ASSIGNMENT 2 FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	Unit 5: Security		
Submission date	20/08/2022	**Date Received 1st submission**	19/08/2022
Re-submission Date	-	**Date Received 2nd submission**	-
Student Name	Bùi Hương Linh	**Student ID**	GBH200662
Class	GCH1002	**Assessor name**	Michael Omar
Student declaration I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.			
		Student's signature	Linh

Grading grid

P5	P6	P7	P8	M3	M4	M5	D2	D3

☼ Summative Feedback:	☼ Resubmission Feedback:

Grade:	Assessor Signature:	Date:
Lecturer Signature:		

Table of Contents

Introduction

Data routinely moves freely between individuals, organizations, and businesses in today's data - driven. Cybercriminals are well aware of the monetary value of data. As a result of the continuous growth in cybercrime, so does the demand for security professionals to protect and defend a business. This report will help you understand more about security including discussing Risk assessment procedures ; Explaining data protection processes and regulations as applicable to an organization and designing a security policy for an organization ...

Task 1 – Discuss risk assessment procedures (P5)

I. Define a security risk

The likelihood of exposure, loss of key assets, and data damage or loss as a result of a cyber threat... Security risk must remain a top priority across industries, and businesses should work to develop a security risk management strategy to protect against ever-changing cyber threats. (Threatanalysis, 2022)

Figure 1: Security risk (Sourse: Internet)

II. Risk assessment procedures

1. Define a risk assessment

Key security controls in applications are found, evaluated, and put into place by a security risk assessment. Additionally, it emphasizes avoiding application security flaws and vulnerabilities. An enterprise can see the application portfolio holistically—from the viewpoint of an attacker—by conducting a risk assessment. It aids managers in deliberating wisely about the use of resources, tools, and security control implementation. Therefore,

completing an assessment is a crucial step in the risk management process of a firm. (Synopsys , 2022)

Figure 2:Risk Assessment (Source: Internet)

2. How does a security risk assessment work?
   The depth of risk assessment models is influenced by variables including size, growth rate, resources, and asset portfolio. If an organization is limited by time or money, it can nonetheless conduct broad assessments. The specific mappings between assets, associated threats, identified risks, effects, and mitigation controls, however, may not always be provided by generalist assessments.
   A more thorough examination is required if the findings of the generalized assessment don't show a strong enough association between these areas.
   (Synopsys , 2022)
3. Risk assessment procedures
   - **Identification:**
     Find out what the infrastructure's most important technological assets are. Next, determine whether these assets are producing, storing, or transmitting sensitive data. For each, create a risk profile.
   - **Assessment:**
     Implement a strategy to evaluate the important assets' identified security threats. Determine ways to effectively and efficiently deploy time and resources toward risk mitigation after rigorous review and assessment. The methodology or assessment strategy must examine the relationships among assets, risks, vulnerabilities, and mitigating controls.
   - **Mitigation:**
     Define a mitigation approach and enforce security controls for each risk.

- **Prevention:**
  Implement tools and processes to reduce the likelihood of threats and vulnerabilities occurring in your firm's resources.
  (Synopsys , 2022)

III. Define assets and threats

- **Assets:** Information, property, and people. Employees, clients, and other invited parties like contractors or guests may all be considered people. Both tangible and intangible elements that can be given a value make up property assets. Reputation and confidential information are examples of intangible assets. Databases, software code, important corporate records, and many other intangible objects can all be considered forms of information. (Threatanalysis, 2022)
- **Threats:** Threats are security conditions that could have negative effects on people's lives or property. It could take the form of physical or verbal warnings intended to frighten a specific demographic. (Threatanalysis, 2022)

IV. Threat identification procedures with examples

1. Threat identification procedures
   - Analyzing and comprehending the threat portfolio unique to your organization and its operations.
   - Prioritizing the assessment of your system's vulnerabilities.
   - Determining how specific threat actors or actions may exploit those vulnerabilities.
   - Providing a detailed report of findings that allows your organization to implement risk management actions in advance.
     (Warditsecurity, 2022)
2. Examples of threat identification procedures
   - **Identification Threat in Asset: Physical document**
     - Threat identification:
       + The vulnerability is that the document is not housed in a fire-proof safety box (the threat is that the document's availability will be lost).
       + Unauthorized access, the important document is not locked and secured in a safe box (possible loss of confidentiality) is a flaw.
       + Earthquakes, fires, and so on... and there is no backup of these paper documents (possible availability loss) ….
   - **Identification Threat in Asset: Digital document data**
     - Threat identification:
       + A virus-caused vulnerability occurs when anti-virus software is out of date or contains numerous security holes (possible confidentiality, integrity and availability loss)

