Joint Universities Computer Centre Limited
(“JUCC”)
Information Security Awareness Training- Session Four

Data Handling in University
Business Impact Analysis (“BIA”)

Agenda

- Overview
- Terminologies
- Performing BIA
- Example - how to do BIA
- Business Continuity Planning
- Conclusion

Overview

BUSINESS IMPACT ANALYSIS

the operation activities

the measure of failure

the evaluation process

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?

- Financial loss
- Business continuity
- Legal requirements

What for?

- Determine criticality
- Allocate resources (limited) to 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.*

What is Business Impact Analysis (BIA)

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

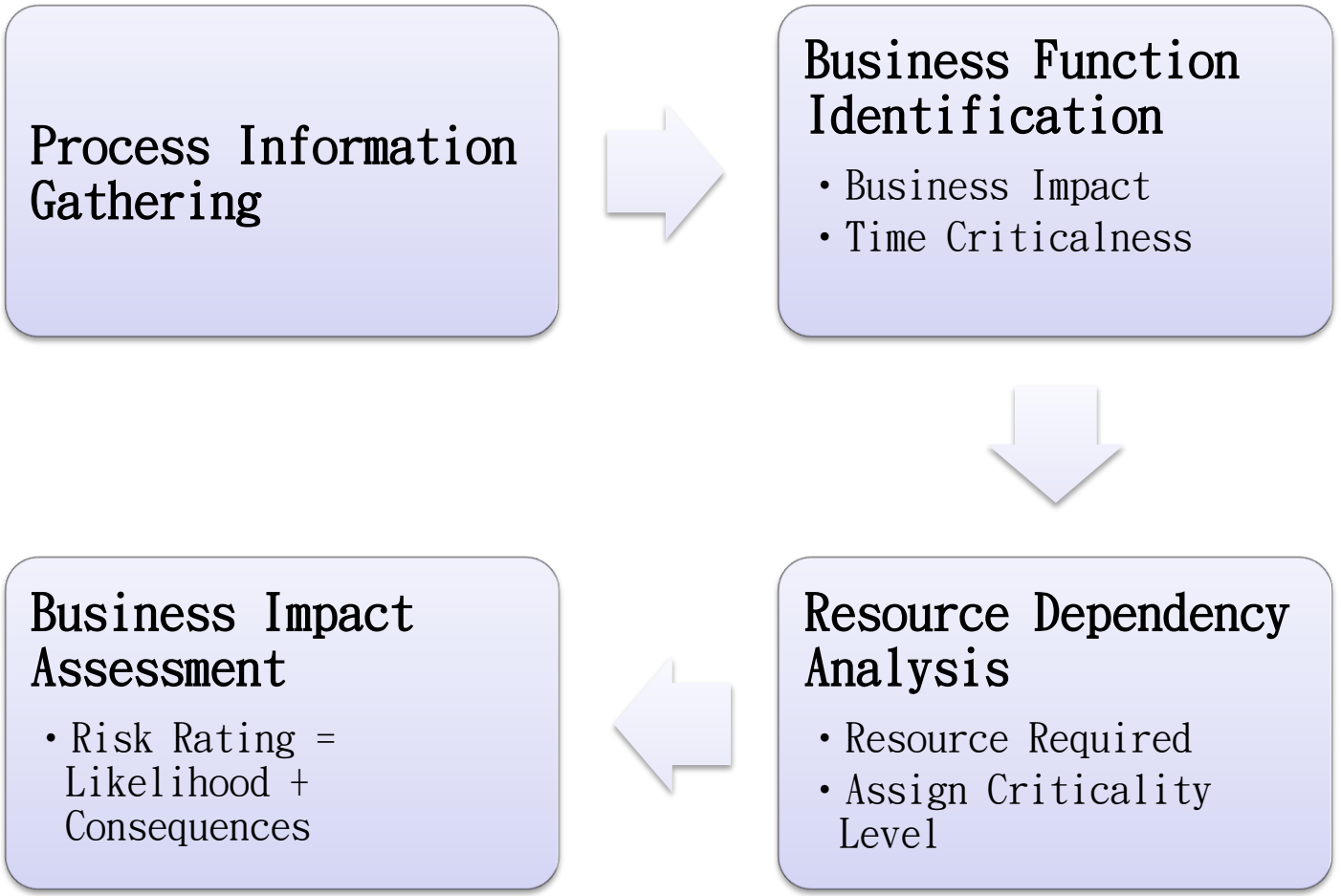
BIA- the Risk Management Perspective

- 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).
- *For example, if information about known threats, vulnerabilities, and actual events lead an analyst to believe a threat will cause a weakness to interrupt business operations once every four years, the probability of occurrence is .25.*
