SECURITY

Assignment:- 2

**Contents**

[RISK ASSESSMENT 3](#_Toc55120873)

[RISK ASSESSMENT PROCEDURE AND METHODS 3](#_Toc55120874)

[DEFINE YOUR RISK ASSESSMENT METHODOLGY 3](#_Toc55120875)

[COMPILE A LIST OF YOUR INFORMATION ASSETS 3](#_Toc55120876)

[IDENTIFY THREATS AND VULNERABILITIES 3](#_Toc55120877)

[EVALUATE RISK 4](#_Toc55120878)

[MITIGATE THE RISK 4](#_Toc55120879)

[COMPILE RISK REPORTS 4](#_Toc55120880)

[REVIEW MONITOR AND AUDIT 4](#_Toc55120881)

[ISO 27005 5](#_Toc55120882)

[INFORMATION SECURITY RISK MANAGEMENT 5](#_Toc55120883)

[ISO 27005 RISK MANAGEMENT PROCESS 5](#_Toc55120884)

[CONTEXT ESTABLISHMENT 6](#_Toc55120885)

[RISK ASSESSMENT 6](#_Toc55120886)

[RISK TREATMENT 6](#_Toc55120887)

[RISK ACCEPTANCE 6](#_Toc55120888)

[RISK COMMUNICATION 6](#_Toc55120889)

[RISK MONITORING AND REVIEW 6](#_Toc55120890)

[DATA PROTECTION 7](#_Toc55120891)

[PURPOSE OF DATA PROTECTION 7](#_Toc55120892)

[DATA SECURITY PROCESSES APPLICABLE TO AN ORGANIZATION 7](#_Toc55120893)

[TRAIN YOUR WORKFORCE 7](#_Toc55120894)

[EMBRACE A DATA CENTRIC SECURITY STRATEGY 7](#_Toc55120895)

[IMPLEMENT MULTI FACTOR AUTHENTICATION (MFA) 7](#_Toc55120896)

[SET STRICT PERMISSIONS FOR THE CLOUD 7](#_Toc55120897)

[EXERCISE VIGILANCE FOR PATCH MANAGEMENT 8](#_Toc55120898)

[ISO 31000 8](#_Toc55120899)

[IT SECURITY AUDIT 9](#_Toc55120900)

[IMPORTANT OF SECURITY AUDIT 9](#_Toc55120901)

[AUDIT WORKFLOW 9](#_Toc55120902)

[DEFINE ASSESSMENT CRITERIA 9](#_Toc55120903)

[PREPARE THE SECURITY AUDIT 9](#_Toc55120904)

[CONDUCT THE SECURITY AUDIT 9](#_Toc55120905)

[COMPLETE AND SHARE THE RESULTS 9](#_Toc55120906)

[TYPES OF IT SECURITY AUDITS 10](#_Toc55120907)

[ONE TIME ASSESSMENT 10](#_Toc55120908)

[TOLLGATE ASSESSMENT 10](#_Toc55120909)

[PORTFOLIO ASSESSMENT 10](#_Toc55120910)

[THE RESPONSIBILITIES OF EMPLOYEES AND STAKEHOLDERS IN RELATION TO SECURITY 11](#_Toc55120911)

[GENERAL RESPONSIBILITY FOR SECURITY 11](#_Toc55120912)

[RESPONSIBILITIES OF SENIOR MANAGER 11](#_Toc55120913)

[RESPONSIBILITIES OF MANAGER 11](#_Toc55120914)

[RESPONSIBILITIES OF EMPLOYEES 11](#_Toc55120915)

[RESPONSIBILITIES OF PARTNER 11](#_Toc55120916)

[DATA PROTECTION 12](#_Toc55120917)

[DATA PROTECTION METHODS 12](#_Toc55120918)

[RISK ASSESSMENT 12](#_Toc55120919)

[BACKUP 12](#_Toc55120920)

[ENCRYPTION 12](#_Toc55120921)

[PSEUDONYMISATION 13](#_Toc55120922)

[ACCESS CONTROL 13](#_Toc55120923)

[DISTRUSTION 13](#_Toc55120924)

[WHY HAVE A SECURITY POLICY 14](#_Toc55120925)

[WHAT IS A SECURITY POLICY 14](#_Toc55120926)

[GETTING STARTED 14](#_Toc55120927)

[RISK ANALYSIS (IDENTIFYING THE ASSETS) 15](#_Toc55120928)

