GJØVIK UNIVERSITY COLLEGE

Security planning and Incident Management

Marie Moe, NSM/HiG

Gjøvik 27.01.14

AGENDA

Risk Management

- *Identify and explain the basic concepts of risk management*
- *Discuss its interface with related disciplines*

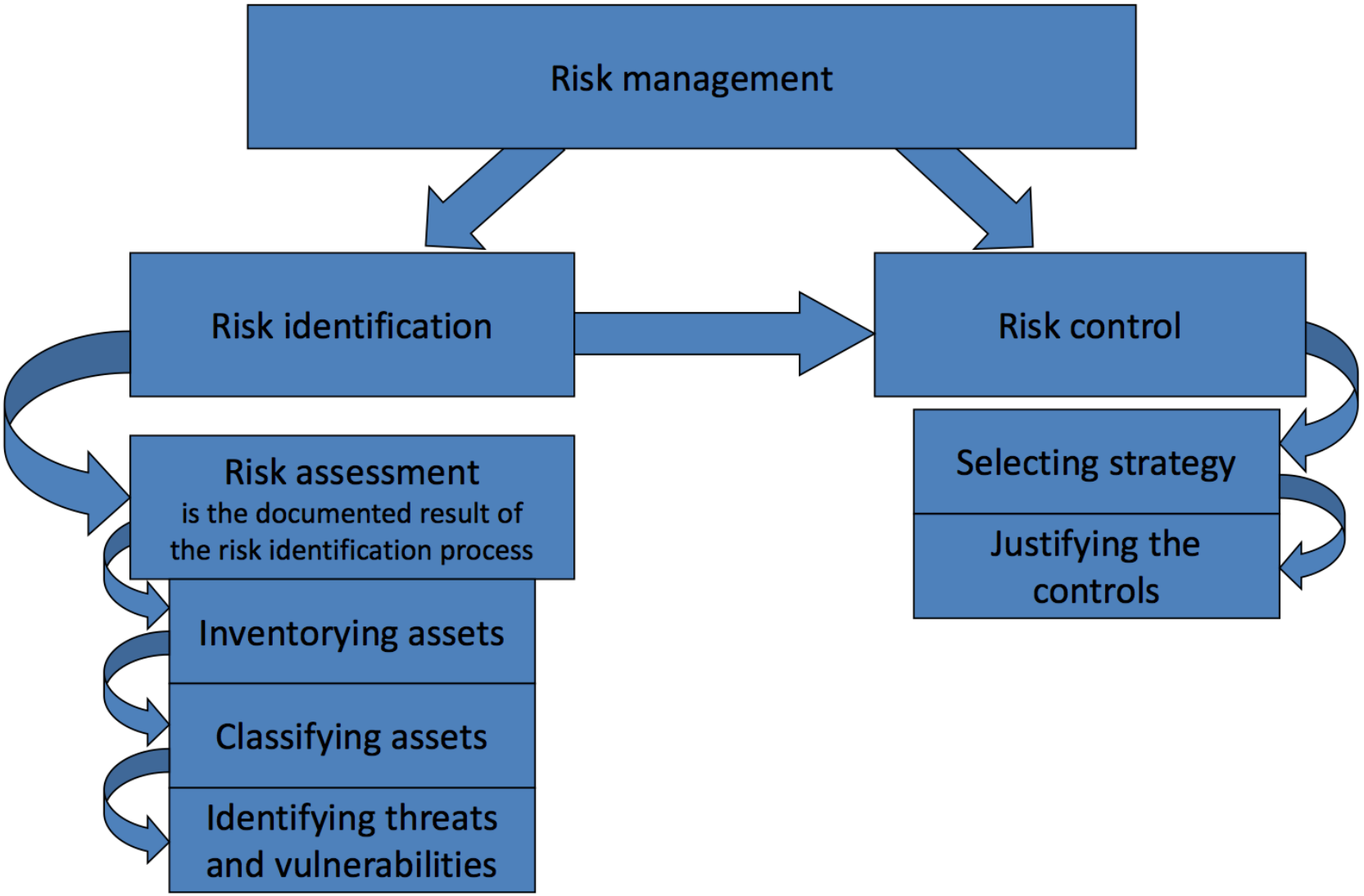
Contingency Planning

- *List and discuss the components of contingency planning*
- *Describe the role of information security policy in the development of contingency plans*

RISK MANAGEMENT

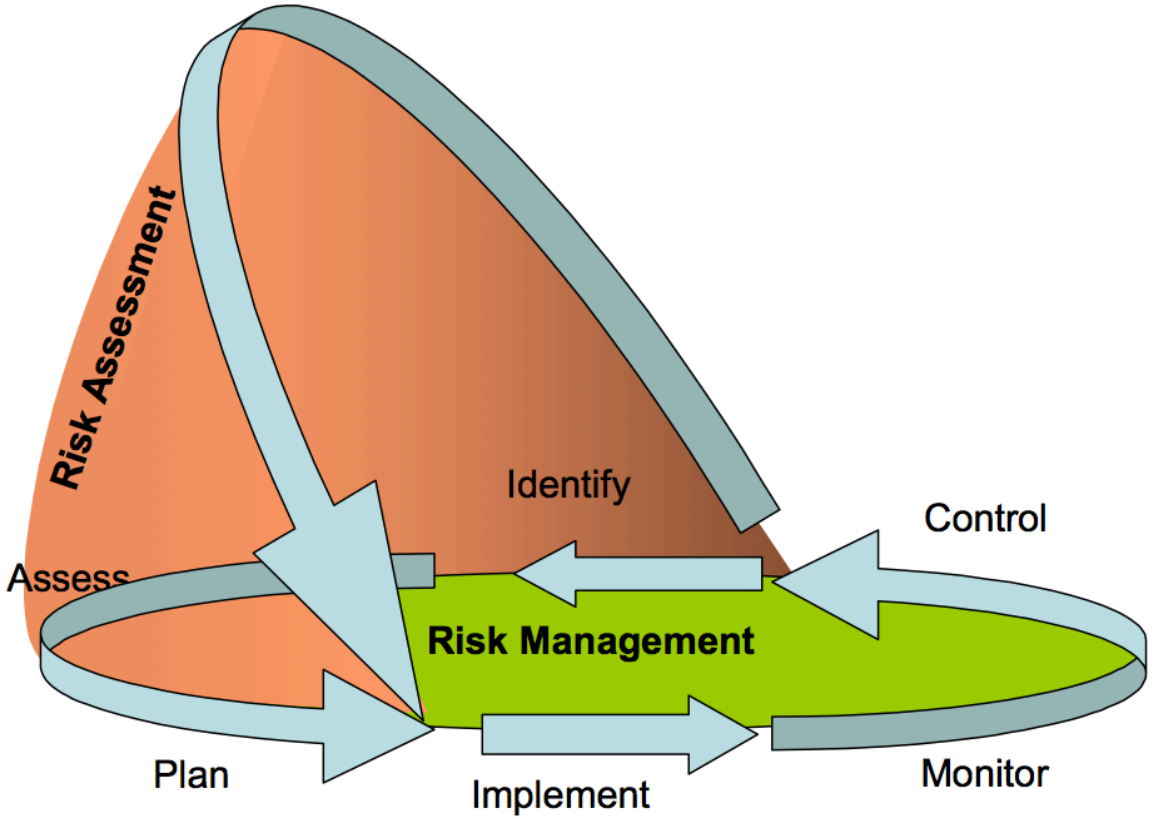
Risk management *is the process of* ***identifying vulnerabilities*** *in an organization's information systems and taking carefully reasoned steps* ***to ensure the confidentiality, integrity and availability*** *of all the components of the organization's information system.*

