UNIVERSITY of GREENWICH
Alliance with FPT Education

BTEC

Higher Nationals in Computing

UNIT 5

SECURITY

ASSIGNMENT

No.2

Learner's name: Trinh Thi Dieu Huyen

Assessor name: Dang Thai Doan

Class: GCS0801B.2

Learner's ID: GDD18606

Subject's ID: 1623

Assignment due: May 2020

Assignment submitted: May 2020

UNIVERSITY of GREENWICH
Alliance with FPT Education

BTEC

ASSESSMENT BRIEF

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number	Unit 5: Security		
Assignment title	Assignment 2		
Academic Year	2019 – 2020		
Unit Tutor	Dang Thai Doan		
Issue date	May 2020	**Submission date**	May 2020
IV name and date	Dang Thai Doan April 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: The security risks faced by the company. How data protection regulations and ISO risk management standards apply to IT security. The potential impact that an IT security audit might have on the security of the organization. The responsibilities of employees and stakeholders in relation to security. **Part 2** Following your report: You will now design and implement a security policy 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**
L03 Review mechanisms to control organizational IT security		**D2** Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment.
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.	
L04 Manage organizational security		**D3** Evaluate the suitability of the tools used in an organizational policy.
P7 Design and implement a security policy for an organization. **P8** List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion.	**M5** Discuss the roles of stakeholders in the organization to implement security audit recommendations.	

UNIVERSITY of GREENWICH
Alliance with FPT Education

BTEC

ASSIGNMENT FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 5: Security**		
Submission date	May 2020	**Date Received 1st submission**	May 2020
Re-submission Date		**Date Received 2nd submission**	
Student Name	Trinh Thi Dieu Huyen	**Student ID**	GDD18606
Class	1623 GCS0801B.2	**Assessor name**	Dang Thai Doan

Student declaration

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student's signature	

Grading grid

P5	P6	P7	P8	M3	M4	M5	D2	D3

❒ Summative Feedback:	❒ Resubmission Feedback:

Grade:	Assessor Signature: Dang Thai Doan	Date:
Signature & Date:		

Table of Contents

Table of figure 7

Table of table 7

Introduction 8

LO3 Review mechanisms to control organizational IT security 9

P5 Discuss risk assessment procedures 9

P6 Explain data protection processes and regulations as applicable to an organization 12

M3 Summarize the ISO 31000 risk management methodology and its application in IT security 13

M4 Discuss possible impacts to organizational security resulting from an IT security audit 19

D2 Consider how IT security can be aligned with organizational policy, detailing the security impact of any misalignment 21

LO4 Manage organizational security 23

P7 Design and implement a security policy for an organization 23

P8 List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion 31

M5 Discuss the roles of stakeholders in the organization to implement security audit recommendations 34

D3 Evaluate the suitability of the tools used in an organizational policy 35

Conclusion 38

Evaluation 38

References: 39

Table of figure

Figure 1: Security Risk Assessment Steps 9
Figure 2: ISO 31000 2018 risk management standard 14
Figure 3: Process of design a successful management framework 16
Figure 4: Risk management process 18
Figure 5: Security audit benefits 19
Figure 6: Policy must and should statements 21
Figure 7: Policy Specifics and Procedures 32

Table of table

Table 1: The proposal is used to assess the risks commonly have cause adversely affecting the organization and solutions (possibly with low efficiency). 11
Table 2: Levels of management in organization 24
Table 3: Security policy for an organization 25
Table 4: Security policy for an organization responsibility matrix 29

Introduction

I work for a security consultant as an IT security specialist. One of the best manufacturing companies is Wheel Wheelie in Ho Chi Minh City producing bicycle parts. My mission is to propose a Security Policy for their organization, after reading stories in the media related to security breaches, etc. in organizations and their ramifications.

Detail:

- ✓ Give security risks faced by the company
- ✓ Explain data protection regulations and ISO risk management standards apply to IT security
- ✓ Give potential impacts that an IT security audit might have on the security of the organization
- ✓ Description responsibilities of employees and stakeholders in relation to security
- ✓ Design and implementation of security policies
- ✓ Explain why give the above components into Wheelie's disaster recovery plan
- ✓ Evaluate the proposed tools use within the policy and how they align with IT security (include sections on how to administer and implement these policies)

LO3 Review mechanisms to control organizational IT security

P5 Discuss risk assessment procedures

I will give steps in security assessments before assessing risks by comparing them with criteria, in order to contribute to determining the damage caused by an attack and the vulnerability that is the risk for with organization. Have seven steps **[1]**.

SECURITY RISK ASSESSMENT STEPS	
Step 1	Identify the information all valuable assets of the organization that could be damaged by threats
Step 2	Identify the asset owners who is responsible for assets above
Step 3	Identify threats/risks, vulnerabilities and their level
Step 4	Establish a risk management framework
Step 5	Analyze risks and assess the likelihood and potential impact if the risk were to materialize
Step 6	Determine the levels of risk then create a risk management plan using data collected by documenting the result
Step 7	Select risk treatment options as well as prioritize the analyzed risks for treatment

Figure 1: Security Risk Assessment Steps

First, identify the information assets. Means any information or assets that are valuable to the business and contribute to its operability and profitability. Need to search for templates (Databases, Infrastructure or Electronic Documents, etc..) and scan for all valuable assets of the organization that could be damaged by threats in a way that result in potential consequences such as financial loss (Hardware, Software, Data, User, Interfaces, Functional Request, Physical Security Environment, Flow, Storage Protection, etc..). This step is important because each organization has a limited budget to assess and handle risks, so it is necessary to limit the scope of the project to determine the importance of each asset as well as protect valuable assets.

Second, identify the property owner responsible for the above assets. Because, it is the best source of knowledge regarding about potential vulnerabilities and threats to assets. Also, can assess the likelihood and impact of identified risks whenever it becomes available actualization.

Third, identify risks / threats, vulnerabilities and theology level. Means anything that could exploit the vulnerability to compromise the security, integrity and availability of information. Need to make a list of assets to get started or follow an existing list is property-based approach - This is the best method. Besides hackers and malware, there are many other types of risks such as natural disasters (Storms, Floods, Earthquakes and Fires, etc..).

