Learner's name: Vo Thi Le Na

ID: GCS190745

Assessor name: Ho Hai Van

Class: 0806_PPT

Subject code: 1623

ASSIGNMENT 2

Unit 5: Security

Security Presentation

Ensure a secure network environment

Assessment Brief

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number	Unit 5: Security		
Assignment title	Security Presentation		
Academic Year			
Unit Tutor			
Issue date		**Submission date**	
IV name and date	Khoa Canh Nguyen, Michael Omar, Nhung 9th/01/2020		

Submission Format
Part 1 The submission is in the form of an individual written report. This should be written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs, subsections and illustrations as appropriate, and all work must be supported with research and referenced using the Harvard referencing system. Please also provide a bibliography using the Harvard referencing system. The recommended word limit is 2,000–2,500 words, although you will not be penalized for exceeding the total word limit. **Part 2** The submission is in the form of a policy document (please see details in Part 1 above). **Part 3** The submission is in the form of an individual written reflection. This should be written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using the Harvard referencing system. Please also provide a bibliography using the Harvard referencing system. The recommended word limit is 250–500 words, although you will not be penalized for exceeding the total word limit.

Unit Learning Outcomes
LO3 Review mechanisms to control organizational IT security. **LO4** Manage organizational security.
Assignment Brief and Guidance
You work for a security consultancy as an IT Security Specialist. A manufacturing company "Wheelie good" in Ho Chi Min City making bicycle parts for export has called your company to propose a Security Policy for their organization, after reading stories in the media related to security breaches, etc. in organizations and their ramifications. **Part 1** In preparation for this task, you will prepare a report considering: 1. The security risks faced by the company. 2. How data protection regulations and ISO risk management standards apply to IT security. 3. The potential impact that an IT security audit might have on the security of the organization. 4. The responsibilities of employees and stakeholders in relation to security. **Part 2** Following your report: 1. You will now design and implement a security policy 2. While considering the components to be included in disaster recovery plan for Wheelie good, justify why you have included these components in your plan. **Part 3** In addition to your security policy, you will evaluate the proposed tools used within the policy and how they align with IT security. You will include sections on how to administer and implement these policies

Learning Outcomes and Assessment Criteria		
Pass	**Merit**	**Distinction**
LO3 Review mechanisms to control organisational IT security		
P5 Discuss risk assessment procedures. **P6** Explain data protection processes and regulations as applicable to an organisation.	**M3** Summarise the ISO 31000 risk management methodology and its application in IT security. **M4** Discuss possible impacts to organisational security resulting from an IT security audit.	**D2** Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment.
LO4 Manage organisational security		
P7 Design and implement a security policy for an organisation. **P8** List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.	**M5** Discuss the roles of stakeholders in the organisation to implement security audit recommendations.	**D3** Evaluate the suitability of the tools used in an organisational policy.

Table of contents

List of figures:

Introduction

First of all, I would like to introduce myself, I am Vo Thi Le Na, an IT security specialist of FPT. My company recently received a contract from the "Wheelie good" production company (which is a bicycle parts maker for export in Ho Chi Minh City). Due to the current complexity of cybersecurity breaches, they are concerned about their corporate security policy. With the beginning of the project, my company tasked me to prepare a detailed report.

This report will include an investigation into the current security situation of the company "Wheelie Good". Specifically, the report is divided into 3 parts with 3 separate groups of tasks. Part one, I will have to explore all the security risks this company might face, look at how ISO is applied, the potential impact on the security of the organization, the responsibility of the organization. security stakeholders and related parties. In Part 2, I will conduct the design and implementation of a security policy. And finally, in part 3, In addition to my privacy policy, I will look at the recommended tools used in the policy.

Figure 1: Network Security (BTS Website, 2021)

The above is only a summary of the content of the report, but the following will be specific lists of tasks to do in each of the above-mentioned sections:

- First, I will discuss risk assessment procedures in section P5. The first step is to identify and evaluate risks. Then the explain asset, threat and threat identification procedure, to clarify this task, I will give a concrete example to illustrate. Explain the risk assessment process and finally list the steps to determine the risk.

- With P6, I will use it to explain data protection procedures and regulations as they apply to this company. Specifically, I must define data protection, explain the data protection process with its relationship with this company, and the importance of data protection.

- In P7, the main task is to design and implement the corporate privacy policy "Wheelie good", and some other small tasks like defining and discussing what the privacy policy is, giving examples of policies, make the most & should exist while creating the policy, explain and write down the element of the security policy, give the steps to design the policy.

- With P8, I will list the main components of an organization's disaster recovery plan, explaining the reasons for inclusion. Specifically, I will discuss with an explanation of business continuity, listing the components of the recovery plan, writing down all the steps required in the disaster recovery process, explaining some key books and procedures needed to run business continuity

Body of the report

P5 Discuss risk assessment procedures.

1. **Define Risk & risk assessment.** (What is IT risk? | nibusinessinfo.co.uk, 2021)

   Here I will proceed to find out what is the definition of risk, and risk assessment, the word "risk" is used in many areas, and it has the same meaning and is defined as risk in IT.