+ Unauthorized access is a threat so many people were granted access that it created a vulnerability (potential loss of confidentiality, integrity, and availability).
+ Unauthenticated access from unknown websites. Poorly established access control strategy Vulnerability, SQL injection from unknown persons (potential loss of confidentiality, integrity, and availability)
+ Storage data failure and no document backup (potential loss of availability)

(Warditsecurity, 2022)

V. List risk identification steps

- **Step 1:**
  Risk Identification: The purpose of risk identification is to show what, where, when, why and how could affect a company's ability to operate. For example, a Central California company might include "potential wildfires" as an event that could disrupt business operations.
- **Step 2:**
  Risk Analysis: This step entails determining the likelihood of a risk event occurring as well as the potential outcomes of each event. Using the California wildfire as an example, safety managers could assess how much rain fell in the previous 12 months and the extent of damage the company could face if a fire broke out.
- **Step 3:**
  Risk Evaluation: The magnitude of each risk is compared and ranked according to prominence and consequence. For example, the consequences of a potential wildfire may be weighed against the consequences of a potential mudslide. Whichever event is determined to have a higher likelihood of occurring and causing damage ranks higher.
- **Step 4:**
  Risk Treatment: Risk treatment is also known as risk treatment planning. In this step, risk mitigation strategies, preparedness and contingency plans are developed based on each risk estimate. Using the Wildfire example, a risk manager could place an additional network of his servers offsite so that business can continue even if his server onsite is damaged. Risk managers can also develop employee evacuation plans.
- **Step 5:**
  Risk Monitoring: Risk management is a never-ending process that evolves and changes over time. Repeating and continuously monitoring the processes can help ensure that all known and unknown risks are covered.
  (Safetymanagement, 2020)

Task 2 – Explain data protection processes and regulations as applicable to an organization (P6)

I. Define data protection

Data protection is the process of securing digital information while keeping it usable for business purposes without jeopardizing the privacy of customers or end users. As the number of devices to monitor and protect grows, data protection becomes more complicated. It now includes IoT devices and sensors, industrial machines, robotics, wearables, and other technologies. Data protection reduces risk and enables a company or government agency to respond quickly to threats. (Security Intelligence, 2022)

Figure 3: Data Protection (Source: Internet)

II. Explain the data protection process in an organization

1. CIA triads

- Definition CIA triads:
  "CIA triad" is an acronym that stands for Confidentiality, Integrity, and Availability. The CIA triad is a widely used model that serves as the foundation for the development of security systems. They are used to identify vulnerabilities as well as methods for developing solutions. (Fortinet , 2022)
- Why should you use the CIA Triad?
  The CIA triad provides a straightforward yet comprehensive high-level checklist for assessing your security procedures and tools. A successful system meets all three requirements: confidentiality, integrity, and availability. A lack of one of the three aspects of the CIA triad in an information security system is insufficient.
  The CIA security triad is also useful in determining what went wrong—and what worked—following a negative incident. For example, perhaps availability was compromised as a result of a malware attack, such as ransomware, but the systems in place still maintained the confidentiality of critical information. This information can be used to correct flaws and replicate successful policies and implementations.

(Fortinet , 2022)

2. AAA
    - Define AAA:

      A security framework that controls access to computer resources, enforces policies, and audits usage is known as authentication, authorization, and accounting (AAA). AAA and its associated processes play an important role in network management and cybersecurity by screening users and monitoring their activity while connected. (Fortinet, 2022)
    - Why is the AAA framework important in network security?

      AAA is an important component of network security because it restricts who has access to a system and tracks their activity. Bad actors can thus be kept out, while a presumably good actor who abuses their privileges can have their activity tracked, providing administrators with valuable intelligence about their activities.

      For networking, there are two types of AAA: network access and device administration:
        - Network Access:

          Network access entails blocking, granting, or limiting access based on a user's credentials. AAA validates a device's or user's identity by comparing the information presented or entered against a database of approved credentials. Access to the network is granted if the information matches.
        - Device Administration:

          Device administration entails controlling access to sessions, network device consoles, secure shell (SSH), and other resources. This type of access differs from network access in that it does not restrict who can enter the network but rather which devices they can access.

          (Fortinet, 2022)
3. GDPR
    - Define GDPR:

      The General Data Protection Regulation (GDPR) is a legal framework that establishes guidelines for the collection and processing of personal information from European Union residents (EU). Because the Regulation applies regardless of where websites are hosted, all sites that attract European visitors must comply, even if they do not specifically market goods or services to EU residents. (Nadeau, 2020)
    - What type of privacy data does the GDPR protect?
        - Basic identity information such as name, address and ID numbers
        - Web data such as location, IP address, cookie data and RFID tags
        - Health and genetic data

- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

(Nadeau, 2020)

III. Why are data protection and security regulations important?

In less than a year, the General Data Protection Regulation (GDPR) law will change. This represents the most significant data protection regulation change in 20 years. As a set of rules governing the use of personal data within the EU, it is of great importance to most businesses in the region.