- *During a qualitative BIA, the analyst uses probability of occurrence (PO) and business impact (BI) to arrive at a risk score. The risk score is a measure of the amount of damage resulting from one or more failed critical processes.*

The BIA Process



Terminologies

- 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.

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.
- RTO is established during the Business Impact Analysis (BIA) by the owner of a process. The RTOs are then presented to senior management for acceptance.

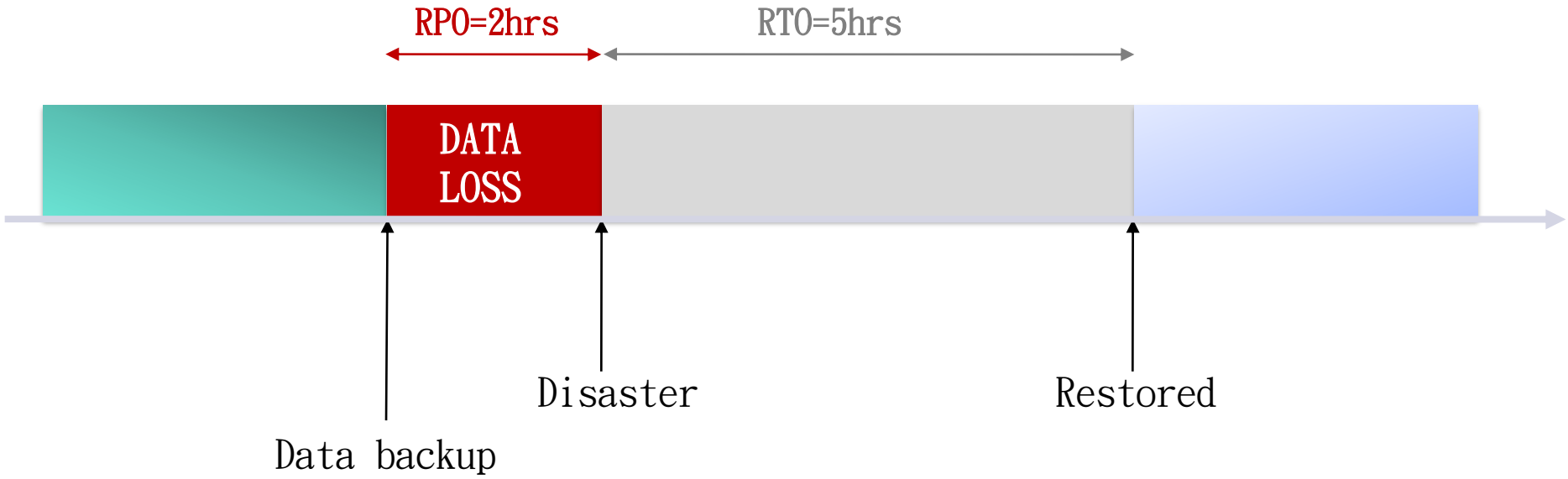
Recovery Time Objective ("RTO")

- The RTO attaches to the business process and not the resources required to support the process.
- The RTO and the results of the BIA provide the basis for identifying and analysing viable strategies for inclusion in the business continuity plan.
- Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO.
- This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTOs

The "O" in RTO stands for objective, not mandate. In reality, strategy is often selected that will not meet the RTO. In this instance the RTO will not be met but should still remain an objective of future strategy revision.

