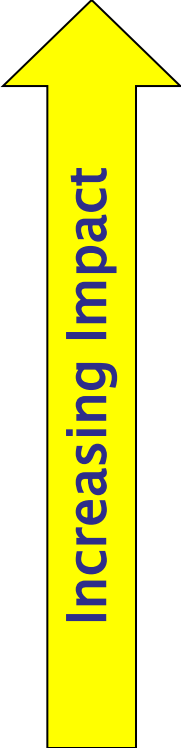
Estimate risks

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 risk estimation example

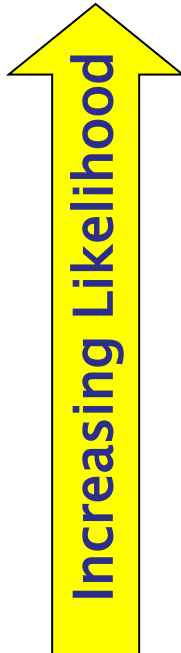
Qualitative Impact level scale



Impact Level	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 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 (2 years).
Low	The event should happen at some time (5 years).
Unlikely	The event could happen at some time (10 years).

Qualitative risk estimation example

Additive risk derivation: Add likelihood & impact level

		Impact 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

Multiplicative risk derivation: : Multiply likelihood & impact

Impact level

		Impact level				
		(0) Nil	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major
Likelihood	(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

