

GJØVIK UNIVERSITY COLLEGE



Security planning and Incident Management

Marie Moe, NSM/HiG

Gjøvik 03.02.14

AGENDA

Business Impact Analysis

- *The elements needed to begin the contingency planning process*
- *Business impact analysis and its components*

Contingency Strategies

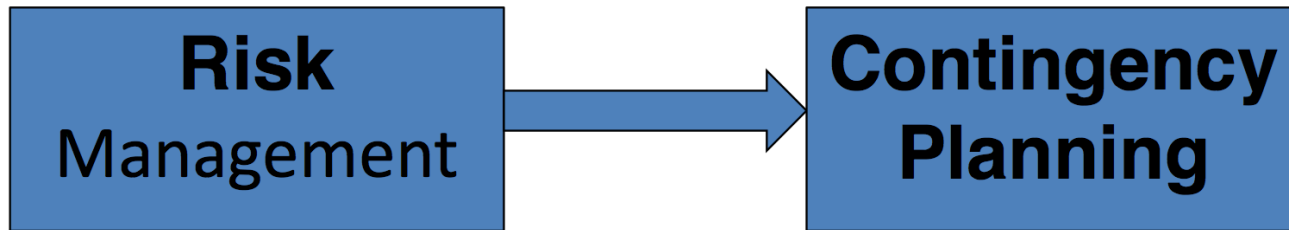
- *Techniques used for data and application backup and recovery*
- *Strategies for resumption of critical business processes at alternate and recovered sites*

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

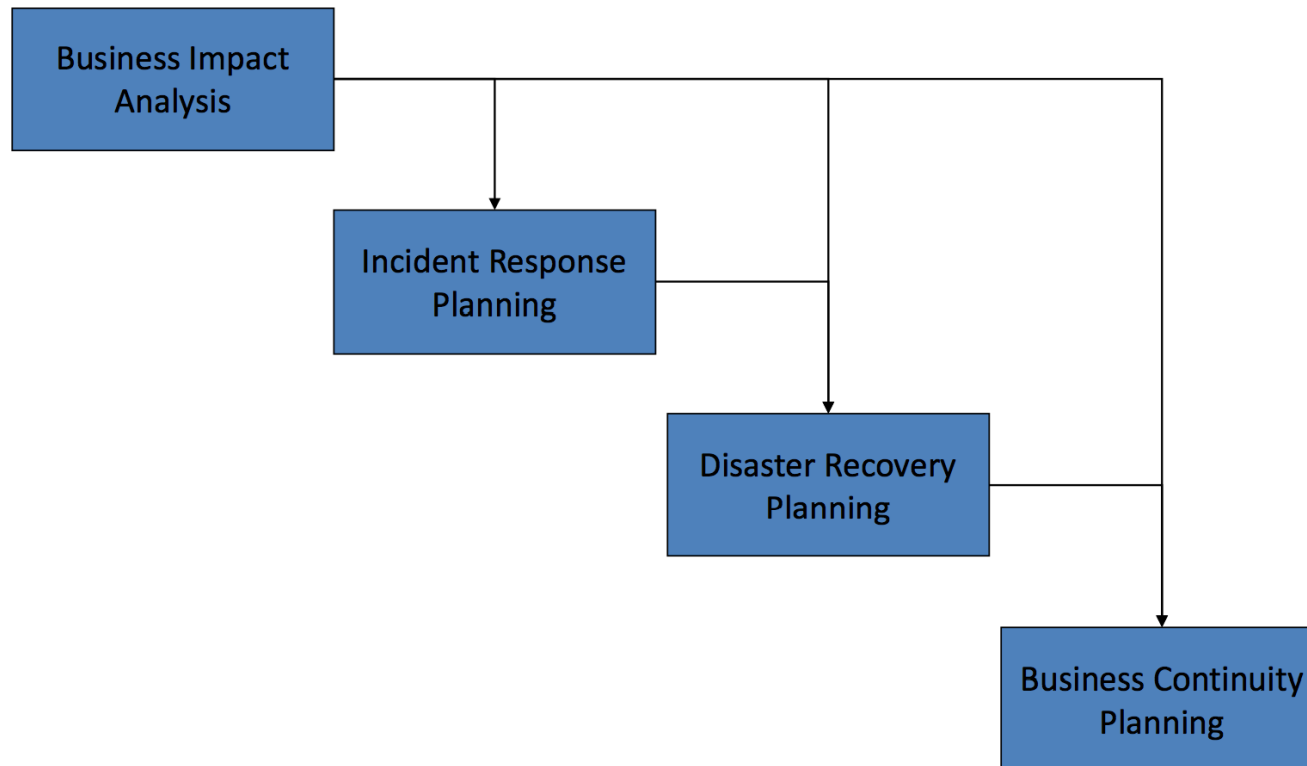
- Preparing for unexpected, undesired events
- Responding to the incident
- Restoring the organization to normal business operations



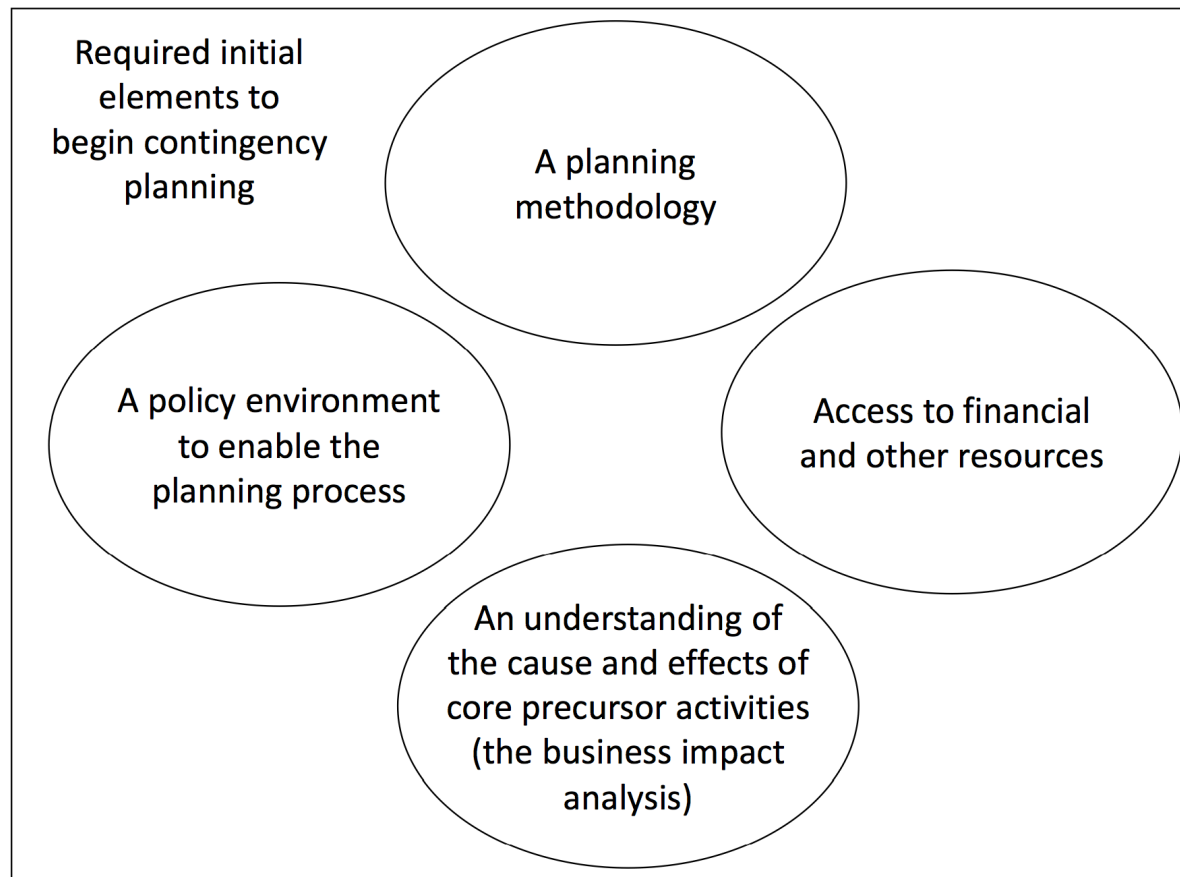
Prevention

In case prevention does not work!