Fourth, establish a risk management framework. This step provides policies to manipulate risk identification methods in the risk assignment section for risk treatment. The impact of risks affects the security, integrity and availability of data. It also calculates / estimates the damage for each scenario and its probability such as: risk scale, baseline security criteria, asset-based risk assessment, risk appetite or Methodology scenario.

Fifth, analyze risk and assess ability / potential impacts if risks occur. It is necessary to identify and manage potential threats and vulnerabilities that each asset may encounter. Then estimate the likelihood that these threats will occur. After the risk assessment, it is necessary to estimate the risks of each risk against a predetermined level of acceptable risk, in or select which risks to address and which risks to ignore. In addition, it is necessary to assess the risks using a logical formula and register to use high, medium and low lists to assess the likelihood of an attack along with the approximate cost of each occurrence.

Sixth, determine the level of risk. After that, create a risk management plan. To made this, need use the data collected by recording the results to assist management in making appropriate financial decisions, policies, procedures, etc. For every single threat, the report should describe the security gaps, likelihood, control recommendations, affected assets and impacts on information technology infrastructure.

Finally, risk option to treatment or risk priorities are analyzed to treatment in general. There are about four ways to can handle risks. It is Hold / Accept, Modify, Avoid and Share. *Hold / Accept* the risk, if risk fails in established risk acceptance criteria - this is the best option when nothing can be done to address, minimize risks, or when potential losses are less than the cost of hedging, or when the

potential benefit is worth accepting the risk. *Modify* risks by applying security controls and reducing risks. *Avoid* the risk by destroying it completely - This is a good option when accepting risks associated with not being beneficial to the organization or when the cost of handling the effects is not worthwhile. *Share* the risk with a third party through insurance or by outsourcing it.

Table 1: The proposal is used to assess the risks commonly have cause adversely affecting the organization and solutions (possibly with low efficiency).

Risk Category	Probability	Impact	Possible Consequences	Responsibility	Solution
Unauthorized use of a system	Occasional	Critical	Data breach, loss of money, etc..	Anyone, employee or staff who is relevant	Protection and use and authenticated passwords
Unauthorized removal or copying of data or code from a system	Probable	Critical	Loss of money for financial repercussions	Security officer, system manager	Protection and use of passwords or access codes
Damage to or destruction of physical system assets and environment	Rarely	Medium	Loss of money for recover assets and environment	Anyone who related to the destruction	Configure access control devices (locks, biometric controls)
Damage to or destruction of data or code inside or outside the system	Seldom	Critical	Loss of data money for recover code of the system	Anyone who manage the data and code of the system	Limit the visibility of the data, allocate access authority
Naturally occurring risks	Rarely	Critical	Loss of financial for recover after occurrence	Whole organization	Operational continuity planning, disaster recover planning

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

Data protection is the process of safeguarding important information from corruption, compromise or loss **[3]**. For some organizations that apply data protection processes and regulations, regulations will protect freedoms of natural persons and in particular organization's right to the protection of personal data. This means that the organization has some kind of formal data protection process to ensure the security of all customers, partners, employees and any other individuals whose data is held by that organization hold.

There are three processes to data protection. That is *analysis*, *transformation* and *sustainability* **[4]**.

About analysis, through the use of unique algorithms and knowledge of business process weaknesses, allow responsible for protecting the data, identify vulnerabilities and liabilities. Means extensive and valuable analysis that captures how data, infrastructure, and relationships are managed to ensure they meet data protection requirements and help reduce the likelihood of breaches data **[3][4]**.

About transformation - provide evidence of regulatory compliance. Based on analysis step, it enables organizations to transform both business processes and application systems to gain insights in to any potential risks or data breaches **[3][4]**.

About sustainability, organization is able to continue to maintain its understanding around movement, use and guardianship of its data as well as keep abreast of the latest regulatory changes and updates. That mean that it is not an end in itself, but rather the beginning of an ongoing and continuously improved process while of data protection management **[4]**.

In short, these processes do not address existing regulatory issues, but can also actively manage any new issues.

Data protection regulations set out rules regarding the protection of natural persons, the processing of personal data and the free movement of personal data. In addition, it protects the basic freedoms of natural persons and especially the

protection of personal data. I will list some of the rules that apply to the organization.

First, the personal data will be processed lawfully, fairly and in a transparent manner in relation to the data subject **[5]**.

Second, it must adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **[6]**. Mean, the data will be collected for specified, explicit, legitimate purposes and not further processed in a manner that is incompatible with those purposes such as: Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, not be considered to be incompatible with the initial purposes.

Third, the data must accurate and where necessary will be kept up to date **[6]**. Everything must be done reasonably to ensure that, if personal data is inaccurate relates to the purposes for which they are processed, then will be deleted or delayed **[5]**. Means, it will be stored in a form that allows data object recognition. This is necessary for the purposes for which personal data is processed such as: personal data may be stored for longer periods of time as it be processed solely for the sake of storage public interest, scientific / historical research or statistical purposes must take appropriate technical and organizational measures in accordance with provision to protect the rights of data subjects.

Finally, integrity and confidentiality **[6]**. Data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using not suitable technical or organizational measures.

In a nutshell, if personal data is leaked, it can result in significant damage to companies' reputation and also bring along penalties. This is why data protection and regulations are important.

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

Simply put, ISO 31000 is a standard for risk management **[7]**. It is used by people who create and protect value in organizations by managing risks making before decisions setting to achieving objectives and improving performance. ISO 31000 can be customized for any organization or any of contexts. Because, it provides common approach to managing any kind of risk even though that is not a specific industry or sector. In addition, it also can be throughout the fife of the organization and to any activity, including decision-making at all levels.

ISO 31000 has three main sections basically and combination of these three sections make up a risk management methodology. It starts by listing a set of principles in risk management. Next, these principles are used to guide the establishment of the risk management framework. After that, the frameworks used to guide the establishment of the risk management process.