All companies and organizations that handle data of EU citizens must comply with the new GDPR. The UK has announced that it will implement the EU GDPR despite Brexit. It is all the more important that your company is familiar with the new regulations.

Task 3 – Design and implement a security policy for an organization (P7)

I. Define security policy

A security policy is a documented set of controls and statements. It specifies how the company will achieve a secure position. More importantly, it defines business systems' Confidentiality, Integrity, and Availability (CIA triad). (Isgovern, 2022)

Figure 4: Security Policy (Source: Internet)

II. Discussion on policies

1. HR Policy
    - Definition:

HR policies are an important part of any organization because they help to establish clear guidelines for how the company operates. It is a way to safeguard your company and avoid future misunderstandings. (Bhasin, 2021)

- The importance of HR Policy:
  - It ensures that employees are fairly compensated.
  - They are necessary because they ensure that eligible employees receive their allotted holidays and paid vacations on time.
  - It is regarded as critical because it aids in the maintenance of organizational discipline.
  - It ensures that the organization's employees' needs are respected and met.
  - It ensures that employees receive appropriate training and development opportunities to meet the needs of the organization.
  - It assists in addressing employee issues, complaints, and grievances and even provides a means of resolving them.
  - It protects employees from anyone within the organization.
  - It ensures that employees receive adequate compensation for their efforts. (Bhasin, 2021)

2. IR Policy (incidence response policy)
   - Definition:
     Industrial relations are a set of procedures and systems used by employers and employees to determine the following:
     - Workplace conditions and employee treatment.
     - Employment terms and conditions: Terms are intended to ensure and protect the interests of both employees and employers. It ensures that neither employers nor employees are exploited.

   - The importance of IR Policy:
     - Accountability and optimum use of scarce resources
     - Initiates an environment for change
     - Promotes democracy
     - Avoids conflicts between management and unions
     - Economic growth and development
     - It prompts the depiction of sound labor legislation
     - Boosts employee morale
3. AUP Policy (acceptable use policy)
   - Definition:

Acceptable use policy is defined as the set of rules that the creators, owners, or administrators of various resources (e.g., services, systems, and networks) use to limit the authorized use of those resources by users. (Bhasin, 2021)

- General AUP Stipulations used by ISPs:
  - To prevent misuse of their services, Internet service providers typically enforce various types of AUPs. Such requirements may include:
    + Not using the service in any way that violates any laws.
    + Avoiding any firms or individuals from hacking or breaking into any servers or network owners.
    + Using the "unlimited" internet bandwidth in accordance with the stated FUP (fair usage policy).
    + Accepting the risk of broadband internet suspension or termination for violating the above-mentioned FUPs.
    + Not engaging in DDoS attacks to bring down any website's server.

  (Bhasin, 2021)

III. Give an example for each of the policies

Example of AUP Policy:

- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, (Company) personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any (Company) Information Resource.
- Access control policy (ACP): An ACP establishes the guidelines for user access, network access controls, and system software controls. Techniques for monitoring how systems are accessed and used, removing access when an employee leaves the organization, and securing unattended workstations are frequently included as supplemental items.
- Remote access policy: According to an IBM study, remote work during COVID-19 increased the cost of a data breach in the United States. An overseas access policy that outlines and defines procedures for remotely accessing the organization's internal networks can be implemented by organizations. When there are dispersed networks with the ability to expand into unsecured network locations, such as home networks or coffee shops, organizations must implement this policy.

  (Bhasin, 2021)

IV. Give the most and should that must exist while creating a policy

- ENSURE THAT THERE IS A POLICY ON POLICIES: It may seem obvious, but it is critical to work within a predefined and agreed-upon framework when developing policy. A simple policy on policies that defines the organization's process for developing new policies is an important first step in policy maturation. This "meta policy" should include guidance on what situations necessitate the creation of a new policy, the format for new policies, and the approval process for new policies. Without a policy formation process and framework, you risk significant inconsistency in outcomes and inconsistency in creation, which can lead to poor or difficult enforcement. (Lowe, 2012)
- IDENTIFY ANY OVERLAP WITH EXISTING POLICIES: This one is simple. Before you create a new policy, check to see if the policy you're planning to create already exists or if portions of it exist in other policies. If so, consider revising existing policies rather than creating a brand new one. (Lowe, 2012)
- DON'T DEVELOP THE POLICY IN A VACUUM: I've seen people sit behind their desks and draft policies that they felt were necessary and that they created entirely on their own. This has most often occurred in organizations that lack any kind of policy governance structure. Most policies lacked key elements and were slanted in ways that were detrimental to the organization. However, as one might expect, the policies benefited the person who devised them. (Lowe, 2012)
- STEP BACK AND CONSIDER THE NEED: Is it your intention to create a policy because one is required, or because someone did something you didn't like? There is a significant difference, and I have seen policies implemented out of spite and retribution. Obviously, such behavior would not occur in a reasonable organization. However, it will not happen in a company that has a strict policy on policies, because the policy will generally go through multiple levels of approval, and somewhere along the way, someone will step back and ask, "Why do we need this?"
  When there is a clear need and a clear problem to solve, policies should be enacted. (Lowe, 2012)
- USE THE RIGHT WORDS SO THERE IS NO MISUNDERSTANDING INTENT: To be effective, policies must be understood. This effort is aided by the use of clear and unambiguous grammar. Use simple and specific terminology that everyone can understand. In the body of the policy, use the words "must" or "will" rather than "should." The latter implies that the action is optional, casting doubt on the policy's necessity. When something is optional, use the word "should," but not when it is mandatory. (Lowe, 2012)
- WHEN POSSIBLE, INCLUDE AN EXCEPTIONS PROCESS: In most cases, there is an exception to every rule. It is much easier to define how an exceptions process will work before the policy is implemented. Think twice before saying, "I will never allow exceptions." A situation will arise at some point that will necessitate an exception. Because policies are intended to control behavior and level the playing field, it is critical that