COMPONENTS OF CONTINGENCY PLANNING




GETTING STARTED WITH CONTINGENCY PLANNING



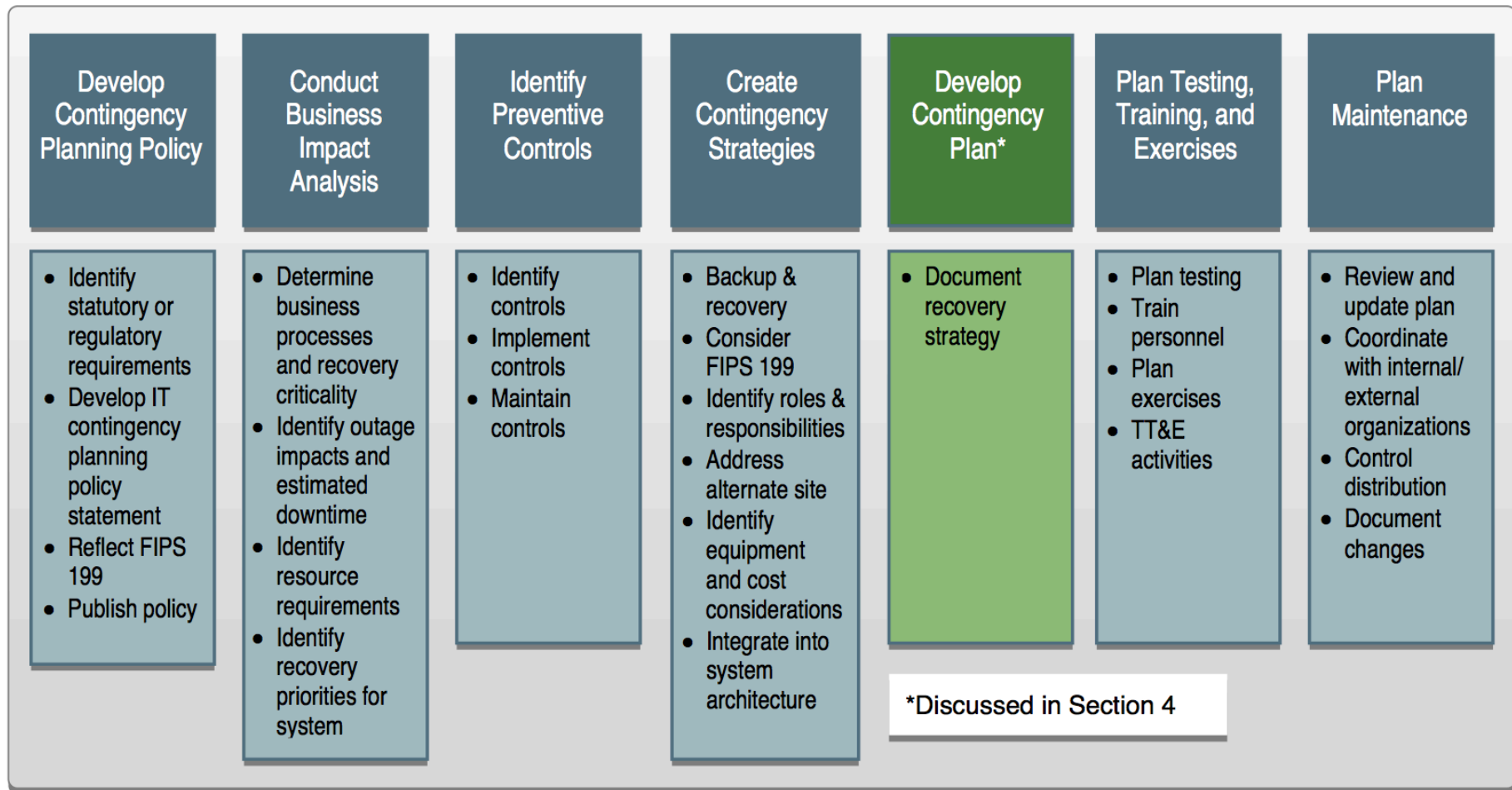
Based on Whitman and Mattord 2007, p. 51

THE SEVEN STEP CONTINGENCY PLANNING PROCESS

- 
1. Develop the contingency planning policy
 2. Conduct the business impact analysis (BIA)
 3. Identify preventive controls
 4. Create contingency strategies
 5. Develop an information system contingency plan
 6. Ensure plan testing, training, and exercises
 7. Ensure plan maintenance

M. Swanson, P. Bowen, A. Phillips, D. Gallup and D. Lynes, "Contingency Planning Guide for Federal Information Systems", NIST Special Publication 800-34 Rev. 1, accessed February 2014 from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Also see Whitman and Mattord 2007 p. 51 or Whitman, Mattord and Green 2014 p. 53



CONTINGENCY PLANNING POLICY

Purpose:

- To provide the formal authority and guidance necessary to develop an effective contingency plan

What it does:

- Defines the scope of CP operations
- Establishes managerial intent for timetables of
 - *Response to incidents*
 - *Recovery of disasters*
 - *Reestablishment of operations*
- Determines who is responsible for the development and operation of the *contingency planning management team* (CPMT)
- May determine the *constituencies* of all CP-related teams

EXAMPLE OF CONTINGENCY PLANNING POLICY

Contents:

1. Issue Statement
2. Organization's position
3. Applicability
4. Roles and Responsibility
5. Contingency Plan Policy
6. Compliance
7. Supplementary Information
8. Points of Contact