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. It's typically calculated as part of a BIA and is used during risk calculations.
- At a high level, a BIA begins with identifying critical processes, describes resources necessary to maintain them, calculates the financial or reputation impact on the business if the process fails, and determines process MTD.
- Other processes which depend on the failed process' output also suffer. So a BIA must also describe the interrelationship between all critical processes and factor this into their MTDs.
- A process MTD is an adjustable value.

Performing BIA

1. Business Function Identification
2. Resource Dependency Analysis
3. Business Impact Assessment
4. Mitigation

Aim: to rank business processes by criticality

Performing BIA - Business Function Identification

Determine Business Processes

- Obtain an understanding of business processes within the entity
- Identify business processes and dependencies
- Identify process owners (department management/ key staff)
- Information for assessing business impacts and identifying resources requirement can be obtained by sighting internal documentation and conducting interviews with process owners:
    - Interviews
    - Workshops
    - Surveys

Identify Business Impact

- Business impacts include
  - Financial impact (actual & potential);
  - Operational impact;
  - Impact of regulatory, legislative non-compliance; and
  - Any other negative impacts to the business in the event of disaster.

1

Performing BIA - Business Function Identification

- **Financial Impact**
  - The direct and indirect results may be lost sales, lost revenue, loss of business opportunities, impaired cash flow, contractual fines or other penalties, etc.
- **Operational Impact**
  - Operational impacts are the result of disruption to daily operations. Impacts may include:
    - Negative public image (reputation)
    - Client satisfaction and loyalty
    - Employee morale
    - Health & safety
- **Regulatory/ Legislative/ Non-compliance**
  - Potential regulatory penalties
  - Breach of regulatory requirement
  - Litigation

Time Criticalness

- Time criticalness is ranked by the following two criteria:
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)

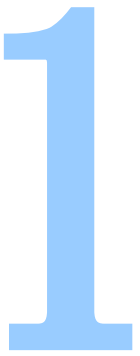
Business Function 001

Process Owner: xxxxxx

Dependency: BF008/BF009

Potential Impact on Disruption:
……..

Time Criticalness: RTO=xx RPO=xx



Performing BIA - Resource Dependency Analysis

- Summarize the minimum set of recovery facilities, resources and services that would be required by each business unit at different times during disaster recovery.
  - Identify the resource required to accomplish the process
  - Classify the resources required (e.g. facility, capital, manpower, services…)

2

Performing BIA - Business Impact Assessment

- Potential risk events (e.g. power outage, virus infection…) impacting the critical business functions processes.
- For each risk identified, rate the
  - Likelihood
  - Criticality (RTO)
  - Consequence of occurrence.

3

Performing BIA - Mitigate Risks

- Once identified failure exceeds acceptable risk threshold:

4

Example - How to do a BIA

Example: Student record maintenance by Registry

No	Dept	Key Business Functions	Consequences of disruption	RTO	RPO	Service level Commitment	Notes
		Critical processes or services that are business unit' s responsibility.	Impact of loss of function e.g. financial loss, loss of business, operational impact, regulatory, legislative non-compliance, etc	Maximum time the business can tolerate without this function	Maximum amount of data the business can afford to lose	Internal or external Service Level Agreements (SLAs) in place for this function.	Other comments
1	Registry	Student record maintenance	Unable to provide student data for faculties and administrative departments when requested	1 week	12 hrs	N/A	

Example - How to do a BIA

How long before the absence or service degradation of the process/department becomes critical? (Mark one box noting the number of hours, days or weeks)	Criticality Level				
	1 (0-3 days)	2 (3-5 days)	3 (5-7 days)	4 (1-2 weeks)	5 >2 weeks
(**Registry**- Student Record Maintenance)				X	

