




ASSIGNMENT 2

Qualification	BTEC Level 5 HND Diploma in Computing		
Unit number and title	Unit 5: Security		
Submission date	December 17, 2021	Date Received 1st submission	
Re-submission Date		Date Received 2nd submission	
Student Name	Quach Cong Tuan	Student ID	BHAF200014
Class	PBIT17101	Assessor name	Le Van Thuan
Student declaration I certify that the assignment submission is entirely my work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.			
		Student's signature	

Grading grid

P5	P6	P7	P8	M3	M4	M5

☐ Summative Feedback:

☐ Resubmission Feedback:

Grade:

Assessor Signature:

Date:

Signature & Date:

TABLE OF CONTENTS

INTRODUCTION	7
P5. Discuss risk assessment procedures.....	8
1. Risk & risk assessment.....	8
1.1. Define Risk.....	8
1.2. Risk assessment.....	8
2. Asset, threat, and threat identification procedure.	9
3. The risk assessment procedure	10
3.1. Importance of regular IT security assessments	10
3.2. IT risk assessment components: The Four Key Component	11
4. List risk identification steps	12
P6. Explain data protection processes and regulations as applicable to an organization.....	14
1. Define data protection	14
2. The data protection process with relation to the organization.....	14
3. The importance of data protection regulation	15
Here are 7 ways I recommend protecting data:	16
P7. Design and implement a security policy for an organization.....	18
1. Define and discuss what is a security policy	18
1.1. Definition.....	18
1.2. Discuss.....	18
1.3. The important.....	18
2. Examples of policies	19
2.1. Acceptable Use Policy (AUP).....	19
2.2. Data breach response policy.....	19
2.3. Access control policy	19
3. The element of security policy.....	20
3.1. Purpose	20
3.2. Scope.....	20
3.3. Information security objectives	20
3.4. Authorization and access control policy.....	21
3.5. Classification of data.....	21
3.6. Data support and operations	21
3.7. Security awareness sessions	22
3.8. Responsibilities, rights, and duties of personnel	22

3.9. Other items that an information security policy may include	22
4. The steps to design a policy.....	23
4.1. Identify the need	23
4.2. Identify who will take lead responsibility.....	23
4.3. Gather information.....	23
4.4. Draft policy	23
4.5. Consult with appropriate stakeholders.....	23
4.6. Policy finalization/approval	24
4.7. Consider whether procedures are required.....	24
4.8. Implementation.....	24
4.9. Monitor, review, modify.....	24
5. Design and implement a security policy for the organization	25
P8. The main components of an organizational disaster recovery plan, justifying the reasons for inclusion.	28
1. Business Continuity	28
2. The components of the recovery plan.	28
2.1. The scope of your plan	28
2.2. Organizational roles and responsibilities	28
2.3. Your critical business functions and the tolerance for downtime	29
2.4. The strategies, processes, and procedures to resume your critical business functions.....	29
2.5. A communication plans	30
2.6. Schedule for Testing, Reviewing & Improving.....	30
3. The steps required in the disaster recovery process.....	31
4. The policies and procedures that are required for business continuity.	32
4.1. Define.....	32
4.2. Purpose	32
4.3. Important	32
M3. Summaries the ISO 31000 risk management methodology and its application in IT security.....	34
1. Define.....	34
2. Introduction to ISO	34
3. Management System Standard	34
4. Benefit of ISO 31000.....	35
5. Process of ISO 31000.....	36
6. Framework of ISO 31000.....	37

6.1. Leadership and commitment.....	37
6.2. Integration.....	37
6.3. Design.....	38
6.4. Implementation.....	38
6.5. Evaluation.....	38
6.6. Improvement.....	38
M4. Discuss possible impacts to organizational security resulting from an IT security audit.....	40
1. Define IT Security Audit.....	40
2. Benefits Of Security Audits.....	40
3. Type of IT Security Audit.....	41
4. Importance of an IT Security Audit.....	41
5. Conduct an IT Security Audit.....	42
M5. Discuss the roles of stakeholders in the organization to implement security audit recommendations	43
1. Definition Stakeholder.....	43
2. The Role of a Stakeholder.....	43
3. The Main Types of Stakeholders.....	43
4. Stakeholders of North Star.....	44
5. Discuss.....	45
CONCLUSIONS	46
References.....	47

TABLE OF FIGURES

Figure 1 Business Continuity Procedure 1	33
Figure 2 Business Continuity Procedure 2	33
Figure 3 Conduct an IT Security Audit	42

INTRODUCTION

In this assignment 2, I was assigned to NorthStar Secure Company as a Trainee Security Specialist and Head of Security. I'll have to create a presentation to train new employees in tools and procedures that enable research and defense against information security threats in conjunction with the organization's business-critical data and device protection activities.

In this 2nd mission, I will continue to take on the role of a security specialist working at North Star. I will clarify the issues in the following section.

P5. Discuss risk assessment procedures.

1. Risk & risk assessment.

1.1. Define Risk

Risk in cybersecurity refers to the probability of property or data loss, damage, or destruction. A threat is a bad event, such as a security flaw being exploited. A vulnerability, on the other hand, is a flaw that exposes you to threats, increasing the possibility of a negative outcome.

When a danger exploits a vulnerability, the risk is defined as the possibility of loss or damage. Risk can also be calculated using the formula: **Risk = Threat x Vulnerability.**

1.2. Risk assessment

A security risk assessment is an assessment that involves the identification of risks. Processes need to be specifically verified with control measures and protection from security threats. The standards in the security risk assessment are all evaluated according to the PCI-DSS (payment card security) standards. For services, the required risk assessment standard for compliance with ISO 270001, HIPAA, or HITRUST CSF.

A Security Risk Assessment is a thorough examination of anything that could jeopardize the company's security or compliance. Each assessment is custom-made to meet the client's particular needs and scope. Any of the following aspects can be included in an assessment:

- Infrastructure
- Network
- Information Security
- Servers & Systems
- Application Scanning
- Policies

2. Asset, threat, and threat identification procedure.

With the threats and possible risks of network security, the risk of information loss, data can be stolen by hackers. They can steal data, threaten, blackmail with that information. Threats, potential risks, and threats to network security were covered by me in exercise 1. In this P5 section, I will cover security risk assessments in more depth.

To assess and identify security risks we need to identify the factors and requirements for a comprehensive North Star security detail assessment:

- Identify content such as North Star networks, servers, applications, data centers.
- Create a risk assessment profile for each asset.
- Measure the rating/riskiness of assets and prioritize them for detailed assessments.
- Apply mitigation controls to the content based on the results of the assessment.
- Scan and check the entire system for vulnerabilities, this will help us to manage and detect security holes, viruses, or malicious software.
- Check for system intrusion or external influences. System intrusion control will help us assess the potential threat to North Star's systems. Based on those results and make judgments with severity levels or not.
- Security risk is not a one-time security project; it is an ongoing activity that should be conducted at least once per year. The assessment will help identify and update the threats and risks North Star may face.