   + Define of Risk: Information technology risk is the possibility of losses occurring when performing activities related to information technology systems. Information technology risks are related to management and use of hardware, software, communications, system

interfaces, operations and people. Categories of IT risks: IT risk spans a range of business-critical areas, such as:

- **Security**: compromised business data due to unauthorized access or use
- **Availability**: inability to access your IT systems needed for business operations
- **Performance**: reduced productivity due to slow or delayed access to IT systems
- **Compliance:** failure to follow laws and regulations (ex: data protection)

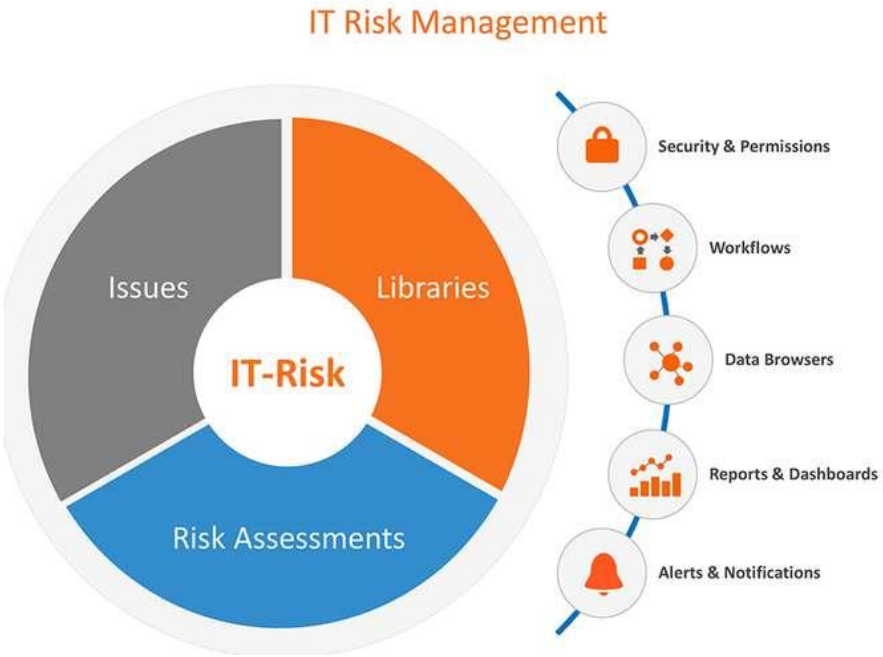

Figure 2: IT Risk (ITC596 IT Risk Management Oz Assignments, 2021)

+ Risk assessment: Risk assessment is the determination and analysis of relevant risks that affect the operation of an enterprise. To identify and analyze risks, administrators should:

- Setting the organization's goals, on the basis of the identified objectives, the administrator will conduct analysis, identification and risk management during implementation.
- Risk identification: Risk can be affected at the level of the whole unit or affect some parts of the unit.

- Risk analysis and assessment: Because risks are difficult to quantify, risk analysis and assessment are often quite complex. However, the process of risk analysis and assessment usually includes the following steps: Estimating the possible damage, considering the likelihood, the probability of the risk occurring, and preventive measures.

Figure 3: Risk assessment (Assessment, 2021)

2. Explain Asset, threat and threat identification procedure, give example

I will continue to explain asset, threat, and threat identification procedural definitions, thereby illustrating them with examples.

+ **Asset**: An organization's information art products include systems of hardware and software owned by that organization such as all-computer systems, routers, switches, servers, firewalls, all software, tools, cables ... Tracking IT assets in IT asset management systems can be critical to the operational or financial success of a business. Asset IT is an integral part of an organization's system and network infrastructure. (What is an IT Asset? - Definition from Techopedia, 2021)

Figure 4: Asset management (Scott Ford,2019)

+ Threat: A threat refers to a newly discovered or new problem that has the potential to harm your entire system or company, in other words the ability to accidentally or intentionally compromise information security. Trust, loss of confidentiality, integrity or availability, or impaired functionality that provides authenticity and does not deny information There are three main types of threats:

- Natural threats, such as floods, hurricanes or tornadoes
- Unintentional threats, such as an employee's mistaken access to information
- Intentional threats, such as spyware, malware, adware companies or the actions of a disgruntled employee

  (Stephen Watts, 2020)

Figure 5: Some IT threats (Pin on Flat style | Vector Graphics, Symbols, Illustrations, Icons, Design Elements, Logos & Clipart., 2021)

+ Threat identification procedure: The Threats Identification Procedure is the Threat Identification process that examines IT vulnerabilities and determines the potential for compromises of your system. It is an important element of an organization's risk management program. Threats identification allows the organization to take precautionary and protective actions in advance, preventing the organization from being inactive when those threats turn into action. (Threat Identification: Types of Threats Control Analysis Impact Analysis Occurrence of threat Information Systems Computer Science, 2021)

The following is a example for a process of a representative threat identification procedure:

- **Step 1**: Identify all possible threats, including all physical threats (such as human factors: hacker, cracker, employee, ..., environmental factors: water, fire, energy variations, failure equipment, ...) and logic threats (such as viruses, worms, logical intrusion, ...)

- **Step 2**: Determining the probability of the threats that means whether a threat can occur is high or low.
- **Step 3**: Determination of the potential impact of threats to the system
- **Step 4**: Identification of security vulnerabilities that can be exploited by a specific agent or threat action.
- **Step 5**: Control capacity analysis: is the analysis of protection measures integrated into computer hardware, software and firmware, such as control mechanisms, identification and authentication of mechanisms and methods. encryption, intrusion detection software, etc.

3. Explain the risk assessment procedure (Compliance and Assessment, 2021)

In the following I will draw upon my understanding and a search for knowledge of procedural risk assessment to explain this concept.

+ Risk assessment procedure is the process of identifying and evaluating risks for assets that could be affected by cyberattacks. Basically, you identify both internal and external threats; evaluate their potential impact on things like data availability, confidentiality and integrity; and estimate the costs of suffering a cybersecurity incident. With this information, you can tailor your cybersecurity and data protection controls to match your organization's actual level of risk tolerance.

Figure 6: Risk Assessment Process (Facilities Management Daily Advisor Staff, 2019)

+ The following is 9 steps of risk assessment procedure:

- **Step 1: Identify and Prioritize Assets**: Create a list that includes all valuable artistic assets including servers, hardware, software, databases, document sensors, ... and then plan it specifically to protect them.

- **Step 2: Identify threats**: In addition to notable threats such as hackers and malware, special attention must be paid to threats of natural disasters, hardware failure, and kernel threats. Bad members, malicious behaviours, ... can harm the organization.