Whitman, Mattord and Green 2014, page 13

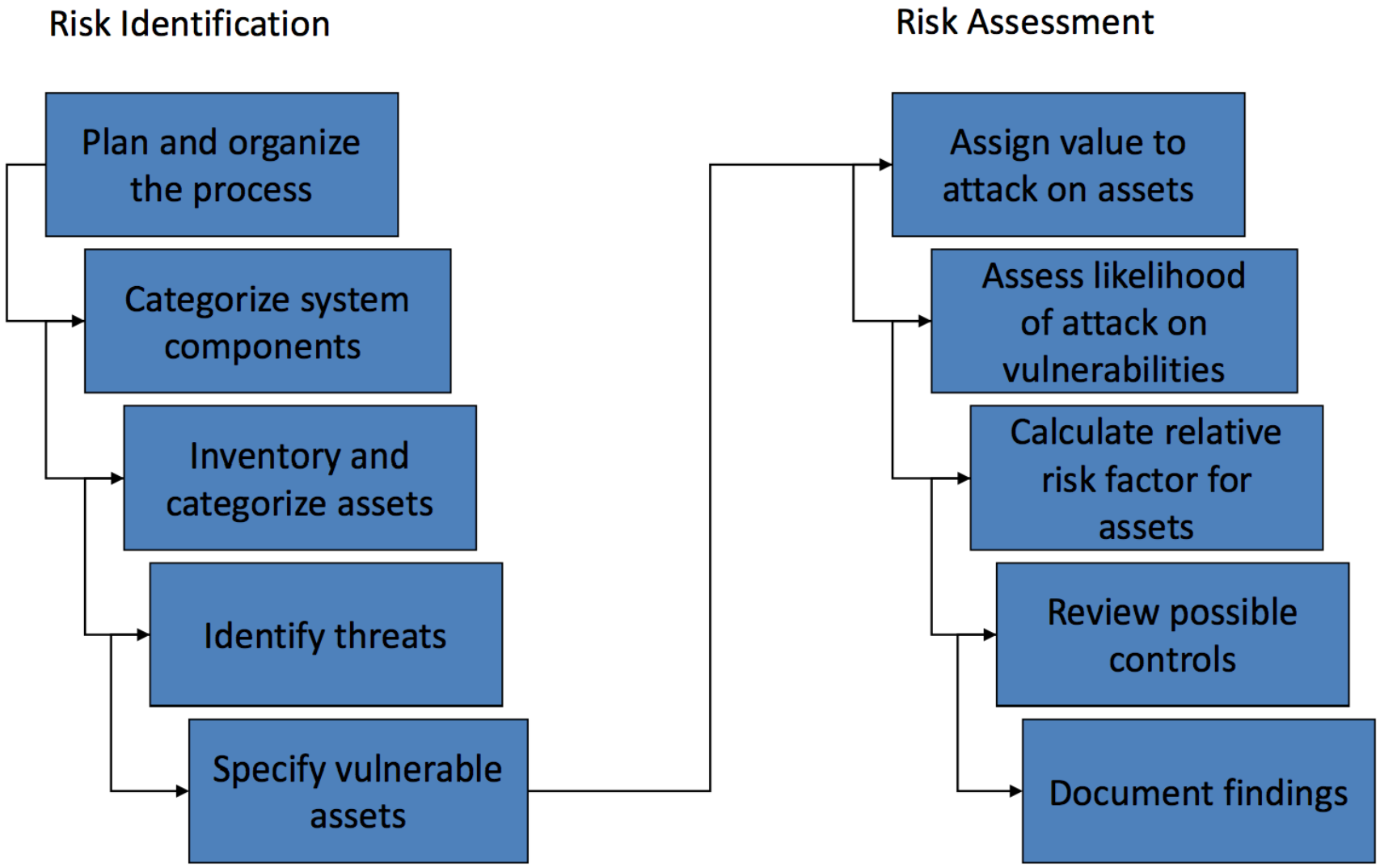


Whitman and Mattord 2007, p. 12.

THE RELATIONSHIP BETWEEN RISK MANAGEMENT AND RISK ASSESSMENT



ENISA Deliverable: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, p. 6



Adapted from Whitman and Mattord 2007, p. 14.

CATEGORIZE SYSTEM COMPONENTS

Categories should be **comprehensive** and **mutually exclusive**

Examples of system components:

- A server
- An ERP system

A system component may serve one or more ***information assets***:

- A server may contain the customer list and information about the customers

Assets should be **identified** and **ranked** according to importance to the organization

INVENTORY AND CATEGORIZE ASSETS

Questions to ask that help determine criteria for *prioritizing assets*:

- Is this asset the most **critical to the organization's success**?
- Does it generate the **most revenue**?
- Does it generate the **most profit**?
- Would it be the most **expensive to replace**?
- Will it be the most **expensive to protect**?
- If revealed, would it cause the most **embarrassment** or greatest **damage**?
- Does the **law** or other **regulations** require us to protect this asset?

Whitman, Mattord and Green 2014, page 15

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

Whitman, Mattord and Green 2014, page 16

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
Criterion Weight (1-100) Must total 100	*30*	*40*	*30*	

Whitman, Mattord and Green 2014, page 16

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
Criterion Weight (1-100) Must total 100	*30*	*40*	*30*	
EDI Document Set 1 – Logistics BOL to outsources (outbound)				
EDI Document Set 2 – Supplier Orders (outbound)				
EDIT Document Set 2 – Supplier fulfillment advice (inbound)				
Customer order via SSL (inbound)				
Customer service request via email				

Whitman, Mattord and Green 2014, page 16

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
Criterion Weight (1-100) Must total 100	*30*	*40*	*30*	
EDI Document Set 1 – Logistics BOL to outsources (outbound)	0.8			
EDI Document Set 2 – Supplier Orders (outbound)	0.8			
EDIT Document Set 2 – Supplier fulfillment advice (inbound)	0.4			
Customer order via SSL (inbound)	1.0			
Customer service request via email	0.4			

Whitman, Mattord and Green 2014, page 16

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
Criterion Weight (1-100) Must total 100	*30*	*40*	*30*	
EDI Document Set 1 – Logistics BOL to outsources (outbound)	0.8	0.9		
EDI Document Set 2 – Supplier Orders (outbound)	0.8	0.9		
EDIT Document Set 2 – Supplier fulfillment advice (inbound)	0.4	0.5		
Customer order via SSL (inbound)	1.0	1.0		
Customer service request via email	0.4	0.4		

Whitman, Mattord and Green 2014, page 16

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
Criterion Weight (1-100) Must total 100	*30*	*40*	*30*	
EDI Document Set 1 – Logistics BOL to outsources (outbound)	0.8	0.9	0.5	
EDI Document Set 2 – Supplier Orders (outbound)	0.8	0.9	0.6	
EDIT Document Set 2 – Supplier fulfillment advice (inbound)	0.4	0.5	0.3	
Customer order via SSL (inbound)	1.0	1.0	1.0	
Customer service request via email	0.4	0.4	0.9	

Whitman, Mattord and Green 2014, page 16

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
Criterion Weight (1-100) Must total 100	*30*	*40*	*30*	
EDI Document Set 1 – Logistics BOL to outsources (outbound)	0.8	0.9	0.5	75
EDI Document Set 2 – Supplier Orders (outbound)	0.8	0.9	0.6	78
EDIT 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 email	0.4	0.4	0.9	55

Whitman, Mattord and Green 2014, page 16

IDENTIFY THREATS

Questions to ask when performing a *threat assessment*:

- Which threats present a **danger to an organization's assets** in the given environment?
- Which threats represent **the most danger** to the organization's information?
- How much would it **cost to recover** from a successful attack?
- Which of the threats require the greatest **expenditure to prevent**?

Whitman, Mattord and Green 2014, page 17

SPECIFY VULNERABLE ASSETS

Review **each information asset** for **each threat** it faces

List **all of the vulnerabilities** of the organization's assets that may be used by each identified threat

- This list is likely to be very long!

This is a somewhat subjective process

- *It is therefore good to have groups of people with diverse backgrounds collaborating*

ASSIGN VALUE TO ATTACK ON ASSETS

Ask the same questions as before:

- Which threats present a **danger to an organization's assets** in the given environment?
- Which threats represent **the most danger** to the organization's information?
- How much would it **cost to recover** from a successful attack?
- Which of the threats require the greatest **expenditure to prevent**?