[RISK MANAGEMENT (IDENTIFYING THE THREATS) 15](#_Toc55120929)

[PHYSICAL/DESKTOP SECURITY 15](#_Toc55120930)

[INTERNET THREATS 16](#_Toc55120931)

[RECEVING THE SECURITY POLICY 16](#_Toc55120932)

[THE IMPLEMENT OF THE POLICY 17](#_Toc55120933)

[CONCLUSION 17](#_Toc55120934)

[IT SECURITY CAN BE ASSOCIATE WITH ORGANIZATION POLICY 18](#_Toc55120935)

[PASSWORD/PIN POLICY 18](#_Toc55120936)

[DEVICE CONTROLS 18](#_Toc55120937)

[INTERNET/WEB USAGE 18](#_Toc55120938)

[ENCRYPT AND PHYSICAL SECURITY 18](#_Toc55120939)

[SECURITY POLICY REPORTING REQUIREMENTS 19](#_Toc55120940)

[EMPOWER YOUR TEAM 19](#_Toc55120941)

[DESIGN AND IMPLEMENT A SECURITY POLICY FOR eBay ORGANIZATION 20](#_Toc55120942)

[MEASURES TO ENSURE SECURITY 20](#_Toc55120943)

[SECURITY PROTOCOLS IN INTERNET 21](#_Toc55120944)

[SECURE SOCKET LAYER (SSL) 21](#_Toc55120945)

[SECURE HYPERTEXT TRANSFER PROTOCOL (SHTTP) 21](#_Toc55120946)

[SECURE ELECTRONIC TRANSACTION 21](#_Toc55120947)

[RESPONSIBILITIES OF EMPLOYEES AND STAKEHOLDERS IN RELATION TO SECURITY 22](#_Toc55120948)

[ROLES OF STAKHOLDERS IN THE ORGANIZATION TO IMPLEMENT SECURITY AUDIT RECOMMENDATIONS 22](#_Toc55120949)

[REFERANCE 24](#_Toc55120950)

**PART 1:-**

**PART 1.1:-**

# RISK ASSESSMENT

In the context information risk management a risk assessment helps organizations assess and manage incidents that have the potential to cause harm to your sensitive data.

The process involves identifying hazards whether they are vulnerabilities that a cyber criminals could exploit or mistakes that employees could make.

You then determine the level of risk they present and decide on the best course of action to prevent them from happening.

# RISK ASSESSMENT PROCEDURE AND METHODS

## DEFINE YOUR RISK ASSESSMENT METHODOLGY

You should tailor your approach to the needs of your organization. To do this you need to review certain things. First you should look at your organization’s context.

This consists of your legal regulatory and contractual your objectives both concerning information security and business more widely and the needs and expectations of its stakeholders.

Next you should look at the risk criteria. This is an agreed way of measuring risks usually according to the impact they will cause and the likelihood of them occurring. These need to be clearly defined and widely understood.

Finally you need to determine your risk acceptance criteria. You can’t eradicate every risk you face so you must decide the level of residual risk you are willing to leave unaddressed.

## COMPILE A LIST OF YOUR INFORMATION ASSETS

ISO 27001 gives organizations the choice of evaluating through an asset based approach.

Although each have their pros and cons I generally recommend taking an asset based approach in part because you can you can work from an existing list of information assets.

This includes hard copies information electronic files removable media mobile devices and intangibles such as intellectual property.

## IDENTIFY THREATS AND VULNERABILITIES

Once you have created your list of information assets it’s time to determine the risk associated with them.

For Example when analyzing work issued laptops one of the risks you highlight will be the possibility of them being stolen. Another will be that when in a public place employees might use an insecure internet connection or someone might see sensitive information on their screen.

## EVALUATE RISK

Some risks are more sever then others so at this stage you need to determine which ones you need to be most concerned about.

This is where your risk criteria come in handy. It provides a guide that helps you compare risks by assigning a score to the likelihood of it occurring and the damage it will cause.

By evaluating the risks in this way you get a consistent and comparable assessment of the threats your organizations face.

## MITIGATE THE RISK

There are four ways organizations threat risks.

* **Modify the risk** by applying security controls that will reduce the likelihood of it occurring and damage it will cause.
* **Retain the risk** accept that it falls within previously established risk acceptance criteria or via extraordinary decisions.
* **Avoid the risk** by changing the circumstances that are causing it.
* **Share the risk** with a partner such as an insurance firm or a third party that is batter equipped to manage the risk.

