Joint Universities Computer Centre Limited
("JUCC")
Information Security Awareness Training- Session Three

Information Security- Perspective for Management
Business Impact Analysis ("BIA") and Business Continuity Management

Agenda

- Business Impact Analysis
  - Overview
  - Terminologies
  - Process
- Business Continuity Management
  - Overview
  - Functions
  - Process

Overview

BUSINESS IMPACT ANALYSIS

- the operation activities
- the measure of failure
- the evaluation process

Business Impact

Business Impact

- Business impact is a **measure** of how an organisation might be **affected by a process failure**, caused by technology, premise, or human resource issues.
- Impact is classified as either revenue or non-revenue.
  - **Revenue impact** includes the full or partial failure of any process which produces, collects, or processes business income.
  - **Non-revenue impact** is caused by challenges that do not directly affect short term realisation of revenue.
  - Although causes of non-revenue impact might not result in immediate financial losses, some could result in long term financial damage through loss of investor or customer good will.

Business Impact

- Business impact can be calculated using either a **qualitative** or a **quantitative** approach.

Qualitative

- Qualitative analysis depends on the experience of employees and consultants to arrive at risk scores.

Quantitative

- The results of the quantitative approach are estimates of potential dollar losses based on known costs or revenue streams.

Business Impact Analysis - definition:

- BIA- "An impact analysis results in the differentiation between critical (urgent) and non-critical (non-urgent) organization functions/ activities."

-Wikipedia

Why Critical?

- Contain financial loss
- Allow business continuity
- Fulfill legal requirements

What for?

- Determine criticality
- Allocate limited resources limited for recovery requirements

Business Impact Analysis

- BIA is an essential component of an organisation's business continuity plan
- Assumptions:
  - *Every component of the organisation is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster.*

BIA

- **Reveals** any vulnerabilities
- **Identifies** costs linked to failures
  Such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits…
- **Quantifies** the importance of business components
- **Suggests** appropriate fund allocation for measures to protect them
- **Assesses** the possibilities of failures in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance.
- **Expresses** impact monetarily for purposes of comparison
  For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence.
- **Develops** strategies for minimising risk

What is Business Impact Analysis (BIA)

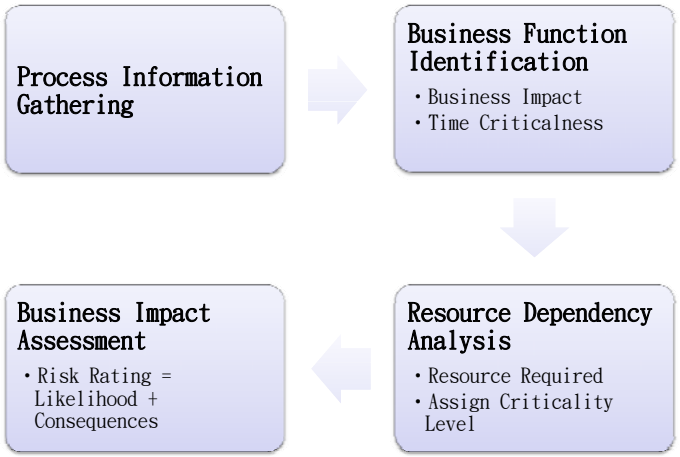
BIA- the Risk Management Perspective

- Impact vs Risk

  Risk = Probability of Occurrence (PO) x Business Impact (BI)

- **Probability** of occurrence is calculated using the threat and vulnerability analysis. It's represented as the number of occurrences expected in a single year. This is known as the Annual Rate of Occurrence (ARO).

The BIA Process



BIA- Terminologies

- Data and process owners are required to determine a number of figures
- Management should be aware of these terminologies
- Senior management should be responsible for the review and approval of the follow:
  - Criticality/ Time-sensitivity
  - Recovery Point Objective ("RPO")
  - Recovery Time Objective ("RTO")
  - Maximum Tolerable Downtime ("MTD")

Criticality/ Time-sensitivity

- Organisations do not hire staff to perform non-essential tasks.
- Every function has a purpose, but some are more time-sensitive than others when there is limited time or resources available to perform them.
- The organisation needs to look at every function.

Criticality/ Time-sensitivity:

- How long can the entity not perform this function without causing significant financial losses, or significant penalties or fines from regulators or from lawsuits?

Recovery Point Objective ("RPO")

- Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time.
- The **point in time** for which data must be restored in order to resume transaction processing.
- Generally defining what the organisation 's "**acceptable loss**" in a disaster situation.

Recovery Point Objective ("RPO")

Example (RPO=2hrs)

- Backup at 11:00am
- System crashed at 12:59pm without new backup
- The loss of the data written between 11:00am and 12:59pm will be lost.
- Data loss is acceptable because of the 2 hour RPO.
- This is the case even if it takes an additional 3 hours to get the site back into production.
- The restored system will continue with data at the point in time of 11:00am.
- All data in between will have to be manually recovered through other means.