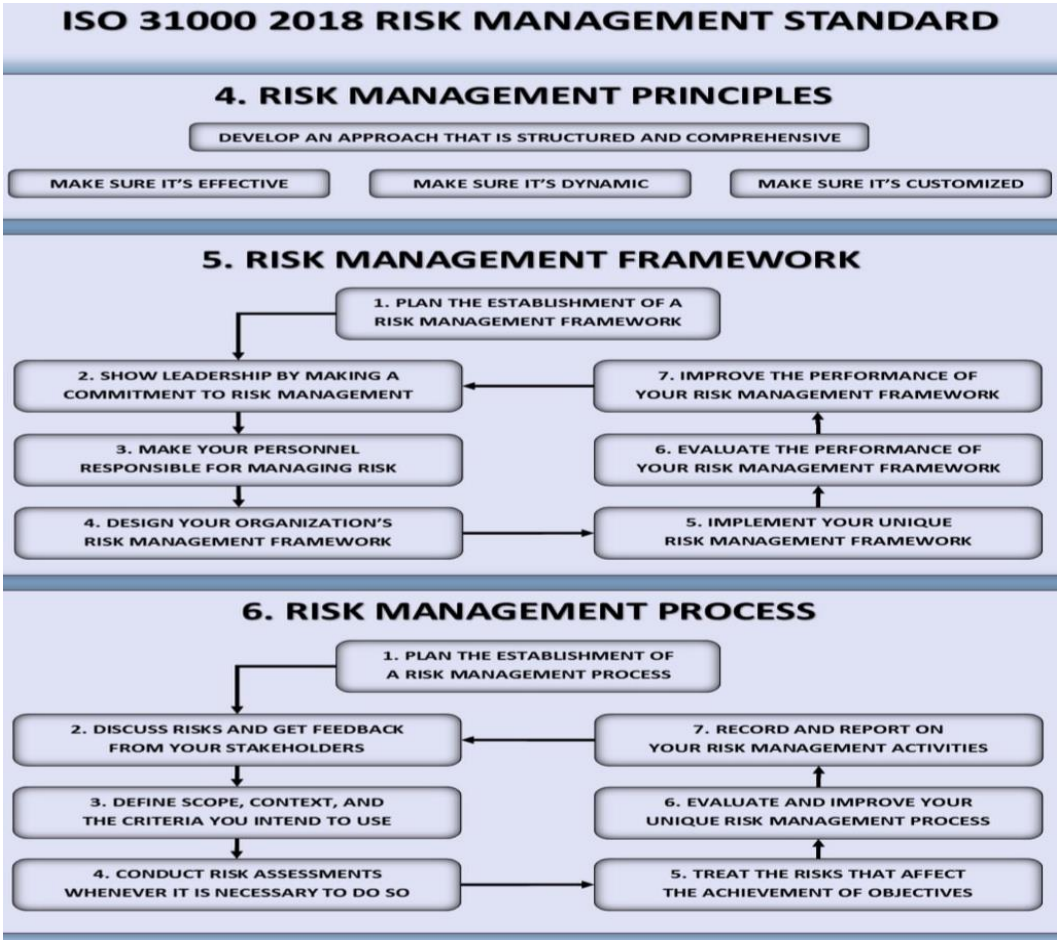

Figure 2: ISO 31000 2018 risk management standard

To make ISO 31000 more accurate. Before identifying the types of risks to implement the risk management process, organizations should be aware of all types of risks that having or risk may face in the future the organization when they operate. This can be done by reviewing all past risk registers and determining whether any past risks that has been processed with or are still present. There are two possible situations. *First*, if the organization has absolutely no risk register, the top management should provide the risk management group with enough information about past risks and what its source is. *Second*, organizations that do not face any past risks, should continue to identify potential risks so as not to have any negative consequences. Security and legal activities or financial, credit and integration activities are some types of risks that organizations may face.

About design a risk management framework - a comprehensive knowledge of the risk types that can be faced by the organization and the principles of risk management has been gained by the risk management team, to the organization can start design a suitable risk management framework with the support and leadership of the top-level management. According to ISO 31000, the development of a framework will fully integrate risk management process for organization which assures that an organization-wide process is supported, iterative and effective. In addition, risk management will be an important component governance or a strategy to planning management reporting processes, policies, values and culture. So, ISO 31000 requires the engagement and awareness of stakeholders which allows organizations to explicitly address uncertainty in decision-making while also ensuring that any new or subsequent uncertainty can be taken into account as it arises.

The activities of a successful framework include:

- Demonstrating leadership and commitment to risk management
- Integrating risk management into organizational processes
- Designing the framework for managing risk
    - *Understanding the organization and its context*
    - *Articulating risk management commitment to assigning roles, authorities or responsibilities / accountabilities*
    - *Allocating appropriate resources*
    - *Establishing communication and consultation*
- Implementing the risk management process by evaluating the risk management process, adapting and continually improving the framework

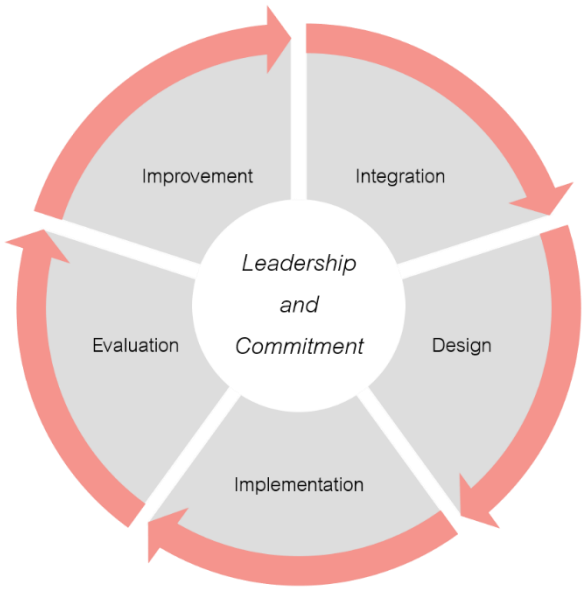

Figure 3: Process of design a successful management framework

Implementing an organization's risk management process should involve systematic application of policies, procedures, and practices to communication / consulting activities to establish context, assessment, treatment, monitor, reviewed, record and report risk. *The effective implementation / integration of a risk management process includes the following steps*:

Establishing the organization's context needs to take into account the external (political, social, etc.) and internal environment (strategic goals, structure, ethics, discipline, etc.) of organization. Means the organization should determine the purpose, scope of risk management activities and the objectives of the risk management process or the specific objectives of the risk assessment. In addition, the organization should define the scope and boundaries specified for the risk management process or identify all constraints that affect the scope and risk criteria used throughout the process **[8]**.