Whitman, Mattord and Green 2014 p. 55

Source: <http://csrc.nist.gov/groups/SMA/fasp/archive.html>

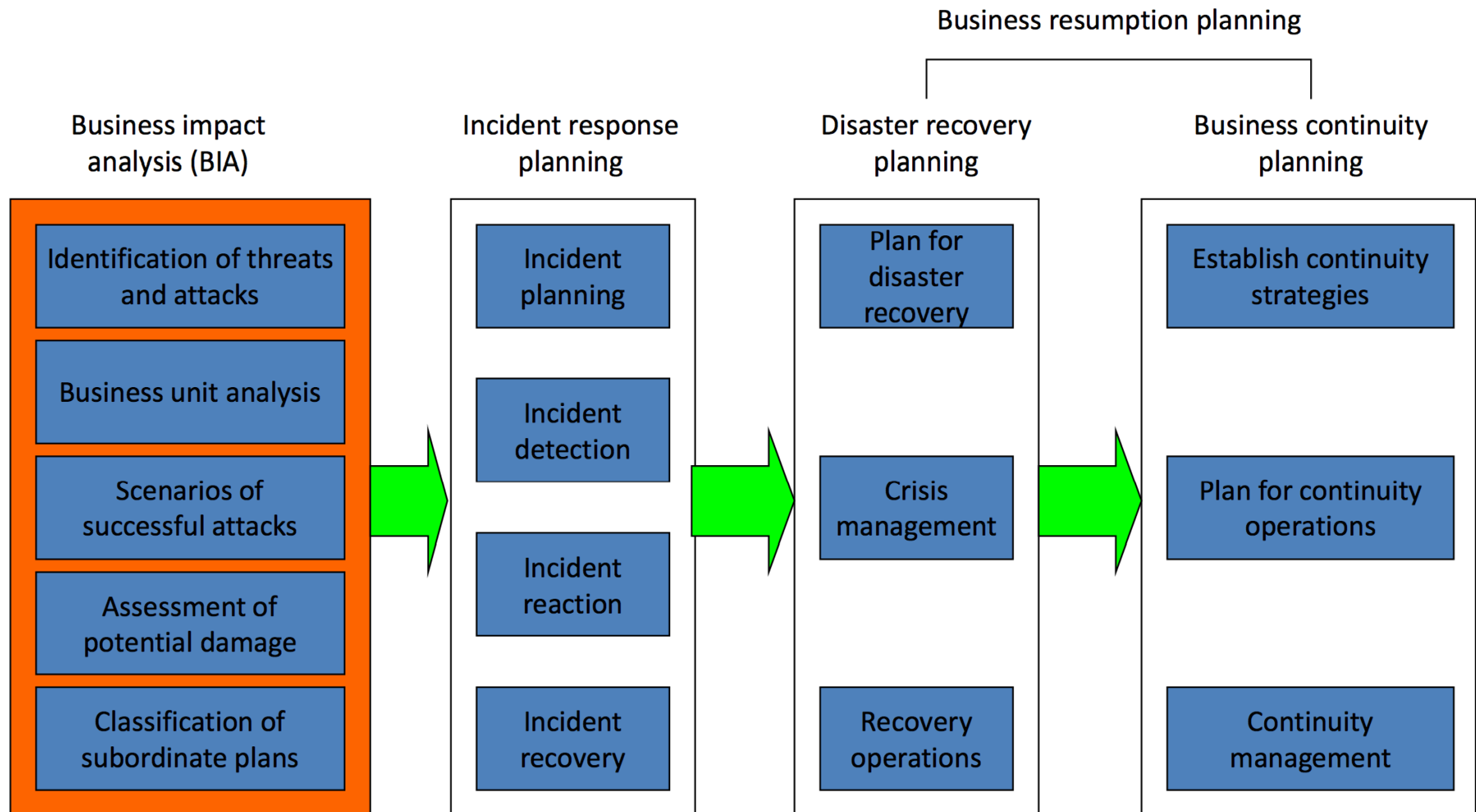
BUSINESS IMPACT ANALYSIS

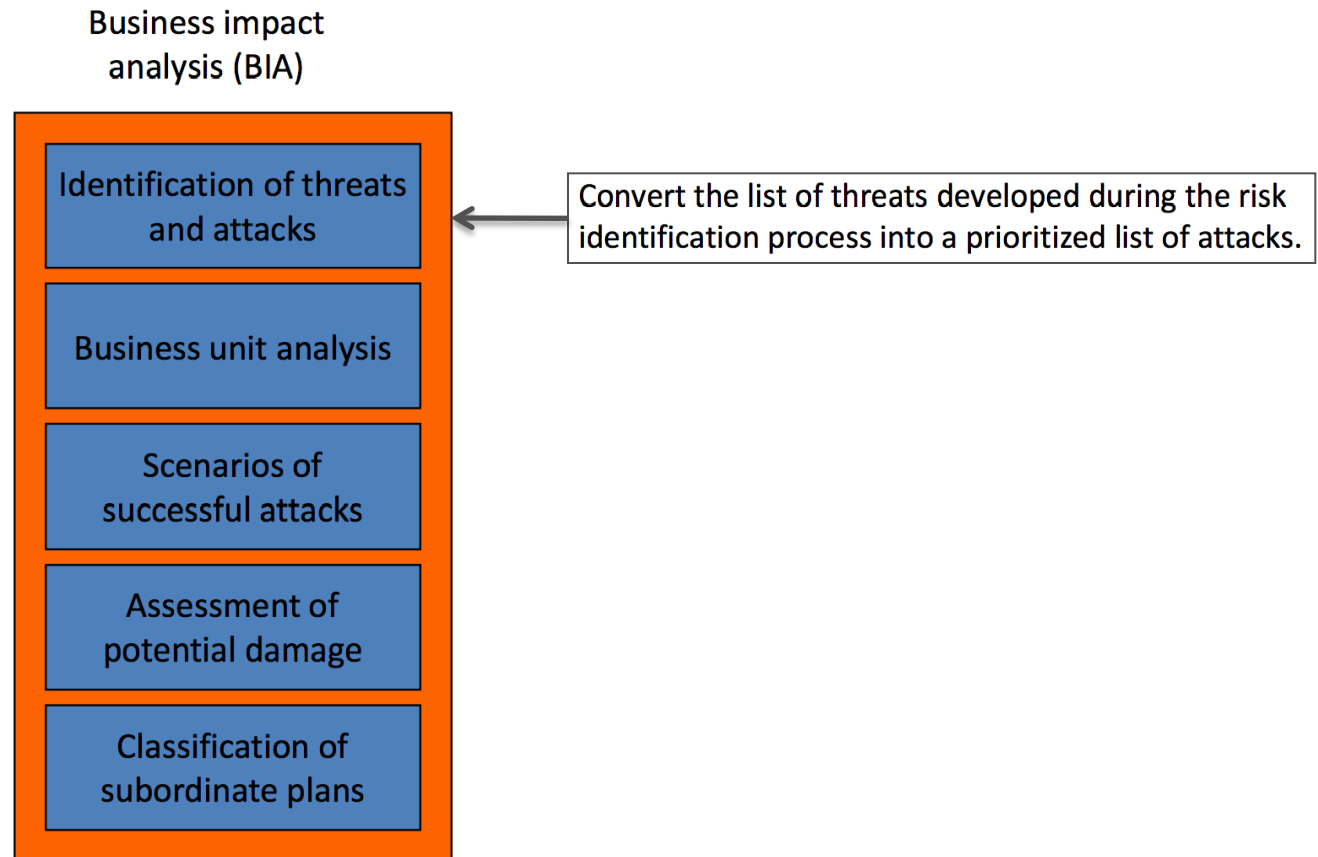
*“The **business impact analysis (BIA)** is an investigation and assessment of the impact that various events or incidents can have on an organization.”*

Whitman, Mattord and Green 2014, p. 57

A BIA may be conducted in three stages:

1. Assessment of **business processes** and **recovery criticality**
2. Identification of **resource requirements**
3. Identification of **recovery priorities**



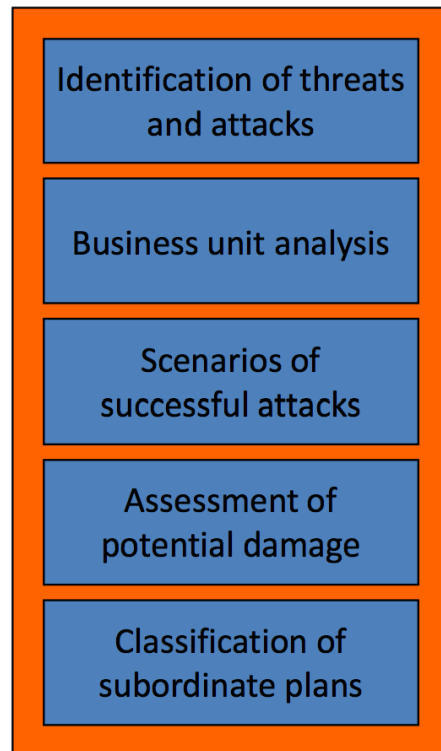


Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts 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
Deviation in quality of service by service providers	Power and WAN quality-of-service issues service providers
Technical hardware failure or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

IDENTIFICATION OF THREATS AND ATTACKS

Threat	Attack
Deliberate acts of theft	Illegal “taking” of organizational assets
Deliberate software attacks	E-mail viruses worms and malware, other viruses, worms and malware Email and instant messaging based social engineering Web-based malicious script Denial-of-service attacks on organizational information assets Distributed denial-of-service attacks on organizational information assets
Forces of nature	Fire, flood, earthquake, lightning, landslide, mudslide, tsunami
Deviation in quality of service by service providers	Network connection outage due to cable severance (phone or ISP) Network connection outage due to service faults (phone or ISP) Power blackout, brownout, surge, spike, fault and sag Other issues (water, sewage, garbage and other utilities)

Business impact analysis (BIA)



Analyze and prioritize business units to determine critical business functions which have to be protected and for which contingency plans have to be developed.

BUSINESS UNIT ANALYSIS

Business process: A task performed by an organization or organizational subunit in support of the organization's overall mission.

- Which business function is the most critical to the organization in the event of a major incident or disaster?
- Collect critical information from each business unit
- Try to avoid “turf wars”!
- May be facilitated by a weighted analysis worksheet

BUSINESS UNIT ANALYSIS EXAMPLE

The company Hierarchical Access LTD (HAL) provides Internet access, Web registration and hosting alternatives for small office/home office individuals and organizations.

Business functions identified (partial list):

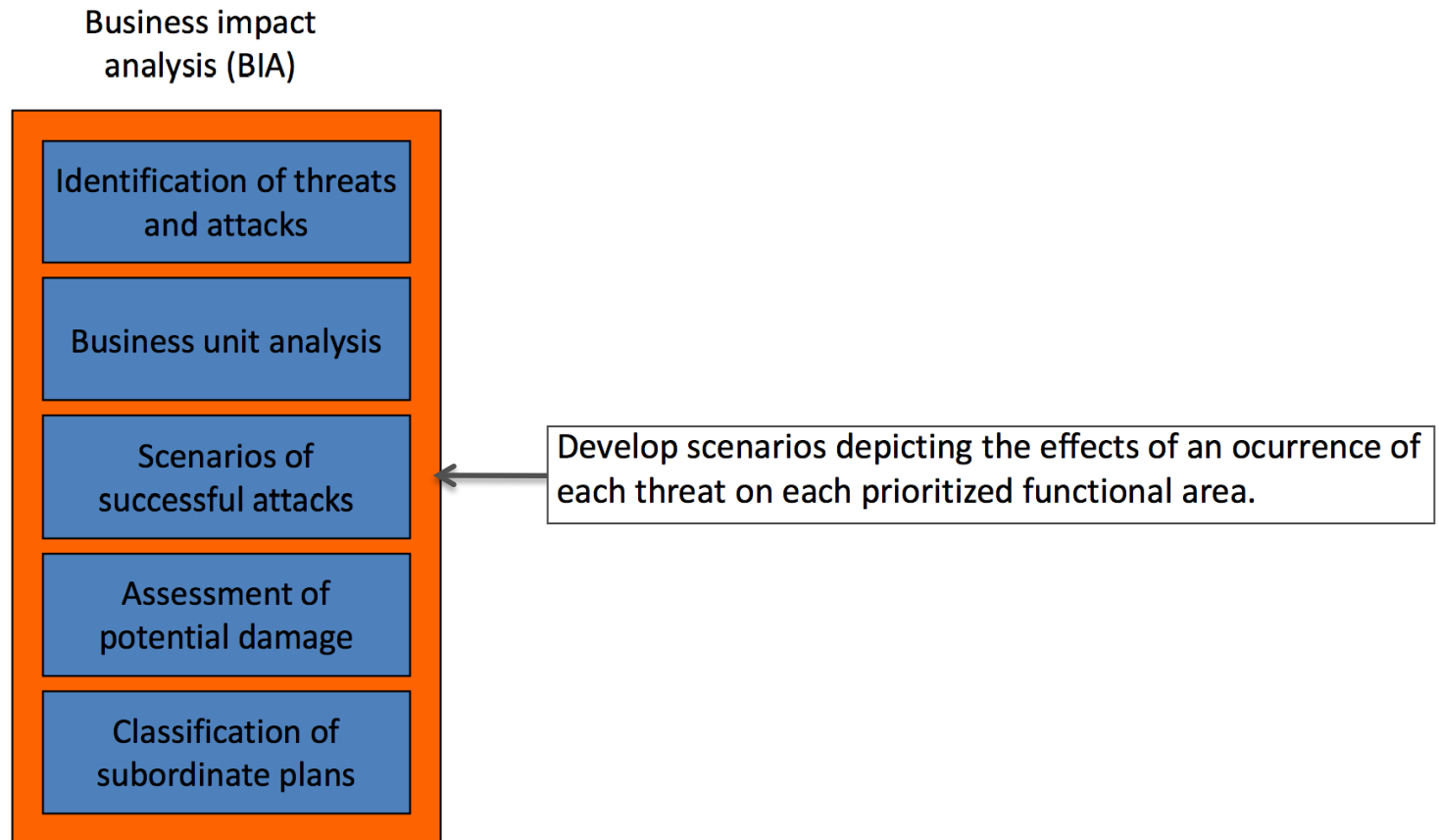
- Enrolling new customers
- Managing customer accounts
- Providing Internet access
- Providing Internet services
- Providing help desk support
- Advertising services
- Supporting public relations