- **Step 4: Analyse controls**: Analyse controls that have been implemented or are in the planning phase to minimize or eliminate the probability that a threat will exploit a vulnerability. Engineering controls include encryption, intrusion detection mechanisms, and identity and authentication solutions. Non-technical controls include security policies, administrative actions, physical mechanisms and the environment.

- **Step 5: Determine the likelihood of a failure**: Evaluate the probability that a vulnerability can actually be exploited, taking into account the type of vulnerability, the potential and the motivation of the source of the threat and its existence and effectiveness of your control measures.

- **Step 6: Evaluate the impact a threat may have**: Analyse the impact of an incident on lost or damaged assets using either quantitative or qualitative means to determine the impact of an incident. harmful effects to the organization's information assets, such as loss of confidentiality, integrity, and availability.

- **Step 7: Prioritize the Information Security Risks:** For each threat/vulnerability pair, determine the level of risk to the IT system, based on the following: The likelihood that the threat will exploit the vulnerability, the approximate cost of each of these

occurrences, the adequacy of the existing or planned information system security controls for eliminating or reducing the risk.

- **Step 8: Recommend controls:** Depending on the level of risk, determine the necessary actions to reduce it. For example, at high level, it is necessary to develop a plan for corrective measures as soon as possible, medium level needs to be overcome in a reasonable time, while low level must decide to accept risks. or take corrective action.

- **Step 9: Record the results:** Develop a risk assessment report to assist management in making appropriate decisions about budgets, policies, procedures, etc. For each threat, the report should describe the respective vulnerabilities, the assets at risk, the impact on your IT infrastructure, the likelihood of occurrence, and recommendations for control.

4. List risk identification steps

Maybe we already know the concept of risk identification, but if we already know the specific steps to take it, so now we'll learn about those specific ones.

*** Definition Risk identification:** is the process of identifying and assessing threats to an organization, its activities and workforce. Examples of risk identification can include an assessment of IT security threats such as malware and ransomware, crashes, natural disasters, and other potentially harmful events that could disrupt business activity. joint. general. Companies that develop robust risk management plans are more likely to find that they can mitigate the impact of threats, when and if they happen.

*** Risk identification steps:**

*** Step 1: Risk Identification**: The purpose of risk identification is to disclose what, where, when, why and how something can affect a company's ability to function. For example, a business located in central California might include a "possibility of a wildfire" as an event that could disrupt the business.

*** Step 2: Risk Analysis**: This step involves establishing the probability that a risky event will occur and the potential outcome of each event. Using the California wildfire example, safety managers can assess how much rain has happened over the past 12 months and how much damage the company could face if it did.

*** Step 3: Risk Assessment**: Risk assessment compares the magnitude of each risk and ranks them by degree of prominence and consequence. For example, the impact of a forest fire can be weighed against the impact of a potential landslide. Any event identified as having a higher probability of occurrence and causing more harm, the higher the event rating.

*** Step 4: Risk treatment**: Risk treatment is also known as risk response planning. In this step, risk reduction strategies, preventive care and contingency plans are created based on the assessed value of each risk. Using the wildfire example, risk managers can choose to place additional external network servers, so that the business can continue if the on-premises server goes down. The risk manager can also develop evacuation plans for employees.

*** Step 5: Risk monitoring**: Risk management is an ongoing process that adapts and changes over time. Repetition and continuous monitoring of processes can help ensure maximum coverage of known and unknown risks.

Figure 7: Risk identification step (TRIAL, 2021)

P6 Explain data protection processes and regulations as applicable to an organization.

Data is very important so we need to protect them, so what is the concept of data protection, let's learn together.

1. Define data protection

* Data protection is the process of data protection and involves the relationship between data collection and dissemination and technology, public perceptions and expectations about privacy and political grounds. and the legislation surrounding that data. It aims to strike a balance between individual privacy rights while allowing the data to be used for business purposes.

* Data protection must always be applied to all types of data, whether it's personal or corporate data. It deals with both data integrity, protection from corruption or error, and data privacy, it is only accessible to those with privileges to access it.

Figure 8: Data protection (STRASBOURG, 2021)

2. Explain data protection process with relations to organization

I will explain the database protection responsibility to all stakeholders / relationships of an organization in the following to ensure the most secure data.

+ Senior data managers: They are the ones who have direct access to all of the organization's data, so they need to ensure absolute safety when exposed to data, not to data. leaked by actors inside and outside the organization. In particular, they are not allowed to use data for private or unauthorized purposes. Carefully consider empowering subordinate employees as they work with data. Must be in control of the data traffic.

+ Employees: Must understand their personal responsibility when processing data. When collecting information, it must be accurate, and must be properly stored. They must obtain the approval of the data manager when they need to work with it, specifically what it is for. Not allowed to expose internal data to the outside. The data should be manipulated only with the company's devices such as phones, computers, laptops, ... should not let employees work with internal data right on their devices to avoid loss.

+ Partners, contractors, ...: If there is cooperation between the organization and a certain partner, the partner must strictly comply with the responsibility to protect the safety of data exchanged between the two parties about the parties. cooperation agreement, do not leak information to avoid unnecessary risks in the future.

+ Customer: When required by the organization to provide personal information for a certain service purpose, the customer has the right to disclose information or not to ensure his personal information is safe.

3. Why are data protection and regulation important?

We all know data is very sensitive for an organization, so I will give you the reasons why data protection is so important and paramount.

For a company or organization, it can be said that data is the most valuable asset, data is something that contains sensitive information that can be related to: current employees and their partners or relatives of surname; shareholders, business partners and customers; customers and other members of the public. So once data is lost, there is a high risk that the company or organization can be threatened or lead to collapse, because attackers like hackers,

extortionists take advantage of this loophole to have the ability. would threaten the safety of the organization. In addition, sensitive information of customers is also threatened, they may have information stolen such as full name, phone number, address, credit card account number, ...