Risk identification is a formal, structured process that includes risk sources, events, their causes and potential consequences. In other words, it is about the creation of a comprehensive list of risks (both internal and external) that the organization faces, and can involve input from sources such as historical date theoretical analysis, expert options, and stakeholders needs. Due for using it that the organization is able to identify its assets, risk sources, risk events, existing measures and consequences. Also, by identifying such elements the organization will be ready to begin the risk analysis process **[9]**.

Risk analysis is a formal technique to consider the consequence and likelihood of each risk. These techniques can be qualitative, semi-quantitative or a combination based on the circumstances and the intended use **[9]**.

Risk evaluation is which rank the relative importance of each risk, so that a treatment priority can be established **[9]**.

Risk treatment for the organization includes: avoidance of the activity from which the risk originates, risk sharing, managing the risk by the application of controls risk acceptance and taking no further action, or risk taking and risk increasing in order to pursue an opportunity.

Another step of the risk management process based on ISO 31000 is the recording and reporting **[9]**. This is important for reasons such as: communication of the risk management activities and outcomes pertaining to those activities throughout the organization or providing the necessary basis and information for making informed decisions.

Finally, monitor and review. It includes actions such as examining the progress of treatment plans, monitoring the established controls and their effectiveness or ensuring that activities which are proscribed are being avoided, and checking that the environment has not changed in a way that effects the risks **[9]**.

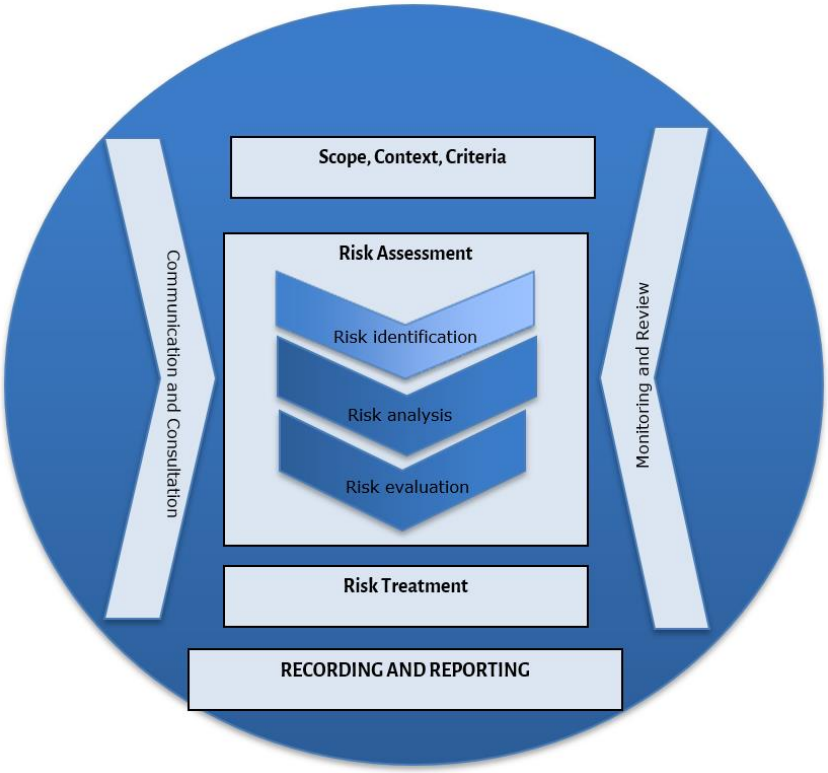

Figure 4: Risk management process

Overall, ISO 31000 was developed with the purpose of providing the structure and best practice guidelines for all risk management activities. In addition, it targets those who create and protect value in organizations through risk management, decision making, setting, achieving goals, and improving performance. On the other hand, it is also the standard that contains the set of comprehensive risk management principles, risk management frameworks and processes that we have discussed. Although, when applying ISO 31000 will not be able to prevent all bad business decisions or issues. But one thing is for sure that, it gives organizations the opportunity to understand the causes and determine the treatments they need to establish to reduce uncertainty about their future decisions.

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

A security audit is the high-level description of the many way organizations can test and assess their overall security posture, including cybersecurity. Might employ more than one type of security audit to achieve your desired results and meet business objectives **[10]**.

Figure 5: Security audit benefits

The results from the information security audit are verified by a third-party organization and are used as a basis to assess whether the general state of the current safeguards is up to standard the organization may take action on the impact of this audit for organizational security. There are two possibilities. *First*, if the results inform that the security of the organization is good, we just need to continue to maintain and look for potential risks. So, the value of the organization will be promoted as well as the confidence of partners and customers also advanced. *Second*, if the poor audit results on an organization's security, then will have a lot of tasks to do because the organization's security is verified to be bad and not sufficient to protect the security of the company or organization.

The first impact, information technology security audits assessing the flow of data is one of the key assets that require top security manipulation **[11]**. It determines the type of information the organization has, how it is accessed, and who accesses it. In addition, the audit reviews all technologies and processes related to data breaches to ensure that no data is lost, stolen, misused or mishandled. However, it will lead to legal disputes with customers or other affected parties.

The second impact, information technology security audit - identifying vulnerable points and problem areas in the system **[11]**. It may include a number of components such as hardware, software, data and procedures. In addition, it can also determine the exact location if there are any potential problem areas in the system. It can even check to see if hardware or software tools are configured and working properly or access security risks from the past that reveal weaknesses in the organization's security.

The third impact, the information technology security audit - determines if you must alter security policies and standards or not **[11]**. Based on the result of the audit, we would have a clear assessment if the organization have fully security measures that are consistently implemented within the system.

- For example: If the result report that instances of unauthorized wireless networks that could pose risks beyond acceptable level, the organizational security must be reconsidered to figure out solution for this risk.

The fourth impact, auditing - suggesting the use of information technology in organizational security **[11]**. It will determine whether you need to focus on security solutions on all devices or use special software for each risk area or not. However, it can also prevent the organization from trying to secure every server or application whenever the results report that the level of risk is not worthy of it.

The last impact, it delivers an in-depth analysis of both internal and external information technology practices and system **[11]**. As a result of the information technology security audit provides a detailed list of audit team results. It is completed with an executive summary, support data and appendices. The result will highlight problem areas, proposed solutions related to risk areas, and comply with industry standard security policies, etc.