Whitman, Mattord and Green 2014, p. 59

WEIGHTED ANALYSIS WORKSHEET EXAMPLE

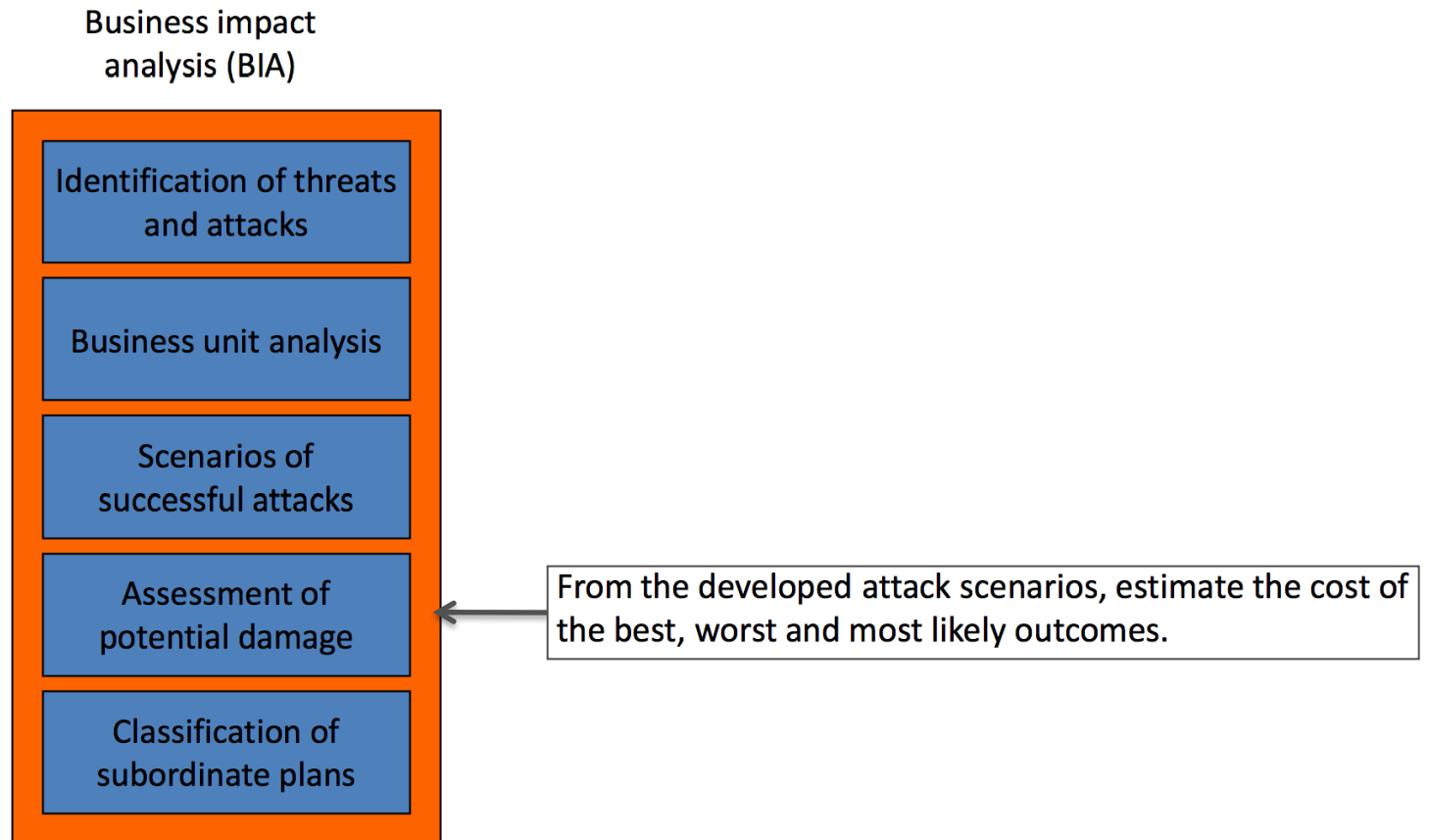
Business Function	Impact on Profitability (40 percent)	Contribution to Strategic Objectives (30 percent)	Impact on Internal Operations (20 percent)	Impact on Public Image (10 percent)	Total Weights (100 percent)
Enrolling new customers	8	8	3	6	6.8
Managing customer accounts	8	7	6	7	7.2
Providing Internet access	10	8	4	8	8
Providing Internet services	9	10	4	8	8.2
Providing help desk support	5	6	6	8	5.8
Advertising services	6	9	4	9	6.8
Supporting public relations	4	6	2	10	4.8

Whitman, Mattord and Green 2014, p. 59



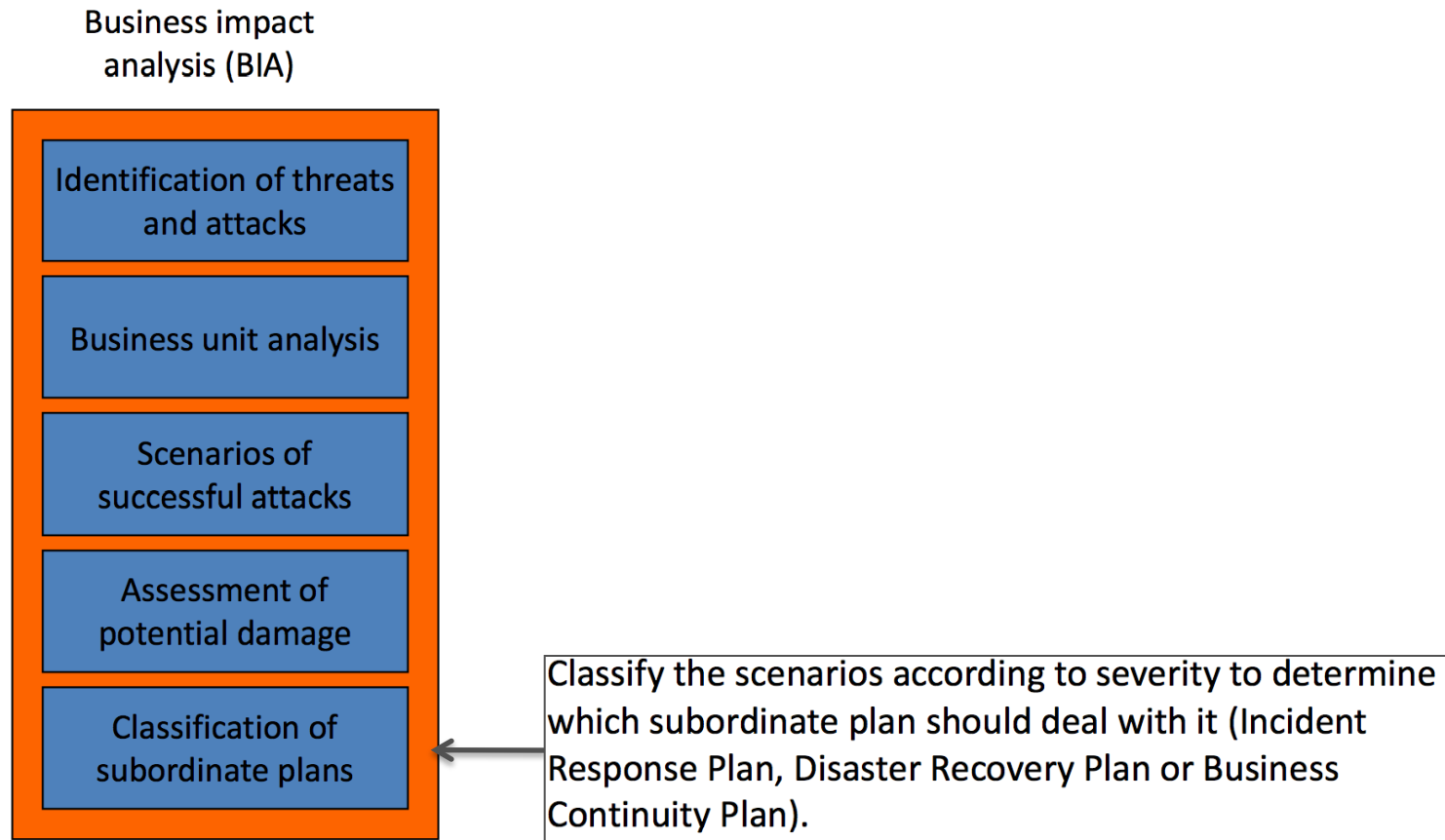
SCENARIOS OF SUCCESSFUL ATTACKS

Date of analysis:	June 23rd, 2009
Attack name/description:	Malicious code via e-mail
Threat/probable threat agents:	<ul style="list-style-type: none"> •Vandalism/script kiddies •Theft/experienced hacker
Known or possible vulnerabilities	<ul style="list-style-type: none"> •Emergent weaknesses in e-mail clients •Inappropriate actions by employees, contractors and visitors using e-mail clients •Emergent weakness in e-mail servers or gateways
Likely precursor activities	Announcements from vendors and bulletins
Likely attack activities or indicators of attack in progress:	<ul style="list-style-type: none"> •E-mail volume measurements show variance •Unusual system failure among clients •Unusual system failures among servers •Notification from e-mail recipients who may be ahead of us in attack life cycle