P7 Design and implement a security policy for an organization.

1. Define and discuss what is security policy

The phrase "privacy policy" may not be too unfamiliar to many people in the IT field, but if few people really know the details of what it means, then I will define and explain it.

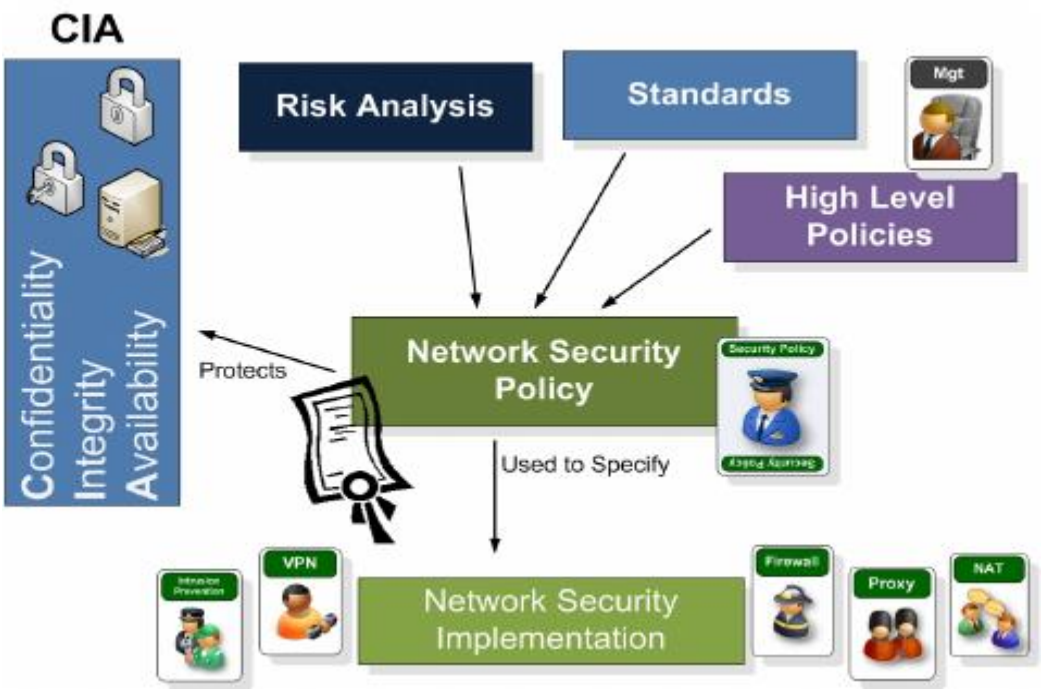

Figure 9:Network security policy (Richard J Macfarlane, 2011)

+ The Information Technology (IT) Security Policy defines the rules and procedures by which individuals can access and use an organization's IT resources and resources. An effective IT security policy is the organization's culture, in which rules and procedures are driven by the employee's approach to information and work. Therefore, an effective IT security policy is a single document for each organization, built on people's perspectives on risk tolerance, how they see and value their information. . as well as the availability with which they maintain that information. For this reason, many companies will find inadequate pre-written IT security

policies due to a lack of consideration about how people in the organization actually use and share information between them and with the public.

+ The goals of the IT security policy are to maintain the confidentiality, integrity, and availability of the systems and information used by members of the organization. These three principles make up the CIA trilogy:

- **Confidentiality** is related to the protection of assets from unauthorized entities
- **Integrity** ensures content modification is handled in a specific and authorized manner
- **Availability** is a state of the system in which authorized users have continuous access to said content.

2. Give examples of policies

Here I will give a typical example to illustrate the "information security policy", this example is the customer information protection policy of TP Bank.

+ TP Bank's security principles:

- Only ask customers to provide information relating to their financial needs and transactions between the customer and the bank.
- Using customers' personal information to deliver better service and product quality.
- Do not disclose personal information to outside organizations unless agreed by the customer or required by law.
- Customer information is kept accurately and updated.
- Use a tight security system to prevent unauthorized people from accessing customers' information, including bank employees.
- Individuals or third parties with access to personal customer information are explicitly required to comply with the confidentiality obligation set by the bank.

+ TP Bank’s data security:

- Client: In the process of providing information, customers can be assured that 256-bit Secure Socket Layer (SSL) encryption technology will protect information during transmission over the Internet.
- Servers: TP Bank's servers are protected by a “firewall” and the “intrusion detection and prevention (IDS / IPS)” system is continuously monitored by administrators to prevent any unauthorized or suspicious access. The client's password is encrypted one-way, so even the server administrator cannot know the client's password.
- When having security problems, customers need to immediately contact the Bank, to avoid fraudsters taking advantage of loopholes.

+ TP Bank's accounts security:

- All customers' account information that interacts with the TP Bank system is through receiving and sending email. Therefore, to ensure their personal information, customers need to keep their email information confidential.
- Do not write your account information anywhere, but keep in mind.
- Customers must pay attention to log out of TP Bank's online banking service by clicking the "Exit" button in the right corner of the screen, and do not turn off the browser.
- TP Bank will never ask customers for an account password to ensure that only the customer knows the password. Do not choose easy-to-guess numbers such as birthdays, phone numbers or part of your name as a password. If the customer thinks that the account information or secret code has been disclosed to a third party, is lost or stolen, and from there may arise a transaction not conducted by the customer himself, the customer is responsible for informing TP Bank immediately.
- Both banks and customers play an important role in combating fraud. It is the responsibility of the customer not to intentionally or unintentionally disclose his account information to others.

3. Give the most & should that must exist while creating policy. (Cindy NG, 2020)

There are a lot of important factors around creating a perfect security procedure, but here I will mention only the two most important requirements: what to have and what to have in the process creation a policy.