exceptions be granted in a fair and equitable manner. If you abuse the exceptions procedure, the entire policy may be called into question. (Lowe, 2012)

- ALLOW SOME SHADES OF GRAY: So you've crafted an impenetrable policy and defined an exceptions procedure that no one can question. That's a good goal, but it's difficult to achieve for every policy. Because policies are supposed to create equitable conditions, this is the point that may face the most criticism. However, I believe that some policies should leave some ambiguity in order for people to make decisions. That is not to say that the policy should simply allow people to do whatever they want, but there appear to be far too many instances where people are allowed to use "that's policy" or "zero tolerance" excuses to avoid doing the right thing. (Lowe, 2012)
- DEFINE POLICY MAINTENANCE RESPONSIBILITY: Most policies require periodic review to ensure their continued applicability. Further, as questions are raised about the policy, someone needs to be able to provide clarifying information. Make sure that you always identify the office — not the individual person — that is responsible for the policy. You don’t identify individuals since they come and go. (Lowe, 2012)
- KEEP SENIOR EXECUTIVES OUT OF THE ROUTINE WHEN POSSIBLE: When possible, I mentioned the need to identify an exceptions process for policies. That was the CEO's responsibility in one organization I worked for. That was, frankly, a waste of his time. The exceptions procedure should empower someone within the organization to handle exceptions. Except where required by regulation or law, the identified person does not need to be a VP or the CEO. Also, don't expect senior executives to create every policy. However, the senior team should be in charge of reviewing new policies before they go into effect. (Lowe, 2012)
- ESTABLISH A POLICY LIBRARY WITH VERIONING: There are numerous tools available these days, such as SharePoint, that allow you to save versions of documents. Every employee should have constant access to all relevant policies. How can employees be expected to follow policies if they do not have access to them? When it comes to versioning, as policies evolve, it's helpful to look at their history to see what has changed over time. (Lowe, 2012)

V. Explain and write down elements of a security policy

- PURPOSE:
  First state the purpose of the policy, which may be to:
  - Create a comprehensive approach to information security.
  - Detect and prevent data security breaches such as network, data, application, and computer system misuse.
  - Maintain the organization's reputation while adhering to ethical and legal obligations.

- Customer rights must be respected, including how to respond to inquiries and complaints about noncompliance.

- AUDIENCE:
  Define the audience to whom the information security policy applies. You can also indicate which target groups are outside the scope of the policy (for example, employees in different business units that manage security separately may not be within the scope of the policy).
- INFORMATION SECURITY OBJECTIVES:
  Assist your management team in developing well-defined strategy and security objectives. The primary goals of information security are as follows:
  - Confidentiality - Only authorized individuals should have access to data and information assets.
  - Integrity - Data must be intact, accurate, and complete, and IT systems must remain operational.
  - Availability - Users should have access to information or systems when they need it.
- AUTHORITY AND ACCESS CONTROL POLICY:
  - A senior manager may have the authority to decide what data can and cannot be shared and with whom. A senior manager's security policy may differ from that of a junior employee. The policy should specify the level of authority each organizational role has over data and IT systems.
  - Users can only access company networks and servers through unique logins that require authentication, such as passwords, biometrics, ID cards, or tokens. All systems should be monitored and all login attempts should be recorded.
- DATA CLASSIFICATION:
  The policy should categorize data into categories such as "top secret," "secret," "confidential," and "public." Your goal in data classification is:
  - To prevent individuals with lower clearance levels from accessing sensitive data.
  - To protect critical data while avoiding unnecessary security measures for unimportant data.
- DATA SUPPORT AND OPERATIONS:
  - Data protection regulations require that systems that store personal or sensitive data adhere to organizational standards, best practices, industry compliance standards, and relevant regulations. Most security standards require encryption, a firewall, and anti-malware protection as a bare minimum.
  - Data backup — Encrypt backup data in accordance with industry best practices. Backup media should be securely stored or moved to secure cloud storage.