- For example: The audit results report that the quality of optimal security controls is not good despite setting up a firewall on the server, but if the internal operations are weak or corrupt, important data the organization remains at risk.

In summary, the results of an information technology security audit have a lot of impact on the security of the organization. It will useful, when to point out potential security issues or remind the organization to pay attention to methods of improvement / protection for these risks. In addition, it also compares the differences between existing safeguards with identified security standards and policies, and then makes further recommendations for improvement. Besides, the results of information technology security audits contribute to increasing the confidence of partners, customers and the value of the organization. So, it becomes the platform to receive ISO verification by a third-party organization.

D2 Consider how IT security can be aligned with organizational policy, detailing the security impact of any misalignment

Linking information technology security with an organization's policy is essential to protect the organization against breaches and intrusions. With role as a security leader, need it is responsible for the effective deployment of information technology security to improve the overall development of the organization. Next, to make it easier to decide what to do, take a closer look at how the both are related. When designing security policies, need note the two statements are "*must*" and "*should*" to keep the link between information technology security and organizational policy. *So, why do we need to follow those claims*? To explain this problem, let analysis into the issue and go into it.

Security Policy Must	Security Policy Should
Be able to implement and enforce it.	State reasons why the policy is necessary.
Be concise and easy to understand.	Describe what is covered by the policy.
Balance protection with productivity.	Outline how violations will be handled.

Figure 6: Policy must and should statements

First, about the "*must*" policy - the mandatory security policy. This means that policies of this type require a balance between security policy and organizational policy. They must be implemented and everyone in the organization must run it because they are essential elements that directly affect the security of the entire

organization. Therefore, these policies must be short and easy to understand so that everyone can understand and follow them. In addition, the "*must*" policy has the same characteristics as its name. Means anyone must obey or will be punished for not governing. Other way these policies are created to prevent dangerous risks or attacks can destroy the organization or be violated by the majority of people in the organization, them must be carefully reviewed and guaranteed that when applied to an organization them will have a good impact or not creating a distinction between security and the entire organization.

- For example: the policy name: "*Do not allow anyone else to use ID / tokens and their user passwords on any information technology system*". That means it does not affect the business. In other words, it can be seemed as basic the principle and unacceptable if somebody violate them.

Second, on the "*should*" policy - an optional privacy policy. This policy does not require management. It is only a recommendation and only needs to know cause appears, what is covered by it and the potential consequences if not managed. This is a solution to align information technology security with organizational policy. There are many policies that can be applied in specific aspects (such as security) and this does not mean that all organizations have it. So, "*should*" policies be used to balance information technology and organizational security as advice to everyone. However, these polls do not require everyone to perform, but only one or two aspects of the organization. Means maybe one aspect appropriate but other aspects inappropriate. From that it can be concluded that it is the only option to link between the two security and other things like organizational policy

- For example: the policy name: "*Use virus detection and virus settings*". This is just an optional suggestion, because the virus detection software has many different options and everyone can choose a different software as long as computers are protected.

In addition, the wrong adjustment of security policy and information technology organization policy can cause many problems to solve and potential problems that it can cause when reducing revenues / profits, increasing many risks in misunderstood privacy policies, etc. Information technology payment policy was

created to reduce risks for the entire organization, it started with bulky technology and business resistance. However, when the security policies are too strict and inappropriate, it will cause resistance in the business.

- For example: a student uses a laptop access the internet to study. However, there are a few other students trying to hack the school website. When the head of the school recognizes it, the school will decide to implement a policy that prohibits students from using laptops on campus. From that, it can be seen that the security issue has been solved but the school has encountered another big problem. Just because a few percent of students use the laptop for the wrong purpose while others are studying very hard that school forbid all students to use. This may cause students to feel uncomfortable or react negatively to the new policy. It is clear that the new policy is not in line with organizational policy and information technology security. This can lead universities to lose confidence in coming up with a very bad solution. Therefore, the number of students enrolling in the school will certainly decrease with the value and operation of the school.

In short, in the commands to keep the link between information technology security, organizational policies and prevent the adverse effects of misalignment. Organizations need to carefully review their policies. See which ones are required, which ones are optional options. Only one way to check the effectiveness of the policy has been designed. That is, the organization should put itself into each specific strategy to see how the policy works. From there, organizations will be able to understand and decide the best solution help balance these strategies.

LO4 Manage organizational security

P7 Design and implement a security policy for an organization

A security policy is a written document in an organization, it outlining how to protect the organization from threats and including computer security threats or how to handle situations when they do occur **[2]**.

A security policy must identify all of a company's assets as well as all the potential threats to those assets. Company employees need to be kept updated on the

company's security policies. The policies themselves should be updated regularly as well **[2]**.

There are five essential elements of a security policy:

- ✓ Purpose
- ✓ Range
- ✓ Target
- ✓ Control of rights
- ✓ Awareness on information technology security

I will define the management levels in a sample organization before designing and implementing security policies.

Table 2: Levels of management in organization

Levels	Components
Top	The board of directors, president, vice-president and CEO (run the organization, give and approval all issues)
Middle	General managers, branch managers and department managers (responsible before senior management for functions for each department)
Low	Supervisors, section leads and foremen (management focus on controlling and directing)
Ordinary	Staff (implementation of the above issues given or proposed ideas wait approval)