+ Security policy must:

- **Be implementable and enforceable:** Implementable means we do a feasibility study, put all policy-related elements into analysis including economic, technical, legal, and planning aspects to define. the potential for success of the policy when it is applied. And enforceable is the guarantee that after the policy is finalized, it will be applied and strictly followed in security.

- **Be concise and easy to understand:** This requires the policy to be created in a concise manner but still fully covers all policy requirements and provisions. In addition, the policy must not use too complicated words, or too high, confusing expressions, misunderstanding for the reader.

- **Balance protection with productivity:** This is a very difficult factor for policy makers, they have to find a way to balance the inherent protection of the security policy, not be compromised, and pay close attention to the issue of maintaining or even boost current productivity. Can't let overprotection cause productivity to decline, nor can it be too eager for productivity to loosen protection.

+ Security policy should:

- **State the reason why the policy is necessary:** Faced with so many security threats today, only a small gap in protecting the system will immediately cause an entire information system to be compromised, stolen or even destroyed. enjoy, huge damage. So having a strong security system against them, we also have a policy to keep that security stable.

- **Describe what is covered by the policy**

  * Who will be the owner of this privacy policy?

  * Who is my audience for this policy?

  * Which regulations apply to your industry (eg GLBA, HIPAA, Sarbanes-Oxley ...)?

  * Who needs access to your organization's data?

  * Who owns the data you manage? Your organization? Your customer?

  * How many requests are received per week to provide access to data?

  * How are these requests fulfilled?

  * How and when is access considered?

  * How can you ensure that no containers are open to a global access group (People, Domain Users, Authenticated Users ...) without explicit permission from (s) appropriate data owner and management?

  * How will all access authorization activity be recorded and made available for inspection?

  * If data is not accessed for 18 months, how will it be determined and restricted so that only the new data owner (s) have access until another individual requests access?

  * How will you tailor your privacy policy to the organization's business goals?

- **Outline how violations will be handled:** Anyone in the organization can violate the security policy, for example data managers may abuse their power to disclose important information to the outside. To deal with security breaches, strong detection controls must be in place and widely communicated to ensure that everyone knows they are being tracked and that policies are violated. security will have serious consequences. That said, detecting security breaches can be a tough job and sometimes impossible as the offenders can be highly technical, who can remove their tracks later. when they reach their goal.

4. **Explain and write down the element of security policy** (Laura Taylor, 2021)

A strong security policy is created to ensure the following elements are included:

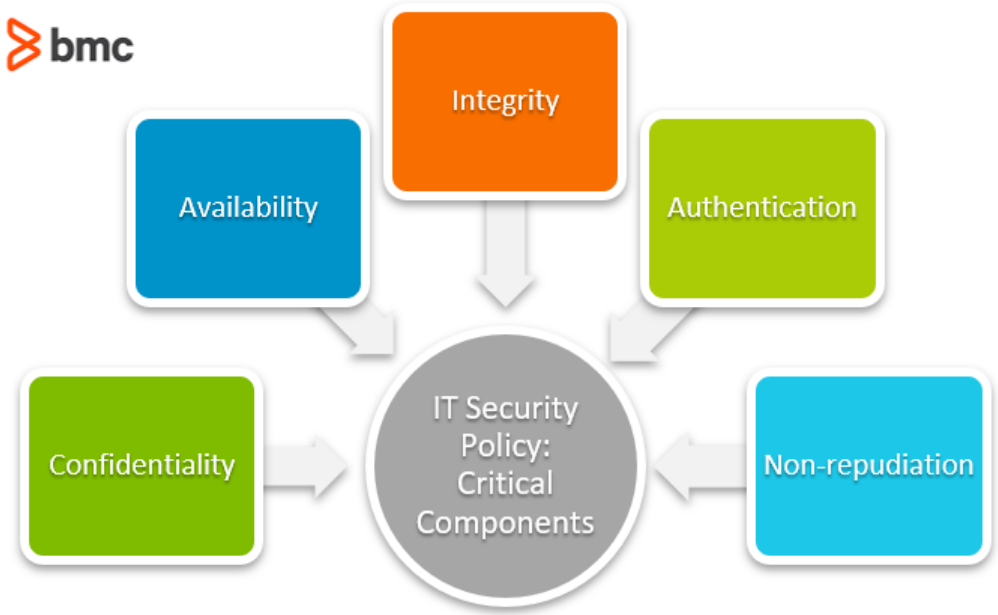

Figure 10: Components of security policy (Joseph Mathenge, 2021)

- **Purpose**: Create a holistic approach to information security. Detect and prevent information security breaches such as misuse of network, data, applications and computer systems. Maintain the organization's reputation and uphold ethical and legal responsibility. Respect customer rights, including how to respond to inquiries and complaints about noncompliance.
- **Security Accountability**: Stipulates the role and responsibility of the security of the general user, primary employee, and management. This section should also define different data classes, such as internal, external, public, and secret. By categorizing the data, you can make rules about what types of employees are responsible and allowed to modify or distribute, specific data classes.
- **Network service policy:** Create policies for secure remote access, manage and configure IP addresses, routers and switches security procedures, and access list (ACLs) regulations.). Identify which key officers need to review which change procedures before they are implemented.
- **System Policy**: Defines the server security configuration for all critical operating systems and servers. Includes which network services to run on, account management policies, password management policies, messaging, databases, antivirus, server-based intrusion detection, and wall policy fire.