  - Data transfer — Only use secure protocols to transfer data. Encrypt any data copied to portable devices or sent over a public network.
- SECURITY AWARENESS AND BEHAVIOR:
  Inform your employees about IT security policies. Conduct training sessions to educate employees on your security procedures and mechanisms, such as data protection, access control, and sensitive data classification.
  - Social engineering — Emphasize the dangers of social engineering attacks (such as phishing emails). Employees should be held accountable for detecting, preventing, and reporting such attacks.
  - Policy regarding clean desks — A cable lock can be used to secure laptops. Documents that are no longer needed should be shredded. Keep printer areas clean to avoid documents falling into the wrong hands.
  - Policy for acceptable Internet usage—define how the Internet should be restricted. Do you allow YouTube and other social media websites? Using a proxy, you can block unwanted websites.
- ENCRYPTION POLICY:
  Encryption is the process of encoding data in order to make it inaccessible or hidden from unauthorized parties. It aids in the protection of data at rest and in transit between locations, ensuring that sensitive, private, and proprietary information remains private. It can also improve client-server communication security. An encryption policy assists organizations in defining:
  - The devices and media that must be encrypted by the organization.
  - When encryption is required.
  - The minimum requirements for the encryption software chosen.
- DATA BACKUP POLICY:
  A data backup policy establishes the guidelines and procedures for creating backup copies of data. It is an essential part of a comprehensive data protection, business continuity, and disaster recovery strategy. The following are the primary functions of a data backup policy:
  - Identifies all of the data that the organization needs to back up.
  - Determines backup frequency, such as when to perform an initial full backup and when to run incremental backups.
  - Defines a backup data storage location.
  - Lists all roles in charge of backup processes, such as backup administrators and IT team members.
- RESPONSIBILITIES, RIGHT, AND DUTIES OF PERSONNEL: Appoint staff to carry out user access reviews, education, change management, incident management,

implementation, and periodic updates of the security policy. Responsibilities should be clearly defined as part of the security policy.

- SYSTEM HARDENING BENCHMARKS: The information security policy should reference security benchmarks the organization will use to harden mission critical systems, such as the Center for Information Security (CIS) benchmarks for Linux, Windows Server, AWS, and Kubernetes.
- REFERENCES TO REGULATIONS AND COMPLIANCE STANDARDS: The information security policy should reference regulations and compliance standards that impact the organization, such as GDPR, CCPA, PCI DSS, SOX, and HIPAA.

(Cassetto, 2022)

VI. Give the steps to design a policy

- There are numerous existing tools and techniques to support the Open Policy Making process; however, this Toolbox focuses on a novel approach - leveraging open data to accelerate the collection of policy evidence and the time to policy implementation. This is accomplished by employing advanced policy visualizations. We begin the process with four key steps in the policy design cycle:
  - Problem setting
  - Policy formulation
  - Scenario analysis
  - Decision.

➢ **Step 1: Problem setting**

There are numerous existing tools and techniques to support the Open Policy Making process; however, this Toolbox focuses on a novel approach - leveraging open data to accelerate the collection of policy evidence and the time to policy implementation. This is accomplished by employing advanced policy visualizations. We begin the process with four key steps in the policy design cycle:

- Analyzing existing policies and their consequences in order to determine their effectiveness in dealing with the problem;
- Identifying key stakeholders and, if possible, their perspectives;
- Identifying a link between the problem and a possible cause;
- Creating quantitative dimensions for the problem:
  - ✓ Problem description
  - ✓ Overarching policy goals
  - ✓ Specific policy objectives

➢ **Step 2: Policy formulation**

Once the problem has been identified, the hypotheses have been confirmed, and the goals and objectives have been identified and shared with the larger community,

policy formulation can begin. Policy formulation seeks to define and mobilize a set of solution options in relation to the issue, with the goal of determining which option is best suited to address the problem in light of available resources and existing constraints. The creation of scenarios (both written and visual) can aid in the comprehension and formulation of alternative strategies and actions. The primary activities are as follows:

- Developing pertinent strategies - strictly related to political decisions
- Defining potential actions - operationalizing the strategies
- Impact calculation - the potential systemic consequences of implementing the options strategy.

