Lab #7: Assessment Worksheet
Part A – Perform a Business Impact Analysis for an IT Infrastructure

Course Name: Risk Management in Information Systems (IAA202)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 4/3/2023

Overview

When performing a BIA, you are trying to assess and align the affected IT systems, applications, and resources to their required recovery time objectives (RTOs). The prioritization of the identified mission critical business functions will define what IT systems, applications, and resources are impacted. The RTO will drive what kind of business continuity and recovery steps are needed to maintain IT operations within the specified time frames.

1. Performa BIA assessment and fill in the following chart:

Business Function Or Process	Business Impact Factor	Recovery Time Objective (RTO)	IT Systems/ Apps Infrastructure Impacts
Internal and external voice communications with customers in real-time	Critical	8 hours	Server, Intra/Internet, Network, Telephone system
Internal and external e-mail communications with customers via store and forward messaging	Important	6 hours	Servers, Intra/Internet, DNS, LAN/WAN Network
DNS - for internal and external IP communications	Critical	15 minutes/ 24 hours	Servers, DNS, Network
Internet connectivity for e-mail and store and forward customer service	Minor	4 hours/ 24 hours	Servers, DNS, LAN/WAN Network
Self-service website for customer access to information and personal account information	Critical	12 hours/ 4 hours	Servers, Database, Network
e-Commerce site for online customer purchases or scheduling 24x7x365	Critical	1 hour/ 4 hours	Servers, Database, Intra/Internet, Network
Payroll and human resources for employees	Major	24 hours/ 12 hours	Database, Application, Network
Real-time customer service via website, e-mail, or telephone requires CRM	Critical	4-12 hours	Servers, DNS, Intra/Internet, Database
Network management and technical support	Critical	4 hours	Network, Intra/Internet, Remote Monitoring, Remote Management

Marketing and events	Minor	3-7 days	Software, Server
Sales orders or customer/ student registration	Critical	5 hours/ 2 days	Database, Servers, Intra/Internet
Remote branch office sales order entry to headquarters	Critical	8 hours	VPN, Intra/Internet, Server, Database
Voice and e-mail communications to remote branches	Critical	8 hours	Servers, DNS, LAN/WAN
Accounting and finance support: Accts payable, Accts receivable, etc.	Major	24 hours	Servers, Database, Network

Part B – Craft a Business Impact Analysis Executive Summary

Craft a BIA executive summary, follow this structure and format:

a. Goals and purpose of the BIA – unique to your scenario
- Explain why you conducted the BIA, what objectives and scope you defined, and what methodology you used.

b. Summary of Findings – business functions and assessment
- Provide a high-level overview of your findings for each business function and assessment. Include information such as impact categories, recovery time objectives (RTOs), recovery point objectives (RPOs), dependencies, resources, etc.

c. Prioritizations – critical, major, and minor classifications
- Classify your business functions into critical, major, and minor categories based on their RTOs and RPOs. Explain how you determined these classifications and what they mean for your recovery strategies.

d. IT systems and applications impacted - to support the defined recovery time objective
- List the IT systems and applications that support your critical business functions and their RTOs. Identify any gaps or risks that need to be addressed to ensure their availability.

Overview

After completing your BIA report for your scenario and IT infrastructure, answer the following Lab #7 – Assessment Worksheet questions. These questions are specific to your BIA you performed for your scenario and IT infrastructure. Justify your answers where needed

Lab Assessment Questions

1. What is the goal and purpose of a BIA?

- **Answer**: The goal and purpose of a BIA are to identify and evaluate the potential effects of a disruption of business functions and provide strategies to mitigate and minimize the risk to your business. A BIA helps you confirm the business continuity program scope, identify legal and regulatory obligations, clarify the business continuity strategy budget, capture preliminary content for a business continuity plan, and estimate the impact of a disaster in terms of downtime. A BIA is an essential component of an organization's business continuity plan (BCP).