- **Physical security**: Defines how buildings and card readers need to be secured, where internal cameras are installed, how visitors are handled, and inventory rules and regulations that receivers and operators Your transfer is subject to.
- **Troubleshooting and response to incidents**: Specify the procedures to be followed in the event of a security breach or incident. Include policies such as how to evaluate a security incident, how to report it, how to resolve it, and which key personnel your organization should be involved in in the process.
- **Acceptable use and behavior policies**: Stipulate what kind of behavior is expected of your employees and management team and forms and documents to be read, reviewed, filled out, and followed according to the. Employees must be asked to read and sign an acceptable use policy to give management the option to take disciplinary action in the event that the policy is violated.
- **Security training**: Define a security training plan for key employees who manage daily security operations to maintain your privacy policy and keep your security staff up to date. latest technique.

5. Give the steps to design a policy:

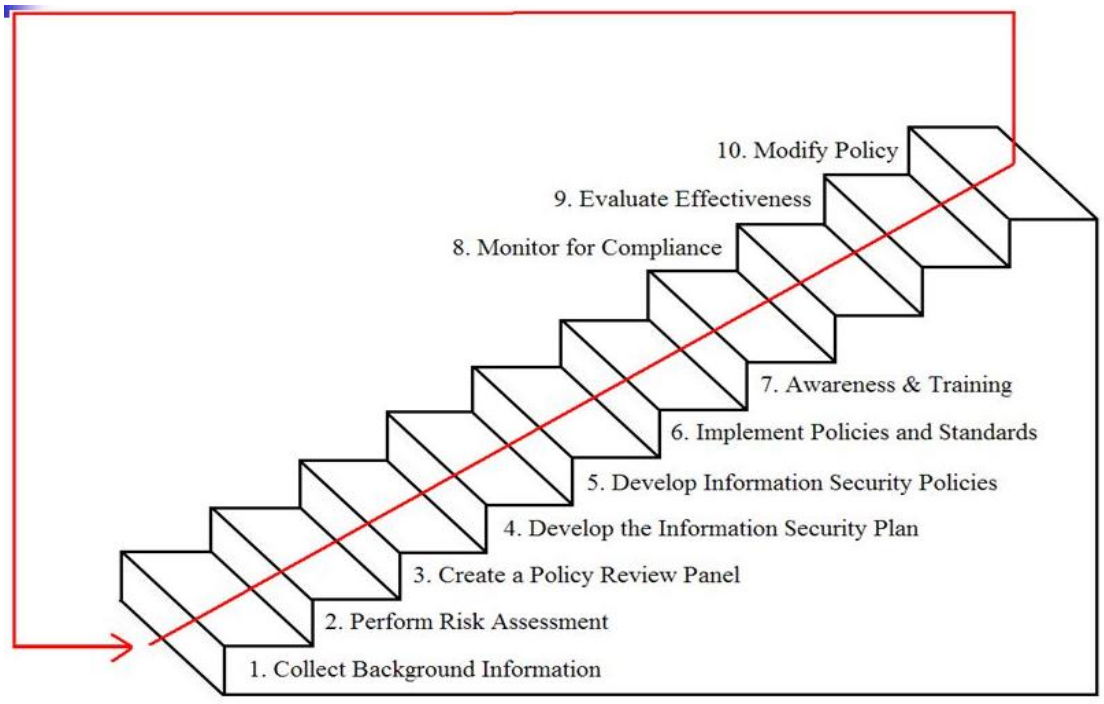

Figure 11: Steps to design a policy (Information Security Policies and Standards - ppt video online download, 2021)

Here I will go into detailing and explaining each step in creating a privacy policy

- **Step 1: Identify your risks:** What are your risks from inappropriate use? Do you have information that should be restricted? Do you send or receive a lot of large attachments and files? Are potentially offensive attachments making the rounds? It might be a nonissue. Or it could be costing you thousands of dollars per month in lost employee productivity or computer downtime. A good way to identify your risk can be through the use of monitoring or reporting tools. In addition, it must be ensured that employees record all activities for the purpose of risk assessment, and completely free from any unauthorized infringements.

- **Step 2: Learn from others:** There are many types of privacy policies, so it's important to see what other organizations like yours are doing.

- **Step 3: Ensuring compliance with legal requirements**: Depending on your data holdings, jurisdiction, and location, you may be required to adhere to certain minimum standards to ensure privacy. privacy and integrity of your data, especially if your company holds personal information.

- **Step 4: Level of security = level of risk**: Too much security can be as bad as too little. Excessive security can be a hindrance to smooth business operations, so make sure you don't overprotect yourself.

- **Step 5: Include staff in policy development**: Keep staff informed as the rules are developed and tools are implemented. If people understand the need for a responsible security policy, they will be much more inclined to comply.

- **Step 6: Train your employees**: In practice, it's probably one of the most useful phases. It not only helps you to inform employees and help them understand the policies, but it also allows you to discuss the practical, real-world implications of the policy.

- **Step 7: Get it in writing**: Make sure every member of your staff has read, signed and understood the policy. All new hires should sign the policy when they are brought on board

and should be required to reread and reconfirm their understanding of the policy at least annually.

- **Step 8: Set clear penalties and enforce them**: Network security is no joke. Your security policy isn't a set of voluntary guidelines but a condition of employment. Have a clear set of procedures in place that spell out the penalties for breaches in the security policy. Then enforce them.

- **Step 9: Keep your employees up to date:** The privacy policy is a dynamic document because the network itself is evolving. Therefore, it is necessary to update staff to accommodate these changes.

- **Step 10: Install the tools you need**: The investment in tools to enforce your security policy is probably one of the most cost-effective purchases you will ever make.

P8 List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion.

1. Discuss with explanation about business continuity

+ Business continuity can be defined as 'processes, procedures, decisions and operations to ensure that an organization can continue to operate through operational disruption'. In other words, it's about coming up with proactive and reactive plans to help your organization avoid crises and disasters and can quickly get back to 'business as usual' if they happen. .

+ Business continuity involves two distinct areas:

- Business continuity planning - in which a plan is developed, when implemented, helps prevent operational disruptions, crises, and disasters from occurring and will help the organization quickly get back into shape. 'business as usual' status if any of these events occur. Once prepared, the business continuity plan must be reviewed and implemented to ensure that it will work as expected.