Table 3: Security policy for an organization

Policy category	***Component***	***Compulsory***	***Optional***
1. Acceptable use policy	1.1. Computer access control	1.1.1. Use ID / tokens or passwords to access to the IT system	1.1.7. Don't use someone else's user ID and password to access organization's IT systems
		1.1.2. Don't allow anyone else to use ID/token or password on any IT system	
		1.1.3. Log out of a user account at any time on a computer that is not monitored and unlocked	1.1.8. Don't to password unprotected
		1.1.4. Don't attempt to access unauthorized data	
		1.1.5. Don't connect any non-authorized device to the network or IT system	1.1.9. Don't perform any authorized changes to organization's IT systems or information
		1.1.6. Don't provide, transfer data or software to any outside person / organization when not permission	
	1.2. Internet and email conditions of use	1.2.1. Use of organization's internet and email is intended for business use	1.2.5. Don't place any information on the internet related to the organization or express any opinion about it, unless specifically authorized to do so.
		1.2.2. Don't use the internet or email for personal purposes	
		1.2.3. Don't connect devices to the internet using non-standard	1.2.6. Don't store organization

		connections	data on unauthorized devices
		1.2.4. Don't download any software from the internet without prior approval of the IT department	
	1.3. Software	1.3.1. Use only software that is authorized by organization's computers	1.3.3. Don't store personal files on organization's IT equipment
		1.3.2. All software on organization's computers must be approved and installed by the organization's IT department	
	1.4. Viruses	1.4.1. To detect and remove any virus automatically, all PCs have antivirus software installed	1.4.4. Use virus detection software and virus kill software installation recommended by IT department
		1.4.2. Don't remove or disable anti-virus software installed by the company	
		1.4.3. Except than by the use of approved antivirus software and procedures, don't attempt to remove virus-infected files or clean up	
2. Human resource policy	2.1. Compensation	2.1.1. Responsible for any loss about assets caused by themselves	2.1.2. Don't touch anything when destruction or damage is caused to identify the responsibility
	2.2. Time	2.2.1. Provide report for the reasons when login to the organization's IT system in the	2.2.3. Attempt to go to work on the working time to not meet any issues about issues access assets

		holidays or vacation	overtime
		2.2.2. Provide report for the reasons why login to the organization's IT system outside the standard working time	
3. Password management policy	3.1. General	3.1.1. Accounts with access to the organization must have a unique password from all other accounts held by that users	3.1.3. Change password every 3 months
		3.1.2. Don't insert passwords into email messages or other forms of electronic communication	
	3.2. Guidelines	3.2.1. Don't set password same as the user ID	
		3.2.2. Not be transmitted plaintext outside the secure location	
		3.2.3. Set password has minimum length of eight characters on all systems	
	3.3. Protection standard	3.3.1. Don't share passwords with anyone	3.3.5. Don't talk about a password in front of others
		3.3.2. Don't use the remember password feature of applications	
		3.3.3. Don't write passwords and store it anywhere in your office	3.3.5. Don't hint at the format of a password or anything related to password
		3.3.4. Don't store passwords in files on any computer system	

		when unencrypted yet	
4. Privacy policy	4.1. General	4.1.1. What the organization is doing with personal information from users before collecting information will be clearly revealed	4.1.4. Respect users' choice of the information they choose to provide
		4.1.2. Company will collect abilities such as view, update or request the removal of personal data	
		4.1.3. Entirely responsible for the accuracy and security of the collected personal information	
5. Disposal and destruction policy	5.1. General	5.1.1. Dispose assets when it is no longer necessary for business use provided that the disposal does not conflict with data retention policies our customers or any of regulatory obligations	5.1.3. May not be donated or sold storage media in laptop
		5.1.2. Do not use an USB driver or external backup program like a CD / ROM driver to store confidential information	5.1.4. Clean all organizational media storage equipment regularly

Table 4: Security policy for an organization responsibility matrix

Category	Policy	Top-level	Middle-level	Low-level	Ordinary-staff
1.1.	1.1.1.	☐	☐	☐	☐
	1.1.2.	☐	☐	☐	☐
	1.1.3.	☐	☐	☐	☐
	1.1.4.	☐	☐	☐	☐
	1.1.5.	☐	☐	☐	☐
	1.1.6.	☐	☐	☐	☐
	1.1.7.	☐	☐	☐	☐
	1.1.8.	☐	☐	☐	☐
	1.1.9.	☐	☐	☐	☐
1.2.	1.2.1.	☐	☐	☐	☐
	1.2.2.	☐	☐	☐	☐
	1.2.3.	☐	☐	☐	☐
	1.2.4.	☐	☐	☐	☐
	1.2.5.	☐	☐	☐	☐
	1.2.6.	☐	☐	☐	☐
1.3.	1.3.1.	☐	☐	☐	☐
	1.3.2.	☐	☐	☐	☐
	1.3.3.	☐	☐	☐	☐
1.4.	1.4.1.	☐	☐	☐	☐
	1.4.2.	☐	☐	☐	☐
	1.4.3.	☐	☐	☐	☐

	1.4.4.	☐	☐	☐	☐
2.1.	2.1.1.	☐	☐	☐	☐
	2.1.2.	☐	☐	☐	☐
2.2.	2.2.1.	☐	☐	☐	☐
	2.2.2.	☐	☐	☐	☐
	2.2.3.	☐	☐	☐	☐
3.1.	3.1.1.	☐	☐	☐	☐
	3.1.2.	☐	☐	☐	☐
	3.1.3.	☐	☐	☐	☐
3.2.	3.2.1.	☐	☐	☐	☐
	3.2.2.	☐	☐	☐	☐
	3.2.3.	☐	☐	☐	☐
3.3.	3.3.1.	☐	☐	☐	☐
	3.3.2.	☐	☐	☐	☐
	3.3.3.	☐	☐	☐	☐
	3.3.4.	☐	☐	☐	☐
	3.3.5.	☐	☐	☐	☐
4.1.	4.1.1.	☐	☐	☐	☐
	4.1.2.	☐	☐	☐	☐
	4.1.3.	☐	☐	☐	☐
	4.1.4.	☐	☐	☐	☐
5.1.	5.1.1.	☐	☐	☐	☐
	5.1.2.	☐	☐	☐	☐

	5.1.3.	☐	☐	☐	☐
	5.1.4.	☐	☐	☐	☐

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

Business continuity can be defined as the ability of an organization to maintain its operations and services in the face of disruptive events. This event can be as simple as a power failure or catastrophic as a category five storm.

Business continuity planning and testing involves identifying exposure to threats, creating and recovering from preventive processes, and then to inspect them to determine if they are sufficient or not.

In short, business continuity planning and testing is designed to ensure that an organization can continue to operate (in continuous operation) under natural circumstances (floods, storms, earthquakes, etc.) or of human origin (plane crash, terrorist attack, denial of service, etc.). It can also involve planning or predetermining who will be authorized to take over in the event of the invalidity or death of key personnel.

Common technology services designed for business continuity consist of cloud data backups, cloud-based disaster recovery as a service (DRaaS) for infrastructure outages, and managed security plans that protect against increasingly sophisticated cyberattacks.