Legend

M: moderate risk; Responsibility must be specified

L: low risk; Manage by routine procedures

VL: very low risk; Manage by routine procedures

Neg: negligible risk; Can be ignored

Nil: nil risk; No risk exists, ignore

E: extreme risk; Immediate action required

VH: very high risk; Priority action action

H+: high risk +; Management attention

H: high risk; Management attention

M+: moderate risk +; Responsibility must be specified

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

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

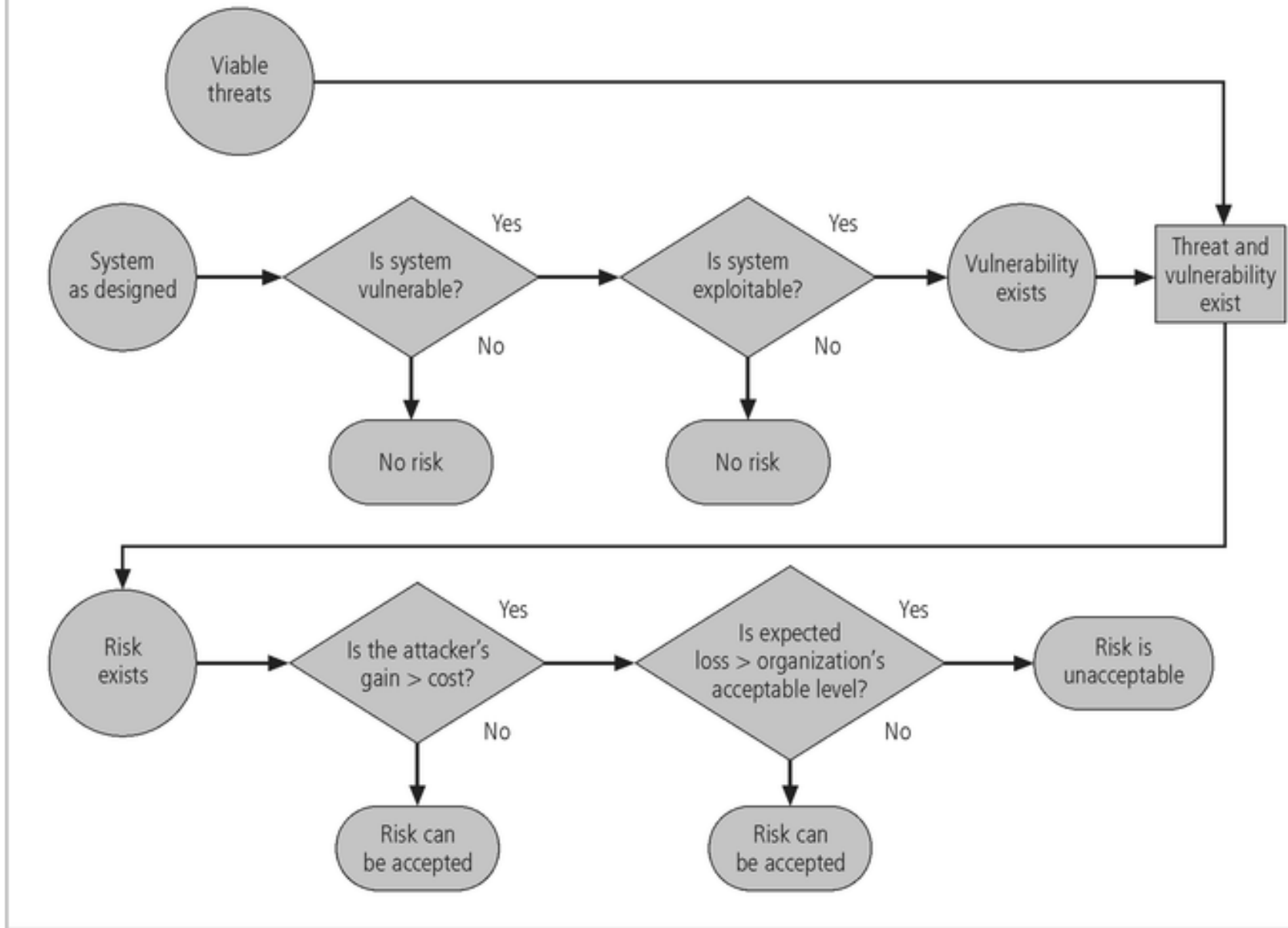


FIGURE 5-2 Risk Handling Decision Points⁷

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

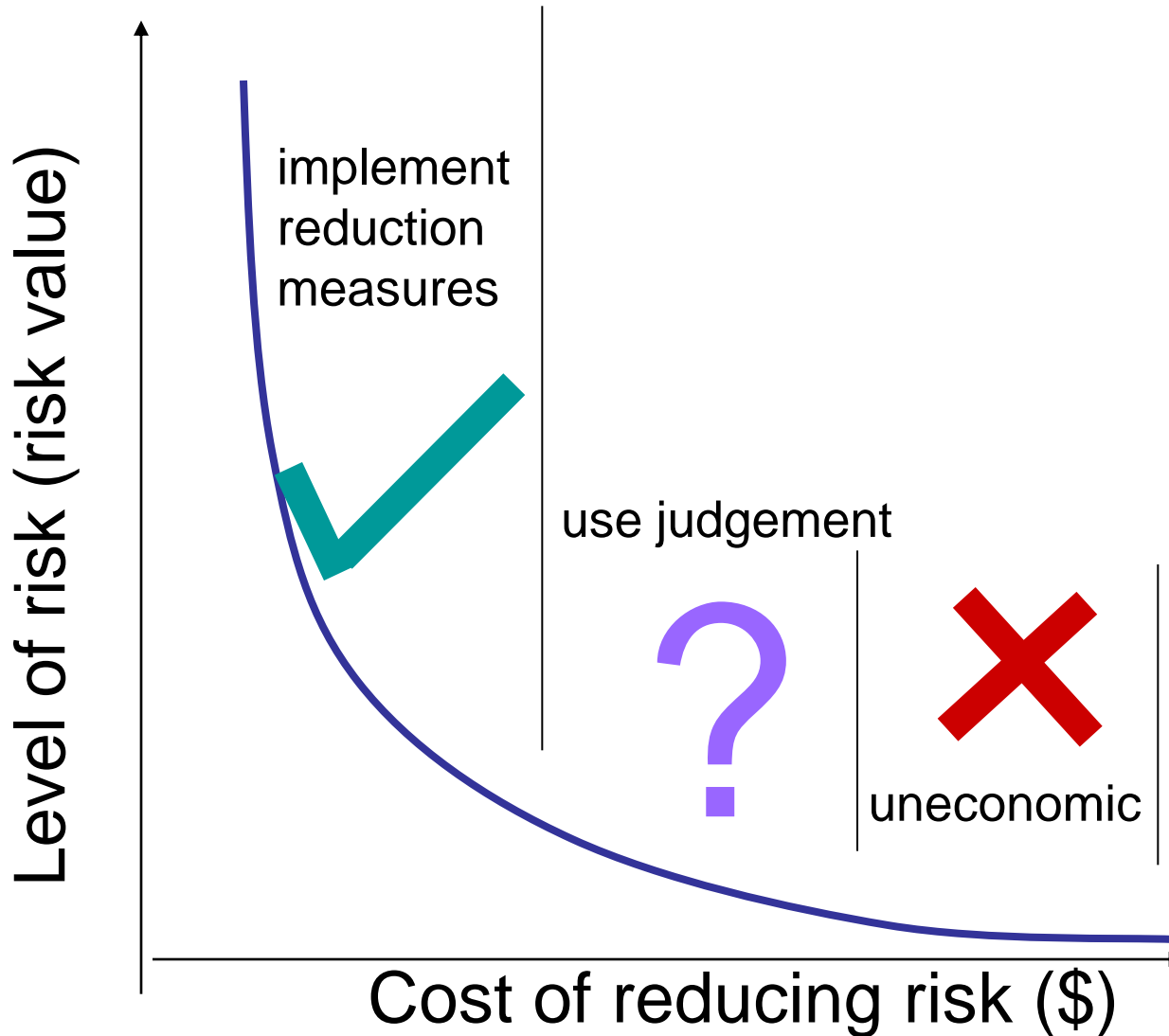
Risk Control Strategies

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

Treat risks economically

- Assess risk treatment 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 economy



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) Formula

- CBA determines if alternative being evaluated is worth cost incurred to control vulnerability
- Calculated using ALE assessed before and after implementation of proposed control.
- 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 (control)

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

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
 - **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

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
- Implement metrics for measuring effectiveness of controls
- 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

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%)

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 Plan (BCP)



From end of
disaster ...