POTENTIAL DAMAGE ASSESSMENT

- Evaluate each of the developed scenarios for **potential cost** to the organization
- **Best** case, **worst** case and **expected** case
- Add this to the scenario descriptions



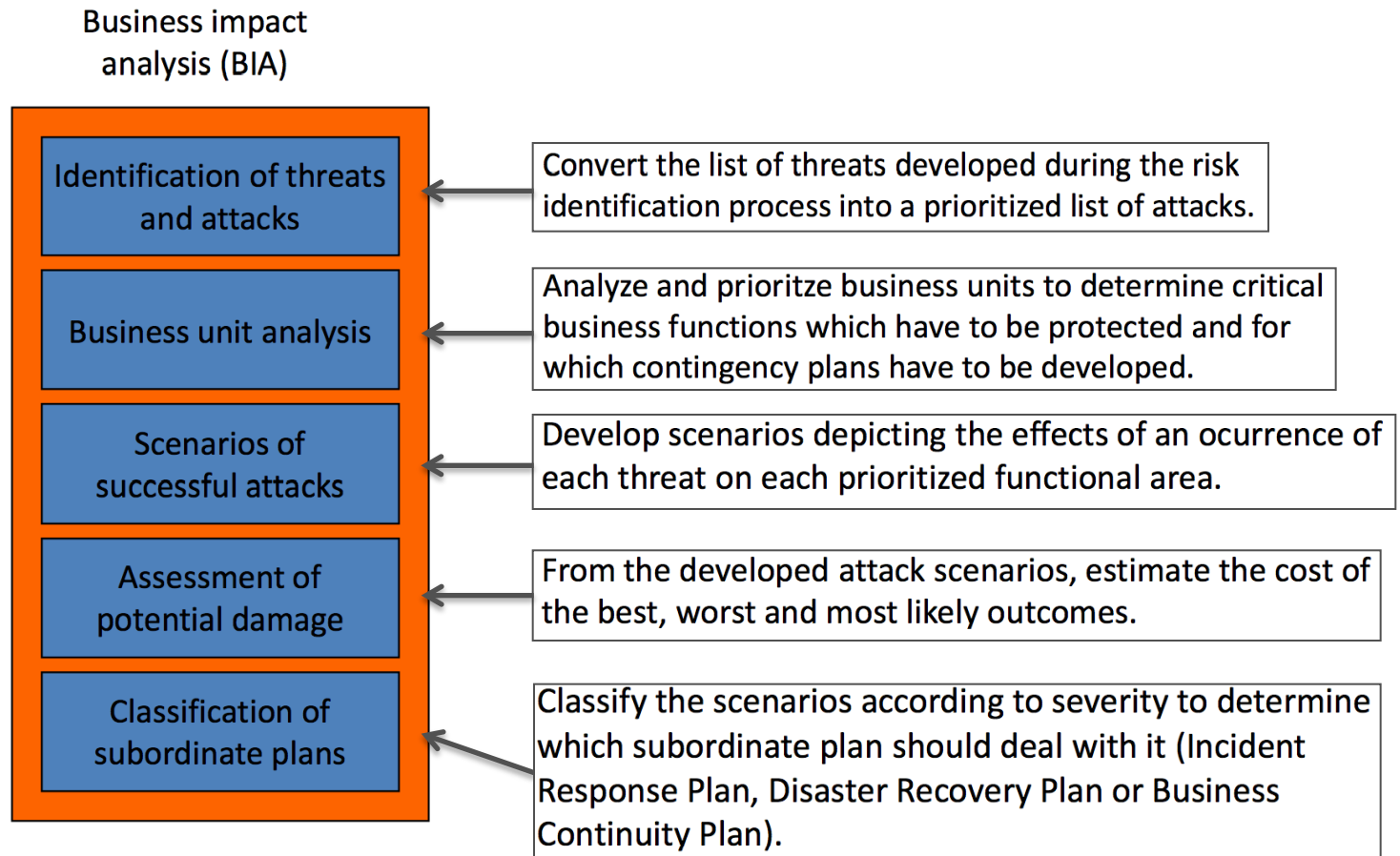
SUBORDINATE PLAN CLASSIFICATION

Identify appropriate plan for dealing with the aftermath of the attack:

- Incident response plan
- Disaster recovery plan
- Business continuity plan

Within each of the IR, DR or BR plans identify if there are subordinate plans that can handle the identified attack scenarios:

- If there are, check if addendums/adaptions are needed
 - *If yes, mark plan for updating*
- If not, develop new subordinate plan



BUSINESS IMPACT ANALYSIS DATA COLLECTION

- Is a continuous process
- Provides data on which analysis and decisions can be based
- BIA usually requires a large quantity of data
- A data collection plan should be established early on

BUSINESS IMPACT ANALYSIS QUESTIONNAIRE

Function description	What is the function of the business unit? What is it's purpose?
Dependencies	On what other business units or processes does the function depend on. What has to happen or needs to be available before the function can be performed.
Impact profile	Is there a specific time of day, day of week, week of the month, month of the year that the function is more vulnerable or the impact to the business would be greater?
Operational impacts	When would the operational impact to the business be realized if the function was not performed?
Financial impacts	When would the financial impact to the business be realized and what would it be if the function was not performed?
Legal impacts	Is it likely that the organisation will suffer lawsuits or undergo other legal proceedings after a disruption?
Competitive analysis	Is there a competitive impact if the function is not performed? When would the impact occur? When would the company potentially start losing customers?
Work backlog	At what point would the work backlog start to impact the business?
Impact on safety	Can a disruption endanger health, environment or safety (HES)?

BUSINESS IMPACT ANALYSIS QUESTIONNAIRE

Business function manager	Who is in charge of the business unit?
Organizational chart	What does the organizational chart look like? Who is responsible for the different parts of the business function?
Personnel requirements	What personnel resources are required to support the function?
Cross-training	Are personnel cross trained to perform other people's jobs?
Recovery resources	What kind of resources are needed to support the function? How many are needed and how soon after a disruption? (For example phones, desks, PCs)
Technology resources	What software and applications are needed to support the function?
Stand-alone PCs or workstations	Does the function require a stand-alone PC or workstation?
Local area networks	Does the function require access to the LAN?
Internet	Does the function require access to the Internet?

BUSINESS IMPACT ANALYSIS QUESTIONNAIRE

Work-around procedures	Are there currently in place manual work-around procedures that enable the function to be performed in the event that IT is unavailable? How long can manual work arounds continue to be used?
Work at home	Can the function be performed from home?
Workload shifting	Is it possible to shift workloads to another part of the business that might not be impacted by disruption?
Business records	Are certain business records needed to perform the function?
Regulatory reporting	Are regulatory documents created as a result of the function?
Work inflows	What input is recieved, either internally or externally, that is needed to perform the function?
Suppliers and vendors	Does the function depend on input from suppliers and/or vendors? What is the impact if the input is missing?
Work outflows	Where does the output go after it leaves the functional area, or who would be impacted if the function was not performed?
Clients	Does the output go to external clients? What is the impact to them if the output is missing?