## COMPILE RISK REPORTS

Documentation process which is necessary for audit and certification purposes.

The most important documents are the RTP (risk treatment plan) which documents the decisions you’ve made regarding risk treatment and the SoA (Statement of Applicability).

Clause 6.1.3 of the standard states an SoA must:

* Identify which controls an organization has selected to tackle identified risks.
* Explain why these have been selected.
* State whether or not the organization has implemented the controls and.
* Explain why any controls have been omitted.

Every controls should have its own entry and cases where the control has been selected the SoA should link to relevant documentation about implementation.

## REVIEW MONITOR AND AUDIT

ISO 27001 requires your organization to continually review update and improve the ISMS to make sure it is working as its intended.

You will need to repeat the assessment process annually to make sure you’ve accounted for changes in the way your organization operates and for the changing threat environment.

You should also use the opportunity to look for ways in which your ISMS can be improved. This might involve using a different control to address a risk or by switching to different risk treatment option altogether.

**PART 1.2:-**

# ISO 27005

ISO 27005 is the international standards that describes how to conduct an information security risk assessment in accordance with the requirements of ISO 27001.

Risk assessment are one of the most important parts of an organization ISO 27001 compliance project. ISO 27001 requires you to demonstrate evidence of information security risk management risk actions taken and how relevant controls from annex a have been applied.

ISO 27005 is applicable to all organization regardless of size or selector. It supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

# INFORMATION SECURITY RISK MANAGEMENT

Information security risk management is integral to information security management. It defines the process of analyzing what could happen and what the consequences might be and helps organization determine what should be done and when to reduce risk to an acceptable level. Information security risk management should be a continual process that contributes to.

* Identifying and assessing risk.
* Understanding risk likelihood and the consequences for the business.
* Establishing a priority order for risk treatment.
* Stakeholder involvement in risk management decisions.
* The effectiveness of risk treatment monitoring. And
* Staff awareness of risks and the actions being taken to mitigate them.

Organization should adopt a systematic approach to information security risk to accurately determine their information security needs.

# ISO 27005 RISK MANAGEMENT PROCESS

Although ISO 27005 does not specify any specific risk management methodology it does imply a continual information risk management process based on six key components.

1. Context establishment
2. Risk assessment
3. Risk treatment
4. Risk acceptance
5. Risk communication
6. Risk monitoring and review

Figure 1 Risk Management Process

## CONTEXT ESTABLISHMENT

This risk management context sets the criteria for how risks are identified who is responsible for risk ownership how risk impact the confidentiality integrity and availability of the information and how risk impact and likelihood are calculated.

## RISK ASSESSMENT

Many organization choose to follow an asset based risk assessment process comprising five key stages.

* Compiling information assets.
* Identifying the threats and vulnerabilities applicable to each asset.
* Assigning impact and likelihood values based on risk criteria.
* Evaluating each risk against predetermined levels of acceptability.
* Prioritizing which risks need to be addressed and in which order.

## RISK TREATMENT

There are fore ways to treat a risk.

* Avoid the risk by eliminating it entirely.
* Modify the risk by applying security controls.
* Share the risk with a third party (through insurance or outsourcing).
* Retain the risk (if the risk falls within established risk acceptance criteria).

## RISK ACCEPTANCE

Organization should determine their own criteria for risk acceptance that consider existing policies goals objectives and shareholders interests.

## RISK COMMUNICATION

Effective communication is pivotal to the information security risk management process. It ensures that those responsible for implementing risk management understand the basis on which decisions are made, and why certain actions are required. Sharing and exchanging information about risk also facilitates agreement between decision makers and other stakeholders on how to manage risk.

## RISK MONITORING AND REVIEW

Risks are not static and can change abruptly. Therefore, they should be continually monitored in order to quickly identify changes and maintain a complete overview of the risk picture.

Organizations should also keep a close eye on.

* Any new assets included within the risk management scope.
* Asset values that require modification in response to changing business requirements.
* New threats, whether external or internal, that have yet to be assessed; and
* Information security incidents.

# DATA PROTECTION

Data protection is the process of safeguarding important information from corruption, compromise or loss.

The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates. There is also little tolerance for downtime that can make it impossible to access important information.

Consequently, a large part of a data protection strategy is ensuring that data can be restored quickly after any corruption or loss.