Assign weighted scores to each information asset

- Example: 100 = high, 50 medium, 1 low
- More granular approaches are also possible

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

NIST FIPS PUB 199 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)

ASSESS LIKELIHOOD OF ATTACK ON VULNERABILITIES

*Likelihood is the **probability** that a specific **vulnerability** within an organization will be **successfully attacked***

Sometimes data is available to estimate this

- For example, insurance companies have sufficient data to calculate the probability that a house is going to burn down or be broken into

Often it is only partially available or not at all

- Must be estimated subjectively
- Use of a rating scheme: E.g., 1 = high, 0.5 medium, 0.1 = low
- *It is important to use the rating model consistently!*

CALCULATE RELATIVE RISK FACTOR FOR ASSETS

Risk is

The **likelihood** of the occurrence [exploitation] of a vulnerability
X
The **value** of the information asset
-
The percentage of risk mitigated by **current controls**
+
The **uncertainty** of current knowledge of the vulnerability

Whitman, Mattord and Green 2014, page 18

PITFALLS IN QUANTITATIVE RISK ASSESSMENT

Remember that every number in the equation has been estimated by someone!

Common pitfalls:

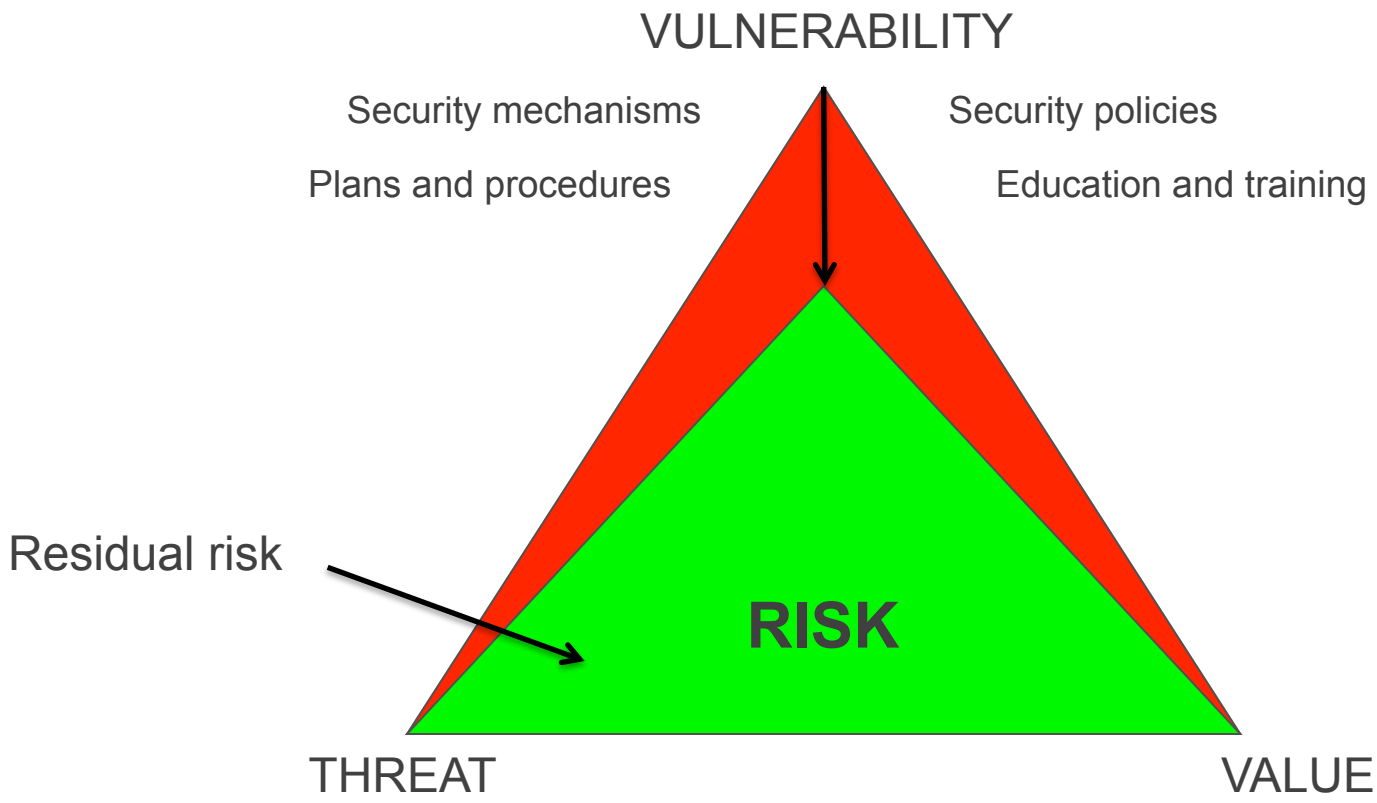
- Inappropriate scope
- Assessment out of context
- Forgetting about third-party risk
- Under-estimating the importance of physical security
- Not taking human factors into account
- Focusing too much on the vulnerabilities instead of the assets
- Failing to identify all threats
- Inconsistent models used to estimate likelihood
- Problems with estimating tangible asset value
- Not involving a team of the right people
- Not acting on the results of the assessment

RISK CONTROL STRATEGIES

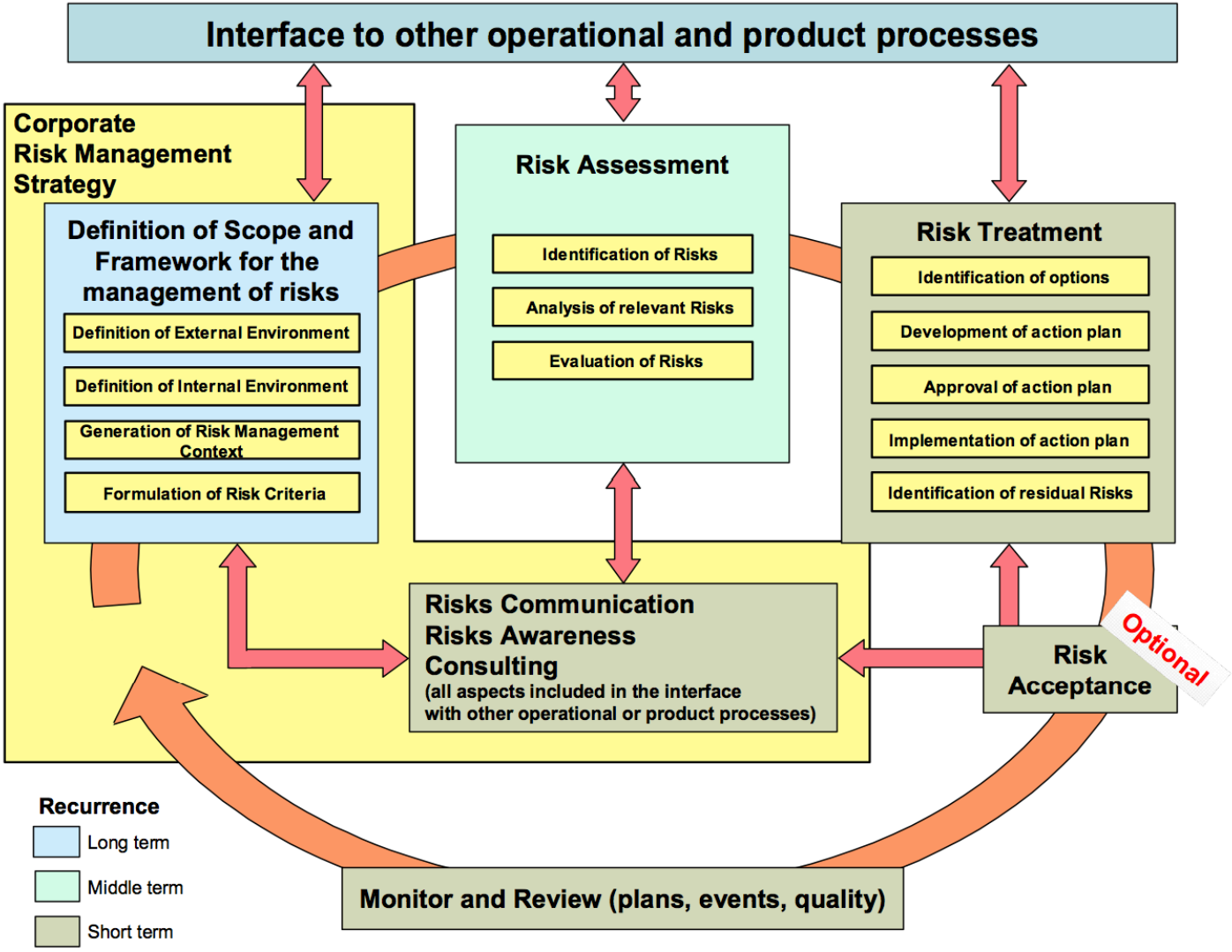
Strategy	Description
Avoidance	Use policy, training and education and technological means **to avoid the risk.**
Transference	**Shift the risk to other assets, processes or organizations.** Also known as outsourcing. Outsourcing can be risky. Requirements for risk management must be written into contracts and the service provider audited to make sure risk management is properly done.
Mitigation	**Use planning and preparation to reduce impact of an incident when it occurs.** Includes contingency planning (business impact analysis, incident response planning, disaster recovery planning and business continuity planning). Contingent upon ability to detect incidents as early as possible, and ability to respond quickly, efficiently and effectively.
Acceptance	**Do nothing to avoid, transfer or mitigate the risk.** Only a valid approach when: 1) The level of risk has been determined. 2) Probability of attack has been assessed and potential damage has been estimated. 3) Controls have been evaluated. 4) A cost-benefit analysis shows that the cost of protection exceeds the loss from an incident.