The main components of recovery plan:

- ✓ Communication plan and role assignments
- ✓ Plan for your equipment
- ✓ Data continuity system
- ✓ Backup check
- ✓ Detailed asset inventory

- ✓ Pictures of the office and equipment (before and after prep)
- ✓ Vendor communication and service restoration plan

Steps required in the disaster recovery planning process:

- ✓ Evaluate and determine potential sources of the outage
- ✓ Assess business impact
- ✓ Document the server in concise language
- ✓ Defines resources, actions, and data required to reinstate critical business processes that have been damaged or disabled because of a disaster
- ✓ Determine potential threats

Some of the policies and procedures that are required for business continuity:

- ✓ Security policy
  - General statement that dictates what security means to the organization
  - Establishes how the security program is organized
  - Describes policy's goals
  - Identifies who is responsible
  - Describes strategic value of the policy
- ✓ Human resources policy
  - Incident response policy - covers how to deal with a security incident after it has transpired*: Steps to establish*: Preparation, Detection, Containment, Eradication, Recovery, Follow up.

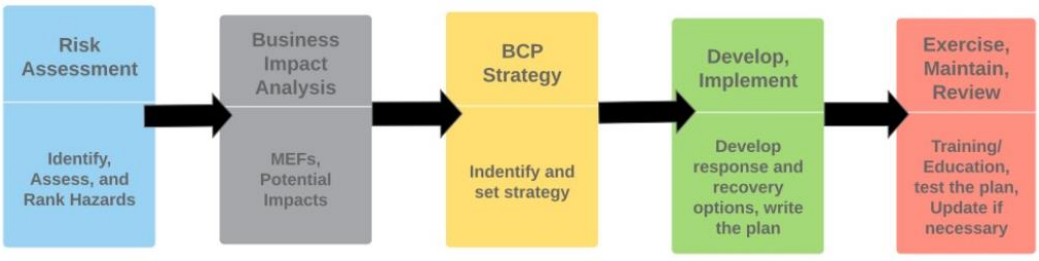

Figure 7: Policy Specifics and Procedures

Important policy considerations

The main thing to consider when developing a business continuity policy is the specific risks that an organization may face.

- For example: Is the company in an area prone to storms and other major weather events or has there been a problem caused about malwares in the past that needs special attention.

So, organizations should take all these factors into account when creating a business continuity policy.

Although business continuity policy and risk assessment are different. However, there are still similarities. Rely on these points to create a business continuity policy.

- ✓ Identify hazards
- ✓ Determine what or who may be harmed
- ✓ Assess risks and create control measures
- ✓ Record the findings
- ✓ Review and update reviews

Business impact analysis (BIA) will be followed to help form the backbone of business continuity policy. The BIA identifies the impact of a potential disaster on an organization by identifying existing gaps. Although similar to a risk assessment, BIAs usually take place first, and focus primarily on business impact to meet recovery time and recovery point targets.

Next, monitoring and verifying business continuity policy is another factor to note, if there are legal requirements to be followed. When non-compliance is found according to the policy, corporate management may be brought in to address it.

- For example: About leadership, such as a corporate executive, can be assigned as a contact person for the BC / DR team, coordinating efforts to resolve any compliance issues. The BC / DR team itself may be tasked with verifying compliance with the policy, along with any necessary internal

departments. Along with establishing processes and personnel, the BC / DR team should regularly verify policy compliance **[12]**.

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

A stakeholder is a person who has an interest in the company, information technology service or its projects. They can be the employees of the company, suppliers, vendors or any partner. They all have an interest in the organization. Stakeholders can also be an investor in the company and their actions determine the outcome of the company. Such stakeholder plays an important role in defining the future of the company as well as its day-to-day workings **[13]**.

Have two types of Stakeholders:

- Internal Stakeholders: They are a part of the management of the company and have voting powers. They are the major investors in the company and a part of the board of directors. Therefore, they have all the powers that other higher-level management have and can change the direction of the company.

- External Stakeholders: Unlike internal stakeholders, their major role is to invest or disinvest in the company. They hardly can bring any change in the company's direction. They do not take part in any internal operations or decision making of the company.

Roles of Stakeholders:

Direct the Management: the stakeholders can be a part of the board of directors, so theirs can help in taking actions. They also can take over certain departments like service, human resources or research, development and manage them for ensuring success.

They bring in money: stakeholders are the large investors of the company and they can anytime bring in or take out money from the company. Their decision shall depend upon the company's financial performance. So, they can pressurize the management for financial reports and change tactics if necessary. Some stakeholders can even increase or decrease the investment to change the share price in the market and make the conditions favorable for them.

Help in decision making: stakeholders can be part of the board of directors. So, they can take decisions along with other board members. They have the power to disrupt the decisions well. They also bring more ideas a threaten the management to obey them. The stakeholders also have all the powers to appoint senior-level management. Therefore, they are there in all the major decision-making areas. They also take decisions regarding liquidations and also acquisitions.

Corporate conscience: Large stakeholders are the major stakeholders of the company and have monitored over all the major activities of the company. They can make the company abide by human rights and environmental laws. They also monitor the outsourcing activities and may vote against any business decision if it harms the long-term goals of the company.

Other responsibilities: They can identify new areas for market penetration and increased sales or can bring in more marketing ideas. They also attract other investors for company. They can be a part of a selection board or a representative for the company. Moreover, they can take all the major social and environmental decisions.

Influence of stakeholders in proposing a security audit in an organization:

If stakeholders involved in the development of information security policy (ISP), it will help create a more balanced policy and it will apply to different stakeholders of the organization, while still identify the organization's security program. Because of the importance of ISPs to an organization and many stakeholders, they need to be involved in developing this policy. As above, if stakeholders also join in the security audit, then data will be security better. In addition, the accuracy is also advanced and their proposals are often most optimal.