➢ **Step 3: Scenario analysis**

Once scenarios are created to represent various policy options for dealing with the identified problem, the best option in terms of strategies and actions can be selected. Scenarios analysis also includes the (re)tuning of existing policy actions, which is done through small experiments (pilot tests) and public debate. On-the-ground experiments typically seek to test various options on a small scale in order to understand potential impacts, which can be a time-consuming and costly process. In many cases, it may be possible to simulate visualisations for various policy options in order to explore the implications digitally. Predicting how traffic flow and density will change due to changes in road access, for example, or how public transportation will cope with demand surges. The following are the primary activities associated with scenario analysis:

- Defining best strategies
- Defining best actions
- Estimating impacts

➢ **Step 4: Decision**

To make a decision, a clear description of the problem, the policy and its scenario, and public acceptance of the policy must be prepared for presentation and discussion within the public unit responsible for the decision. The process narrative is relevant to the decision: how the problem was explored, how data was collected and used, how goals and objectives were identified and translated into strategies and actions, how impacts were simulated and computed, why some options were preferred over others, and what the public's contribution to the entire process was. The policy implementation cycle can begin once a decision has been made and the policy is ready to be translated into an implementation plan.
(PolicyVisuals, 2022)

Task 4 – List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion. (P8)

I. Discuss with an explanation about business continuity

- Define of business continuity:
  Business continuity is the advance planning and preparation undertaken to ensure that an organization can continue to operate its critical business functions in the event of an emergency. Natural disasters, business crises, pandemics, workplace violence, and any other event that disrupts your business operation are examples of events. It is critical to remember that you should plan and prepare not only for events that will completely shut down functions, but also for those that have the potential to negatively impact services or functions. (Inap, 2017)
- What type of events does business continuity planning guard against?
  - ✓ Cybersecurity:
    Cybersecurity threats are a global phenomenon that no business, large or small, can afford to ignore. New threats, such as ransomware, are expected to proliferate. Backing up your data on a regular basis is critical to ensuring that such attacks do not bring your business down. A data breach plan is also essential.
  - ✓ Human error:
    Vulnerability points are frequently found in the cubicle next to you. Employees or vendors can cause outages simply because they are unaware, make innocent mistakes, or have malicious intent.
  - ✓ Natural and man-made disasters:
    Natural disasters such as floods, earthquakes, and fires can obviously cause data loss and system failure, but even a simple electronic malfunction can destroy valuable information. Putting all of your eggs in one basket when it comes to data is a dangerous risk.
  - ✓ Disruptions in the Network:
    Third-party internet networks are susceptible to failure. Fiber can be severed. Your local area network can be turned off. If your company requires continuous connectivity, make network availability a top priority.
    (Inap, 2017)

II. List the components of the recovery plan

- **Create a disaster recovery team:**
  The DRP will be developed, implemented, and maintained by the team. A DRP should identify team members, define each member's responsibilities, and provide contact information for each member. In the event of a disaster or emergency, the DRP should also

specify who should be contacted. All employees should be aware of and understand the DRP, as well as their responsibilities in the event of a disaster.

- **Identify and assess disaster risks:**
  Your disaster recovery team should identify and assess your organization's risks. This step should include natural disasters, man-made emergencies, and technological incidents. This will help the team identify the recovery strategies and resources needed to recover from disasters within a reasonable timeframe.
- **Determine critical applications, documents, and resources:**
  The organization must assess its business processes to determine which are critical to the organization's operations. The plan should prioritize short-term survival measures such as cash flow and revenue generation over long-term solutions such as restoring the organization's full operational capacity. However, the organization must recognize that some processes should not be postponed if at all possible. Payroll processing is an example of a critical process.
- **Specify backup and off-site storage procedures:**
  These procedures should specify what should be backed up, by whom, how the backup should be performed, the location of the backup, and how frequently backups should occur. Back up all critical applications, equipment, and documents. The most recent financial statements, tax returns, a current list of employees and their contact information, inventory records, and customer and vendor listings are all documents you should consider backing up. Critical supplies for daily operations, such as checks and purchase orders, as well as a copy of the DRP, should be kept in a secure location off-site.
- **Test and maintain the DRP:**
  Disaster recovery planning is an ongoing process because the risks of disasters and emergencies are constantly changing. It is recommended that the organization test the DRP on a regular basis to assess the effectiveness and appropriateness of the procedures documented in the plan. The recovery team should update the DRP on a regular basis to account for changes in business processes, technology, and evolving disaster risks. (mksh, 2022)

III. Write down the steps required in the disaster recovery process

- Obtain Top Management Commitment:
  Top management must support and participate in the disaster recovery planning process. Management should be in charge of coordinating and ensuring the effectiveness of the disaster recovery plan within the organization.
  A sufficient amount of time and resources must be dedicated to the development of an effective plan. Financial considerations as well as the efforts of all personnel involved could be considered resources.

