Lab #7: Identify Necessary Policies for Business Continuity – BIA & Recovery Time

Course Name: Policy Development in Information Assurance (IAP301)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 21/10/2023

Part A – Sample Business Impact Analysis for an IT Infrastructure

Overview

When conducting 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 missioncritical business functions will define what IT systems, applications, and resources are impacted. The RTO will drive what type of business continuity and recovery steps are needed to maintain IT operations within the specified time frames

Business Function Or Process	Business Impact Factor	RTO/RPO	IT Systems/Apps Infrastructure Impacts
Internal and external voice communications with customers in real-time	High	1 hour / 0 minutes	CRM, telephony system, Network, telephony infrastructure
Internal and external e-mail communications with customers via store and forward messaging	Medium	8 hours / 1 day	E-mail system, Network, e-mail system infrastructure
DNS – for internal and external IP communications	Medium	8 hours / 1 day	DNS servers, Network, DNS server infrastructure
Internet connectivity for email and store and forward customer service	Medium	8 hours / 1 day	Internet connection, Network, internet connection infrastructure
Self-service website for customer access to information and personal account information	Medium	8 hours / 1 day	Website, Network, website infrastructure
e-Commerce site for online customer purchases or scheduling 24x7x365	Medium	8 hours / 1 day	Website, Network, website infrastructure
Payroll and human resources for employees	Medium	8 hours / 1 day	Payroll system, HR system, Network, payroll system, HR system infrastructure
Real-time customer service via website, e-mail, or telephone requires CRM	High	2 hours / 0 minutes	CRM, website, e-mail system, Network, website, e-mail infrastructure
Network management and technical support	Medium	8 hours / 1 day	Network management system, ticketing system, Network, network

			management system, ticketing system infrastructure
Marketing and events	Medium	24 hours / 1 week	Marketing automation system, content management system, Network, marketing automation system, content management system infrastructure
Sales orders or customer/student registration	High	4 hours / 0 minutes	CRM, website, e-commerce system, Network, website, e-commerce system infrastructure
Remote branch office sales order entry to headquarters	High	4 hours / 0 minutes	CRM, network, Network, network infrastructure
Voice and e-mail communications to remote branches	High	4 hours / 0 minutes	Network, telephone system, Network, telephone infrastructure
Accounting and finance support: Accts payable, Accts receivable, etc.	Medium	8 hours / 1 day	Accounting system, Network, accounting system infrastructure

Part B – Craft a Business Continuity Plan Policy – Business Impact Analysis

Overview

When conducting 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 missioncritical business functions will define what IT systems, applications, and resources are impacted. The RTO will drive what type of business continuity and recovery steps are needed to maintain IT operations within the specified time frames. In this lab, you are to create a Business Continuity Plan Policy Definition – Business Impact Analysis that points to the RTOs and RPOs for the identified missioncritical business functions of the organization

Instructions

Using Microsoft Word, create a Business Continuity Plan Policy Definition using the following policy template

ABC Credit Union
Business Impact Analysis (BIA) Policy

Policy Statement

- ABC Credit Union is committed to ensuring the continuity of its critical business functions and processes in the event of a disruption, and to minimizing the impact on its customers, employees, and stakeholders. ABC Credit Union will conduct a regular Business Impact Analysis (BIA) to identify and prioritize its critical business functions and processes, and to establish the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each function and process. ABC Credit Union will also develop and maintain a Business Continuity Plan (BCP) that outlines the recovery strategies and procedures for each function and process, as well as the roles and responsibilities of the business continuity team. ABC Credit Union will test and review its BCP periodically to ensure its effectiveness and alignment with the business objectives.

Purpose/Objectives

- Define the scope, standards, procedures, and guidelines for conducting a BIA and developing a BCP for ABC Credit Union
- Establish the roles and responsibilities of the business continuity team and other stakeholders involved in the BCP
- Ensure that ABC Credit Union can continue or resume its critical business functions and processes within the RTOs and RPOs defined by the BIA
- Minimize the operational, financial, legal, and reputational impacts of a disruption on ABC Credit Union and its customers, employees, and stakeholders

Scope

- This policy applies to all business functions and processes of ABC Credit Union that are deemed critical by the BIA. This policy also applies to all employees, contractors, vendors, and partners of ABC Credit Union who are involved in or support the critical business functions and processes. This policy covers all types of disruptions that may affect ABC Credit Union, such as natural disasters, cyberattacks, power outages, pandemics, etc.