D3 Evaluate the suitability of the tools used in an organizational policy

Several tools are used in organizational policy:

- ✓ User log-on profiles to limit user access to resources
- ✓ Online software to train and update staff
- ✓ Auditing tools to monitor resource access

- ✓ Penetration testing
- ✓ Gathering and recording information on security
- ✓ Initiating suitable actions for remediation

Almost all policies both use support tools. These tools must conform to all organizational policy's requirements. However, to know whether these tools are suitable or not, we need to perform the following steps:

- ✓ Learn about organization and staff
- ✓ Assess and build digital knowledge
- ✓ Review the organization's current use of digital tools
- ✓ Identify tools that can help organize more effectively, saving you time and money
- ✓ Identify tools that can increase an organization's effectiveness
- ✓ Evaluate available resources and find opportunities to take advantage of new resources

With the increasing complexity of businesses, the number of policies and procedures is also becoming more complex. This is driven by the requirements of policy management tools. Therefore, organizations are now moving towards the IT system architecture to building a powerful system for policy management. Keeping a document on paper is tedious work and cannot analyze them as a whole. Therefore, businesses are establishing an online policy and contract management system.

However, the biggest challenge in moving to a cloud-based system is finding the right software tool for businesses. Since many factors are considered before finalizing one of the platforms, here are some of the most important considerations to keep in mind while selecting the best tool for the business.

The ability to handle specific requirements: while many general-purpose tools are available in different fields, it is important to choose the one that best suits industry requirements. The tools will not be effective to contribute to business growth. Each field is unique with different challenges. It is important that the tool

is integrated with the current policy management system, not vice versa. The system needs to ensure a customized compliance service with an excellent level of service to make everyday compliance easier. The general policy management tool will not provide a high service to a financial company that handles dynamic policies depending on financial market conditions.

Brand-value products: with popular brands serving different industries, many organizations tend to rely heavily on big brands for their success. However, it is important that the success in organizations and which product will help achieve goals. Objectively evaluate product options with little brand focus. This will help choose the tools that are best suited for organizations. Thorough research along with quantitative evaluation parameters will facilitate the process.

After sales support: Implementing a policy management tool into the business system should not be in a hurry. The systematic implementation will waste the organization's extra time and resources to synchronize business processes. With these inherently complex tools after training and sales support is a very important factor. Software vendors should provide quick deployment along with good after-sales support at minimal additional cost. Understand the utility of a product into the system instead of the features of the tool.

Commitment to the tool: users will be required to train on this tool and it is very likely that organization will spend a lot of time to set up the system. It is in the after-sales support process that you know your supplier well. Make sure your employees feel comfortable using the product. This investment is huge, so make sure you get the maximum output from it in the long run. Showing a high commitment to the tool and the tool will yield great results.

Conclusion

Through this report, I have fulfilled all the criteria of each section, which have been marked as specific above, each section has been arranged in a certain order, thereby bringing the most intuitive look. Any questions please contact me via: huyenttdgdd18606@fpt.edu.vn

Evaluation

The information contained in the report and the research results is reliable because it is referenced from books, lecture slides and reputable websites. Besides, there are still some content that is evaluated in my opinion, it is viewed from an objective perspective and my level of understanding so there will be some not quite accurate.

References:

[1] Mark Ciampa, Ph, D., 2018. *Security+ Guide To Network Security Fundamentals*. 6th ed. [ebook] Available at : < https://www.amazon.com/CompTIA-Security-Guide-Network-Fundamentals/dp/1337288780 > [Accessed 12 May 2020].

[2] Techopedia.com. 2017. *What Is Security Policy? - Definition From Techopedia*. [online] Available at: <https://www.techopedia.com/definition/4099/security-policy> [Accessed 14 May 2020].

[3] Rouse, M., 2019. *What Is Data Protection And Why Is It Important? Definition From Whatis.Com*. [online] SearchDataBackup. Available at: <https://searchdatabackup.techtarget.com/definition/data-protection> [Accessed 15 May 2020].

[4] Jorna, M., 2017. *Three Steps To Data Protection*. [online] B2b.com. Available at: <http://www.b2b.com/three-steps-to-data-protection> [Accessed 15 May 2020].

[5] i-SCOOP. 2020. *Personal Data Processing Principles: 9 GDPR Processing Principles*. [online] Available at: <https://www.i-scoop.eu/gdpr/gdpr-personal-data-processing-principles/> [Accessed 15 May 2020].

[6] General Data Protection Regulation (GDPR). 2020. *Art. 5 GDPR – Principles Relating To Processing Of Personal Data | General Data Protection Regulation (GDPR)*. [online] Available at: <https://gdpr-info.eu/art-5-gdpr/> [Accessed 15 May 2020].

[7] Peterson, O., 2019. *What Is ISO 31000? Getting Started With Risk Management | Process Street | Checklist, Workflow And SOP Software*. [online] Process Street. Available at: <https://www.process.st/iso-31000/> [Accessed 15 May 2020].

[8] LACHAPELLE, E., ALIU, F. and EMINI, E., 2018. *ISO 31000:2018-RISK MANAGEMENT GUIDELINES*. [online] Pecb.com. Available at: <https://pecb.com/whitepaper/iso-310002018-risk-management-guidelines> [Accessed 15 May 2020].

[9] National Research Council (U.S.). Committee for Oversight and Assessment (U.S). Department of Energy Project Management. Division on Engineering and Physical Sciences., 2005. *The Owner's Role In Project Risk Management*. [ebook] Washington, DC : National Academies Press, ©2005. Available at: <https://www.nap.edu/read/11183/chapter/4> [Accessed 15 May 2020].

[10] PETTERS, J., 2020. What Is An IT Security Audit? The Basics | Varonis. [online] Inside Out Security. Available at: <https://www.varonis.com/blog/security-audit/> [Accessed 15 May 2020].

[11] PATTERSON, J., 2017. *How IT Security Audit Benefits Your Business Process*. [online] transcosmos. Available at: <http://transcosmos.co.uk/blog/it-security-audit-business-process/> [Accessed 15 May 2020].

[12] Rouse, M., 2019. *What Is Business Continuity Policy? - Definition From Whatis.Com*. [online] SearchDisasterRecovery. Available at: <https://searchdisasterrecovery.techtarget.com/definition/business-continuity-policy> [Accessed 15 May 2020].

[13] Compliance Prime Blog. 2020. *Role Of Stakeholders In Business Organization - Compliance Prime Blog*. [online] Available at: <https://www.complianceprime.com/blog/2019/10/17/role-of-stakeholders-in-business-organization/> [Accessed 15 May 2020].