METHODS TO COLLECT DATA

- Online questionnaires
- Facilitated data-gathering sessions
- Process flows and interdependency studies
- Risk assessment research
- IT application or system logs
- Financial reports and departmental budgets
- BCP/DRP audit documentation
- Production schedules

Whitman, Mattord and Green 2014, p. 64

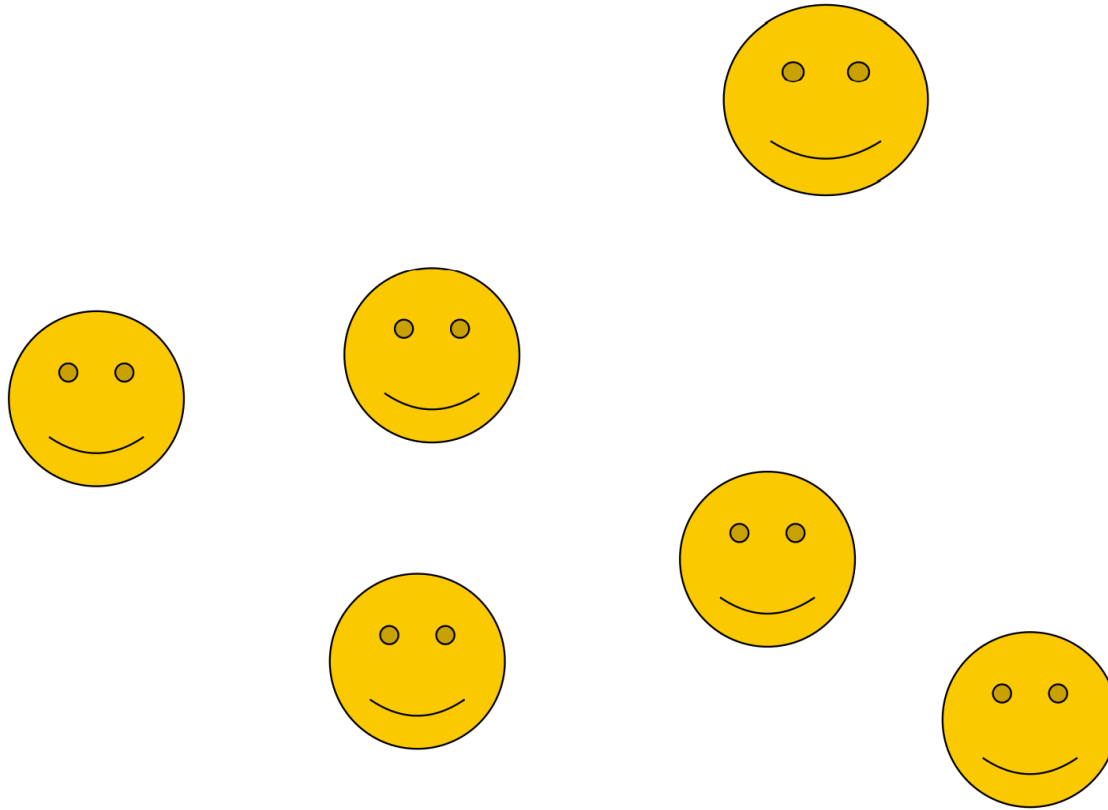
ONLINE QUESTIONNAIRES

- Asks the questions presented on the previous slides
- Most conveniently delivered online, but can also be delivered in paper form
- Highly structured manner of information collection
- Ensures that information is collected in a standard manner (important when information is ample)
- Easy to archive for future reference

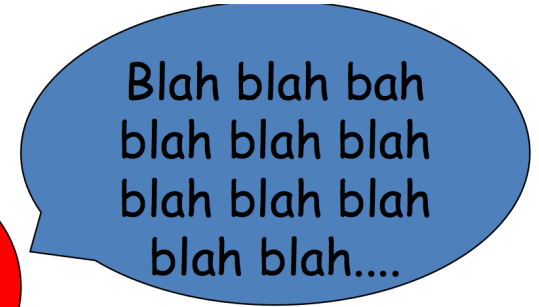
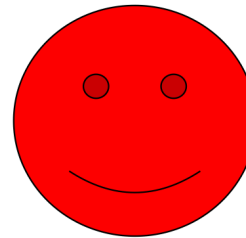
Based on Whitman and Mattord 2007, p. 69-83.



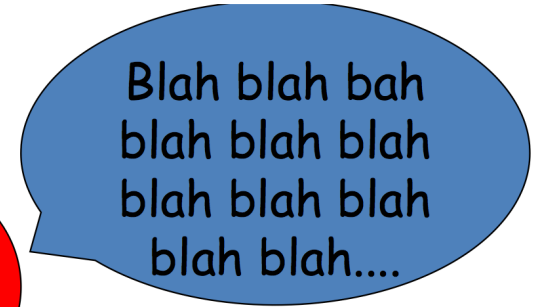
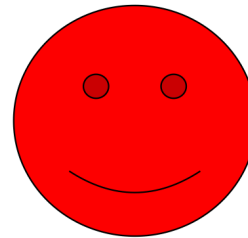
FACILITATED DATA-GATHERING SESSIONS



FACILITATED DATA-GATHERING SESSIONS

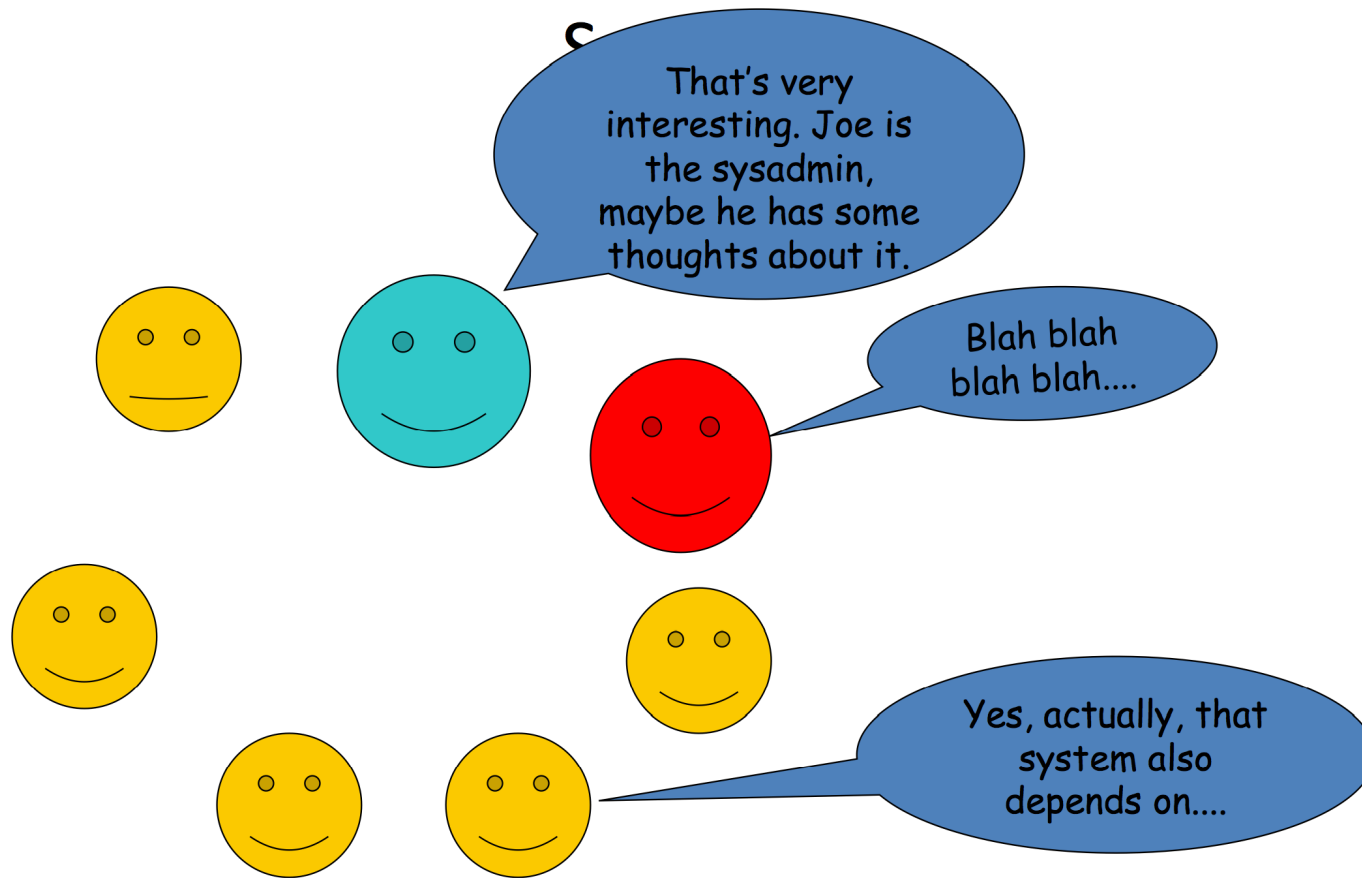


FACILITATED DATA-GATHERING SESSIONS





FACILITATED DATA-GATHERING SESSIONS



PROCESS FLOWS AND INTERDEPENDENCY STUDIES

Advantages:

- Better understanding of business processes
- Possible to detect unexpected and counterintuitive interactions and side effects

Disadvantages:

- The methods are complex
- The BIA team may not have the requisite skills

Unexpected bonus:

- Many organisations regularly create these kinds of diagrams as part of ongoing system development activities