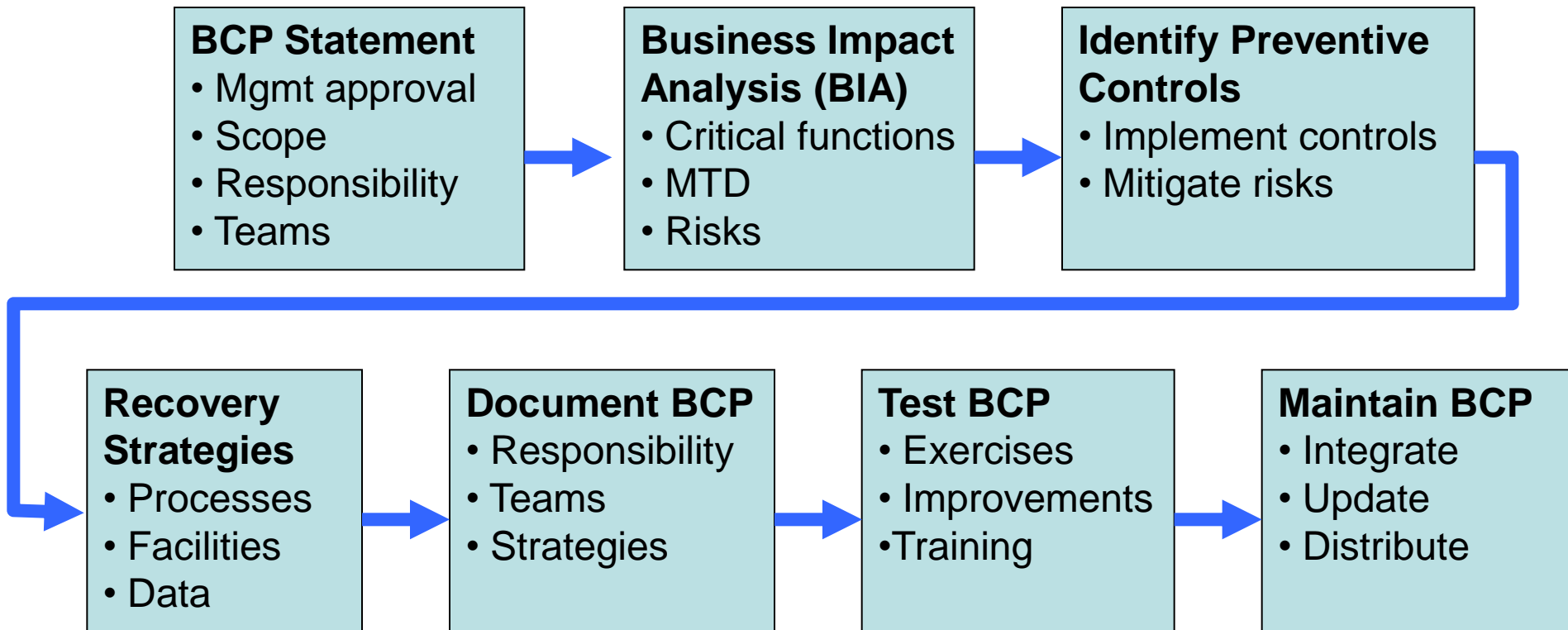
... to back in
business

- 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

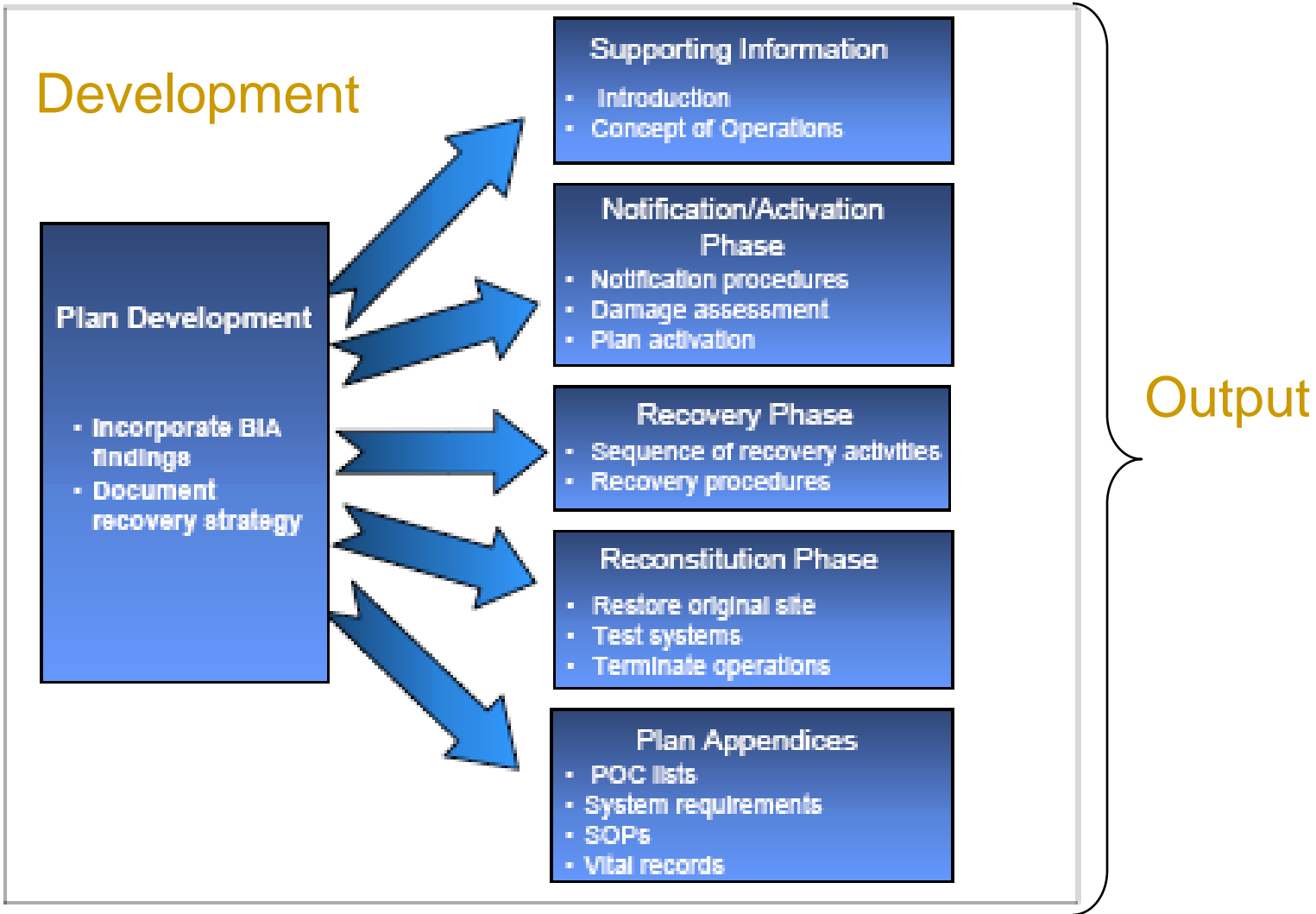
Business continuity management

- 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

BCP Development



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



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

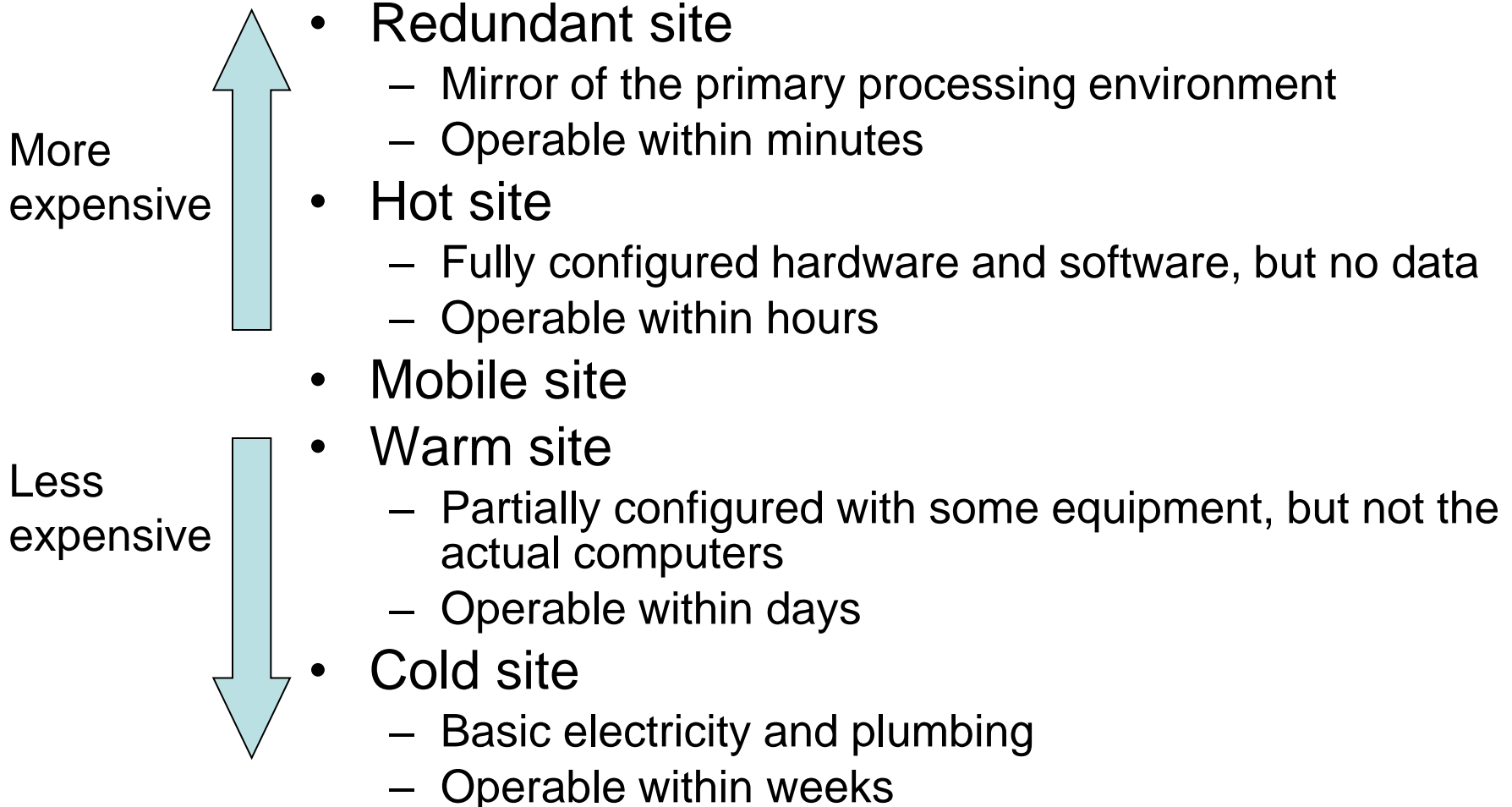
BCP Development - BIA

- 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

- 
- The diagram illustrates the relationship between site types and their associated costs and operational readiness. On the left, two vertical arrows indicate the cost spectrum: an upward-pointing arrow labeled 'More expensive' and a downward-pointing arrow labeled 'Less expensive'. To the right of these arrows, a list of site types is provided, each with its characteristics and operational timeframes. The site types are ordered from most expensive at the top to least expensive at the bottom.
- **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 bureauswith respect to BIA, cost, restoration time and practicality

Data backup alternatives

- Full backup every time.
 - Takes long to make each backup
 - Simple to reinstall in one operation
- Differential backup: First a full backup, then at regular intervals backup changed files since last full backup
 - Time for differential backup increases linearly until new full backup.
 - Reinstall in two operations, first last full backup, then last differential
- Incremental backup: First full backup, then at regular intervals backup changed files since last incremental backup.
 - Time to make incremental backup always small.
 - Reinstallation is complex, first last full backup, then apply all subsequent incremental backups.

Electronic data backup

- Disk shadowing/mirroring: multiple disks have same data
 - Provides high availability and load sharing
 - Expensive in equipment and network usage
- Electronic Vaulting: Backup kept at remote site, modified files copied to backup in batch jobs
 - A form of backup that avoids manual handling of tapes and disks
- Electronic journaling: real-time transmission of transaction logs to remote site, which enables implementation of changes to database at remote site.

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