**Lab #7: Assessment Worksheet**

**Perform a Business Impact Analysis for an IT Infrastructure**

**Course Name: IAA202**

**Student Name: Vu Hoang**

**Instructor Name: Ho Hai**

**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?

The purpose of a business impact analysis (BIA) report is to describe the potential risks specific to the organization studied. One of the basic assumptions behind BIA is that every component of the organization 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. For example, a business may be able to continue more or less normally if the cafeteria has to close, but would come to a complete halt if the information system crashes.

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

(BCP)?

The BIA is the first step because it is used to identify the impact that can result from disruptions in the business. Without the BIA, the BCP would not identify and prioritize which systems and processes must be sustained and provide the necessary information for maintaining them.

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

infrastructure?

a. Risk assessment relates to a business impact analysis by showing the amount of risk in making a business deal, by comparing the potential loss to the percent the loss could occur.

b. Risk management relates to a business impact analysis by identifying resources and associated risks, determining their magnitude, identifying what safeguards are needed, and maintain the proper techniques to mitigate the risks.

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)?

The RTO is the time in which the system or function must be recovered. The RTO would be equal to or less than the MAO. For example, if the MAO is one hour, the RTO would be one hour or less.

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.

True

6. If you have an RPO of 0 hours – what does that mean?

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 lost.

7. What must you explain to executive management when defining RTO and RPO objectives for the

BIA?

The RPOs identify the maximum amount of data loss an organization can accept. This is the acceptable data latency. For example, a database may record hundreds of sales transactions a minute. The organization may need to recover this data up to the moment of failure. This would be expensive. Another database may import data once a week. You’d only need to restore the data since the last import to ensure nothing is lost. This is less expensive.

8. What questions do you have for executive management in order to finalize your BIA?

a. Is there money in the budget for a separate backup site?

b. If there is money in the budget for a separate backup site, how many of the backup servers will be stored there?

c. How often will we need to do a full back-up?

9. Why do customer service business functions typically have a short RTO and RPO maximum

allowable time objective?

Customer service business functions typically have a short RTO because the time frame needs to be short because the longer they are down, the more sales they are losing.

The RPO has to be short as possible because when you’re dealing with customer service, time is money. With some organizations, 30 minutes of down time equals millions of dollars lost.

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?

Business Continuity Plan : 2

Disaster Recovery Plan : 3

Risk Management Plan : 4

Business Impact Analysis : 1