Whitman and Mattord 2007, p. 19.

RISK CONTROL BY REDUCING VULNERABILITIES



CYCLE OF A RISK MANAGEMENT PROCESS



ENISA Deliverable: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, p. 13

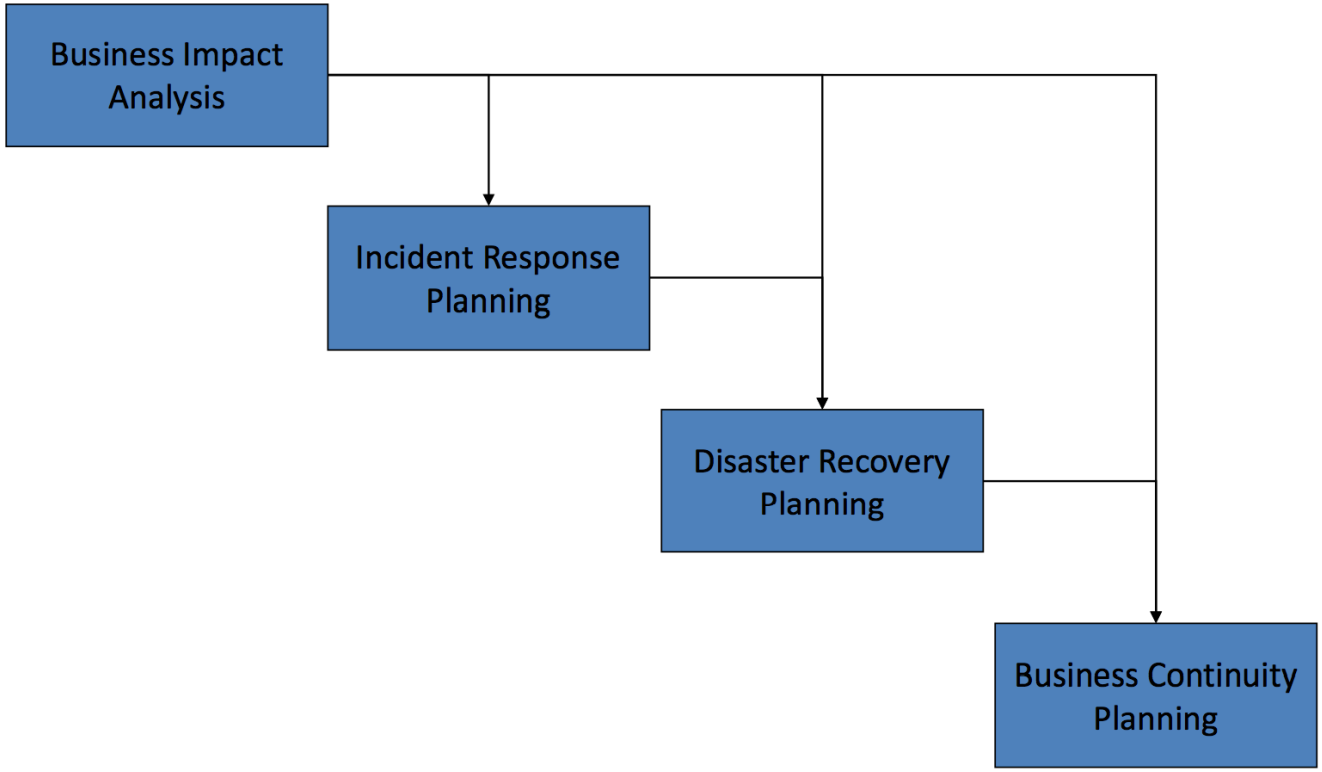
DEFINITION OF CONTINGENCY PLANNING

*"A contingency plan (CP) is prepared by the organization to **anticipate**, **react to** and **recover** from events that threaten the security of information and information assets in the organization."*

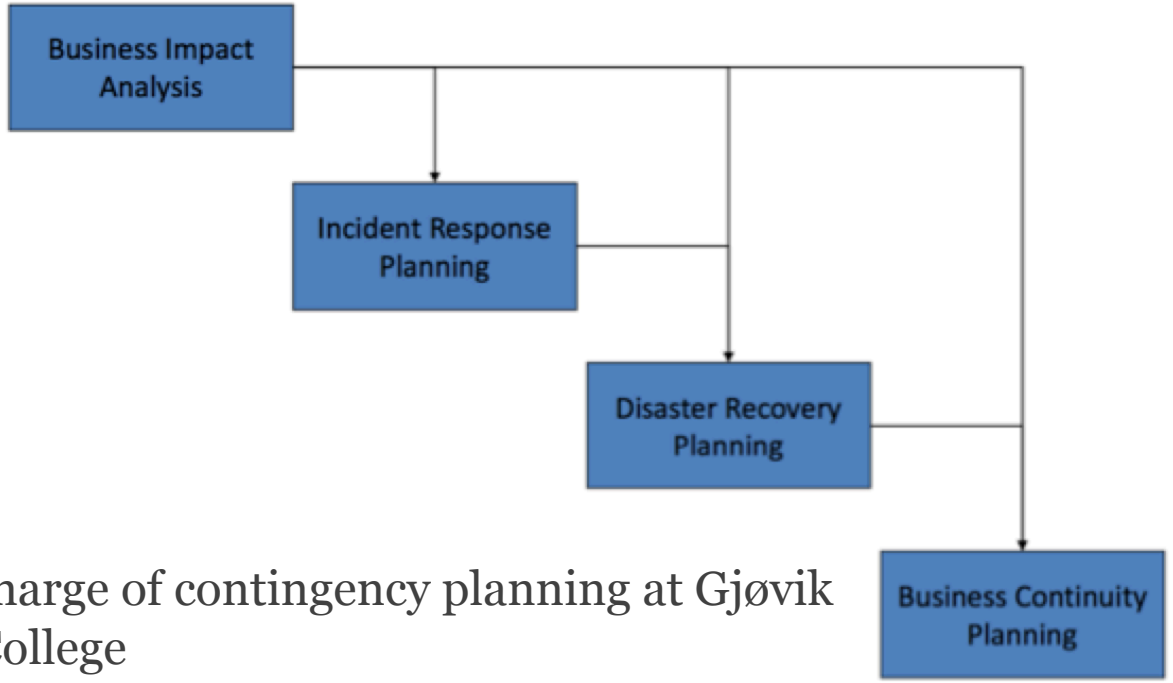
Whitman and Mattord 2007, p. 23

- Preparing for unexpected, undesired events
- Responding to the incident
- Restoring the organization to normal business operations