- Manage business continuity - these are:

  * Continuous management of business plans to ensure that they are always up to date and available; and

* Continuous management of process resilience and process readiness within an organization, with the aim of ensuring that the organization experiences minimal possible daily disruptions.

Figure 12 :Business continuity (Richard Long, 2017)

2. List the components of recovery plan.

+ Documentation: The disaster recovery document should list all the critical components of your IT infrastructure - both hardware and software, a responsible team, as well as a series of measures that should be taken. is done to continue in business. Documentation must be up to date and up to date to comply with all changes taking place in your IT infrastructure.

+ Scope and dependencies: Your recovery scope doesn't necessarily include the entire IT infrastructure, as not all components are equally important to ensure business continuity. Identify the most important virtual machines and bring them into your recovery scope to achieve shorter recovery time goals. Also consider the dependency links between these virtual machines, applications, and IT systems.

+ Responsible Teams & Staff Training: Your disaster recovery plan should clearly identify key roles and those responsible for coordinating disaster recovery activities. Communicate the plan to all your staff and make sure everyone understands who is responsible for what eliminates the risk of confusion, redundancy and delays in the recovery process. In the event of a disaster, your staff should know who to contact or where to start in order to promptly initiate the recovery process.

+ Configure a sub-location: A sub-location is your guarantee that you have hardware and software resources, as well as tools for recovery. Make sure that your DR site is not in the same location as your primary production site to avoid the DR site being knocked off offline by the same disaster.

3. List of steps required in recovery process

- **Step 1. Create your disaster recovery contingency planning team**: consider choosing people who can bring a variety of perspectives on the company's vulnerabilities to the table. Make sure you include representatives from all the main departments within your business, including HR, facilities and high-level managers.

- **Step 2. List all names and contact details**: Next, create a list of all employees' names with all methods of communication for each one, ensuring that this is regularly updated. You may need to access this info quickly, so it needs to be accurate. Communication should include personal and work contact details.

- **Step 3. Determine a chain of command**: A system disaster is a high stress event. This means that a clear chain of command and authority needs to be put in place well in advance to determine who's in charge if and when any key personnel are missing. During a critical incident, this will help your whole team understand who's in charge in the chaos that may ensue after a disaster has taken place.

- **Step 4. Consider your risk assessment**: review as many potential disaster scenarios as you can, and create a checklist of things that might possibly go wrong. Then consider how each one of those situations would affect your core business, your revenue streams, your customer service and your employees.
- **Step 5. Do you have a 'Plan B'?** : Your 'Plan B' planning is when you think about what'll happen if your primary disaster recovery plan is not actionable.

- **Step 6. Protect your company data**: Data loss can have a huge impact on your business. Data protection and recovery is a key aspect of all disaster recovery planning, so getting on top of them will result in good business continuity.

- **Step 7. Test, test and test again!** I suggest that you run a regular testing drill to make sure your new disaster recovery plan actually works. And scheduling regular recovery simulations ensures that your systems are up and running before the CEO – and your customers – even notice!

Figure 13: Steps recovery process (Services, 2021)

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

4.1. Some policies that are required for business continuity

+ Governing Policy: The purpose of this policy is to plan for, respond to and manage critical servers that may disrupt the Critical Functions of an organization. The Business Continuity - Governing Policy and Business Continuity Management Plan are part of the organization's broader protection, resilience, and Sustainability system. The purpose of this suite of documents is to identify and respond to critical to, mitigate the loss of organization assets and operations, protect the organization's reputation, reduce the

impact on the University's people, the community, and the environment and return to business-as -usual as soon as practical.

+ Emergence management policy: it is aimed at preventing emergencies from occurring, and if not, will initiate an effective plan of action to minimize the outcome and impact of any emergency. The development of emergency plans is a cyclical process, common to many areas of risk management such as business continuity and security risk management: Risk identification or identification, rating or assessing risks, dealing with significant risks, controlling and planning resources, planning responses, reporting and monitoring risk performance, reviewing the risk management framework.

4.2. Some procedures that required for business continuity

+ Physical security procedure:

- **Step 1. Access Control:** Controlling access to work areas is one way to keep your business safe. Establish a key distribution process, including who gets the keys and how you track the keys when employees leave the company.
- **Step 2. Setting up a security system**: Regular use of a security system protects the physical safety of your employees and company property. Choose a security system that is monitored by an outside company so that emergency personnel are automatically notified if an emergency occurs at the business.
- **Step 3. Monitoring**: Physical tracking of what happens in and around your small business helps you notice suspicious behavior before it becomes an issue. Practice the habit of commuting frequently to observe the workplace. Remind staff to always be on the lookout while at work and when coming and going.
- **Step 4: Communication system setup**: Set up emergency communication and response policies. Describe how employees react to threats such as intruders, attackers, or suspicious behavior.

+ Emergency procedure:

- Step 1. Contact your property manager: talk to your property manager about emergency and disaster preparedness.

- Step 2. Install alarm systems: security alarms, fire alarms, even carbon monoxide detectors should be set up.
- Step 3: Purchase and maintain emergency equipment: protective gear, fire extinguishers, defibrillators and first-aid kits.
- Step 4. Specify the assembly areas: In some emergencies, such as an industrial accident, a fire or a situation where an attacker is in operation, everyone in the company needs to be on the safe side. Canopy and move to that shelter.
- Step 5. Establish a chain of command: designate and train staff who are normally in the office during standard business hours to act as commanders who take steps to ensure compliance in stuations emergency.
- Step 6. Set up procedures: Many people panic when faced with an emergency because they simply don't know what to do. By setting up procedures and making sure employees understand them, you can protect your workers if the impossible happens ..