Standards

- RTO: The maximum acceptable time for restoring a critical business function or process after a disruption
- RPO: The maximum acceptable amount of data loss for a critical business function or process after a disruption
- BIA questionnaire: A survey tool used to collect information from managers and others within the business about the criticality, impact, dependencies, resources, and recovery timeframes of each business function or process
- BIA report: A document that summarizes the results of the BIA questionnaire and prioritizes the critical business functions and processes based on their RTOs and RPOs
- BCP document: A document that outlines the recovery strategies and procedures for each critical business function or process, as well as the roles and responsibilities of the business continuity team
- BCP test: A simulation or exercise that evaluates the effectiveness and readiness of the BCP in different scenarios
- BCP review: A periodic assessment that updates and improves the BCP based on changes in the business environment, feedback from stakeholders, lessons learned from tests or incidents, etc.

Procedures

- Conduct a BIA using the BIA questionnaire at least once a year or whenever there is a significant change in the business environment or operations
- Analyze the results of the BIA questionnaire and prepare a BIA report that identifies and prioritizes the critical business functions and processes based on their RTOs and RPOs
- Develop a BCP document that details the recovery strategies and procedures for each critical business function or process, as well as the roles and responsibilities of the business continuity team
- Train and educate all employees, contractors, vendors, and partners on their roles and responsibilities in relation to the BCP
- Test the BCP using different scenarios at least once every six months or whenever there is a significant change in the BCP document

- Review the BCP based on the feedback from stakeholders, lessons learned from tests or incidents, changes in the business environment or operations, etc. at least once every year or whenever there is a significant change in the BCP document
- Communicate any changes or updates in the BCP document to all relevant stakeholders

Guidelines

- Ensure that the BIA and BCP are aligned with the business objectives and strategies of ABC Credit Union
- Involve all relevant stakeholders in the BIA and BCP processes and solicit their input and feedback
- Assign clear roles and responsibilities to the business continuity team and other stakeholders and ensure accountability and coordination
- Use best practices and industry standards for conducting a BIA and developing a BCP
- Document and report any incidents, issues, or gaps in the BIA or BCP and take corrective actions as soon as possible
- Maintain a backup and recovery plan for the BIA and BCP documents and data
- Review and update this policy as needed to reflect any changes in the BIA or BCP

PART C

Overview

After completing your Business Continuity Plan Policy Definition, answer the following Lab #7 – Assessment Worksheet questions. These questions are specific to the sample BIA report provided with this lab

Lab Assessment Questions & Answers

1. Why must an organization define policies for an organization's Business Continuity and Disaster Recovery Plans?

Answer: An organization must define policies for its Business Continuity and Disaster Recovery Plans because these policies provide the framework and guidance for preparing and responding to potential disruptive events. Policies help to establish the scope, objectives, standards, procedures, and roles and responsibilities for Business Continuity and Disaster Recovery. Policies also help to align the Business Continuity and Disaster Recovery plans with the organization's mission, vision, values, and goals. Policies also ensure that the organization complies with any legal, regulatory, or contractual obligations related to Business Continuity and Disaster Recovery.

2. When should you define a policy definition and when should you not define one?

Answer:

You should define a policy definition when you want to:

- Clarify the intent and objectives of a policy
- Provide a framework and guidance for implementing and enforcing a policy
- Communicate the policy to the relevant stakeholders and ensure their compliance
- Evaluate and improve the effectiveness and efficiency of a policy

3. What is the purpose of having a Business Continuity Plan policy definition that defines the organization's Business Impact Analysis?

Answer:

- Ensure that the BIA is conducted in a consistent and comprehensive manner across the organization.
- Provide clear guidance to employees on the BIA process and their roles and responsibilities.
- Establish the BIA as a critical component of the organization's BCP.
- Ensure that the BIA is used to inform the development of recovery plans and other BCP activities.