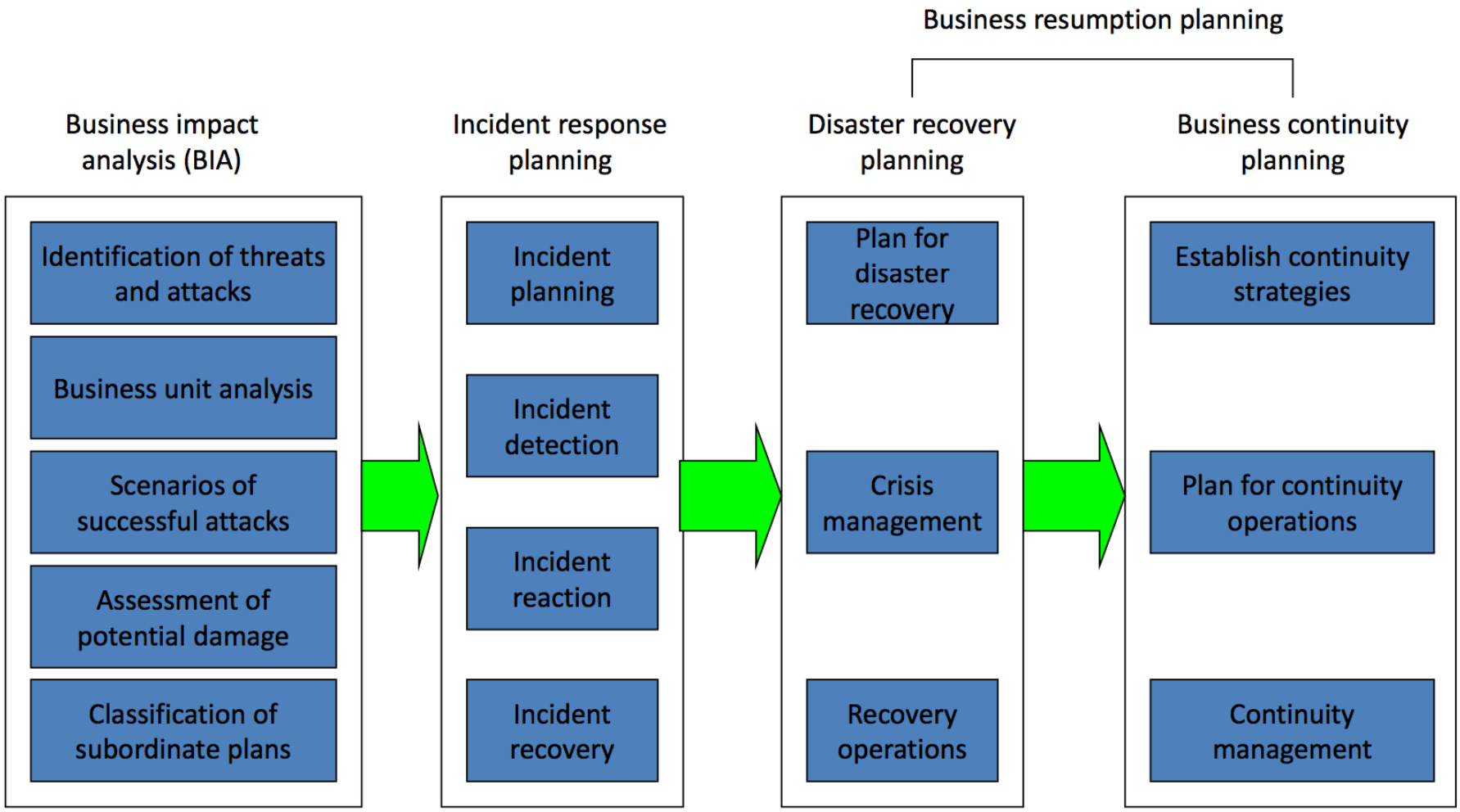
COMPONENTS OF CONTINGENCY PLANNING



Whitman and Mattord 2007, p. 24-25

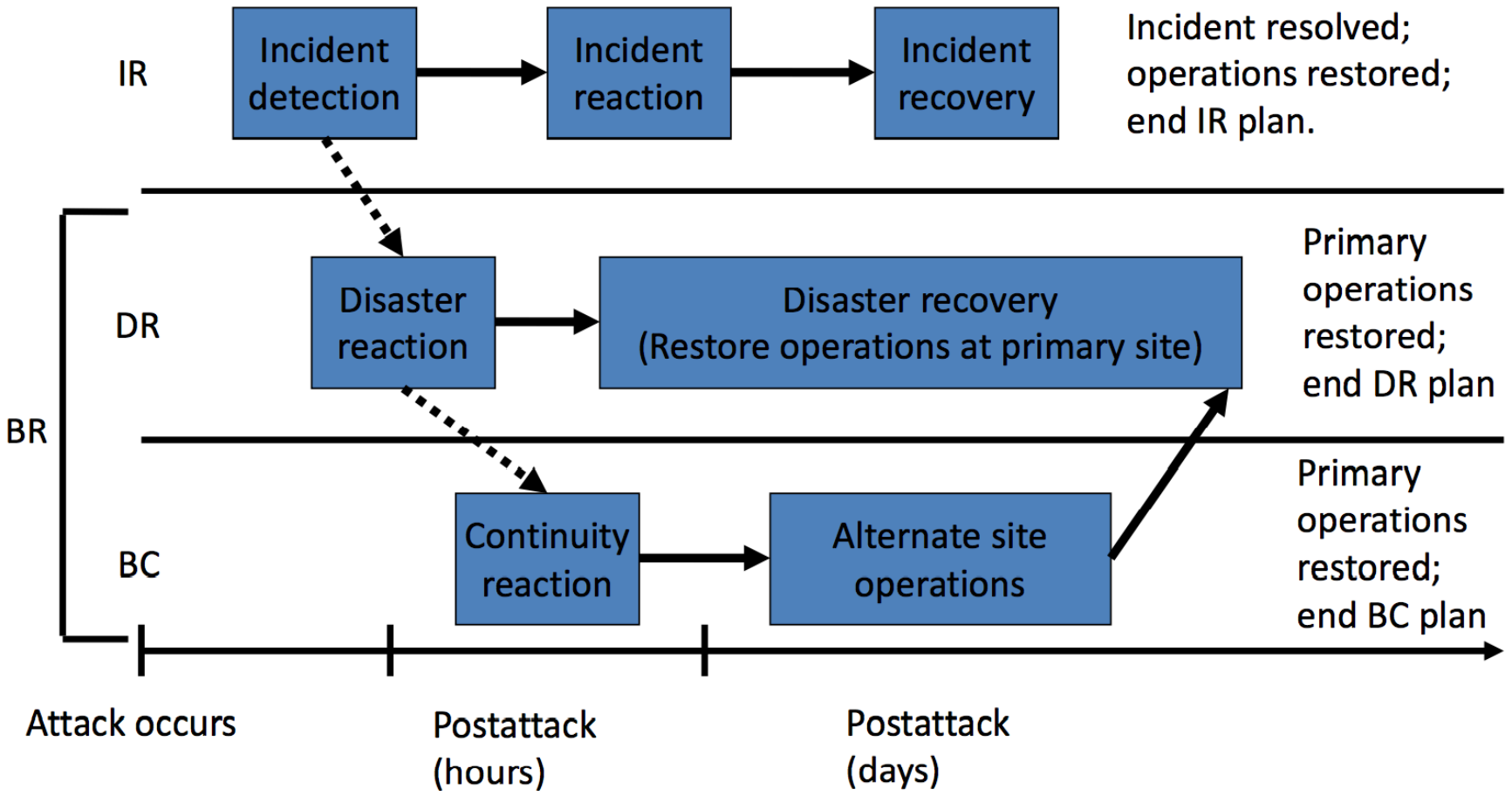


- You are in charge of contingency planning at Gjøvik University College
- Your job is to plan for and implement the above four activities
- What would you do?
- What could the consequences be if you don't have a plan?