3. The risk assessment procedure

3.1. Importance of regular IT security assessments

Conducting a thorough IT security assessment regularly helps North Star develop a solid foundation for ensuring business success. In particular, it enables them to:

- Identify and remediate IT security gaps
- Prevent data breaches
- Choose appropriate protocols and controls to mitigate risks
- Prioritize the protection of the asset with the highest value and highest risk
- Eliminate unnecessary or obsolete control measures
- Evaluate potential security partners
- Establish, maintain and prove compliance with regulations
- Accurately forecast future needs

3.2. IT risk assessment components: The Four Key Component

There are four main components to an IT risk assessment. We'll go into how to evaluate each one later, but first, here's a quick rundown:

1. Threat — Any incident that has the potential to harm an organization's employees or assets is considered a danger. Natural disasters, website outages, and corporate espionage are all examples.
2. Vulnerability — Any potential weak point that could allow a threat to harm is referred to as a vulnerability. Obsolete antivirus software, for example, is a weakness that can allow a malware assault to succeed. Having a server room in the basement is a vulnerability that raises the risks of equipment being ruined and downtime being caused by a hurricane or flood. Disgruntled personnel and aged hardware are two further examples of vulnerability. The National Vulnerability Database (NVD) of the National Institute of Standards and Technology (NIST) keeps track of specific code-based flaws.
3. Impact — The complete damage an organization would suffer if a vulnerability was exploited by a threat is referred to as the impact. A successful ransomware assault, for example, could result not only in missed productivity and data recovery costs, but also in the revealing of customer data or trade secrets, which could result in lost business, legal bills, and compliance penalties.
4. Likelihood — This is the likelihood of a threat occurring. It is usually a range rather than a specific number.

(Sotnikov, 2018)

4. List risk identification steps

There are 9 steps to a security risk assessment. As detailed below, here are the steps North Star should use to get the most accurate risk assessment and control:

- **Step 1: Inventory and Prioritize Assets:** Provide the content that needs to be identified such as data, software, equipment, ... and evaluate the importance to prioritize protection with levels.
- **Step 2: Identify Threats:** identify threats to the North Star organization. While hackers are intending to attack/infiltrate our system. Below is my classification of possible threat types in the event of hardware failure, natural disaster, malicious behavior, and more. We need to know carefully and properly to take preventive measures.
- **Step 3: Identify Vulnerabilities:** A vulnerability is a flaw in your system that could put your company at risk. Analysis, audit reports, NIST vulnerability databases, vendor data, information security assessment, and testing (ST&E) methods, and testing can all help identify vulnerabilities. Tools for penetration testing and automated vulnerability scanning.
- **Step 4: Analyze Controls:** Analyze the measures in place or in the planning stages to reduce or eliminate the likelihood of a threat exploiting a vulnerability. Encryption, intrusion detection mechanisms, and identity and authentication solutions are examples of technical controls. Security policies, administrative measures, and physical and environmental processes are examples of non-technical controls.
- **Step 5: Determine the Likelihood of an Incident:** Assess the probability that a vulnerability might be exploited, taking into account the type of vulnerability, the capability and motivation of the threat source, and the existence and effectiveness of your controls. Rather than a numerical score, many organizations use the categories high, medium, and low to assess the likelihood of an attack or other adverse event.
- **Step 6: Assess the Impact a Threat Could Have:** Examine the impact of an occurrence on property that has been lost or damaged, including the following:
 - The asset's purpose and any processes that rely on it.
 - North Star's property is worth a lot of money.
 - The property's sensitivity.
- **Step 7: Prioritize the Information Security Risks:** Determine the level of risk to the IT system for each threat/vulnerability pair using the following criteria:

- The likelihood that the threat will take advantage of the flaw.
 - Each of these incidences' estimated cost.
 - The effectiveness of existing or planned information system security controls in reducing or eliminating risk.
- **Step 8: Recommend Controls:** Determine the activities required to lower the risk using the amount of risk as a baseline. For each level of risk, below are some broad guidelines: High, Medium, and Low are the three levels of difficulty.
 - **Step 9: Document the Results:** Create risk assessment reports to aid management in making informed decisions about budgets, policies, and procedures, among other things. Each danger must be described in detail in the report, including the vulnerabilities, assets at risk, impact on North Star's IT infrastructure, likelihood of occurrence, and proposed controls.

(Sotnikov, 2018)

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

1. Define data protection

Data security and data protection are inextricably connected. The process of safeguarding data so that only authorized personnel can access or modify it is known as data security. When it comes to securing your data against physical theft, cyber-attacks, and theft by employees/trusted persons, this is usually the case. "Legitimate control over the access and use of data" is how data protection is defined. Data protection, on the other hand, has a considerably greater scope.

Data security is achieved by a mix of administrative and technical safeguards. Legal aspects are included in administrative measures (privacy policies, terms, and conditions, etc.). The legal basis for processing a subject's data is one of the most significant parts of GDPR. The premise in many circumstances will be "informed permission," which can be revoked at any time. (Stevovic, 2019)

2. The data protection process with relation to the organization

Data Protection's major goal is to safeguard people from having their personal information exploited or mismanaged. This is accomplished in two ways under the Data Protection:

- Individual rights are established as a result of this.
- By establishing obligations for corporations, organizations, and the government, as well as norms for how they use and preserve "personal data," we can make the world a better place.

Personal data is information that identifies or is 'clearly about' a specific individual; anonymous or aggregated data is not covered by the Data Protection Act.

3. The importance of data protection regulation

The value of data is increasing all the time. Furthermore, abilities and chances for obtaining various sorts of personal data are continuously evolving. Unauthorized, careless, or uneducated processing of personal data can be extremely harmful to both individuals and businesses.

- The First, the goal of personal data protection is to safeguard not just a person's data, but also the fundamental rights and freedoms of those who are connected to that data. By safeguarding personal data, it is possible to ensure that people's rights and freedoms are not violated.
- The Second, failing to comply with personal data protection standards can lead to far more serious consequences, such as the theft of all funds from a person's bank account or even the creation of a life-threatening situation by tampering with health information.
- The Third, data protection regulations are required to enable and promote fair and consumer-friendly trade and service offerings. Personal data protection legislation creates a system in which personal data, for example, cannot be freely sold, giving people more control over who makes them offers and what kind of offers they receive.

It's critical to understand what data is being handled to ensure that personal data is protected. It's also crucial to figure out what safety and security measures are in place. All of this is achievable thanks to a complete data protection audit, which determines data flow and compliance with data protection standards. The audit can be completed by answering a set of questions that have been designed specifically for that purpose.

