Lab #7: Assessment Worksheet

Part A – Perform a Business Impact Analysis for an IT Infrastructure

Course Name: IAA202

Student Name: Huynh Ngoc Quang

Instructor Name: Mr. Mai Hoang Dinh

Lab Due Date: October 20, 2024

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.

Business Function or Process	Business Impact Factor	Recovery Time Objective	IT Systems/Apps Infrastructure Impacts
Internal and external voice communications with customers in real-time	Big impact – customers expect quick help	4 hours	Phone systems, VoIP software, call management apps
Internal and external e-mail communications with customers via store and forward messaging	Medium – delays can affect service	6 hours	Email services (e.g., Gmail, Microsoft Outlook), mail servers
DNS – for internal and external IP communications	High – without it, no access to websites or apps	2 hours	DNS servers, routers, network hubs
Internet connectivity for e-mail and store and forward customer service	High – communication stops without it	6 hours	Internet connection, modems, firewalls
Self-service website for customer access to information and personal account information	Medium – delays can annoy customers	12 hours	Website hosting servers, content management system (CMS)
e-Commerce site for online customer purchases or scheduling 24x7x365	Critical – losing sales and customers	4 hours	E-commerce platform, payment gateways, product databases

Payroll and human resources for employees	Medium – delays upset employees but manageable	48 hours	Payroll software, HR platforms, employee data storage
Real-time customer service via website, e-mail, or telephone requires CRM	Critical – keeping customers happy is key	4 hours	CRM system (like HubSpot, Salesforce), helpdesk tools
Network management and technical support	High – needed to avoid bigger issues	8 hours	Network monitoring tools, IT support software
Marketing and events	Low – campaigns can wait a bit	3 days	CRM systems, social media apps, marketing tools
Sales orders or customer/ student registration	Critical – directly affects income	6 hours	Order management software, registration system
Remote branch office sales order entry to headquarters	High – must stay connected for smooth work	8 hours	VPN services, remote desktop tools
Voice and e-mail communications to remote branches	Medium – delays can slow down tasks	12 hours	Email services, messaging tools (Slack, Teams)
Accounting and finance support: Accts payable, Accts receivable, etc.	High – needed for reports and payments	24 hours	Accounting software (QuickBooks, SAP), financial databases

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
For FPT University, the purpose of this Business Impact Analysis (BIA) is to assess critical educational and administrative functions. The goal is to evaluate how potential disruptions—such as IT failures, data breaches, or facility issues—could impact academic operations, student services, and institutional reputation. This BIA helps prioritize recovery strategies to minimize downtime, maintain academic continuity, and protect sensitive student information.

b. **Summary of Findings** – business functions and assessment Key business functions identified include:
   1. **Academic Operations**: Ensuring smooth delivery of courses and maintaining access to e- learning platforms is essential to student success. Disruptions could delay assignments and exams, impacting academic timelines.
   2. **Student Information Systems**: Systems handling student registration, grades, and personal data are critical. Downtime could affect student records and lead to potential data breaches, harming the university's reputation.

3. **IT Infrastructure**: Supporting all digital services, including learning management systems, communication tools, and research databases. Interruptions could halt online learning and administrative functions.
4. **Financial Services**: Tuition processing, payroll, and budgeting are vital for university financial stability. While delays could cause temporary setbacks, the long-term operational impact would be limited.
5. **Campus Security Systems**: These include surveillance and access control systems, critical for student and staff safety. Any disruption could expose the campus to physical security risks.

The university's core systems are heavily reliant on IT, and any vulnerabilities in these areas could lead to service disruptions, financial losses, and damage to the institution's academic reputation.

c. **Prioritizations –** critical, major, and minor classifications

1. **Critical**: These functions are essential for the university's core operations. Any disruption would severely impact academic continuity and student services, leading to significant operational and reputational damage.

   ## Classifications:

   - **Academic Operations**: Ensuring course delivery and access to learning platforms.
   - **Student Information Systems**: Managing student registration, grades, and personal data.
   - **IT Infrastructure**: Supporting e-learning, communication, and research databases.
2. **Major**: These functions are important but can tolerate a slightly longer recovery period than critical functions. Disruptions could cause operational setbacks but wouldn't immediately halt core academic processes.

