# Lab #7: Assessment Worksheet

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

## Course Name: IAA202

**Student Name: Phạm Thành Long Instructor Name: Mai Hoàng Đỉnh Lab Due Date: 20/10/2024**

**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.

Performa BIA assessment and fill in the following chart:

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | Minor | Two weeks | All major computer systems,  both software and hardware, would have been affected. |
| Internal and external e-mail communications with  customers via store and forward messaging | Minor | Two weeks | All major computer systems, both software and hardware, would have been affected. |
| DNS – for internal and external IP communications | Critical | Two to three days | Servers would have been  affected; both remote and local servers should be recovered  for business continuity. |
| Internet connectivity for e-mail and store and forward customer service | Major | One week | Modems and other Wi-Fi  connectivity devices should be restored for business  continuity. |
| Self-service website for customer access to information and personal account  information | Major | One week | If externally hosted, the impact and recovery time shall be  calculated by the hosting  provider; if internally hosted,  all servers should be restored for business continuity. |
| e-Commerce site for online customer purchases or  scheduling 24x7x365 | Critical | One week | Bank transactions take place here; the hosting company and  web infrastructure must be restored to ensure continuous |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | operation and recovery within the specified RTO. |
| Payroll and human resources for employees | Major | One week | Employee data management systems, payroll applications, and databases would need  restoration. |
| Real-time customer service via website, e-mail, or telephone  requires CRM | Critical | Two to three days | CRM systems, communication tools, and web servers would  need immediate recovery. |
| Network management and technical support | Major | One week | Network infrastructure, support systems, and monitoring tools would need  to be restored. |
| Marketing and events | Minor | Two weeks | Marketing platforms, email marketing tools, and event management systems may be  affected. |
| Sales orders or customer/ student registration | Major | One week | Sales/order management systems, registration  databases, and web forms need to be restored. |
| Remote branch office sales order entry to headquarters | Major | One week | Remote access systems, order entry applications, and  communication tools would need recovery. |
| Voice and e-mail  communications to remote branches | Major | One week | Voice over IP systems, email servers, and communication networks would need  restoration. |
| Accounting and finance  support: Accts payable, Accts receivable, etc. | Major | One week | Financial systems, accounting  software, and databases would need to be restored quickly. |

# Part B – Craft a Business Impact Analysis Executive Summary

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

1. **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.

1. **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.

1. **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.
  1. **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.
  1. **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.

1. **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**

## Course Name: IAA202

**Student Name: Phạm Thành Long Instructor Name: Mai Hoàng Đỉnh Lab Due Date: 20/10/2024**

**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 of a Business Impact Analysis (BIA) is to identify the critical business units, operations, and processes essential for the organization's survival and to evaluate the potential impact of disruptions on these areas. This assessment helps prioritize recovery efforts and informs the development of business continuity strategies.

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

 A BIA identifies critical functions and resources, guiding what should be included in the BCP to ensure effective recovery.

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

 Risk management and assessment identify vulnerabilities in IT infrastructure. A BIA expands this analysis to the entire organization, assessing risks to all critical functions.

1. 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)?

 Recovery Time Objective (RTO) is the maximum time allowed to restore operations after a disruption. Defining the RTO is crucial for establishing acceptable downtime limits in an IT Security Policy, ensuring timely recovery of critical services.

1. 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 Recovery Point Objective (RPO) does not match the Recovery Time Objective (RTO), it indicates a potential gap where data may be lost or not backed up sufficiently to recover after a disruption. This mismatch can lead to unrecoverable data loss, impacting business continuity.

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

 An RPO of 0 hours means that no data can be lost; all data is continuously backed up, ensuring complete data availability at all times.

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

 RPO defines the maximum acceptable data loss for the organization, indicating how much data latency is tolerable.

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

 Is there funding for a separate backup site?

If so, how many backup servers will be stored there? How often will we perform full backups?

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

 Short RTO and RPO are necessary because longer downtimes result in lost sales. In customer service, quick recovery is essential since time directly impacts revenue.

1. 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: 1 Business Impact Analysis: 2

* 1. **Risk Management Plan**: Identify risks, threats, and vulnerabilities to inform further planning.
  2. **Business Impact Analysis (BIA):** Assess the potential impacts of those risks on critical business functions.
  3. **Business Continuity Plan (BCP):** Develop strategies to ensure that essential business operations continue during a disruption, based on insights from the BIA.
  4. **Disaster Recovery Plan (DRP):** Create detailed procedures for recovering IT systems and data to support the BCP's objectives.