Lab #8: Assessment Worksheet
Part A – Develop an Outline for a Business Continuity Plan 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: 11/3/2023

Overview

Using the results of Lab #7 – Perform a BIA on an IT Infrastructure, incorporate your BIA into your BCP plan scenario and vertical industry focus. Work in teams of two or three students as assigned by your Instructor. Craft a more detailed BCP outline only (not an entire BCP plan, etc.) based on the following:

Use the same scenario/vertical industry you were provided in Lab #7 – Perform a Business Impact Analysis for an IT Infrastructure assigned by your Instructor:

a. Healthcare provider under HIPPA compliance law

Incorporate the following BCP sections and essential sub-topics in your outline:

- **Initiation of the BCP** – Introduction, Definitions, BCP Organizational Structure, BCP Declaration, BCP Communications and Information Sharing, etc.
- **Business Impact Analysis** – risk assessment and analysis prioritizing business functions and operations aligned to IT systems, applications, and resources.
- **Business Continuity / Disaster Readiness / Recovery** – RTO, RPO, business continuity benchmarks, disaster recovery planning (DRP as a sub-set of a BCP plan), recovery steps and procedures for mission critical IT systems, applications, and data.
- **Develop & Implement the Plan** – the plan is a living and breathing document that requires annual updates and change control revisions. Implementation and the instructions for how to engage the BCP are part of this section
- **Test & Update the Plan** – the most important part of a BCP or DRP is to test the plan with a "mock" business continuity disruption or disaster scenario. Table-top reviews of the processes and procedures can be conducted to inform all BCP and DRP team members of their roles, responsibilities, and accountabilities

----------------------Insert Scenario and Vertical Industry Here----------------------

I. Initiation of the BCP

- Introduction: Explain the purpose, scope, objectives, and assumptions of the BCP.
- Definitions: Define key terms and acronyms related to BCP and HIPPA.
- BCP Organizational Structure: Identify the roles and responsibilities of the BCP team members, such as coordinator, leader, manager, etc.
- BCP Declaration: Establish the criteria and process for declaring a business continuity event or disaster.

- BCP Communications and Information Sharing: Describe how information will be communicated among BCP team members, stakeholders, vendors, customers, etc. during a business continuity event or disaster.

II. Business Impact Analysis

- Risk Assessment and Analysis: Identify and evaluate potential threats and vulnerabilities that could affect IT systems, applications, and resources that handle Electronic Patient Health Information (ePHI).
- Prioritizing Business Functions and Operations: Determine which business functions and operations are critical for maintaining HIPPA compliance and providing healthcare services.

III. Business Continuity/ Disaster Readiness/ Recovery

- RTO (Recovery Time Objective): Define the maximum acceptable time for restoring IT systems, applications, and resources after a disruption.
- RPO (Recovery Point Objective): Define the maximum acceptable data loss that can occur after a disruption.
- Business Continuity Benchmarks: Establish measurable goals and indicators for evaluating the effectiveness of business continuity strategies.
- Disaster Recovery Planning: Develop detailed procedures for recovering IT systems, applications, and resources in a disaster recovery location while ensuring critical business functions continue.

IV. Develop & Implement the Plan

- Plan Development: Document all aspects of the BCP in a clear and concise format that can be easily accessed and updated.
- Plan Implementation: Provide instructions for how to engage the BCP in case of a business continuity event or disaster.

V. Test & Update the Plan

- Testing Methods: Describe how to test the plan with mock scenarios or table-top reviews to evaluate its effectiveness.
- Testing Results: Report on testing outcomes such as strengths, weaknesses, gaps etc.
- Plan Improvements: Recommend actions for improving the plan based on testing results.
- Plan Updating: Review and revise the BCP annually or whenever there are significant changes in IT systems, applications, resources, business functions or HIPPA requirements.

<u>Overview</u>

After completing your BCP outline for your scenario and IT infrastructure, answer the following Lab #8 – Assessment Worksheet questions. These questions are specific to the BCP you performed for your scenario and IT infrastructure. Justify your answers where needed

<u>Lab Assessment Questions</u>

1. How does a BCP help mitigate risk?

- **Answer**: A BCP (Business Continuity Plan) helps to mitigate risk by making sure the organization is ready for any possible disruption to everyday operations. By having an outlined plan of how every department should respond to the disaster, the organization will be able to resume the most critical functions and return to typical business operations as quickly as possible.

2. What kind of risk does a BCP help mitigate?

- **Answer**: A BCP helps to mitigate various types of risks that can affect the company's operations, such as:

  - Natural disasters
  - Cyberattacks
  - Data breaches
  - Terrorism
  - Human errors
  - Unsafe conditions

3. If you have business liability insurance, asset replacement insurance, and natural disaster insurance, do you still need a BCP or DRP? Why or why not?

