

### Lab #7 – Assessment Worksheet

Course Name: IAP401

Student Name: Dang Hoang Nguyen

Business Function	Business Impact	RTO/RPO	IT Systems/Apps
Internal and external voice communications with customers in real-time	Critical	8 hours/ 0 hour	Email server, LAN, WAN Network
Internal and external e-mail communications with customers via store and forward messaging	Critical	8 hours/ 0 hour	Intra/Internet, Network, Email Serve
DNS – for internal and external IP communications	Minor	48 hours/ 24 hours	Email server, DNS, network
Internet connectivity for email and store and forward customer service	Minor	48 hours/ 24 hours	Web servers, email server, LAN, WAN network
Self-service website for customer access to information and personal account information	Critical	2 hours/ 0 hour	Web servers, customer database, account application, WAN network
e-Commerce site for online customer purchases or scheduling 24x7x365	Critical	1 hour/ 0 hour	Web servers, inventory database, scheduling application, purchase application, WAN network, internet access
Payroll and human resources for employees	Major	24 hours/ 12 hours	Employee database, payroll application, LAN network
Real-time customer service via website, e-mail, or telephone requires CRM	Critical	2 hours/ 0 hour	Web servers, email servers, CRM application, CRM database

Network management and	Major	24 hours/ 12hours	LAN, WAN network, internet access, remote management
Marketing and events	Minor	1 week/ 3 days	Marketing and event planning application
Sales orders or customer/ student registration	Critical	2 hours/ 0hour	Web server, account application, internet access, inventory database
Remote branch office sales order entry to headquarters	Critical	8 hours/0hour	VPN application, internet access, inventory database
Voice and e-mail communications to remote branches	Critical	8 hours/0hour	Email server, DNS, LAN, WAN network
Accounting and finance support: Accts payable, Accts receivable, etc	Major	24 hours/12hours	Account application, customer and employee database, LAN network

**Lab #7 – Assessment Worksheet**  
**Part B – Craft a Business Continuity Plan Policy – Business Impact Analysis**

**Course Name: IAP401**

**Student Name: Dang Hoang Nguyen**

**ABC Credit Union**  
**Business Continuity Plan Policy - Business Impact Analysis**

**Policy Statement:**

The objective of ABC Credit Union's Business Continuity Plan (BCP) Policy is to set standards and processes for carrying out a Business Impact Analysis (BIA) in order to evaluate and match impacted IT systems, applications, and resources with their necessary Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). This policy provides the structure for classifying mission-critical business functions, ranking them, and specifying the necessary recovery actions to keep IT running in a timely manner in the event of disruptions or emergencies.

**Purpose/Objectives:**

- To evaluate how prospective interruptions might affect IT systems and business operations.
- To rank mission-critical business operations in order of significance to the company.
- Identifying the recovery point and recovery time objectives (RPOs) for the designated business functions.
- To create a structure for creating recovery and business continuity plans that are in line with RTOs and RPOs.

**Scope:**

This policy is applicable to all ABC Credit Union departments and employees who plan for business continuity and participate in disaster recovery activities. This policy's scope includes identifying, evaluating, and prioritizing mission-critical business functions in addition to establishing RTOs and RPOs for the IT systems, applications, and resources that these functions depend on.

**Standards:**

This policy establishes the following standards and metrics for conducting the Business Impact Analysis (BIA):

- Recovery Time Objectives (RTOs): RTOs specify the amount of time that must pass after an interruption for IT systems and applications to be recovered in order to maintain operations. They are defined as the maximum allowable downtime for each mission-critical business function.

- Recovery Point Objectives (RPOs): RPOs identify the point in time to which data must be recovered following an interruption to minimize the impact on business operations. They are defined as the maximum allowable data loss for each mission-critical business function.

## **Procedures:**

1. Performing the Business Impact Analysis (BIA): o Determine and rank the mission-critical business functions according to how crucial they are to the goals and operations of the firm.

- Evaluate how possible disruptions might affect the IT resources, apps, and systems that support particular business functions.
- After consulting with pertinent stakeholders, establish Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each mission-critical business function.