4. Why is it critical to align the RTO and RPO standards within the policy definition itself?
Answer: It is critical to align the RTO and RPO standards within the policy definition itself because it ensures that the organization has a clear and consistent approach to recovering from disruptions. The RTO is the maximum amount of time that can elapse before a critical business function must be restored after a disruption. The RPO is the maximum amount of data that can be lost before the critical business function can continue to operate.

5. What is the purpose of a Business Impact Analysis (BIA)?
Answer: The purpose of a Business Impact Analysis (BIA) is to identify and assess the impact of potential disruptions on critical business functions. The BIA also helps to develop recovery plans to minimize the impact of disruptions.

6. Why is a business impact analysis (BIA) an important first step in defining a business continuity plan (BCP)?
Answer: A business impact analysis (BIA) is an important first step in defining a business continuity plan (BCP) because it helps an organization identify and prioritize its critical business functions and processes, and the potential impacts of a disruption on them. A BIA also helps an organization determine the recovery time objectives (RTOs) and recovery point objectives (RPOs) for each critical function and process, which are the maximum acceptable time and data loss for resuming them after a disruption. By conducting a BIA, an organization can develop effective recovery strategies and procedures for its BCP, which is a system of prevention and recovery from potential threats to the organization. A BCP aims to ensure the continuity or restoration of the critical business functions and processes within the RTOs and RPOs defined by the BIA. A BCP also helps an organization minimize the operational, financial, legal, and reputational impacts of a disruption, and comply with any legal or regulatory obligations related to business continuity planning

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

- Risk assessment helps to identify and prioritize the IT assets that support the critical business functions and processes, and the potential threats and vulnerabilities that may affect them. This helps to determine the scope and objectives of BIA for an IT infrastructure.
- Risk assessment also helps to quantify the likelihood and impact of various scenarios of disruption to the IT infrastructure, such as data loss, system outage, cyberattack, etc. This helps to calculate the recovery time objectives (RTOs) and recovery point objectives (RPOs) for each critical business function and process, which are the key inputs for BIA.
- BIA helps to evaluate the operational, financial, legal, and reputational impacts of disruptions to the IT infrastructure on the organization’s business continuity and disaster recovery. This helps to develop and implement appropriate recovery strategies and procedures for restoring the IT infrastructure within the RTOs and RPOs defined by risk assessment.
- BIA also helps to identify the dependencies and interdependencies among the IT assets and the critical business functions and processes, as well as the resources and capabilities needed to support them. This helps to optimize the allocation and utilization of IT resources and ensure their availability and resilience in case of a disruption.

8. 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:

- The statement is true. If the RPO metric does not equal the RTO metric, you may potentially lose data or not have data backed-up to recover. This represents a gap in potential lost or unrecoverable data.
- If the RPO is smaller than the RTO, it means that the data backup frequency is higher than the recovery time. This implies that the data loss is minimal and the data can be recovered within the RTO. For example, if the RPO is 15 minutes and the RTO is 1 hour, it means that the data is backed up every 15 minutes and can be restored within 1 hour after a disruption.
- If the RPO is larger than the RTO, it means that the data backup frequency is lower than the recovery time. This implies that the data loss is significant and the data may not be recovered within the RTO. For example, if the RPO is 4 hours and the RTO is 1 hour, it means that the data is backed up every 4 hours and may not be restored within 1 hour after a disruption.
- Therefore, if the RPO does not equal the RTO, there is a gap between the data backup and recovery time, which may result in potential lost or unrecoverable data.

9. What question should an organization answer annually to update its BCP, BIA, and RTOs and RPOs?

Answer:

- What are the changes in the internal and external environment that may affect the organization’s critical business functions and processes, such as new products, services, markets, regulations, technologies, vendors, etc.?
- How do these changes impact the organization’s risk profile, such as the likelihood and severity of potential threats and vulnerabilities?
- How do these changes affect the organization’s recovery requirements and priorities, such as the RTOs and RPOs for each critical business function or process?
- How do these changes affect the organization’s recovery strategies and procedures, such as the resources, capabilities, dependencies, and interdependencies needed to resume the critical business functions and processes within the RTOs and RPOs?
- How do these changes affect the organization’s communication and coordination with all relevant stakeholders involved in the BCP, such as employees, customers, suppliers, partners, regulators, etc.?