Here are 7 ways I recommend protecting data:

1. Update To the Latest Version

When problems and vulnerabilities are uncovered, software companies frequently provide updates to fix them. So, especially with operating systems, don't put off software upgrades. Software that has been outdated for a long time may still contain security holes that expose you to a data or privacy violation.

2. Protect Passwords

Creating strong passwords and never using the same password across sites or devices is one of the best things you can do to protect yourself from digital invasion. Download apps such as Microsoft Authentication or Google Authentication to protect your OTP Code. Always set up 2FA/MFA to protect data.

3. Disable Lock-Screen Notifications

Turning off lock-screen app notifications on your smartphone is a quick and easy way to keep personal information off of your lock screen. To keep text messages and social network notifications out of prying eyes, turn off app notifications.

4. Lock Your Apps

After you've secured your phone, go a step further and secure your apps. App lockers are similar to the lock-screen functionality in that they add an extra layer of security to your apps. The contents of your apps stay protected behind a passcode if someone else uses your phone or if it is stolen.

5. Keep Your Browsing to Yourself

Use a Virtual Private Network (VPN) if you use free WIFI hotspots in public places to protect your personal information from others who may be using the same unprotected public network. The VPN will encrypt all data arriving to or leaving your computer or phone, as well as disguise your location, in addition to safeguarding your surfing information.

6. Encrypt Your Data

Encryption scrambles your data so that no one without a key can decipher what it says. It's not just useful for safeguarding data on your computer, but also for ensuring that your phone's text messages and emails aren't intercepted. Signal and WhatsApp, both free and easy-to-use apps for iPhone and Android, are two examples. On your computer, productivity software like Microsoft Office and Adobe

Acrobat let you set passwords for specific documents and choose the type of encryption to use. You can encrypt files, folders, removable USB devices, flash drives, and more using Encrypting File System (EFS) and disk encryption tools.

7. Back-Up Data

If something happens to the data you create on your devices or network, or if you lose it altogether, if it's backed up, you can restore it quickly and easily. Backups protect your images, documents, and other data against not only technical failure but also ransomware and other harmful hacking. For the best data safety, back up your files to an internet service, an external hard drive, or both.

P7. Design and implement a security policy for an organization.

1. Define and discuss what is a security policy

1.1. Definition

A security policy may be a composed report in an organization that diagrams how to guard the organization against threats, such as computer security dangers, and how to bargain with issues when they emerge. All of a company's resources, as well as all potential dangers to those resources, must be recorded in a security approach.

1.2. Discuss

With the 4.0 era, technology is developing, having a lot of potential risks and risks that can lead to things like hacking and stealing data from the system will expose us to a lot of risks and face many dangers to our company. Creating policies is one of the most important things in every business, with North Star, the need for security policies will prevent a lot of risks from outside agents. This is also considered as a firewall to help us prevent risks and threats from the outside.

1.3. The important

Every organization, regardless of its size or industry, requires established IT Security Policies to help protect its data and other critical assets. It is a requirement for businesses that must adhere to numerous legislation and standards, including GDPR and ISO.

The most important thing is to have "documented" security policies that identify my company's security position. In the event of a data breach, this can be extremely important.

2. Examples of policies

Example with our company North Star:

The company has issued policies for departments to prevent access from devices within the company to the domains Facebook.com, Youtube.com, to prevent employees from playing in now or there are threats to the company's systems.

With access control and authorization policies for employees. North Star employees will be briefed on the company's privacy policies.

I will apply 3 common policies for North Star employees:

2.1. Acceptable Use Policy (AUP)

Each North Star employee will be assigned a company email and ID. Only North Star IDs and emails can use North Star IT systems including WIFI. This will be set up and access permissions for the user.

2.2. Data breach response policy

The goal of the data breach response policy is to describe the process of handling an incident and remediating the impact on the business operations of North Star and its customers. This policy typically defines staff roles and responsibilities in handling an incident, standards and metrics, incident reporting, remediation efforts, and feedback mechanisms.

2.3. Access control policy

An access control policy (ACP) defines standards for user access rights, network access control, and system software control. Additional entries typically include techniques for monitoring how systems are accessed and used, how access is deleted when employees leave the organization, and how unattended workstations should be secured how.

3. The element of security policy

3.1. Purpose

- For a variety of reasons, North Star develops information security policies:
- To develop a comprehensive strategy for information security.
- To detect and prevent information security breaches such as data, network, computer system, and application misuse.
- To safeguard the company's reputation in terms of its ethical and legal obligations
- Customers' rights must be respected. One strategy to achieve this goal is to provide effective mechanisms for responding to complaints and inquiries about actual or apparent policy non-compliance.

3.2. Scope

An information security policy should address all data, programs, systems, facilities, other tech infrastructure, users of technology, and third parties in a given North Star, without exception.

3.3. Information security objectives

An organization that is attempting to create a working information security policy must have well-defined security and strategic objectives. Management must agree on these goals; any existing differences in this area could jeopardize the project's success.

A security expert should ensure that the information security policy is treated with the same importance as other corporate rules. When an organization has a large structure, policies may differ and must be separated to define dealings within the desired subset of the company.

Information security is defined as the protection of three primary goals:

- Data and information assets must be kept confidential and only shared with those who have been granted access.
- Integrity: Maintaining data integrity, completeness, and accuracy, as well as keeping IT systems working.
- Availability: A goal demonstrating that authorized users have access to information or a system when they need it.

3.4. Authorization and access control policy

A security policy usually follows a hierarchical structure. Junior employees are normally forced to keep the limited information they have to themselves unless they have been given explicit permission to do so. A senior manager, on the other hand, may have sufficient authority to decide what data can be shared and with whom, implying that they are not bound by the same information security policy rules. This means that the information security policy should cover every basic role in the company and include specifications for their permission.

Policy refinement occurs concurrently with the definition of administrative control or authority held by individuals inside the organization. In essence, it is a hierarchy-based delegation of control in which an individual may have power over his or her work, a project manager has authority over project files belonging to a group to which he or she has been assigned, and a system administrator has sole authority over system files.

3.5. Classification of data

Data can have a variety of values. Separation and distinct handling regimes/procedures for each kind may be imposed by gradations in the value index. As a result, an information classification system will aid in the protection of data that is critical to the company while excluding inconsequential data that might otherwise overburden the organization's resources.

The following is an example of how a data classification policy might organize the full set of data:

- High-Risk Group: Financial, payroll, and personnel (privacy requirements) data, as well as data protected by state and federal regulations (the Data Protection Act, HIPAA, FERPA), are covered here.
- Class: Confidential Although the data in this class is not legally protected, the data owner believes that it should be protected against unlawful disclosure.
- Class for the general public: This data can be freely disseminated.