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

- **Answer**: A BIA is an important first step in defining a BCP because it helps you understand the key risks and functions of your organization and how they would be affected by a disaster. A BIA also helps you set the priority of systems and services to bring back to full recovery based on their impact on your business operations, finances, reputation, and legal obligations. A BIA provides you with the information you need to create a BCP that aligns with your business objectives and recovery strategies

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

- **Answer**: Risk management and risk assessment are related to a BIA for an IT infrastructure in the following ways:

- Risk management is the process of identifying, analyzing, and mitigating potential threats to your IT infrastructure that could disrupt your business operations.
- Risk assessment is a component of risk management that evaluates the likelihood and impact of various risks on your IT infrastructure and determines the appropriate controls to reduce or eliminate them.
- BIA is another component of risk management that analyzes the effects of a disruption on your IT infrastructure and identifies the critical systems and services that need to be recovered within a specified time frame.
- BIA often takes place before risk assessment to provide input on the recovery objectives, priorities, and strategies for your IT infrastructure. BIA also helps you estimate the costs and benefits of implementing different risk mitigation options.

4. What is the definition of Recovery Time Objective (RTO)? Why is this important to define in an IT Security Policy Definition as part of the Business Impact Analysis (BIA) or Business Continuity Plan (BCP)?

- **Answer**: Recovery Time Objective (RTO) is the target time needed to recover your business and IT infrastructure after a disaster. It is the maximum acceptable downtime for your critical systems and services before they cause significant damage to your business operations, finances, reputation, and legal obligations.

RTO is important to define in an IT Security Policy Definition as part of the BIA or BCP because it helps you:

- Identify the mission-critical business processes and technologies that need to be restored within a specified time frame.
- Allocate the necessary resources and personnel to ensure timely recovery of your IT infrastructure.
- Evaluate the costs and benefits of different backup and recovery solutions based on their ability to meet your RTO requirements.
- Align your IT Security Policy with your business objectives and recovery strategies.

5. 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.
- **Answer**: True

6. If you have an RPO of 0 hours – what does that mean?
- **Answer**: It's common to measure acceptable data loss in minutes, such as 15 minutes. Every minute of data loss represents lost sales revenue. So if you have an RPO of 0 hours, then that means there is no data loss.

7. What must you explain to executive management when defining RTO and RPO objectives for the BIA?
- **Answer**: RTO and RPO are key metrics for a disaster recovery plan (DRP) that are derived from a business impact analysis (BIA). RTO is how quickly a business process must be restored after a disruption, while RPO is how much data can be lost without causing significant harm. When defining RTO and RPO objectives for the BIA, you must explain to executive management the impact of different levels of downtime and data loss on your business operations, reputation, revenue and compliance. You must also balance the costs and benefits of different recovery strategies that can meet your RTO and RPO objectives

8. What questions do you have for executive management in order to finalize your BIA?
- **Answer**:
    - What are your business priorities and objectives?
    - What are your regulatory, legal and contractual obligations?
    - What are your acceptable levels of downtime and data loss?
    - What are your available resources and budget for recovery strategies?

9. Why do customer service business functions typically have a short RTO and RPO maximum allowable time objective?
- **Answer**: Customer service business functions typically have a short RTO and RPO maximum allowable time objective because they are critical for maintaining customer satisfaction, loyalty and retention. Customer service functions often involve direct interactions with customers, such as answering queries, resolving issues, providing support and receiving feedback. If these functions are disrupted for a long time or lose important data, it can damage the reputation and revenue of the business, as well as violate any service level agreements (SLAs) with customers. Therefore, customer service functions need to be restored quickly and with minimal data loss to ensure business continuity and customer trust

10. In order to craft back-up and recovery procedures, you need to review the IT systems, hardware, software and communications infrastructure needed to support business operations, functions and define how to maximize availability. This alignment of IT systems and components must be based on business operations,

functions, and prioritizations. This prioritization is usually the result of a risk assessment and how those risks, threats, and vulnerabilities impact business operations and functions. What is the proper sequence of development and implementation for these following plans?

- **Answer**:
  - Business Continuity Plan : 4
  - Disaster Recovery Plan : 3
  - Risk Management Plan : 1
  - Business Impact Analysis : 2