Conclusion:

In summary, this report covers most of the basics of cybersecurity, in part1, I have clarified the following: the security risks faced by the company, how to apply the regulations. ISO for IT security and standard management risk data protection, the museum of activity where a confidential IT assessment can have against an organization's security, staff accountability and related organizations security. Followed by part 2, in this section covers: design, implementation of policy security, and explanation by including elements in a disaster plan for Wheelie. Finally part 3, outside of my policy security, I have evaluated the recommended tools to be used in the policy and how they fit into the IT security. This part is includes sections on how to manage and implement policies.

Evaluation

As far as I have done in this report, I think this report covers most of the basics that newcomers in the field need to know about cybersecurity. I haven't been able to meet all the requirements of this report, I am happy to stop at completing the tasks of the Pass section, the remaining Merit, and Distinction I can't do because I find them outperformed. it is too much for me. Besides this, this knowledge is explored by me and based on secure websites. Reputable cryptography to reinterpret in the easiest way to understand. All information collected online I will cite the source to show respect for the authors of those resources. For each different information I bring examples and illustrations, this article makes the information clearer and easier to understand.

Reference

Btsconsultant.com. 2021. BTS Website*. [online] Available at: <https://btsconsultant.com/courseDetails/2237> [Accessed 19 April 2021].*

Nibusinessinfo.co.uk. 2021. *What is IT risk? | nibusinessinfo.co.uk*. [online] Available at: <https://www.nibusinessinfo.co.uk/content/what-it-risk> [Accessed 19 April 2021].

Ozassignments.com. 2021. *ITC596 IT Risk Management Oz Assignments*. [online] Available at: <https://www.ozassignments.com/solution/itc596-it-risk-management-oz-assignments> [Accessed 19 April 2021].

Techopedia.com. 2021. *What is an IT Asset? - Definition from Techopedia*. [online] Available at: <https://www.techopedia.com/definition/16946/it-asset> [Accessed 19 April 2021].

Forescout. 2021. *Building a Comprehensive IT Asset Management Strategy - Forescout*. [online] Available at: <https://www.forescout.com/company/blog/building-a-comprehensive-it-asset-management-strategy/> [Accessed 19 April 2021].

BMC Blogs. 2021. *IT Security Vulnerability vs Threat vs Risk: What are the Differences?*. [online] Available at: <https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/> [Accessed 19 April 2021].

Pinterest. 2021. *Pin on Flat style | Vector Graphics, Symbols, Illustrations, Icons, Design Elements, Logos & Clipart.*. [online] Available at: <https://www.pinterest.com/pin/515240013597716234/> [Accessed 19 April 2021].

Zeepedia.com. 2021. *Threat Identification:Types of Threats Control Analysis Impact analysis Occurrence of threat Information Systems Computer Science*. [online] Available at: <https://www.zeepedia.com/read.php?threat_identification_types_of_threats_control_analysis_impact_analysis_occurrence_of_threat_information_systems&b=14&c=30> [Accessed 19 April 2021].

Compliance, S. and Assessment, H., 2021. *How to Perform IT Risk Assessment*. [online] Blog.netwrix.com. Available at: <https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/> [Accessed 19 April 2021].

Facilities Management Advisor. 2021. *An 8-Step Risk Assessment for Your Facility's Security - Facilities Management Advisor*. [online] Available at: <https://facilitiesmanagementadvisor.blr.com/security/8-step-risk-assessment-facilitys-security/> [Accessed 20 April 2021].

Cyber-Security & Safety by Tecnalia. 2021. *TRIAL*. [online] Available at: <https://www.cyberssbytecnalia.com/node/173> [Accessed 20 April 2021].

2021. [online] Available at: <https://www.researchgate.net/figure/Network-Security-Policy_fig1_228941015> [Accessed 21 April 2021].

Inside Out Security. 2021. *How to Create a Good Security Policy*. [online] Available at: <https://www.varonis.com/blog/how-to-create-a-good-security-policy/> [Accessed 21 April 2021].

Taylor, L., 2021. *Seven elements of highly effective security policies | ZDNet*. [online] ZDNet. Available at: <https://www.zdnet.com/article/seven-elements-of-highly-effective-security-policies/> [Accessed 21 April 2021].

BMC Blogs. 2021. *IT Security Policy: Key Components & Best Practices for Every Business*. [online] Available at: <https://www.bmc.com/blogs/it-security-policy/> [Accessed 21 April 2021].

CGE Risk. 2021. *ISO 31000 Blog Series – A complete guide through the risk management standard using the CGE software portfolio - CGE Risk*. [online] Available at: <https://www.cgerisk.com/2019/03/iso-31000-blog-series-a-complete-guide-through-the-risk-management-standard-using-the-cge-software-portfolio/> [Accessed 21 April 2021].

ICT Institute. 2021. *ISO 31000 in relation to ISO 27001 - ICT Institute*. [online] Available at: <https://ictinstitute.nl/iso-31000-explained/> [Accessed 21 April 2021].

indiamart.com. 2021. *Cyber Security Audits*. [online] Available at: <https://www.indiamart.com/proddetail/cyber-security-audits-21267436888.html> [Accessed 21 April 2021].

Ribeiro, M., 2021. *Benifit of IT audit, IT computer network cyber security assessment*. [online] VBS IT Services Inc. Available at: <https://www.vbsitservices.com/2015/07/the-benefits-of-an-it-audit-for-your-business/> [Accessed 21 April 2021].

MHA Consulting. 2021. *What is Business Continuity? - Business Continuity 101*. [online] Available at: <https://www.mha-it.com/2017/08/01/what-is-business-continuity/> [Accessed 21 April 2021].

Services, D., 2021. *Data Recovery Process - Data Recovery Ireland*. [online] Data Recovery Ireland. Available at: <https://www.datarecovery.ie/data-recovery-services/recovery-services-steps/> [Accessed 25 April 2021].