Data owners should determine both the data classification and the exact measures a data custodian needs to take to preserve the integrity by that level.

3.6. Data support and operations

In this part, we could find clauses that stipulate:

- The regulation of general system mechanisms responsible for data protection
- The data backup
- Movement of data

3.7. Security awareness sessions

It's crucial to communicate IT security policies to employees. Just because they have to read and acknowledge a paper does not indicate they are familiar with and comprehend the new policies. A training session, on the other hand, would engage staff and ensure that they are aware of the data protection protocols and systems.

Sharing IT security policy with employees is an important first step. Reading and acknowledging a paper does not imply that they are familiar with and comprehend the new policies. A training session, on the other hand, would engage personnel and ensure that they understand the protocols and methods in place to protect data.

3.8. Responsibilities, rights, and duties of personnel

The responsibilities of personnel assigned to carry out the implementation, education, incident response, user access reviews, and periodic updates of an information security policy are all things to consider in this area.

Theft prevention, information know-how, and industrial secrets that could benefit competitors are just a few of the reasons why a company might wish to use an information security policy to protect its digital assets and intellectual property.

3.9. Other items that an information security policy may include

A variety of distinct items may be included in an information security policy. These include, but are not limited to, virus protection procedures, intrusion detection procedures, incident response procedures, remote work procedures, technical guidelines, audits, employee requirements, non-compliance consequences, disciplinary actions, terminated employees, IT physical security, and more.

4. The steps to design a policy

There are 9 steps to creating a privacy policy. Here are 9 steps I will use to design a privacy policy for North Star:

4.1. Identify the need

Policies can be created in the following ways:

- In advance of a necessity (e.g., child protection policies should be in place once North Star starts to work with children or young people)
- In answer to a requirement (e.g., a policy position on a government strategy may be developed in response to a consultation paper).

North Star must constantly evaluate its actions, responsibilities, and external environment to determine whether policies and procedures are required.

4.2. Identify who will take lead responsibility

According to the expertise required, assign responsibilities to an individual, a working group, a subcommittee, or staff members. (Learn more about the management committee's involvement in policymaking.)

4.3. Gather information

Learn more about the data that other firms have been dealing with. Also, do more study into the threats that North Star may face from other competitors.

4.4. Draft policy

Ensure that the wording and length or complexity of the policy are appropriate to those who will be expected to implement it.

4.5. Consult with appropriate stakeholders

Policies are most effective if those affected are consulted are supportive and have the opportunity to consider and discuss the potential implications of the policy. Depending on whether you are developing policies to govern the internal working of the North Star or external policy positions, you may wish to consult, for example:

- Supporters
- Staff and Interns

- Management Committee members

4.6. Policy finalization/approval

Members of North Star's policy creation and development committee will jointly provide input and development. The policy development manager will summarize and report. The policy will be approved upon approval by management.

4.7. Consider whether procedures are required

Procedures will be managed and opinions collected from North Star's internal department heads/departments. For each department, there will be separate policies or special privileges for them. When employees in the North Star have any policy recommendations, the manager of that department will reflect them as the policy developer.

4.8. Implementation

The policy will be published by department heads/department representatives within North Star. All staff here will have to attend 3 days of instruction with policies. In addition, on the North Star internal page, these policies will be pinned in a separate section.

4.9. Monitor, review, modify

During the policy testing phase, managers will receive requests and monitor their implementation. After the pilot period, the policies will be reviewed and revised.

5. Design and implement a security policy for the organization

Data security policy: Employee requirements

Use this policy

This policy is tailored to North Star and applies to all North Star employees. This policy will cover applicable data management requirements. This must be linked to North Star's AUP (acceptable use policy), security training, and information privacy policy to provide users with guidance on necessary North Star behaviors.

1. Purpose

To avoid damaging our brand and negatively hurting our clients, North Star must preserve restricted, confidential, or sensitive data from loss. The protection of data in scope is a vital business necessity, however, flexibility to access data and work successfully is equally critical.

This technology control is unlikely to be able to deal effectively with a malicious theft scenario or to accurately detect all data. Its main goal is to raise user awareness and prevent inadvertent loss scenarios. This policy specifies the standards for preventing data leakage, as well as the policy's focus and justification.

2. Scope

1. Any North Star employee, contractor, or individual who has access to the company's data or systems.
2. Definition of the data to be safeguarded (you should identify the types of data and give examples so that your users can identify it when they encounter it)
 - PII
 - Financial
 - Restricted/Sensitive
 - Confidential
 - IP

3. Policy – Employee requirements

1. You must take North Star's security awareness course and agree to follow the acceptable use policy.
2. If you see an unfamiliar, un-escorted, or otherwise unauthorized person in North Star, you must report them right away.
3. At all times, visitors to North Star must be escorted by authorized personnel. If you are in charge of guiding visitors, you must limit their access to certain places.
4. You must not publicly or via systems or communication channels not controlled by North Star allude to the subject or substance of sensitive or confidential data. It is not permitted, for example, to distribute data via external e-mail systems that are not hosted by North Star.
5. Please keep your workstation tidy. You must guarantee that all printed in-scope data is not left unattended at your workstation to maintain information security.
6. You need to use a secure password on all North Star systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
7. Terminated employees will be obliged to surrender all records containing personal information, regardless of format. Employees should sign documents confirming their willingness to comply with this rule as part of their onboarding process.
8. If a device containing in-scope data is lost, you must notify immediately (e.g., mobiles, laptops, etc.).
9. If you discover a system or process that you believe is not in compliance with this policy or the information security objective, you have a responsibility to notify them so that they can take immediate action.
10. If you've been given the option to work remotely, you'll need to take extra care to ensure that data is handled properly. If you're unclear about your obligations, ask for help.
11. Please make sure that assets containing data in scope aren't overly exposed, such as in the back seat of your car.
12. Only business-provided secure transfer protocols are to be used to transfer data within North Star (e.g., encrypted USB keys, file shares, email, etc.). North Star will provide you with the appropriate systems or gadgets. Other procedures must not be used to handle

in-scope data. If you have a question about the usage of a transfer mechanism or if it does not fit your business needs, you should contact them.

13. Any data transferred on a portable device (e.g., a USB stick, a laptop) must be encrypted according to industry standards.
14. Any information being transferred on a portable device (e.g., USB stick, laptop) must be encrypted in line with industry best practices and applicable laws and regulations. If there is doubt regarding the requirements, seek guidance.

4. Revision History

Version	Date of Revision	Author	Description of Changes
1.0	December 09, 2021	Quach Cong Tuan	Initial Version

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

1. Business Continuity

Business continuity (BC) refers to keeping or swiftly resuming business functions in the event of a catastrophic disruption, such as a fire, flood, or cybercriminal assault. A business continuity plan lays out the procedures and instructions that an organization must follow in the event of a crisis; it covers business processes, assets, human resources, business partners, and other topics. Business continuity refers to having a plan in place to deal with unexpected events so that your company can keep running smoothly.