10. Why is it a good idea to have critical documentation recordkeeping defined in a policy definition?

Answer:

- To ensure that critical documentation is properly identified and protected. A policy definition can help to ensure that all critical documentation is identified, stored securely, and backed up regularly.
- To establish clear roles and responsibilities for recordkeeping. A policy definition can help to establish clear roles and responsibilities for different aspects of recordkeeping, such as who is responsible for creating, reviewing, and archiving records.
- To ensure that recordkeeping practices are consistent across the organization. A policy definition can help to ensure that recordkeeping practices are consistent across all departments and teams within the organization.
- To comply with regulatory requirements. Many industries have regulatory requirements that specify how records must be kept. A policy definition can help organizations to comply with these regulatory requirements.

11. From Part A - Sample BIA for an IT Infrastructure Worksheet, which systems, applications, and functions were mission critical to this organization?

Answer:

- Internal and external voice communications with customers in real-time
- Real-time customer service via website, e-mail, or telephone requires CRM
- Sales orders or customer/student registration
- Remote branch office sales order entry to headquarters

- Voice and e-mail communications to remote branches

12. From Part B – Define a Policy Definition for a BCP/DRP, how did you answer the procedures for how to implement this policy throughout your business?

Answer:

- The BIA will be conducted on an annual basis. The BIA will be led by a cross-functional team that includes representatives from all departments.
- The BIA will include the following steps:
  - Identify critical business functions.
  - Assess the impact of potential disruptions on critical business functions.
  - Develop recovery plans to minimize the impact of disruptions.
  - Test and update the recovery plans on an annual basis.
- These steps are designed to ensure that the BIA is conducted in a comprehensive and effective manner, and that the results of the BIA are used to develop and maintain recovery plans that meet the needs of the entire business.

13. True or False. It is a best practice to define policy definitions for an organization-wide BCP and DRP?

Answer:

- True. It is a best practice to define policy definitions for an organization-wide BCP and DRP. Policy definitions help to ensure that everyone in the organization understands their roles and responsibilities in the event of a disruption. They also help to establish a consistent approach to BCP and DRP across the organization.

14. True or False. An organization must have a Business Impact Analysis and list of prioritized business functions and operations defined first prior to building a BCP and DRP.

Answer:

- True. An organization must have a Business Impact Analysis (BIA) and list of prioritized business functions and operations defined first prior to building a BCP and DRP. The BIA is a critical step in the BCP and DRP process because it helps organizations to understand the impact of potential disruptions on their business functions. This information is essential for developing recovery plans that will minimize the impact of disruptions and get the business back to normal as quickly as possible.

15. Explain how having proper security controls and documented BIA, BCP, and DRP can help organizations reduce their business liability insurance premiums and errors and omissions insurance premiums.

Answer:

- Security controls are measures that protect the confidentiality, integrity, and availability of information assets and systems. They can help prevent or mitigate the impact of cyberattacks, data breaches, natural disasters, human errors, or other incidents that could cause harm or loss to the organization or its stakeholders. By implementing security controls, organizations can demonstrate their due diligence and compliance with applicable laws, regulations, standards, and best practices. This can lower their risk exposure and liability in the event of a claim or lawsuit.
- BIA is a process that identifies and prioritizes the critical business functions and processes that support the mission and goals of the organization. It also determines the RTOs and RPOs for each critical business function or process based on the potential impact of disruption or downtime. By conducting a BIA, organizations can assess their business impact and recovery needs and allocate their resources accordingly. This can help them optimize their business continuity and disaster recovery strategies and plans.

- BCP is a document that outlines the roles, responsibilities, and procedures for ensuring the continuity of critical business functions and processes in the event of a disaster or disruption. It includes measures around personnel safety, maintaining critical operations, and minimizing financial and reputational losses. By developing a BCP, organizations can prepare for various scenarios and contingencies and reduce the likelihood or severity of business interruption.
- DRP is a document that documents the procedures for activating, executing, and evaluating the recovery of IT systems, applications, data, network, communication, facilities, equipment, staff, vendors, partners, etc. within the RTOs and RPOs defined by the BIA. By developing a DRP, organizations can restore their IT services and operations as quickly and efficiently as possible after a disaster or disruption.