# PURPOSE OF DATA PROTECTION

Storage technologies that can be used to protect data include a disk or tape backup that copies designated information to a disk-based storage array or a tape cartridge device so it can be safely stored. Mirroring can be used to create an exact replica of a website or files so they're available from more than one place. Storage snapshots can automatically generate a set of pointers to information stored on tape or disk, enabling faster data recovery, while continuous data protection (CDP) backs up all the data in an enterprise whenever a change is made.

# DATA SECURITY PROCESSES APPLICABLE TO AN ORGANIZATION

Each year on January 28, the United States, Canada, Israel and 47 European countries observe Data Privacy Day. The purpose of Data Privacy Day is to inspire dialogue on the importance of online privacy. These discussions also seek to inspire individuals and businesses to take action in an effort to respect privacy, safeguard data and enable trust.

## TRAIN YOUR WORKFORCE

Organizations can use a security awareness training program to educate their employees about the importance of data security.

## EMBRACE A DATA CENTRIC SECURITY STRATEGY

organizations should protect their data by doing encryption the right way. They should also look to the Center for Internet Security’s Control Data Recovery Capabilities. As part of their implementation of this Control, organizations should develop a robust data backup strategy and test that strategy and their backups often.

## IMPLEMENT MULTI FACTOR AUTHENTICATION (MFA)

Internet Security’s Control Controlled Use of Administrative Privileges and using multi-factor authentication (MFA) for all administrative account access. They should also encourage users to implement MFA across their personal web accounts.

## SET STRICT PERMISSIONS FOR THE CLOUD

As they increasingly migrate their workloads to the cloud, organizations need to lock down their cloud-based data.

## EXERCISE VIGILANCE FOR PATCH MANAGEMENT

Finally, organizations can strengthen the security of their data by patching vulnerabilities through which malicious actors could gain access to their network assets.

Indeed, they need to follow up a patch’s deployment by scanning their system to confirm that the vulnerability is no longer present. This step will reveal if the patch has addressed the vulnerable components and if organizations need to take additional measures to remediate the vulnerability.

# ISO 31000

ISO 31000, Risk management Guidelines, provides principles, a framework and a process for managing risk.

Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

**PART 1.3:-**

# IT SECURITY AUDIT

A security audit is the high-level description of the many ways organizations can test and assess their overall security posture, including cybersecurity.

# IMPORTANT OF SECURITY AUDIT

If you keep track of cybersecurity news even a little bit, you should have an intuitive understanding of why audits are important.

Here are some more specific benefits to running audits.

* Verify that your current security strategy is adequate or not.
* Check that your security training efforts are moving the needle from one audit to the next.
* Reduce cost by shutting down or repurposing extraneous hardware and software that you uncover during the audit.
* Security audit uncover vulnerabilities introduced into your organization by new technology or processes.
* Prove the organization is compliant with regulations – HIPAA, SHIELD, CCPA, GDPR, etc.
* Uncover flaws introduced by new technology or processes.

# AUDIT WORKFLOW

## DEFINE ASSESSMENT CRITERIA

* Determine the overall goals to be addressed in the audit.
* Break those objectives down to department priorities.
* Agree on how the audit will be performed and tracked

## PREPARE THE SECURITY AUDIT

* Prioritize your success criteria and business objectives.
* Select the required tools and methodologies to meet goals.
* Find or create a method to gather the correct data.

## CONDUCT THE SECURITY AUDIT

* Take care to provide appropriate documentation.
* Monitor audit progress and data points for accuracy.
* Use previous audits and new info to deep dive into findings.

## COMPLETE AND SHARE THE RESULTS

* Share results with all previously determined parties.
* Create a list of action items based on the audit findings.
* Prioritize fixes to remediate the security items discovered.

# TYPES OF IT SECURITY AUDITS

## ONE TIME ASSESSMENT

One-time assessments are security audits that you perform for ad-hoc or special circumstances and triggers in your operation. For example, if you are going to introduce a new software platform you have a battery of tests and audits that you run to discover any new risk you are introducing into your shop.

## TOLLGATE ASSESSMENT

Tollgate assessments are security audits with a binary outcome. It’s a go or no-go audit to determine a new process or procedure can be introduced into your environment. You aren’t determining risk as much as looking for showstoppers that will prevent you from moving forward.

## PORTFOLIO ASSESSMENT

Portfolio security audits are the annual, bi-annual, or (enter your requirements here) regularly scheduled audit. Use these audits to verify that your security processes and procedures are being followed and that they are adequate for the current business climate and needs.