   ## Classifications:

   - **Financial Services**: Tuition processing and payroll systems.
   - **Campus Security Systems**: Surveillance and access control for campus safety.

3. **Minor**: These are secondary functions with a moderate impact on operations. While disruptions may cause some inconvenience, they do not critically affect the university's stability. **Classifications**:
    - **Marketing and Communications**: University outreach, promotional activities, and student engagement efforts.

d. **IT systems and applications impacted** - to support the defined recovery time objectives For FPT University, several IT systems and applications need to be prioritized for recovery to meet the defined recovery time objectives (RTO):

1. **Learning Management Systems (LMS)**: The LMS is crucial for course delivery and interaction between students and faculty. To meet RTO, the LMS must be restored quickly. Regular backups of course materials, student submissions, and communication logs, along with a robust recovery plan, are essential to ensure academic continuity.
2. **Student Information Systems (SIS)**: Managing student data, including registrations, grades, and personal information, the SIS must be operational within a short period. Regular backups and a contingency recovery plan are critical to protect student data and maintain institutional credibility.
3. **IT Infrastructure**: This encompasses servers, databases, and network services that support online learning, research, and communication platforms. Rapid restoration is necessary to avoid significant downtime and disruption to academic operations. Regular system backups and contingency plans ensure continuity.
4. **Financial Management System**: This system tracks tuition payments, payroll, and budgeting. While important, a short-term disruption would not critically impact day-to-day operations. Regular financial data backups and a recovery plan are necessary to mitigate potential losses.
5. **Campus Security Systems**: Including surveillance and access control, these systems protect campus safety. They must be restored quickly to ensure student and staff security. Backups and a recovery strategy ensure minimal risk during outages.
6. **Marketing and Communications Systems**: These include CRM platforms, website management, and email marketing tools. Backing up customer and campaign data helps ensure continuity in outreach efforts during a disruption, though the immediate operational impact is moderate.

Lab #7: Assessment Worksheet

Perform a Business Impact Analysis for an IT Infrastructure

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 goal and purpose of a Business Impact Analysis (BIA) are to identify critical business functions, assess the potential impacts of disruptions, and define the required recovery time objectives (RTO). It ensures that recovery strategies are prioritized to maintain business continuity and minimize financial or reputational losses.

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

A BIA is the foundation of a BCP because it identifies critical systems and processes that must remain operational. It helps organizations pinpoint vulnerabilities, estimate the impact of disruptions, and develop effective strategies to mitigate risks, ensuring the continuity of business operations.

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

Risk management and risk assessment are essential components of a BIA. They identify potential threats and measure the impact these risks could have on business operations. The findings from risk assessments guide the prioritization of IT systems and resources, ensuring that those with the highest risk are addressed with appropriate recovery strategies.

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 maximum acceptable amount of time a system or service can be down before it causes significant disruption to business operations. Defining RTOs in the IT security policy ensures that recovery strategies are aligned with business needs and helps prioritize which systems need to be restored first during an incident.

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. If the RPO (how far back data must be recovered) is longer than the RTO (maximum downtime), there is a risk of data loss because some data generated during that gap may not have been backed up.

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

An RPO of 0 hours means that no data loss is acceptable, and all data must be recovered up to the exact point of failure. This requires real-time backups or continuous data replication.

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

You need to explain the trade-offs between the cost of rapid recovery and the potential business impact of downtime. Clear communication ensures that management understands how RTOs and RPOs align with operational priorities and helps them make informed decisions on resource allocation.

8. What questions do you have for executive management in order to finalize your BIA?
    - Which business functions are considered most critical?
    - What are the acceptable downtime limits for each function?
    - Are there any budget constraints that may affect recovery strategies?
    - Are there regulatory or contractual requirements for recovery timelines?

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

Customer service functions often need quick recovery because they are essential to maintaining customer satisfaction and trust. Extended downtime could result in lost revenue, customer complaints, and damage to the company's reputation.

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	: 3
Disaster Recovery Plan	: 4
Risk Management Plan	: 2
Business Impact Analysis	: 1

- Business Impact Analysis (BIA) – Identifies critical systems and business functions.
- Risk Management Plan – Assesses and mitigates risks identified in the BIA.
- Business Continuity Plan (BCP) – Ensures operations continue during disruptions.
- Disaster Recovery Plan (DRP) – Focuses on restoring IT systems after an incident.