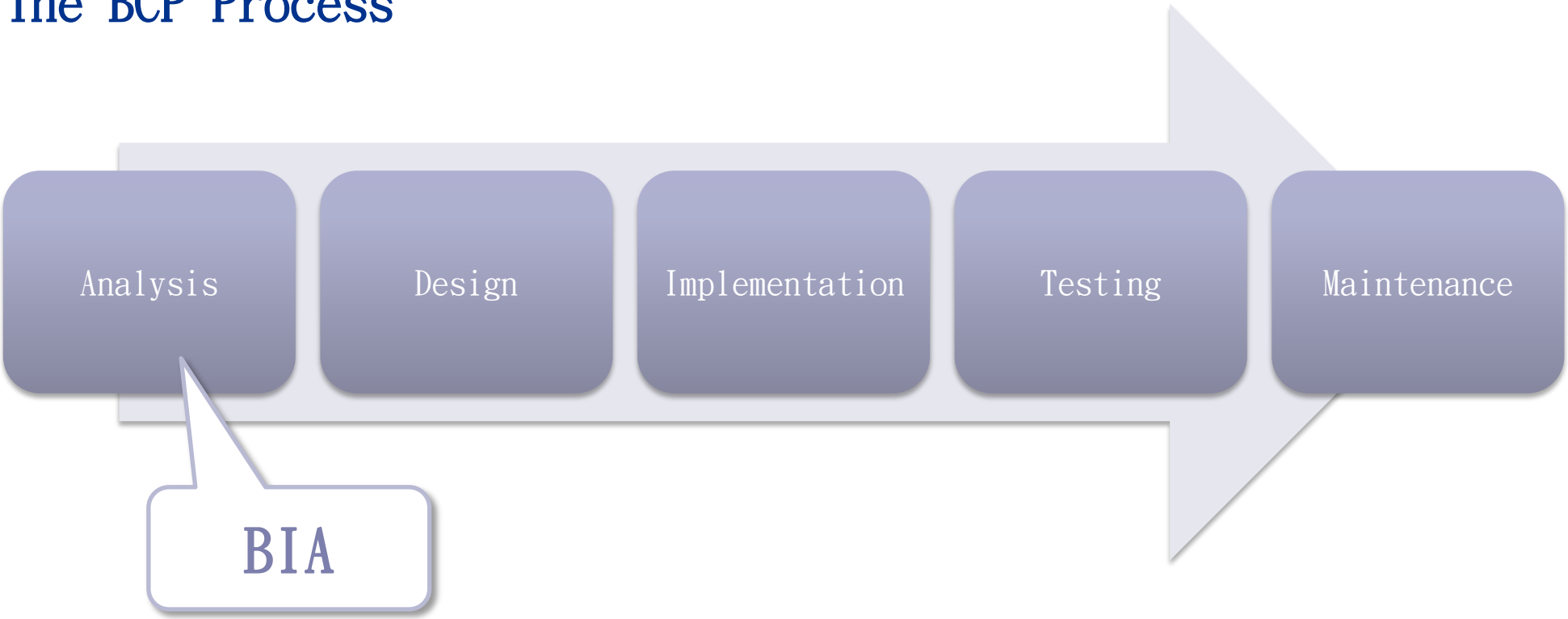
Example - How to do a BIA (Resource Dependency Analysis)

Department: Registry		
Process: Student Record Maintenance	Number of resources required	Critical level
Information Technology Dependencies		
Hardware		
• PC	1	4
• Printer	1	5
Desktop		
• Microsoft Word	1	4
• Microsoft Excel	0	
• Intranet access	1	3
• Internet access	0	
Local Applications		
• N/A	N/A	
Communications		
• Telephones - Landline	1	3
• Telephones - Mobiles	N/A	
Key internal suppliers / interface (i.e.: number of staff temporary borrowed from other Departments during disaster)		
• Clerical staff (for manual record processing)	2	2
Key external suppliers / vendors (i.e. IT system not supported by IT Department)		
• N/A	N/A	

Example - How to do a BIA (Business Impact Assessment)