**PART 1.4:-**

# THE RESPONSIBILITIES OF EMPLOYEES AND STAKEHOLDERS IN RELATION TO SECURITY

## GENERAL RESPONSIBILITY FOR SECURITY

IT staff responsible for security, but everyone in an organization is responsible for security. Everyone needs to follow the security policies that the organization has set out not to contravene regulations to protect the best data. All data access rights require permission. And everyone will be responsible for each part separately. All employees play a key role and are strengthened by strong governance and supervision. For example: they are not allowed to download the software without permission. It is not allowed to turn off the fire during use. They are not allowed to use USB to copy data. This will give hackers the opportunity to attack the organization's security system.

## RESPONSIBILITIES OF SENIOR MANAGER

They are moderators, acceptors, and certifiers for the principles of the law that are enacted. They will make commitments on confidentiality and ensure that policy commitments are brought into the company and communicated to all employees, partners, enforcing the validity of those commitments enforced. Without the approval of senior management, all commitments, policy and decisions about information security become meaningless.

## RESPONSIBILITIES OF MANAGER

The manager plays a role of overseeing and managing his employees. Therefore, the manager must understand the role of information security to the benefits and development of the company and if they do not know. The process of information control will be difficult and inefficient, which will impede the process of company development, and managers must understand how companies use information to accomplish business goals.

## RESPONSIBILITIES OF EMPLOYEES

Employees is the one who knows best about how to use company information. So the IT manager should listen to the employee's comments about the security process of their company. They are responsible for complying with the company's privacy policies. Security policies are communicated to them by managers. If there is a security problem. They are the one who reports to the manager to find a way to fix it.

## RESPONSIBILITIES OF PARTNER

The parties involved in the company such as contractors, suppliers, publishers... also need to have roles and responsibilities regarding the confidentiality of the company's information, they are not allowed to break the requirements of information security, provide information to others without the company's permission. Information security requirements force all everyone to follow the contract.

**PART 1.5:-**

# DATA PROTECTION

Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes.

# DATA PROTECTION METHODS

## RISK ASSESSMENT

The riskier the data, the more protection it has to be afforded. Sensitive data should be closely guarded, whereas low-risk data can be afforded less protection. The major reason for these assessments is the cost benefit, as better data security equals greater expense. However, it is a good test to determine what data needs to be guarded more closely and makes the whole data processing system more efficient.

There are two axes upon which your risk assessment should be based: the potential severity in case of a data breach and the probability of a breach. The higher the risk on each of these axes, the more sensitive the data is. These assessments will often require the assistance of a data protection officer (privacy officer) who will help you establish valid ground rules. Avoid doing it on your own unless you are absolutely certain you know what you are doing. Mischaracterized data, if lost, could prove disastrous.

## BACKUP

Backups are a method of preventing data loss that can often occur either due to user error or technical malfunction. Backups should be regularly made and updated. Regular backups will impose an additional cost to your company, but potential interruptions to your normal business operations will cost even more. Time is money!

Backups should be performed in accordance with the principle explained above data of low-importance does not have to be backed up as often, but sensitive data does. Such backups should be stored in a safe place, and possibly encrypted. Never store sensitive data in the cloud. Periodically check storage media for deterioration, as per the manufacturer guidelines, and make sure to store them according to official recommendations (check for humidity, temperature, etc.)

Tape-storage methods are still a cheaper option (by two-thirds) compared to hard disks. However, hard drives are more versatile and better-suited to small scale operations. Data access is also much faster with disk-storage methods.

## ENCRYPTION

High risk data is the prime candidate for encryption every step on the way. This includes during acquisition (online cryptographic protocols), processing (full memory encryption) and subsequent storage (RSA or AES). Well-encrypted data is inherently safe; even in cases of a data breach, the data will be useless and irrecoverable to attackers.

For that reason, encryption is even explicitly mentioned as a method of data protection in the GDPR, meaning its proper use will certainly bring you favors in the eyes of the regulators. For example, if you experience a breach that affects encrypted data, you do not even have to report it to the supervisory authorities, since the data is considered adequately protected! For this reason alone, you should consider encryption as your #1 data security method.

## PSEUDONYMISATION

Pseudonymisation is another method advocated in the GDPR that increases data security and privacy of the individuals. It works well with larger sets of data, and consists of stripping identifying information from snippets of data. For example, you replace the names of persons with randomly generated strings. The identity of a person and data they supplied therefore become impossible to link together.