2. The components of the recovery plan.

A disaster recovery plan is an important aspect of your overall business continuity plan (BCP), and its goal is to help your organization and its employees minimize the effects of a disaster and get back to business as quickly as possible. To clarify, a disaster recovery plan differs from an incident response plan (also included in your BCP), in that an IRP is designed to assist you in dealing with a crisis immediately before, during, or after it occurs, whereas a DRP is more concerned with getting your business back up and running in the long run.

To make sure your plan is set to get your business up and running, you should make sure it includes certain key elements:

2.1. The scope of your plan

There are multiple types of crises that could affect organizations and multiple dimensions of an organization that need to be protected, so as simple as it seems, the first part of your disaster recovery plan should define what scope it covers.

2.2. Organizational roles and responsibilities

For recovery to take place, your organization should have a designated disaster recovery team that is well-acquainted with the documented recovery processes and plays a specific role in the plan. Responsibilities of the recovery team should not only cover what do during and post-disaster, but also, in advance of, such as:

- Ensuring more than one person knows how to perform necessary tasks, so if something happens, there isn't the risk it won't be done properly or at all.

- Ensuring your staff knows the manual way to perform certain processes (if they exist) as software or hardware might be damaged or disrupted during a disaster and not be available.
- Training of all staff, so they are prepared for how to act and do their jobs safely in the event of a disaster. Especially if your organization operates in a high-risk environment, adequate training can significantly reduce the impact of a crisis.

The team is responsible for the consequences when there is a risk:

Location	Stakeholder
Executive management	<ul style="list-style-type: none"> Managers
IT Team	<ul style="list-style-type: none"> Manager IT Security Security Analyst
Public Relations	<ul style="list-style-type: none"> Public Relations
ICT Specialists	<ul style="list-style-type: none"> IS Professional System Administrator

2.3. Your critical business functions and the tolerance for downtime

Your critical business functions (CBFs) are the vital functions of your organization that without which it cannot operate properly or at all. In determining the strategies that will help your business recover from a disaster, you have to identify these functions as well as determine how long you can last without them before experiencing a severe loss. This is also known as your Recovery Time Objective or RTO. By outlining your CBFs and how long you can survive until they are restored, you can better prioritize the processes listed in your recovery plan.

2.4. The strategies, processes, and procedures to resume your critical business functions

Now that you have identified the functions of your business that need to be restored for your business to run, you can design your strategies accordingly.

For each critical business function, you should document the following:

- Preventative/Recovery actions that should be taken to back up or restore the CBF

- Resources/Equipment required to facilitate those actions
- Recovery time objective (So you know how you quickly actions must happen)
- Responsibility (Who is in charge of making sure the actions happen)

2.5. A communication plans

If disaster strikes, the last thing you might want to do is address your customers, employees, or other stakeholders, but effective communication is key to showing you are in control of the situation and that it will be resolved. Effective communication doesn't just mean communicating everything as soon as possible, but knowing the necessary chain of communication and reporting accurate information. This is why it's important to outline a thorough communication plan that covers these elements.

This plan should include contact lists of those who will need to be communicated to (internally and externally), a protocol for what information can be communicated, and how it should be conveyed, depending on the situation.

2.6. Schedule for Testing, Reviewing & Improving

As businesses change and evolve quickly, disaster recovery plans need to evolve as well. Unfortunately, it's not as simple as you creating a DRP, and then your business is ready for anything. Your company should dedicate time to test or rehearse your plan to make sure it's useful and review the plan so that it stays up to business and industry standards. If the business is booming and your staff doubles, for example, you'll need to account for those additional staff or office space in your disaster recovery plan. Depending on the rate of growth or change in your organization, schedule testing of your plan quarterly to annually.

3. The steps required in the disaster recovery process

During the development of the North Star, to repair the damage caused by the disaster we needed a recovery process. This includes six general steps:

1. Define the scope of the plan.
2. Identify key business areas.
3. Identify important functions.
4. Identify dependencies between different business domains and functions.
5. Define acceptable downtime for each critical function.
6. Plan to maintain operations.

4. The policies and procedures that are required for business continuity.

4.1. Define

A business continuity policy is a collection of criteria and principles that a company follows to guarantee that it is resilient and risk-aware. Business continuity strategies differ by company and industry, and they must be updated regularly as technology advances and business risks shift.

A business continuity policy describes the methodology and concepts that guide a company's BC activities, as well as the responsibilities for managing and coordinating business disruption situations. An event is a disruption that has the potential to affect the firm's employees, operations, technology, suppliers, and/or facilities' routine business activities. The required governance, monitoring, controls, and reporting, as well as the review and escalation of Events, are all documented in a Policy. A Policy governs an organization's BC activities, including those of its global operational affiliates and subsidiaries, and handles some parts of the firm's duties relating to third-party risk. It also guides all BC procedures.

BC Procedures describe the precise processes and/or operating instructions for implementing BC strategies by the firm's Policy. Business Continuity Planning, BC Testing, BC Crisis Management, BC Pandemic Preparedness, and BC Training and Awareness are all required by the BCM Booklet.

4.2. Purpose

A business continuity policy's purpose is to codify what is required to keep a company running on normal business days as well as during emergencies. The corporation can establish reasonable expectations for business continuity and disaster recovery (BC/DR) processes when the policy is well-defined and followed. This policy can also be used to figure out what went wrong and how to fix the issues. Finally, a business continuity policy is developed and implemented at the discretion of the organization, by its industry and regulatory standards.

4.3. Important

A risk assessment is a solid way to identify prospective risks and assess their likelihood. A risk assessment analyzes possible hazards and suggests solutions to mitigate their effects on the company. Risk assessments differ from business continuity policies; however, they always follow the same basic steps:

- Identify the hazards.

- Determine what or who could be harmed.
- Evaluate the risks and create control measures.
- Record the findings.
- Review and update the assessment.