Whitman and Mattord 2007, p. 27

TIMELINE FOR CONTINGENCY PLAN EXECUTION



CONSEQUENCES OF NOT HAVING A PLAN

- **Damage to data, systems and networks** due to not taking timely action
  - Increased costs
  - Loss of productivity
  - Loss of business

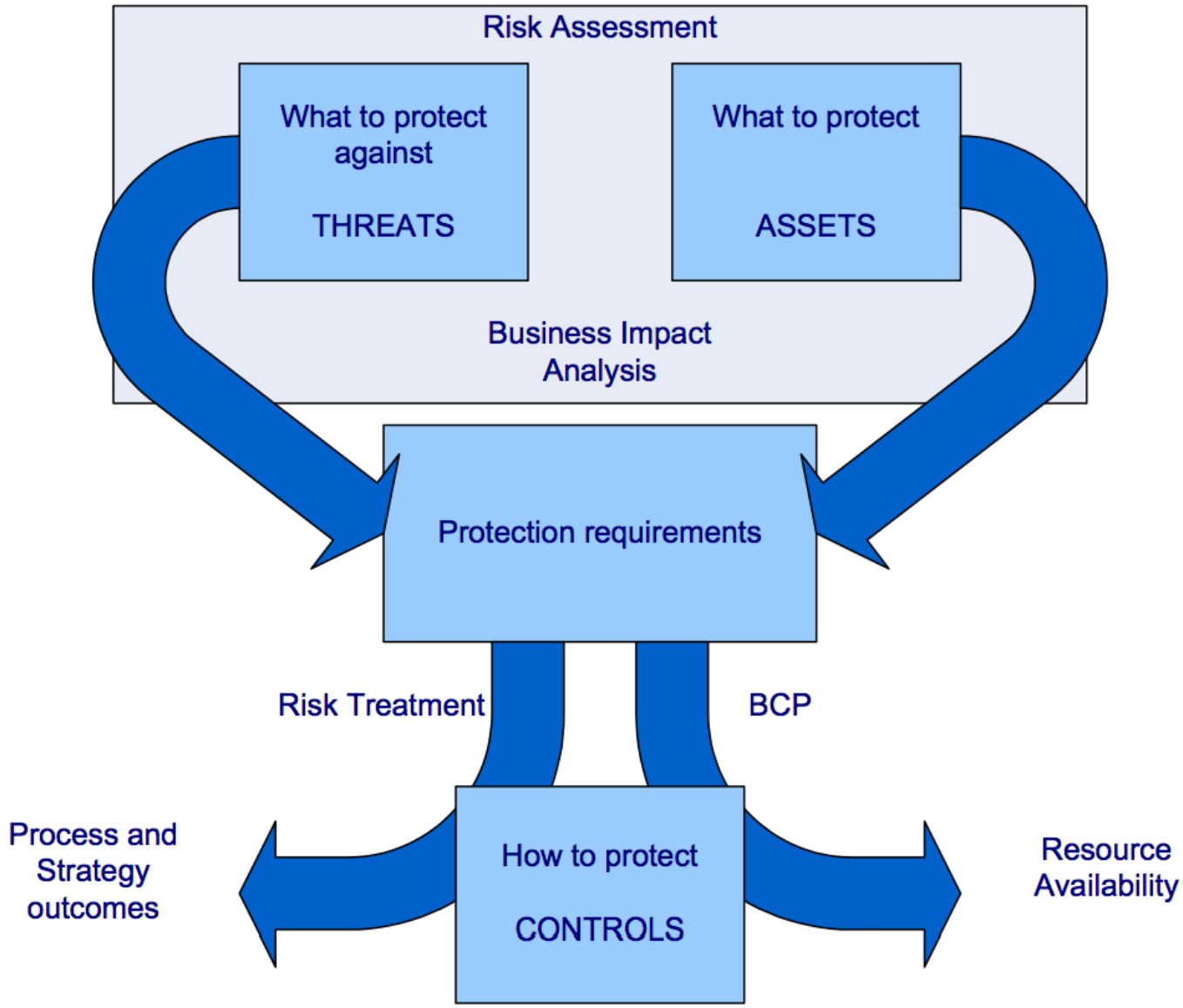
- An intrusion **affecting multiple systems** both inside and outside the organization because staff did not know who else to notify and what additional actions to take
- Negative **media exposure**
- **Legal** liability and prosecution

Whitman, Mattord and Green 2014, p. 24, Source: Carnegie Mellon University

COMPARISON OF RISK MANAGEMENT AND BUSINESS CONTINUITY

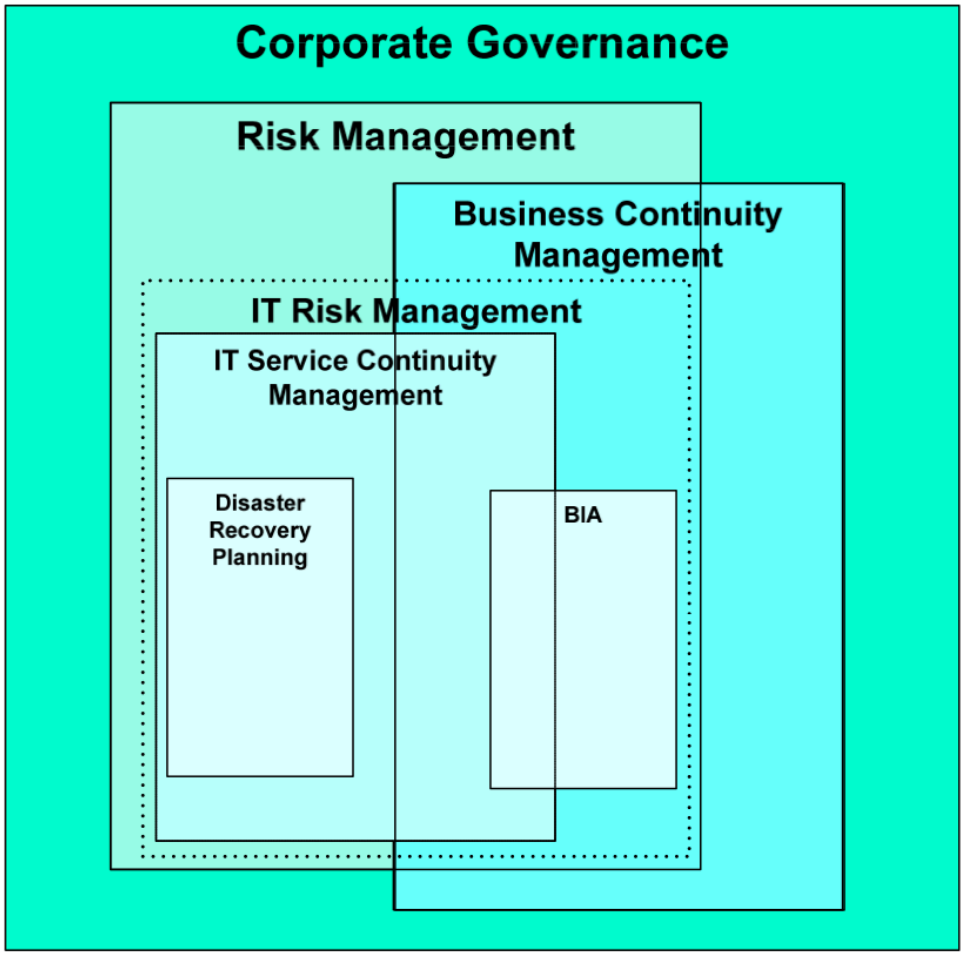
	Risk Management	Business Continuity Management
Key Method	Risk Analysis	Business Impact Analysis
Key Parameters	Impact and Probability	Availability and Impact
Type of incident	All types of events	Events causing significant business disruption
Size of events	All events affecting the organisation	Those threatening availability of organisation's core processes
Scope	Focus primarily on management of risks to core business objectives, to prevent or reduce incidents	Focus mainly on incident management and recovery of critical business processes following an incident
Intensity	All, from gradual to sudden	Sudden or rapid events (although response may also be appropriate if a creeping incident suddenly becomes severe)