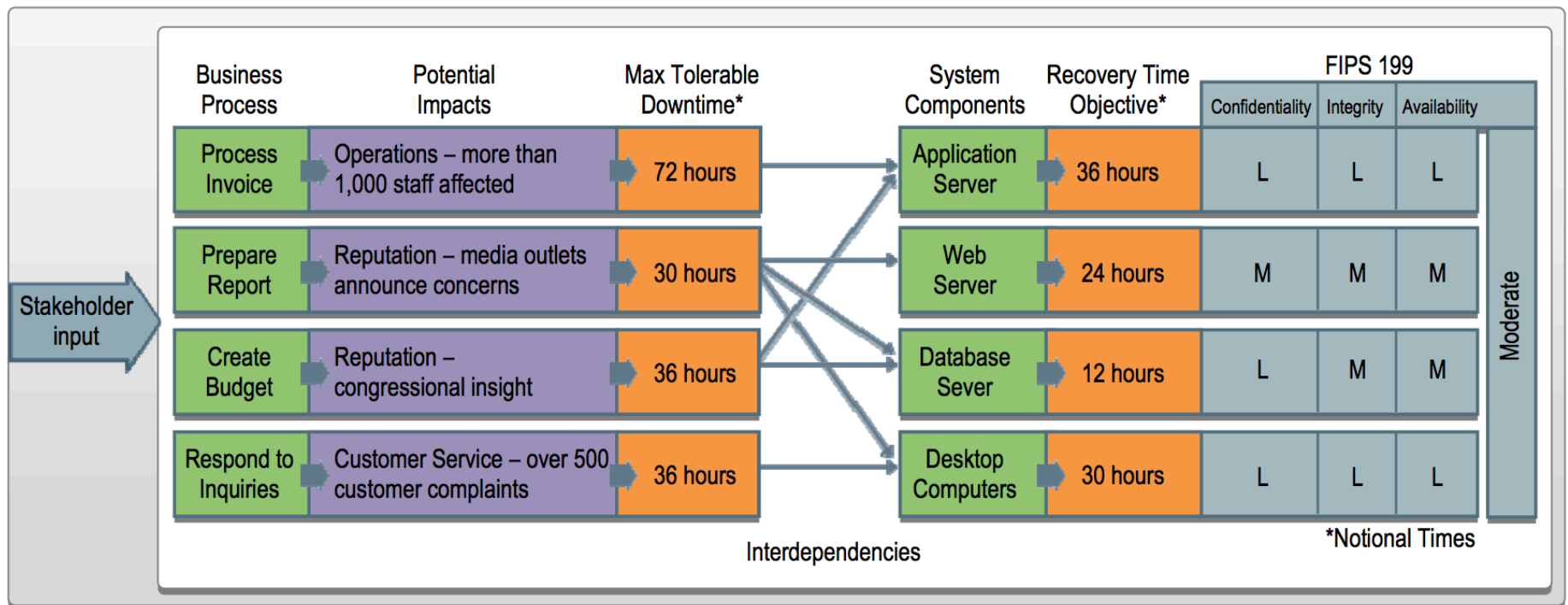
RECOVERY CRITICALITY ASSESSMENT

Key **downtime metrics**:

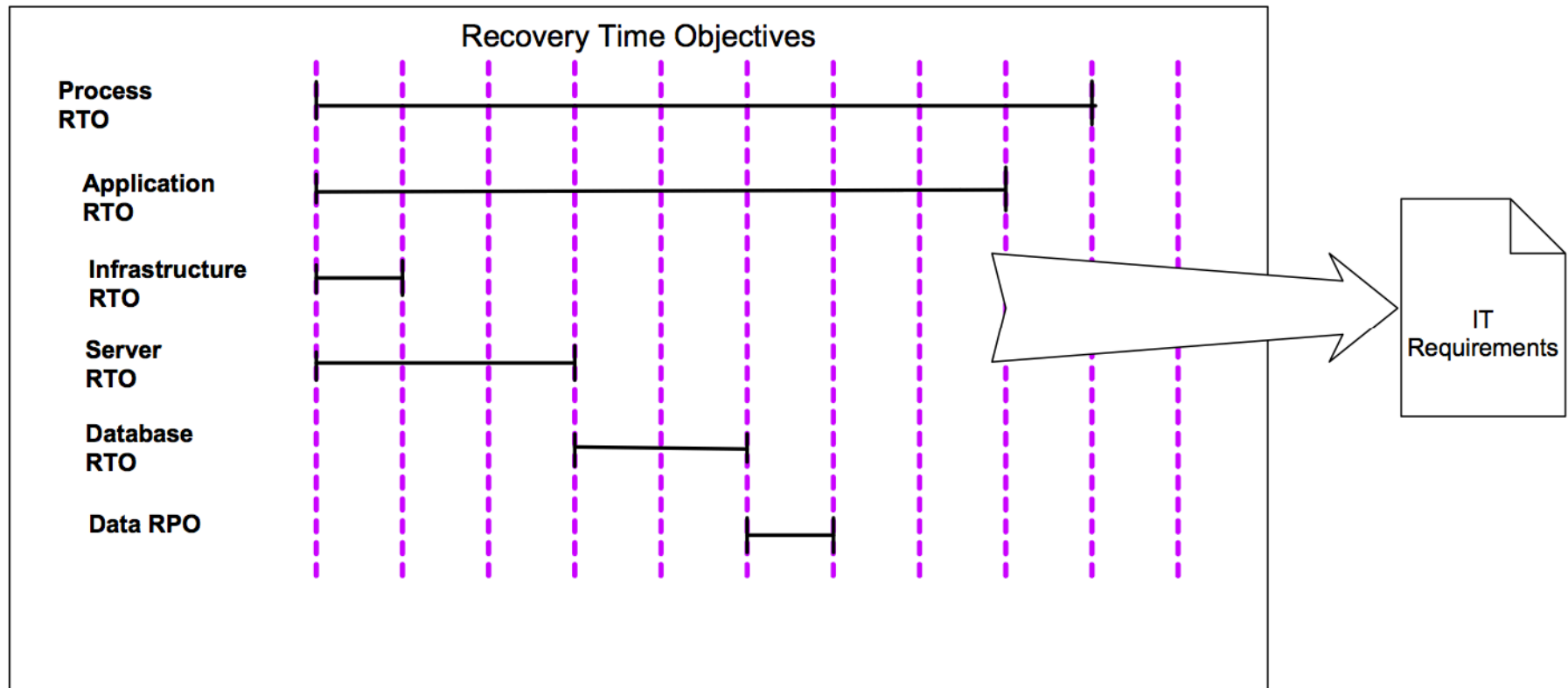
- Maximum tolerable downtime (MTD)
 - *The maximum downtime the system owner is willing to accept for a business process outage or disruption*
- Recovery time objective (RTO)
 - *The period of time within which system, applications or functions must be recovered after an outage*
- Recovery point objective (RPO)
 - *The point in time to which lost systems and data can be recovered after an outage as determined by the business unit*

Whitman, Mattord and Green 2014, p. 60-61

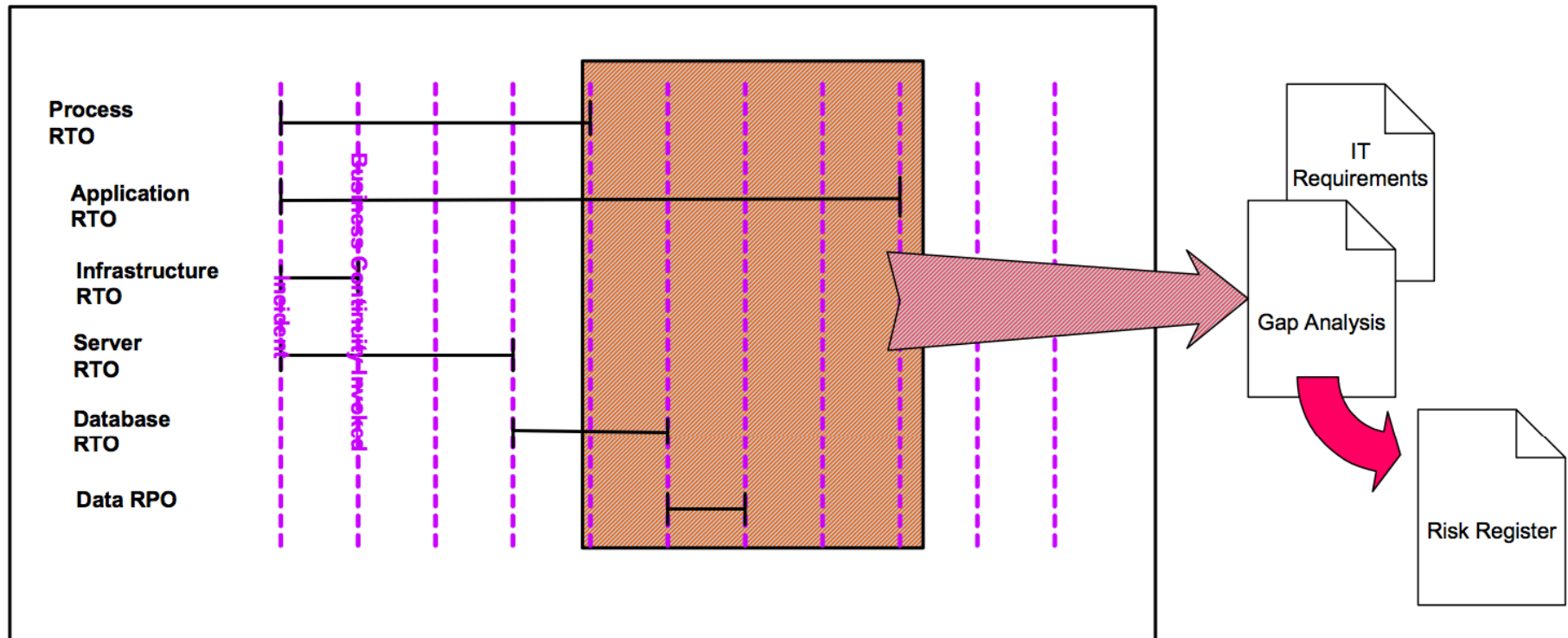
RECOVERY CRITICALITY AND INTERDEPENDENCIES



CRITICAL PROCESSES AND COMPONENTS RTO



GAP BETWEEN CRITICAL PROCESSES RTO AND COMPONENTS RTO



RESOURCE REQUIREMENTS AND RECOVERY PRIORITIES

Develop a **recovery profile** that specifies:

- *What is being recovered over time*
- *Specific resources required at any time to support the recovery*

The recovery profile will allow the identification of a number of possible **recovery options**.