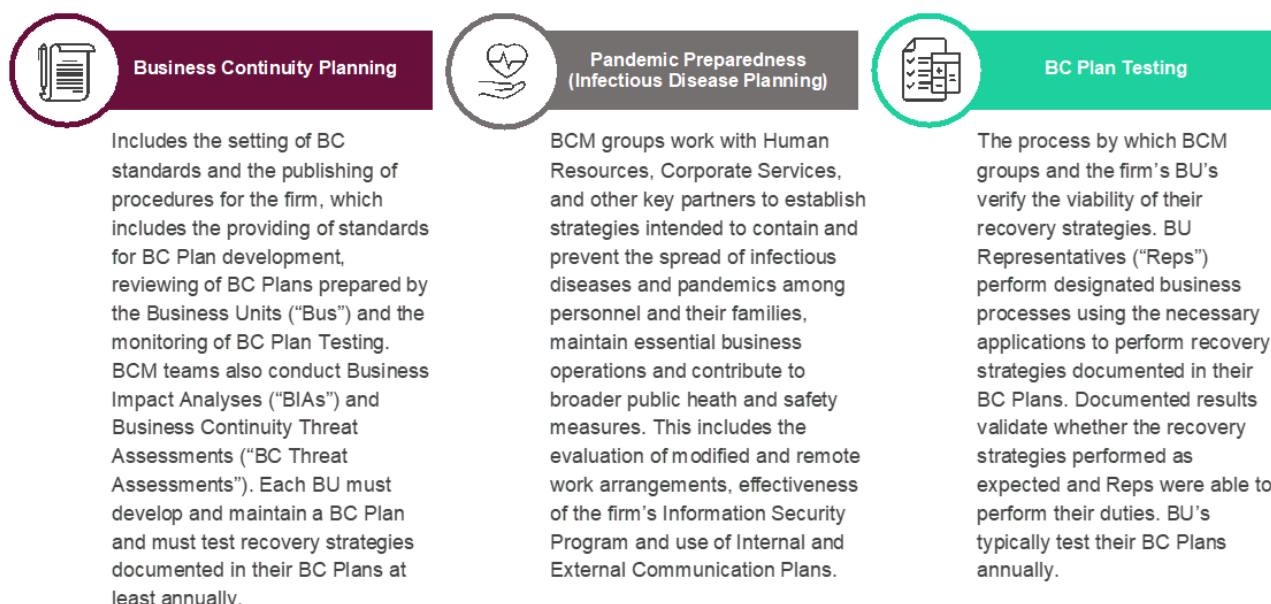


Figure 1 Business Continuity Procedure 1



Figure 2 Business Continuity Procedure 2

M3. Summaries the ISO 31000 risk management methodology and its application in IT security.

1. Define

ISO 31000 is a risk management standard. It presents several recommendations aimed at improving the efficiency of risk management in businesses. The ISO 31000:2018 standard is part of the ISO 31000 series of risk management standards. The ISO 31000 risk management standards are designed to be used generally, across a wide range of industries, niches, and business types, to provide the best practice structure and advice to all companies interested in risk management principles.

2. Introduction to ISO

A standard is just a set of specifications that have been defined and agreed upon by a large number of people. The International Organization for Standardization, a standard-making agency based in Geneva, Switzerland, is in charge of setting the standard in this situation. An ISO standard must be verified by several different representatives from a variety of different standards bodies before it can be published. It's vital to remember that ISO 31000 is a list of recommendations rather than a set of rules. Many ISO standards, such as ISO 9001 and ISO 14001, are requirements, which means they contain a collection of particular requirements that can be certified against. It's not like that with ISO 31000; it can't be certified to. It's nothing more than a set of best practices.

3. Management System Standard

There are numerous ISO standards, many of which are centered on the concept of a management system. ISO standards that share a common management system standard (MSS) structure include quality management (ISO 9001), environmental management (ISO 14001), and risk management (ISO 31000).

4. Benefit of ISO 31000

ISO 31000 may be extremely useful in preparing a company for any eventuality; by anticipating the worst-case situation, a company can better utilize the resources and opportunities already available to them. The following are some of the advantages of ISO 31000:

- ISO is an internationally recognized emblem for quality standards, giving you a competitive advantage.
- Increasing employee understanding of organizational risks by incorporating them in the management framework and assigning them responsibility for the procedures they use regularly Reduce the frequency of and eventually eliminate, risks by educating employees and stakeholders on identified risks.
- Maintain transparency and communicate risks to increase stakeholder trust (and demonstrate risk responsibility and mitigation)
- Encourage employees to think ahead by urging them to consider all possible outcomes in a particular situation.
- Improve business culture by bringing various departments together to share new ideas and brainstorm ways to collaborate more effectively.
- Improve the success rate of all corporate operations by focusing on the process, thinking ahead rather than reacting, and empowering workers to own their work duties.

5. Process of ISO 31000

The activity conducted in response to the discovery, analysis, and evaluation of hazards is known as risk treatment. According to ISO 31000, the success of risk management is determined by the management's efficacy.

The risk management process should be:

- An integral part of management;
- Embedded in the culture and practices;

Tailored to the business processes of the organization.

The risk management process comprises the following activities:

Communication and consultation: At all stages of the risk management process, communication and consultation with external and internal stakeholders should take place.

Establishing the context: The organization articulates its objectives, identifies the external and internal elements to be considered when managing risk, and establishes the scope and risk criteria for the remaining process by establishing the context.

6. Framework of ISO 31000

The effectiveness of the management framework provides the foundations and arrangements that will embed risk management throughout the business at all levels, according to ISO 31000. ISO 31000 states that the success of risk management will depend on the effectiveness of the management. More specifically, ISO 31000 defines six distinct areas that make up the total “framework” for risk management:

- Leadership and communication
- Integration
- Design
- Implementation
- Evaluation
- Improvement

The eight risk management concepts listed above are closely related to the ISO 31000 framework's areas. The concept of a well-integrated risk management system, for example, is both one of the principles and one of the framework's essential components.

6.1. Leadership and commitment

- The need for leadership and dedication is central to the ISO 31000 framework for risk management. Aligning risk management with the company's entire business objectives, strategy, and culture is part of this component.
- Issuing statements, announcements, or policies that identify the risk management approach, plans, goals, or actions
- Assuring that enough resources are allocated and made accessible for the risk management program.

6.2. Integration

Integration is crucial in any risk management strategy, perhaps second only to leadership and dedication. The extent (and efficiency) with which your risk management strategy is incorporated into all elements of your company, including decision-making processes, will determine its efficacy. In terms of the ISO 31000 framework, this component comprises items such as:

- Organizational management roles and responsibilities
- Ensure that risk management is integrated into all elements of the organization.