ENISA deliverable: Business and IT Continuity: Overview and Implementation Principles, page 18

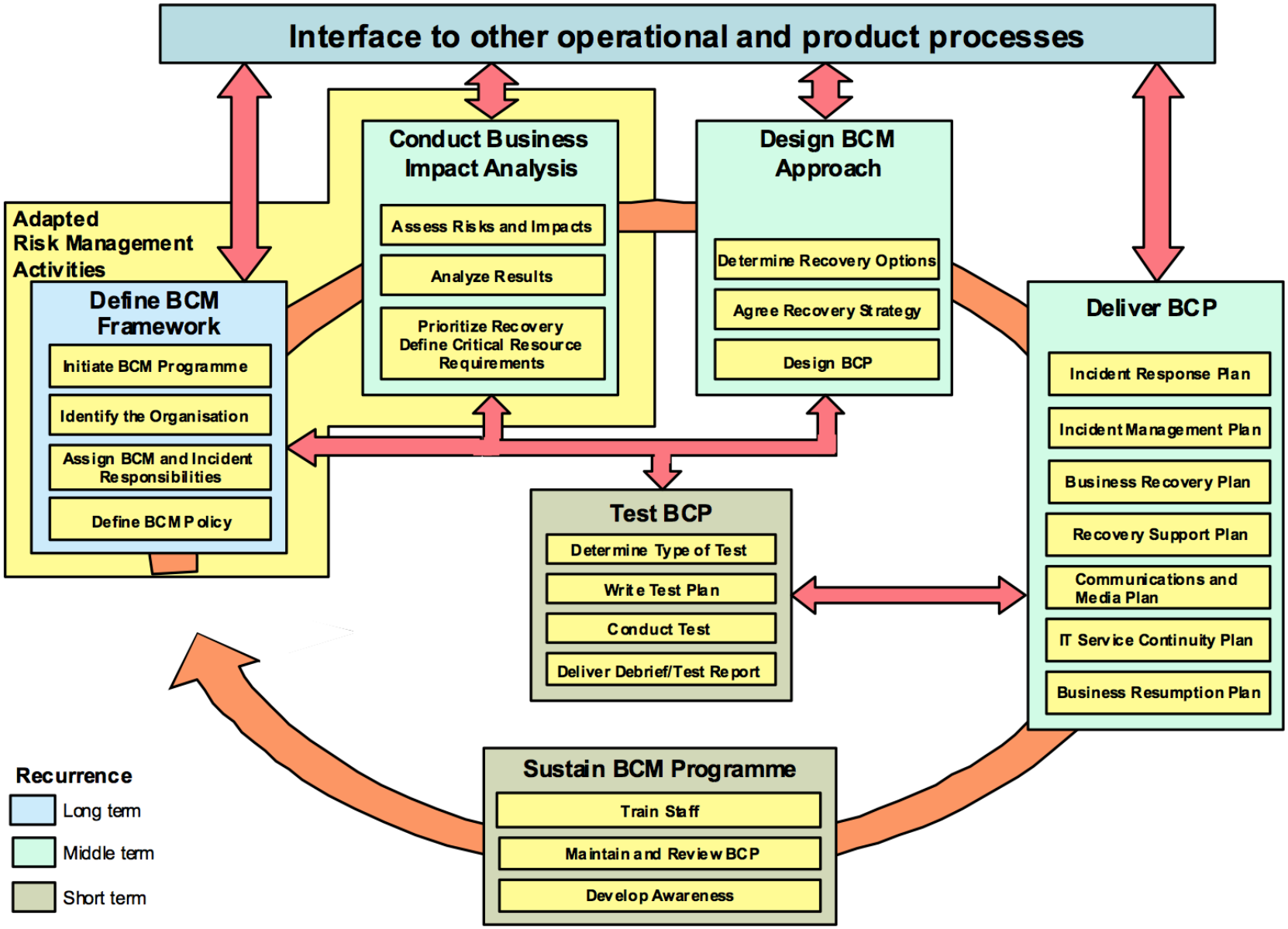


ENISA deliverable: Business and IT Continuity: Overview and Implementation Principles, page 18

PROPOSAL FOR A NESTED RELATIONSHIP OF THE RELATED RISK DISCIPLINES

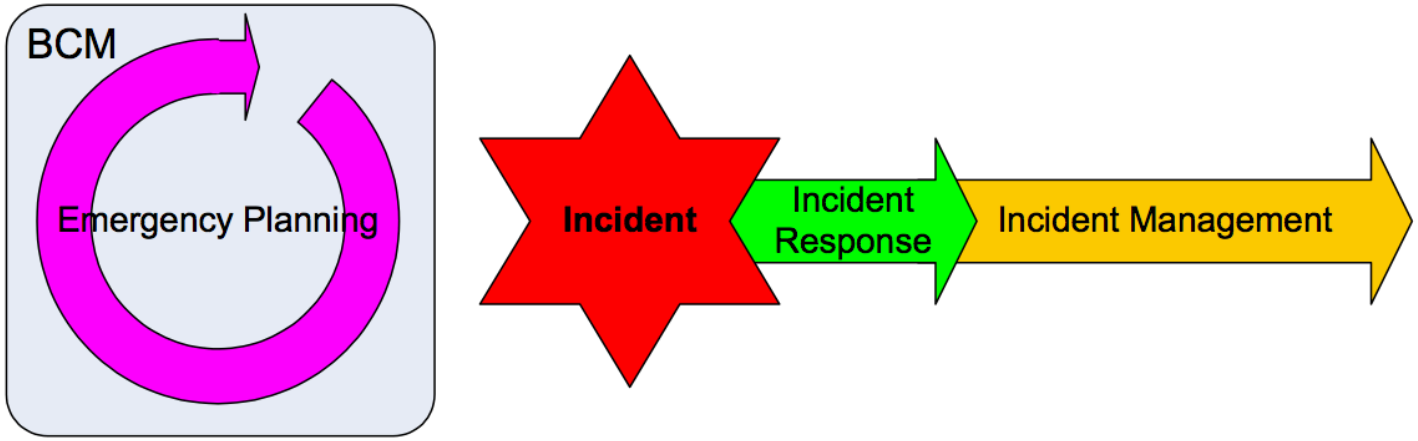


ENISA deliverable: Business and IT Continuity: Overview and Implementation Principles, page 20