- Establish a planning committee:
  A planning committee should be formed to oversee the plan's development and implementation. Representatives from all functional areas of the organization should serve on the planning committee. The operations manager and the data processing manager should be key committee members. The committee should also define the plan's scope.
- Perform a risk assessment:
  The planning committee should conduct a risk analysis and business impact analysis that considers a variety of potential disasters, including natural, technological, and human threats.
  Each organizational functional area should be examined to determine the potential consequences and impact of various disaster scenarios. The safety of critical documents and vital records should also be evaluated during the risk assessment process.
  Historically, fire has been the most dangerous threat to an organization. Intentional human destruction, on the other hand, should be considered. The plan should account for the "worst case" scenario, which is the destruction of the main building.
  It is critical to assess the impacts and consequences of information and service loss. The planning committee should also assess the costs of mitigating potential risks.
- Establish priorities for processing and operations:
  The critical needs of each department within the organization should be carefully evaluated in such areas as:
    - Functional operations
    - Key personnel
    - Information
    - Processing Systems

      ……..

  Processing and operations should be examined to determine how long the department and organization can function without each critical system.
  Critical needs are defined as the procedures and equipment required to maintain operations in the event that a department, computer center, main facility, or a combination of these are destroyed or become inaccessible.
  Documenting all of the functions performed by each department is one method of determining a department's critical needs. After identifying the primary functions, the operations and processes should be prioritized as follows: essential, important, and non-essential.
- Determine Recovery Strategies:
  The most practical alternatives for processing in case of a disaster should be researched and evaluated. It is important to consider all aspects of the organization such as:
    - Hardware

- Software
- Communications
- Data files
- Customer services
- Other processing operations

…….

Alternatives, dependent upon the evaluation of the computer function, may include:

- Hot sites
- Warm sites
- Cold sites
- Reciprocal agreements
- Two data centers
- Multiple computers

…….

Written agreements for the specific recovery alternatives selected should be prepared, including the following special considerations:

- Testing
- Costs
- Special security procedures
- Notification of systems changes
- Hours of operation
- Specific hardware and other equipment required for processing
- Personnel requirements

……

- Perform Data Collection

Recommended data gathering materials and documentation includes:

- Communications Inventory
- Distribution register
- Documentation inventory
- Equipment inventory
- Forms inventory
- Insurance Policy inventory
- Main computer hardware inventory
- Master call list
- Other materials and documentation

……..

It is extremely helpful to develop pre-formatted forms to facilitate the data gathering process.

- Organize and document a written plan
  To guide the development of the detailed procedures, an outline of the plan's contents should be prepared. The proposed plan should be reviewed and approved by top management. After final revision, the outline can be used for the table of contents. Other advantages of this approach include:
    - Aids in the organization of detailed procedures
    - Identifies all major steps prior to beginning writing
    - Identifies redundant procedures that only need to be written once
    - Provides a framework for developing procedures.
- Develop testing criteria and procedures
  The plan must be thoroughly tested and evaluated on a regular basis (at least annually). Document the procedures for testing the plan. The tests will assure the organization that all necessary steps are included in the plan. Other justifications for testing include:
    - Determining the feasibility and compatibility of backup facilities and procedures
    - Identifying areas in the plan that require modification
    - Training team managers and team members
    - Demonstrating the organization's ability to recover
    - Providing motivation for maintaining and updating the disaster recovery plan
- Test the Plan
  Following the completion of testing procedures, an initial test of the plan should be performed by conducting a structured walk-through test. The test will provide additional information on any additional steps that may be required, changes to ineffective procedures, and other appropriate adjustments. The plan should be updated to address any issues discovered during the test. To minimize disruptions to the organization's overall operations, initial testing of the plan should be done in sections and after normal business hours.
  Types of tests include:
    - Checklist tests
    - Simulation tests
    - Parallel tests
    - Full interruption tests
- Approve the plan
  Top management should approve the disaster recovery plan after it has been written and tested. It is the ultimate responsibility of top management to ensure that the organization has a documented and tested plan.
  Management is responsible for:

- Establishing policies, procedures and responsibilities for comprehensive contingency planning.
- Reviewing and approving the contingency plan annually, documenting such reviews in writing

(Wold, 2022)

IV. Explain some of the policies and procedures that are required for business continuity

- Network Monitoring:
  A network monitoring system constantly monitors a computer network to ensure that it is functioning properly. It may also improve data flow and access in a complex environment and assess global network availability. Various software or a combination of plug-and-play hardware and software appliance solutions can be used to monitor networks.
- Auditing:
  Examine documented policies and procedures to ensure adherence to IS disaster recovery and continuity of critical business services in the event of a disruption.
  The scope of the audit included:
  - Determines compliance with federal laws and regulations.
  - Examine the current IS disaster recovery strategy for the existence and effectiveness of the strategy and alignment with the organization's business continuity plans, regulations and processes.
  - Assess the readiness of the IS department in the event of a process disruption.
- Incident Response:
  Make a disaster recovery strategy. A disaster recovery plan is a strategy for quickly restoring all critical company services in the event of a disaster. This plan includes all 19 steps required to deal with an emergency. A disaster recovery strategy that can demonstrate recovery capabilities should be implemented as soon as a crisis occurs. The DRP frequently incorporates technological strategies and is concerned with getting systems up and running as soon as possible and within a reasonable time frame (RTO and RPO). RTO and RPO are DRP objectives for recovery time and recovery point objectives.