6.3. Design

We've reached the framework's final four components: design, implementation, evaluation, and improvement. The Plan-Do-Study-Act cycle, which is a methodology for continuous quality improvement, is made up of four parts. This approach is referred to as Plan, Implement, Measure, and Learn (PIML) in ISO 31000:2018, as seen in the picture below. Despite the variation in names, the technique is essentially the same. Beginning with planning (or design) and concluding with improvement (or learning), there are four unique stages with the common goal of strengthening the risk management framework. This section contains items such as:

- Recognizing the organization and its surroundings (both internal and external)
- The risk management program's planning and resource allocation
- Creating communication standards

6.4. Implementation

Putting the plans into action is the next step. Even yet, some planning takes place here, particularly the specialized planning for the risk management approach's execution. This section contains items such as:

- Creating goals and deadlines
- The decision-making process must be well defined.
- Evaluating and, where necessary, altering the decision-making process

6.5. Evaluation

Examining what's working and what isn't, and determining whether the risk management system is performing as it should. This includes examining the perceived versus expected outcome (e.g., doing a gap analysis) as well as any other analytics or feedback gleaned from the process and implementation thus far. It could contain items such as:

- Measuring the performance of the risk management system
- Assessing success rate
- Determining whether or not objectives are feasible

6.6. Improvement

Risk management is a circular and never-ending process. That is to say, there is always room for growth. Even though the ISO 31000 framework has a step dedicated to it, and the framework is

organized in a series of phases, the most effective risk management systems take a continuous approach to improvement.

Risk management is a cyclical and never-ending process. It follows that there is always room for improvement. Even though the ISO 31000 framework has a step dedicated to it and that the framework is organized in a series of phases, the most effective risk management systems take a continuous approach to improvement.

- Continuously monitoring all aspects of the risk management framework
- Addressing internal and external changes
- Planning and taking actions to improve value creation within the risk management system

M4. Discuss possible impacts to organizational security resulting from an IT security audit.

1. Define IT Security Audit.

An information security audit is a thorough inspection and evaluation of your company's information security system. Regular audits can help you detect weak points and vulnerabilities in your IT infrastructure, as well as evaluate security policies and assure regulatory compliance.

2. Benefits Of Security Audits

An IT security audit, as previously said, uncovers underlying weaknesses and security threats in an organization's IT assets. Identifying hazards, on the other hand, has a positive impact on an organization's overall security.

- With the audit results, helps you create a benchmark for your organization by weighing your present security structure and practices.
- Hacker risks are reduced by detecting probable hacker entry points and security weaknesses ahead of time.
- Verifies your IT infrastructure's compliance with leading regulatory authorities and assists you in complying.
- Finds gaps in your company's security training and awareness and assists you in making informed decisions to improve it.

3. Type of IT Security Audit

An IT security audit can be classified in a variety of ways. In general, it's been divided into categories based on strategy, methodology, and so on. The following are some examples of common classifications:

Approach Based

- Black Box Audit: In this type of audit, the auditor only has access to publicly available information on the business being examined.
- White Box Audit: In this sort of security audit, the auditor is given detailed information (such as source code, personnel access, and so on) about the company being audited.
- To begin the auditing process, the auditor is given certain information in a grey box audit. Although the auditors might acquire this information themselves, it is provided to save time.

Methodology Based

- Penetration Tests: The auditor tries to break into the infrastructure of the company.
- Compliance audits: Only a few parameters are reviewed to establish if the company is following security guidelines.
- Risk Assessments: An examination of vital resources that could be jeopardized in the event of a security breach.
- Vulnerability Tests: Scans are done as needed to identify potential security issues. There could be a lot of false positives.
- Due Diligence Questionnaires: These are used to assess the organization's current security standards.

4. Importance of an IT Security Audit

- Protects an organization's important data resources.
- Maintains compliance with various security certifications.
- Detects security flaws before they are exploited by hackers.
- Keeps the company up to date on security procedures.
- Vulnerabilities in physical security are identified.
- Assists with the development of new security rules for the company.
- Prepares the company for emergency response in the event of a data breach.

5. Conduct an IT Security Audit

Before beginning with the process of security audits, it is important to use the right set of tools. Kali Linux is one such OS that is customized and contains a bundle of tools to conduct a security audit. This OS can be used by installing on a separate machine or making the present machine dual-booted or on a virtual machine. To install it on a virtual machine. (VM Ware - Kali)

Metasploit is a robust exploitation framework that may be used to undertake an IT security audit. Metasploit, which has a huge number of exploits, can be used to check all of the probable vulnerabilities detected using Nikto. To utilize them, go to Kali's terminal and type: **msfconsole**

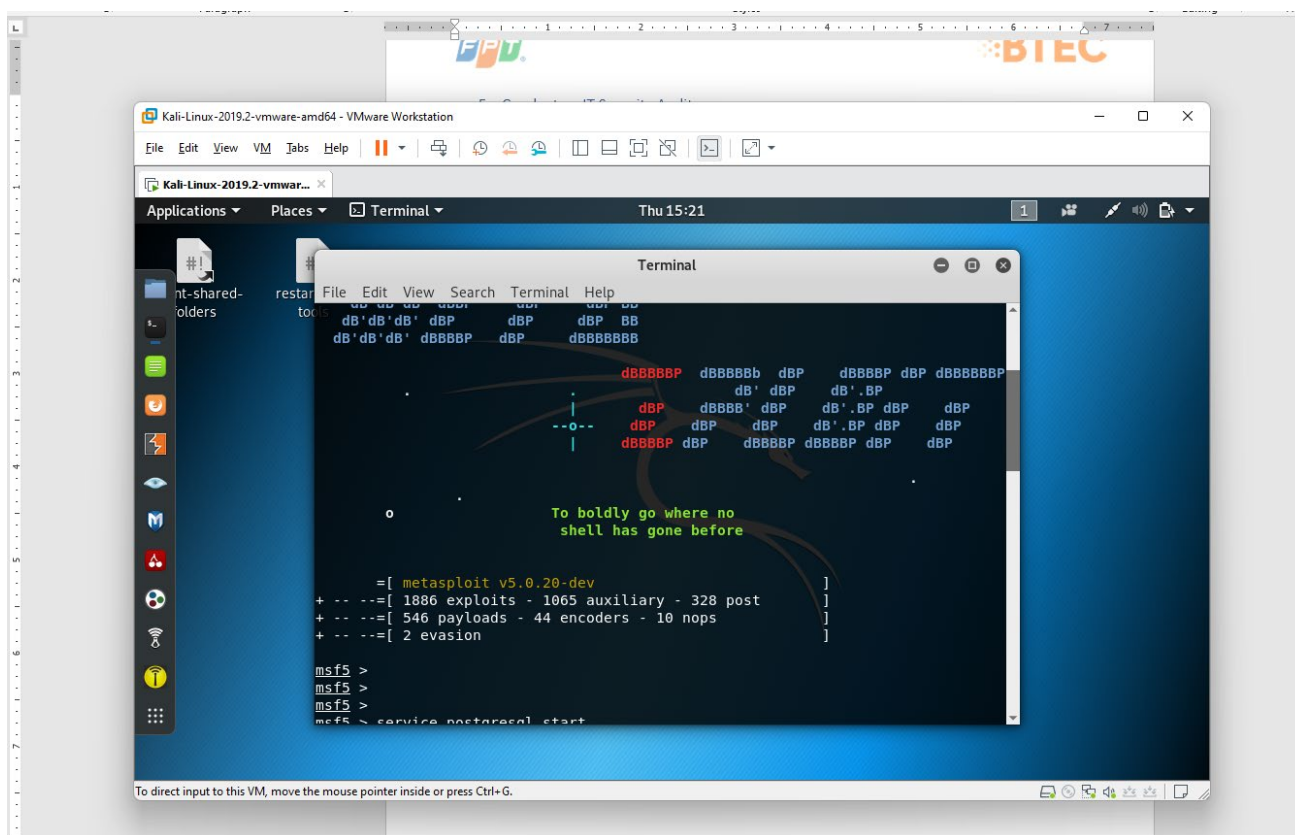


Figure 3 Conduct an IT Security Audit

M5. Discuss the roles of stakeholders in the organization to implement security audit recommendations