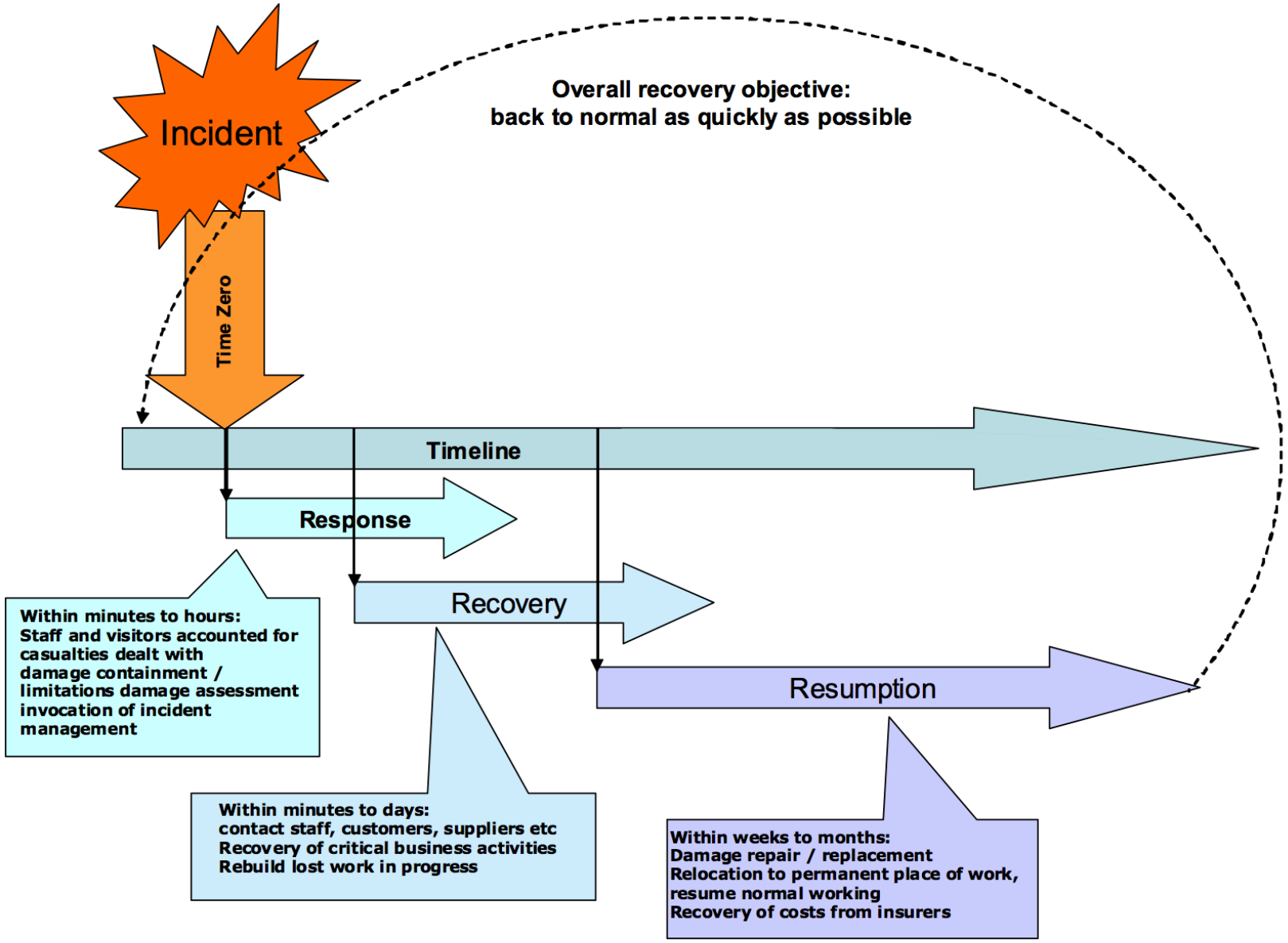


ENISA deliverable: Business and IT Continuity: Overview and Implementation Principles, page 22

INCIDENT TIMELINE



ENISA deliverable: Business and IT Continuity: Overview and Implementation Principles, page 21

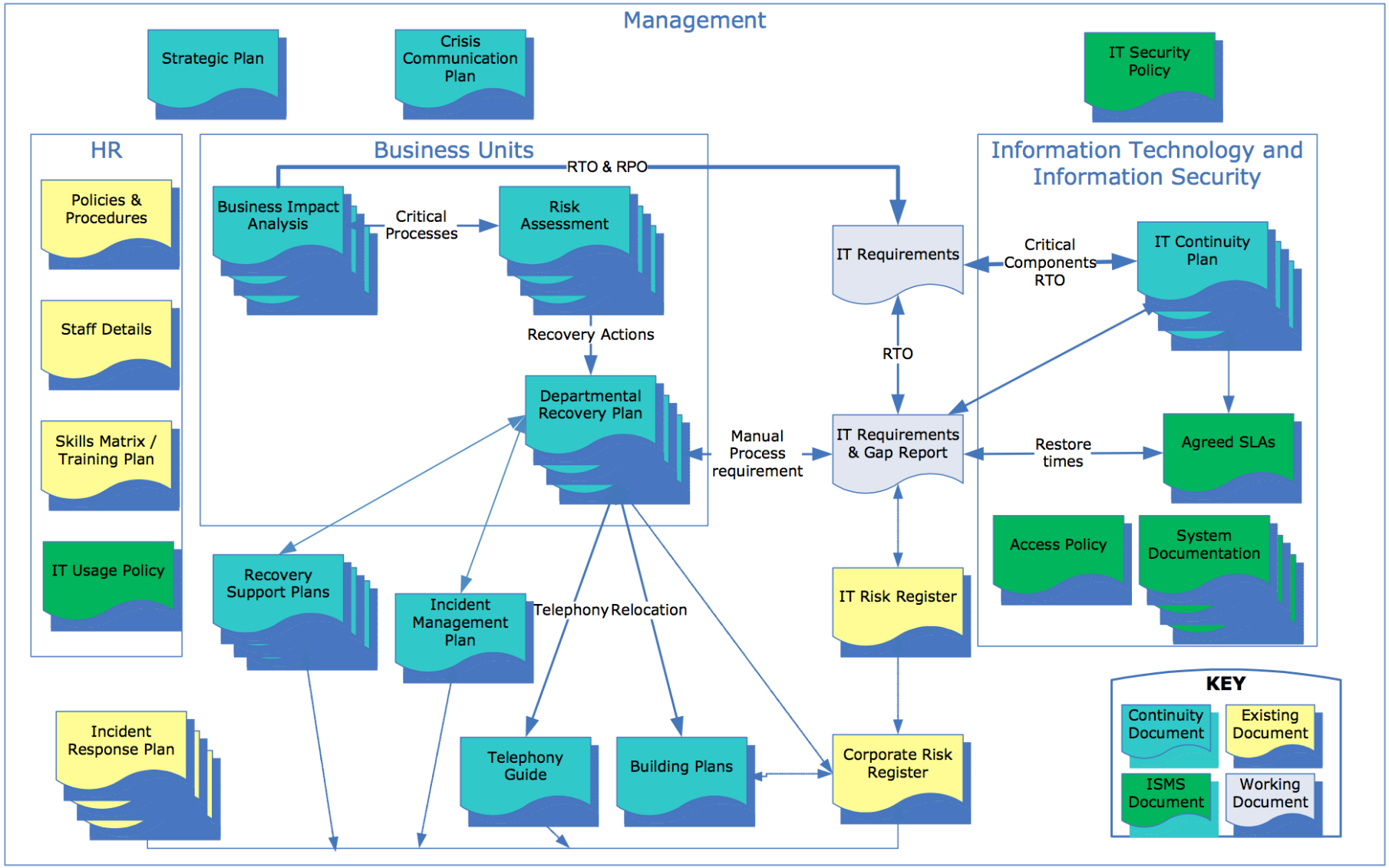

Incident
Overall recovery objective:
back to normal as quickly as possible
Time Zero
Timeline
Response
Recovery
Resumption
Within minutes to hours:
Staff and visitors accounted for
casualties dealt with
damage containment /
limitations damage assessment
invocation of incident
management
Within minutes to days:
contact staff, customers, suppliers etc
Recovery of critical business activities
Rebuild lost work in progress
Within weeks to months:
Damage repair / replacement
Relocation to permanent place of work,
resume normal working
Recovery of costs from insurers

THE ROLE OF INFORMATION SECURITY POLICY

- Policies are written to support the mission, vision and strategic planning of an organization
- Information security policies has a role in developing contingency plans
  - The least expensive control
  - The most difficult to implement correctly
- Policy obliges personnel to function in a manner that adds to the security of information assets rather than as a threat to those assets

Information security is primarily a management problem, not a technical one

Whitman, Mattord and Green 2014, p. 30



ENISA deliverable: Business and IT Continuity: Overview and Implementation Principles, page 49

NEXT LECTURE

The topic of the next lecture on the 3rd of February will be:

Business Impact Analysis

Recommended reading to prepare for the next lecture:

- Chapter 2 & 3 in Whitman & Mattord
- ENISA deliverable: *Business and IT Continuity: Overview and Implementation Principles*