The choice of recovery options will determine **the contingency strategy**.

ENISA deliverable: Business and IT Continuity: Overview and Implementation Principles, page 41

DETERMINE RECOVERY OPTIONS

Options should be determined for the following areas:

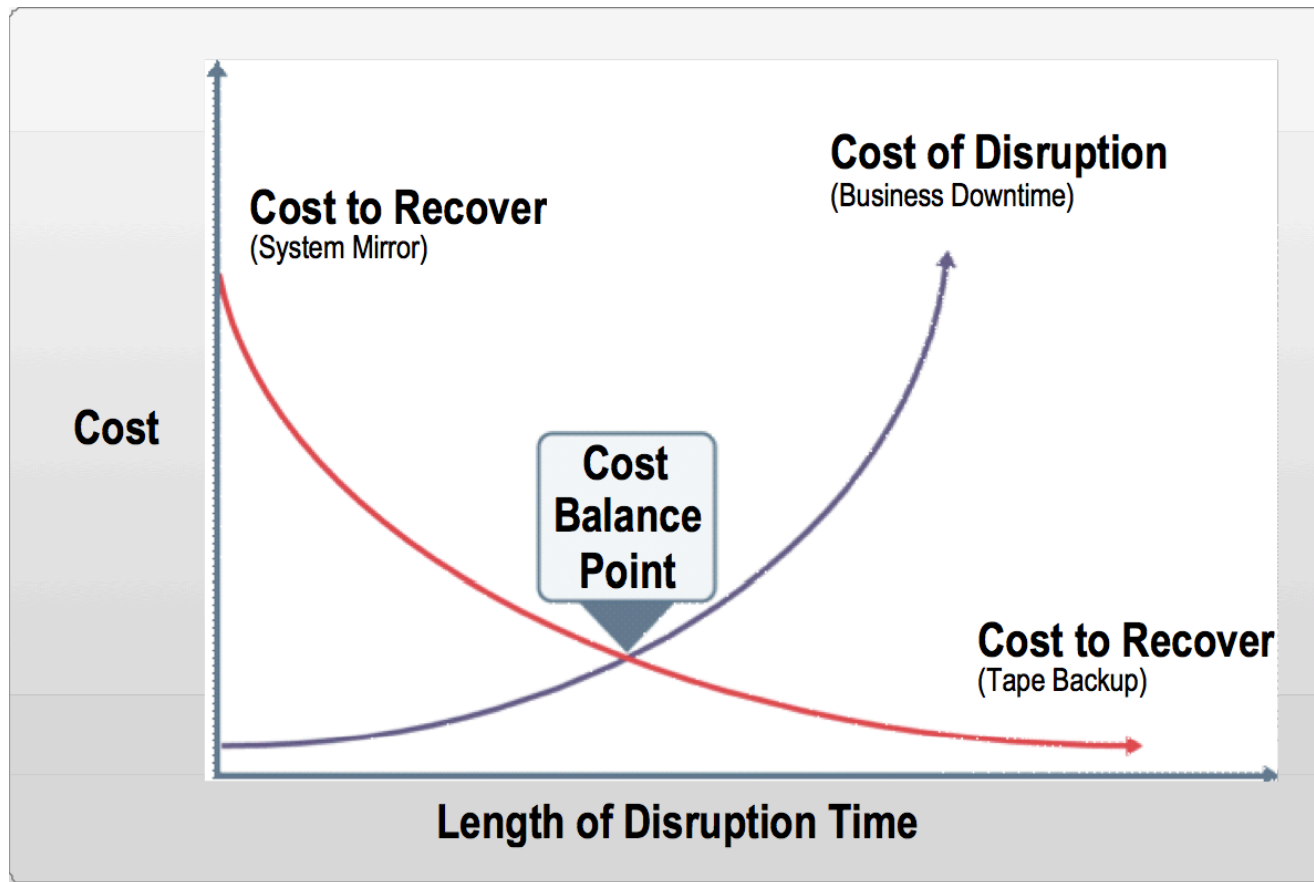
- *Staff*
- *Premises*
- *Technology*
- *Supplies*
- *Stakeholders*

The options will depend on:

- *RTOs for the critical processes*
- *RPOs for the critical data*
- *Interdependencies of components*
- *Costs of implementation of various options*
- *Consequences of inaction*

ENISA deliverable: Business and IT Continuity: Overview and Implementation Principles, pages 43-44

OPTIMIZING CONTINGENCY STRATEGY



PREVENTIVE CONTROLS AND RECOVERY OPTIONS

- Uninterruptible power supplies (UPS)
- Gasoline- or diesel-powered generators
- Air-conditioning systems with adequate excess capacity to prevent failure of certain components
- Fire suppression systems
- Fire and smoke detectors
- Water sensors in the computer room ceiling and floor
- Heat-resistant and waterproof containers for backup media and vital non electronic records
- Emergency master system shutdown switch
- Offsite storage of backup media, non electronic records, and system documentation
- Technical security controls, such as cryptographic key management
- Frequent scheduled backups

TECHNIQUES USED FOR DATA AND APPLICATION BACKUP AND RECOVERY

- On-line backup to a third party data storage (Cloud)
- Disk-to-disk-to-other
 - Disk to disk to tape
 - Disk to disk to Cloud
- Mirroring
 - Electronic Vaulting
 - Remote Journaling
 - Database Shadowing
- Redundancy-based backup and recovery using RAID, virtualization, NAS and SANs

BACKUP AND RECOVERY PLANS

- How and when will backups be created?
- Who will be responsible for creation of the backups?
- How and when will backups be verified so that they are known to be correct and verifiable?
- Who is responsible for the verification of the backup?
- Where will backups be stored and for how long?
- How often will the backup plan be tested?
- When will the plan be reviewed and revised?
- How often will the plan be rehearsed?

ALTERNATE SITE OPTIONS

Site	Cost	Hardware Equipment	Telecoms	Setup Time	Location
Cold	Low	None	None	Long	Fixed
Warm	Medium	Partial	Partial	Medium	Fixed
Hot	Medium/ High	Full	Full	Short	Fixed
Mobile	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored	High	Full	Full	None	Fixed

BACKUP AND RECOVERY STRATEGY EXAMPLE

FIPS 199 Availability Impact Level	Information System Target Priority and Recovery	Backup / Recovery Strategy ²³
Low	Low priority - any outage with little impact, damage, or disruption to the organization.	Backup: Tape backup Strategy: Relocate or Cold site
Moderate	Important or moderate priority - any system that, if disrupted, would cause a moderate problem to the organization and possibly other networks or systems.	Backup: Optical backup, WAN/VLAN replication Strategy: Cold or Warm site
High	Mission-critical or high priority - the damage or disruption to these systems would cause the most impact on the organization, mission, and other networks and systems.	Backup: Mirrored systems and disc replication Strategy: Hot site

M. Swanson, P. Bowen, A. Phillips, D. Gallup and D. Lynes, "Contingency Planning Guide for Federal Information Systems", NIST Special Publication 800-34 Rev. 1, accessed February 2014 from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

CONSIDER RTO WHEN CHOOSING RECOVERY OPTIONS

A process RTO of *several months* may allow the organisation to chose to leave any decisions until after the event.

A process RTO of over *a day or two* may allow time for staff to be relocated to another site.

A process RTO of *less than a day* will require tactics that enable the activity to be taken on by staff at other locations, or quick relocation of affected staff.

ENISA deliverable: Business and IT Continuity: Overview and Implementation Principles, page 44

NEXT LECTURE

The topic of the next lecture on the 17th of February will be:

Incident Response Planning

Recommended reading to prepare for the next lecture:

- Chapter 4 in Whitman & Mattord
- Carnegie Mellon University Handbook: *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*

PROJECT WORK

- Remember to submit your project proposals as soon as possible to me via email
- Trouble finding a group?
 - Raise your hand now and connect after class
 - Or send me an email and I will try to put you in contact with other students in the same situation
- If you wish you may submit preliminary drafts for comments to me via email
- The complete draft must be submitted via Fronter before the 4th of April