1. Definition Stakeholder

Stakeholders are individuals, groups, or organizations who are involved in or impacted by the creation and completion of a project. They have a vested interest in its conclusion since it will benefit them in some manner, either monetarily or in terms of professional promotion, and they have a lot of influence over how it is completed.

2. The Role of a Stakeholder

A stakeholder's major function is to contribute their experience and perspective to a project to assist a company in meeting its strategic objectives. They may also be able to give materials and resources. Their support is critical to a project's success; if they don't like the results, the project may be regarded as a failure, even if all of the objectives were completed.

The fundamental duty of a stakeholder is to contribute their experience and perspective to a project to assist a firm in achieving its strategic goals. They may also be able to provide goods and resources that are required. Their support is critical to a project's success; if they don't like the results, the project is frequently deemed a failure, even if all of the objectives were completed.

3. The Main Types of Stakeholders

There are two types of stakeholders in nearly all projects:

- **Internal Stakeholders:** Internal constituents an internal stakeholder is a person or a group of people who are directly connected to the project's sponsoring company. Employees, who are members of the project team who will see the project through to completion, as well as a project manager, resource manager, and line manager, are all examples of internal stakeholders. Internal stakeholders include top corporate management, such as the president, board of directors, and operating committees, as well as external contributors, such as subcontractors and consultants.
- **External Stakeholders:** Stakeholders outside the company an external stakeholder is a person or organization that is not affiliated with the project's sponsoring company but is affected by its outcomes in some way. Vendors, suppliers, creditors, project consumers, project testers, and a user community for the product are all examples of external stakeholders.

4. Stakeholders of North Star

Security audit plans should be repeatable and updatable by organizations. To achieve the greatest results, stakeholders must be involved in the process. The table below lists the various stakeholders who might be involved in a security audit. Different firms and organizations may have a greater or lesser impact on stakeholders.

Synonym	Stakeholders
User Community	<ul style="list-style-type: none"> ▪ End Users ▪ Computers Users ▪ User Community ▪ Data Entry Staff ▪ Data Processors ▪ Information Collectors ▪ User Group
External Representatives	<ul style="list-style-type: none"> ▪ External Consultants ▪ Clients
Security Specialists	<ul style="list-style-type: none"> ▪ System Security Manage ▪ Security People ▪ Information Security Team
Executive Management	<ul style="list-style-type: none"> ▪ Top Management ▪ Managers ▪ Senior Management ▪ Corporate
ICT Specialists	<ul style="list-style-type: none"> ▪ Technical Computer Specialists ▪ System Designer ▪ IT People ▪ System Administrator ▪ IS Professionals ▪ IT Department ▪ Technical Writers

	<ul style="list-style-type: none"> ▪ Technical Personnel
Legal & Regulatory	<ul style="list-style-type: none"> ▪ Legal Department ▪ Legal Counsel ▪ Legal and Regulatory People ▪ Industrial Standards and Professional Licensure ▪ Audit and compliance

5. Discuss

All six stakeholder positions are likely to be present in the medium to large businesses, represented by one or more individuals who would be active in the organization's Information Security Policy lifecycle.

Individuals are more likely to be involved in several stakeholder positions in smaller firms due to the size of the organization, and some stakeholder jobs may be outsourced. Many roles should be included in the development process of an ISP to ensure that it is properly developed. This will give all stakeholders a complete picture of how the Information Security Policy is being developed.

CONCLUSIONS

In Assignment 2, I presented definitions and clarifications on risk assessment as well as further analysis of data protection. In section P6, I have analyzed and pointed out the important elements of data protection. In section P7, I covered the organization's privacy policy, and I also clarified all the information about the privacy policies and key points. In section P8, I have outlined the factors and processes for developing and managing disaster or disaster risk.

In this 2nd assignment, I tried to analyze more about ISO 31000 as well as clarify about stakeholders. In sections M3, M4 and M5, I have presented clearly and specifically about the factors that the topic gives.

References

- Gibbs, M., 2018. *7 Easy Steps to Take to Protect Your Data*. [Online]
Available at: <https://www.cybintsolutions.com/7-easy-steps-to-protect-your-data/>
[Accessed 11 December 2021].
- Lachapelle, E., 2015. *ISO 31000 Risk Management – Principles and Guidelines*. [Online]
Available at: <https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines>
[Accessed 14 December 2021].
- Peterson, O., 2019. *What Is ISO 31000? Getting Started with Risk Management*. [Online]
Available at: <https://www.process.st/iso-31000/>
[Accessed 15 December 2021].
- Riskology, 2020. *6 Key Components Of A Disaster Recovery Plan*. [Online]
Available at: <https://www.riskware.com.au/risk-management-blog/6-key-components-of-a-disaster-recovery-plan>
[Accessed 15 December 2021].
- SARAP, K., 2018. *Three reasons why we need strict data protection regulations*. [Online]
Available at: <https://www.njordlaw.com/three-reasons-why-we-need-strict-data-protection-regulations>
[Accessed 12 December 2021].
- Security Scorecard, 2021. *6 Examples of Essential Cybersecurity Policies for Businesses*. [Online]
Available at: <https://securityscorecard.com/blog/cybersecurity-policy-examples>
[Accessed 12 December 2021].
- SOPHOS, 2020. *Sample Data Security Policies*. [Online]
Available at: <https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf>
[Accessed 13 December 2021].
- Sotnikov, I., 2018. *How to Perform IT Risk Assessment*. [Online]
Available at: https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/#IT_risk_assessment_components_and_formula
[Accessed 10 December 2021].
- Stefanovic, J., 2019. *Data protection vs. data security*. [Online]
Available at: <https://www.chino.io/blog/data-protection-vs-data-security/>
[Accessed 10 December 2021].
- Varghese, J., 2021. *IT Security Audit: Importance, Types, and Methodology*. [Online]
Available at: <https://www.getastra.com/blog/security-audit/it-security-audit/>
[Accessed 15 December 2021].