2. Developing Business Continuity and Recovery Plans:

- Create and execute plans for business continuity and recovery that are in line with RTOs and RPOs that have been set.
- To guarantee business continuity, document the processes and standards for restoring IT systems, apps, and resources within predetermined time ranges.

3. Testing and Maintenance:

- Regularly test and evaluate business continuity and recovery plans to verify their effectiveness and identify areas for improvement.
- Update and maintain BCP documentation, including RTOs and RPOs, to reflect changes in business requirements and technology infrastructure.

## **Guidelines:**

To ensure successful implementation of this policy, the following guidelines should be followed:

- Work together with important stakeholders from different departments to precisely define and rank the business functions that are essential to the purpose.
- Review and revise RTOs and RPOs on a regular basis in response to increasing risks, changes in business requirements, and technological improvements.
- Train and educate appropriate staff members on their roles and duties in putting the BCP into practice and abiding by set RTOs and RPOs.
- Establish communication protocols and procedures for escalation to aid in decision-making and coordination in the event of business continuity.

**Lab #7 – Assessment Worksheet**  
**Perform a Business Impact Analysis for an IT Infrastructure**

**Course Name: IAP401**

**Student Name: Dang Hoang Nguyen**

**1. Why must an organization define policies for an organization's Business Continuity and Disaster Recovery Plans?**

For the purpose of giving explicit instructions and guidance on how to anticipate, respond to, and recover from interruptions or disasters, organizations must create policies for business continuity and disaster recovery plans. These guidelines guarantee that the company has policies, processes, and procedures in writing to reduce downtime, reduce risks, and safeguard vital resources and operations. Policies also support accountability, uniformity, and adherence to industry best practices and legal obligations.

**2. When should you define a policy definition and when should you not define one?**

When it's necessary to set precise rules, goals, and roles for a certain area of an organization's activities, a policy definition ought to be developed. In order to guarantee uniformity, adherence, and responsibility throughout the company, policies are crucial. But not every facet of organizational operations might necessitate the formal development of a policy. A policy might not be appropriate in situations when judgment, flexibility, or continuous adaptation are required; instead, more relevant methods might be guidelines or standard operating procedures.

**3. What is the purpose of having a Business Continuity Plan policy definition that defines the organization's Business Impact Analysis?**

Establishing rules and processes for evaluating and ranking the effects of prospective interruptions on business operations is the goal of establishing a Business Continuity Plan (BCP) policy definition that incorporates the organization's Business Impact Analysis (BIA). The organization makes sure that there is a methodical approach to identifying mission-critical functions, formulating recovery objectives, and implementing methods to sustain continuity of operations during adverse events by defining the BIA within the BCP policy.

**4. Why is it critical to align the RTO and RPO standards within the policy definition itself?**

To maintain uniformity, clarity, and adherence to set recovery objectives throughout the company, Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) must be in line with each other within the policy definition. The policy's specification of RTOs and RPOs helps stakeholders make informed decisions, allocate resources effectively, and prioritize recovery efforts by outlining the anticipated timescale for restoring operations and data after a disruption.

**5. What is the purpose of a Business Impact Analysis (BIA)?**

A business impact analysis, or BIA, is used to identify important business activities and dependencies, evaluate and rank the effects of probable disruptions on operations, and develop recovery goals and plans to keep things running smoothly. Through educated decision-making and risk management, business impact analysis (BIA) assists firms in comprehending the financial, operational, and reputational ramifications of disruptions.

**6. Why is a business impact analysis (BIA) an important first step in defining a business continuity plan (BCP)?**

Because it offers crucial details regarding crucial business operations, dependencies, and recovery requirements required for creating successful continuity strategies, a business impact analysis (BIA) is a crucial first step in creating a business continuity plan (BCP). Since they both entail

detecting, evaluating, and prioritizing risks that potentially have an impact on business operations, particularly those pertaining to IT infrastructure, risk management and risk assessment are closely related to business impact analysis (BIA). By highlighting the possible effects of interruptions, BIA assists in risk management by assisting in the prioritization of mitigation measures and resource allocation to address the biggest threats to IT infrastructure and business operations.