- **Answer**: You still need a BCP (Business Continuity Plan) or DRP (Disaster Recovery Plan) even if you have insurance for your business. Insurance can help you recover some of your financial losses after a disaster, but it cannot help you resume your operations quickly and effectively. A BCP or DRP can help you prepare for different scenarios that could disrupt your business, such as data loss, system failure, communication breakdown, or staff unavailability. A BCP or DRP can also help you comply with industry standards and regulations that may require you to have a documented plan for business continuity.

4. From your scenario and BIA from Lab #7, what were the mission critical business functions and operations you identified? Is this the focus of your BCP?

- **Answer**: A mission critical task or process is one that is essential to the operation of an organization. For example, an online business's mission critical is its website. If a business operation cannot be interrupted under any circumstance without stopping production, it is considered mission critical to the business. A Business Continuity Plan (BCP) is a document that outlines how a business will continue operating during an unplanned disruption in service. It typically covers resources, equipment, personnel, procedures and communication strategies needed to maintain business operations during a crisis. Therefore, identifying and protecting mission critical functions and operations is usually one of the main focuses of BCP.

5. What does a BIA help define for a BCP?

- **Answer**:

  - The key risks and functions of your organization
  - The priority of systems is to bring back to full recovery in case of a disaster
  - The steps that must be taken in case of an outage or disruption

6. Who should develop and participate in the BCP within an organization?

- **Answer**: Some possible roles and responsibilities are:

- A senior management sponsor who provides leadership and support for the BCP project
- A business continuity coordinator who oversees the development, implementation and maintenance of the BCP
- A business continuity team who identifies critical functions, risks, impacts and recovery strategies
- A disaster recovery team who handles IT disruptions to networks, servers, personal computers and mobile devices
- Key stakeholders who review and approve the BCP documents

7. Why do disaster planning and disaster recovery belong in a BCP?
- **Answer**: Disaster planning and disaster recovery belong in a BCP because they are essential components of ensuring business continuity in the face of unplanned incidents. Disaster planning involves identifying potential threats and risks, assessing their impact and likelihood, and developing strategies to prevent, mitigate, respond to and recover from them. Disaster recovery involves restoring IT infrastructure and data after a disruption. Both disaster planning and disaster recovery aim to minimize downtime, data loss, operational costs and reputational damage.

8. What is the purpose of having documented IT systems, applications, and data recovery procedures and steps?
- **Answer**: The purpose of having documented IT system, application, and data recovery procedures and steps is to ensure that all critical information is backed up and can be restored in case of a disaster or failure. Data recovery can also help users retrieve accidentally deleted files, recover data from damaged disks, or restore data to a mobile device from a cloud-based backup. Backup and recovery of data can protect against software or hardware failure, human error, data corruption, ransomware attacks, malware, and accidental deletion.

9. Why must you include testing of the plan in your BCP?
- **Answer**: You must include testing of the plan in your BCP because it will help you verify the effectiveness of your business continuity strategies and protocols. Testing will also allow you to discover any gaps, flaws, errors, or inconsistencies in your plan and fix them before they lead to damage or injury. Testing should be done at least every 6 months to ensure that your plan is up-to-date.

10. How often should you update your BCP document?
- **Answer**: You should update your BCP document regularly, at least once a year. You should also update your BCP document whenever there is a change in your business processes, products, services, structure, location, or external factors that may affect your business continuity.

11. Within your BCP outline, where will you find a list of prioritized business operations, functions, and processes?
- **Answer**: Business Impact Analysis

12. Within your BCP outline, where will you find detailed back-up and system recovery information?
- **Answer**: Business Continuity/ Disaster Readiness/ Recovery

13. Within your BCP outline, where will you find a policy definition defining how to engage your BCP due to a major outage or disaster?
- **Answer**: Test & Update the Plan

14. Within your BCP outline, where will you find a policy definition defining the resources that are needed to perform the tasks associated with BC or DR?
- **Answer**: Develop & Implement the Plan

15. What is the purpose of testing your BCP and DRP procedures, backups, and recovery steps?
- **Answer**: The purpose of testing your BCP and DRP procedures, backups, and recovery steps is to validate that they work as desired and will help you restore your business operations and data in case of a disaster or disruption. Testing will also help you identify any gaps, errors, inconsistencies, or areas of improvement in your plans and fix them before they cause damage or loss. Testing should be done regularly and with realistic scenarios to ensure that your plans are reliable and effective.