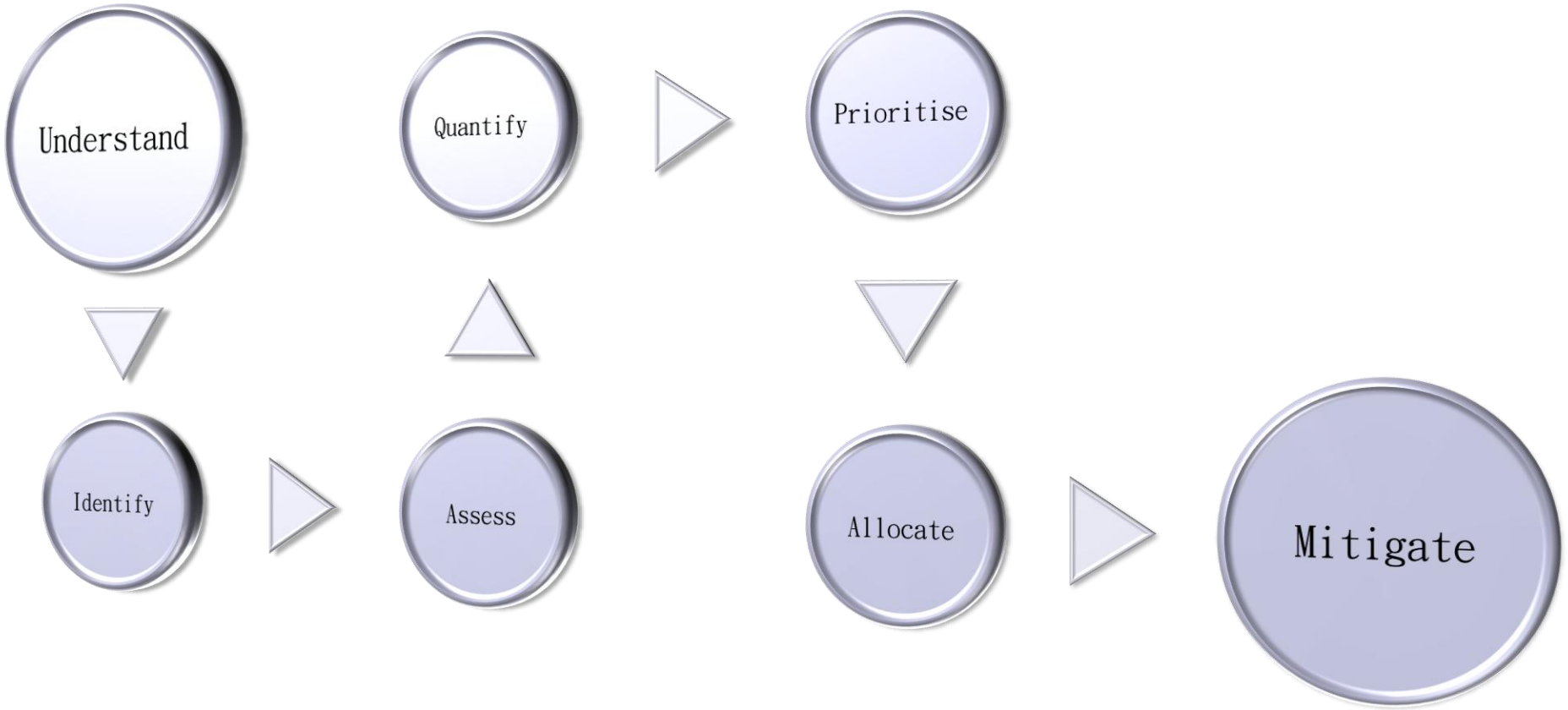
Process Reference & Risk Description		Likelihood	Consequences	Risk Rating	Contingency / Mitigation Action
				Likelihood + Consequences	(e.g. Manual alternatives, escalation procedures)
1.	Student Record Maintenance				
1.1	Student Record System Unavailable due to server outage	1	3	4	User paper records for student record queries

The BCP Process

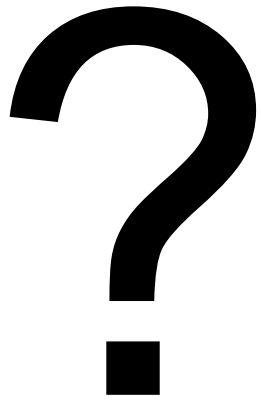


Conclusion

BIA



Q&A



Copyright Statement

copyright@jucc.edu.hk
Joint Universities Computer Centre Limited (JUCC),
Room 223, Run Run Shaw Building,
c/o Computer Centre, The University of Hong Kong,
Pokfulam Road, Hong Kong