**7. How does risk management and risk assessment relate to a business impact analysis for an IT infrastructure?**

Risk assessment determines the possibility and impact of hazards, risk management finds and reduces them, and business impact analysis weighs the effects of disruptions. Risk management in IT infrastructure deals with cybersecurity threats, risk assessment assesses particular risks to IT assets, and business impact analysis (BIA) determines how IT failures affect company operations. When taken as a whole, they provide insight into decisions about resource allocation, business continuity, and risk mitigation.

**8. True or False – If the Recovery Point Objective (RPO) metric does not equal the Recovery Time Objective (RTO), you may potentially lose data or not have data backed-up to recover. This represents a gap in potential lost or unrecoverable data.**

Indeed. There may be a gap in data protection and recovery capabilities if the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) differ. If RPO and RTO are not aligned, the company might not be able to maintain the required data availability and integrity and return operations to a satisfactory level in the allotted period. This gap may cause data to be lost or unavailable, which could interrupt operations and result in financial losses as well as possible noncompliance with regulations.

**9. What question should an organization answer annually to update its BCP, BIA, and RTOs and RPOs?**

A company ought to respond to the query: "Have there been any changes in business processes, technology infrastructure, regulatory requirements, or environmental factors that could impact our business continuity and disaster recovery plans?" In order to guarantee continuous efficacy and relevance, this question asks the company to review and evaluate any changes in its operating environment that would require revisions to the BCP, BIA, and related Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

**10. Why is it a good idea to have critical documentation recordkeeping defined in a policy definition?**

In order to guarantee that crucial documents, including the Business Continuity Plan (BCP), Business Impact Analysis (BIA), Recovery Time Objectives (RTOs), and Recovery Point Objectives (RPOs), are appropriately managed, maintained, and accessible when needed, it is a good idea to include critical documentation recordkeeping in a policy definition. The policy's definition of recordkeeping standards facilitates efficient documentation management and the auditability of business continuity and disaster recovery operations by encouraging uniformity, accountability, and compliance with regulatory requirements.

**11. From Part A - Sample BIA for an IT Infrastructure Worksheet, which systems, applications, and functions were mission critical to this organization?**

I am unable to correctly identify the organization's mission-critical systems, applications, and operations without the sample BIA worksheet that has been provided.

**12. From Part B – Define a Policy Definition for a BCP/DRP, how did you answer the procedures for how to implement this policy throughout your business?**

A Business Impact Analysis (BIA), the definition of Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), the creation of business continuity and recovery plans, testing and maintenance, and recommendations for resolving implementation obstacles were all covered in Part B of my article.

**13. True or False. It is a best practice to define policy definitions for an organization-wide BCP and DRP.**

Indeed. In order to give clear direction, standards, and guidance for business continuity and disaster recovery operations throughout the organization, it is best practice to develop policy definitions for an enterprise-wide business continuity plan (BCP) and disaster recovery plan (DRP). Policies support efficient planning, execution, and upkeep of BCP and DRP projects by assisting in ensuring consistency, accountability, and compliance with legal requirements and industry best practices.

**14. True or False. An organization must have a Business Impact Analysis and list of prioritized business functions and operations defined first prior to building a BCP and DRP**

Indeed. Before creating a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), a company must first perform a Business Impact Analysis (BIA) to determine the important business functions and dependencies, as well as to evaluate and prioritize the impact of potential interruptions on business operations. The BIA offers crucial data that is required for creating efficient continuity plans, specifying recovery goals, and distributing resources within the BCP and DRP in the right ways.

**15. Explain how having proper security controls and documented BIA, BCP, and DRP can help organizations reduce their business liability insurance premiums and errors and omissions insurance premiums**

By demonstrating proactive risk management and preparedness measures to insurers, organizations can lower their business liability insurance premiums and errors and omissions insurance premiums by implementing appropriate security controls and documenting Business Impact Analysis (BIA), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). Organizations that can establish strong security controls and all-encompassing risk mitigation strategies—such as BIA, BCP, and DRP documentation—may be eligible for lower premiums from insurers since these steps lessen the possibility and impact of future disruptions, incidents, and claims. Furthermore, companies with a verified BCP and DRP may be seen by insurers as lower-risk customers, which could lead to better insurance terms and costs.