Conclusion

In other words, this task describes risk assessment procedures, describes data protection procedures and regulations that apply to your organization, designs and implements your organization's security policies, lists the key components of your organization's disaster recovery plan, rationale, etc. And I have completed all the requirements that the post gave. It wasn't very clear, but it helped me understand the topic I was talking about better.

References

Bhasin, H., 2021. *What is Acceptable Use Policy (AUP)? – Definition and Tips.* [Online]
Available at: https://www.marketing91.com/acceptable-use-policy/

Bhasin, H., 2021. *HR Policies – Meaning, Importance and Functions.* [Online]
Available at: https://www.marketing91.com/hr-policies/?fbclid=IwAR0f8DnZExTdqIlWqiQHCRkBruZZe4AAPw81EKvL_iQ4SKJBYrOywVJZE0s

Cassetto, O., 2022. *The 12 Elements of an Information Security Policy.* [Online]
Available at: https://www.exabeam.com/information-security/information-security-policy/

Fortinet , 2022. *CIA Triad.* [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,and%20methods%20for%20creating%20solutions.

Fortinet, 2022. *AAA Security.* [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/aaa-security#:~:text=Authentication%2C%20authorization%2C%20and%20accounting%20(AAA)%20is%20a%20security,enforces%20policies%2C%20and%20audits%20usage.

Inap, 2017. *What is Business Continuity?.* [Online]
Available at: https://www.inap.com/blog/business-continuity/#:~:text=Business%20continuity%20is%20an%20organization%27s,that%20take%20critical%20systems%20offline.

Isgovern, 2022. *What is a Security Policy?.* [Online]
Available at: https://isgovern.com/blog/what-is-a-security-policy/?fbclid=IwAR10pKA7Qn1CVwDifh9ceZOFa7O7Dh-1g3-_0-YCq0ruwNArhW7Epw1wJeI

Lowe, S., 2012. *10 things to consider when creating policies.* [Online]
Available at: https://www.techrepublic.com/article/10-things-to-consider-when-creating-policies/

mksh, 2022. *5 ELEMENTS OF A DISASTER RECOVERY PLAN – IS YOUR BUSINESS PREPARED?.* [Online]
Available at: https://mksh.com/5-elements-of-a-disaster-recovery-plan-is-your-business-prepared/

Nadeau, M., 2020. *General Data Protection Regulation (GDPR): What you need to know to stay compliant.* [Online]
Available at: https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

PolicyVisuals, 2022. *Policy Design.* [Online]
Available at: https://policyvisuals.eu/policy-design/

Safetymanagement, 2020. *Risk Identification: 7 Essentials.* [Online]
Available at: https://safetymanagement.eku.edu/blog/risk-identification/?fbclid=IwAR0FIBgrQm6ikCb74vTTYU3Bp4VEYTPqGFAP5xADysaN8cACYUrRcLb3ix4#:~:text=Risk%20Identification%20Process%20Steps,risk%20treatment%2C%20and%20risk%20monitoring

Security Intelligence, 2022. *What Is Data Protection and Why Does it Matter?.* [Online]
Available at: https://securityintelligence.com/articles/what-is-data-protection/?fbclid=IwAR2lK2u7RnZAayZ6EO_dEc7ThNg3AHw_ZqU6LFjzEE1Ml2iCu7BvLYS94cE

Synopsys , 2022. *Security Risk Assessment.* [Online]
Available at: https://www.synopsys.com/glossary/what-is-security-risk-assessment.html?fbclid=IwAR3rYoJZie4L4NLnISeJU65Pr3k-JvTILWrPL-CNpC8YJOI-N36IGel0-8c

Threatanalysis, 2022. *Threat, vulnerability, risk – commonly mixed up terms.* [Online]
Available at: https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/?fbclid=IwAR3GkJyWL2LejshkJbH5uLoVxgojrihnaxzyPnG7Hs1mON8ynfstPsGwMos

Warditsecurity, 2022. *THREAT IDENTIFICATION.* [Online]
Available at: https://warditsecurity.com/threat-identification/?fbclid=IwAR0S4acb1T4mAYRcje3hQg8TrS_Pk8hAyO_KGQscIeNEdY0At_vM9d9Mcmw

Wold, G. H., 2022. *DISASTER RECOVERY PLAN TEMPLATE.* [Online]
Available at: https://www.disasterrecoveryplantemplate.org/disaster-resilience/disaster-recovery-planning-process/