Recovery Time Objective ("RTO")

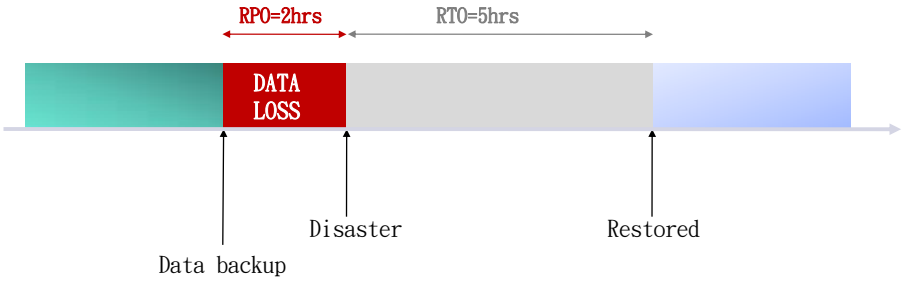
- Recovery Time Objective (RTO) is the **duration of time** and a service level within which a business process must be restored after a disruption in order to avoid unacceptable consequences associated with a break in business continuity.
- RTO includes
  - the time for trying to fix the problem without a recovery
  - the recovery
  - tests and the communication to the users
- Decision time for users representative is not included.

RPO & RTO

- RTO and RPO are objectives, not mandates.
- Current strategy selected may not meet the objectives
- But the RTO and RPO approved by senior management remain as objectives
- Expected deviation from the objectives should be monitored

RPO vs RTO

- If RPO = 2hrs → the entity cannot suffer loss of data made in 2hours time
- If RTO = 5hrs → the entity cannot accept the data being not available for more than 2 hrs

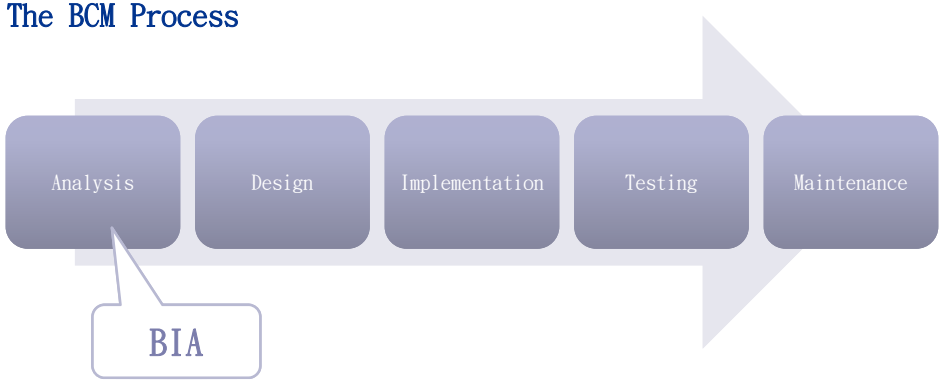


Maximum Tolerable Downtime ("MTD")

- MTD (Maximum Tolerable Downtime) is the maximum time a critical process can be down, or hindered in some way, without irreparable harm to the business.
- Calculated as part of a BIA and is used during risk calculations.
- Interrelationship between critical processes should be factored in to MTDs.
- A process MTD is an adjustable value.

Business Continuity Management (BCM)

The BCM Process



Business Continuity Management (BCM)

BCM

- Activities designed to manage risk by reducing the likelihood and the impact of a physical disaster or significant service interruption
- Assumes a worst-case scenario, in which the primary business location is suddenly rendered totally inaccessible or otherwise unusable for an extended period of time
- IT departments usually lead in disaster recovery planning for computer and data communications resources
- BCM focuses on restoring critical business functions

Business Continuity Management (BCM)

Why BCM?

- Not having a course of action if a devastating disaster or service interruption occurs can result in total loss of the business
- There are legal and board member obligations to protect the lives and assets of the corporation - due diligence

Functions

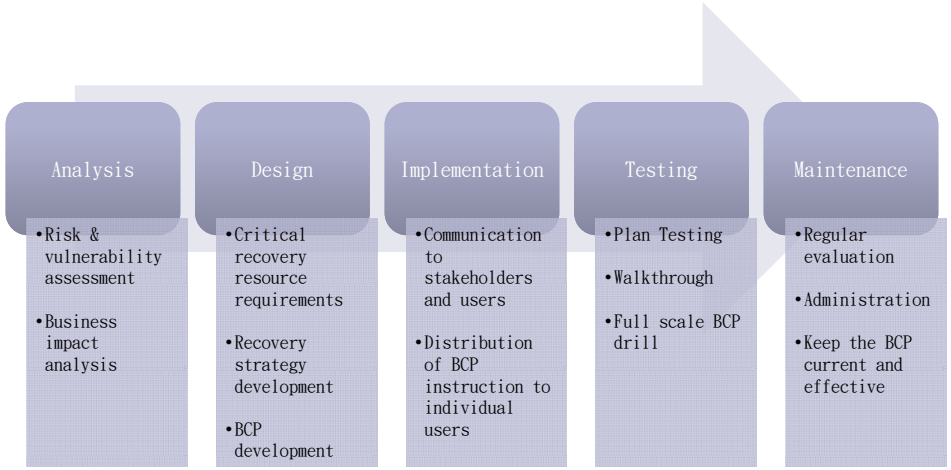
- Minimise decision making during a crisis;
- Define alternatives for continuing critical services;
- Define organisational priorities (BIA) and time frames;

Business Continuity Management (BCM)

Requirements

- Management support
- User commitment and participation
- Well defined recovery requirements
- Evaluation and documentation of impact
- Focus on disaster prevention, impact minimisation and recovery
- Experienced project team
- Understandable, easy to use and easy to maintain business continuity plans

Business Continuity Management (BCM)



Conclusion

Business Impact Analysis

- Understand the criticality and recovery priority of business processes

Business Continuity Management

- Reduce the likelihood and impact of business interruption


Q&A

?