You are still left with somewhat useful data, but it does not contain sensitive identifiable information anymore. Since people cannot be directly identified from pseudonymised data, the procedures in the case of a data breach or loss are much simpler and the risks are greatly reduced. The GDPR recognizes this and the notification requirements have been significantly relaxed in case of pseudonymised data breaches.

Pseudonymisation is also a must when performing scientific or statistical research, so institutions and schools should be well-versed in properly pseudonym sing their data.

## ACCESS CONTROL

The introduction of access controls to your company’s workflow is a very efficient risk reduction method. The fewer people have access to the data, the lesser the risk of (inadvertent) data breach or loss.

You should ensure that you give access to sensitive data only to trustworthy employees who have a valid reason to access it. We recommend you hold regular prior data handling education courses and refreshers, especially after hiring new employees.

With help of your data protection officer, draft a clear and concise data protection policy outlining the methods, roles and responsibilities of each employee (or a group of employees).

## DISTRUSTION

There may come a time where the data you have will need to be destroyed. Data destruction might not seem like a protection method at a first glance, but in fact it is. The data is being protected this way against unauthorized recovery and access. Under the GDPR, you have the obligation to delete the data you don’t need, and sensitive data warrants more comprehensive methods of destruction.

Hard disks are most often destroyed using degaussing, whereas paper documents, CDs and tape drives are shredded into tiny pieces. On-site data destruction is recommended for sensitive data. Encrypted data can easily be deleted simply by destroying the decryption keys, guaranteeing the data will be unreadable… for at least the next few decades, after which it will likely become obsolete anyway.

# WHY HAVE A SECURITY POLICY

As building a good security policy provides the foundations for the successful implementation of security related projects in the future, this is without a doubt the first measure that must be taken to reduce the risk of unacceptable use of any of the company's information resources.

The first step towards enhancing a company's security is the introduction of a precise yet enforceable security policy, informing staff on the various aspects of their responsibilities, general use of company resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

The development (and the proper implementation) of a security policy is highly beneficial as it will not only turn all of your staff into participants in the company's effort to secure its communications but also help reduce the risk of a potential security breach through "human factor" mistakes. These are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other dangerous activities.

Additionally the building process of a security policy will also help define a company's critical assets, the ways they must be protected and will also serve as a centralized document, as far as protecting Information Security Assets is concerned.

# WHAT IS A SECURITY POLICY

The security policy is basically a plan, outlining what the company's critical assets are, and how they must (and can) be protected. Its main purpose is to provide staff with a brief overview of the "acceptable use" of any of the Information Assets, as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the company's critical systems.

The document acts as a "must read" source of information for everyone using in any way systems and resources defined as potential targets. A good and well developed security policy should address some of these following elements:

* How sensitive information must be handled.
* How to properly maintain your ID(s) and password(s), as well as any other accounting data.
* How to respond to a potential security incident, intrusion attempt, etc.
* How to use workstations and Internet connectivity in a secure manner.
* How to properly use the e-mail system.

# GETTING STARTED

provide you with possible strategies and some recommendations for the process of creating a security policy, and to give you a basic plan of approach while building the policy framework.

The start procedure for building a security policy requires a complete exploration of the company network, as well as every other critical asset, so that the appropriate measures can be effectively implemented. Everything starts with identifying the company's critical informational resources, a subject that is discussed in depth.

# RISK ANALYSIS (IDENTIFYING THE ASSETS)

As in any other sensitive procedure, Risk Analysis and Risk Management play an essential role in the proper functionality of the process. Risk Analysis is the process of identifying the critical information assets of the company and their use and functionality an important (key) process that needs to be taken very seriously. Essentially, it is the very process of defining exactly WHAT you are trying to protect, from WHOM you are trying to protect it and most importantly, HOW you are going to protect it.

In order to be able to conduct a successful Risk Analysis, you need to get well acquainted with the ways a company operates; if applicable, the ways of working and certain business procedures, which information resources are more important than others (prioritizing), and identifying the devices / procedures that could lead to a possible security problem.

A basic approach would be:

* Identify what you’re trying to protect.
* Look at whom you’re trying protect it from.
* Define what the potential risks are to any of your information assets.
* Consider monitoring the process continually in order to be up to date with the latest security weaknesses.

# RISK MANAGEMENT (IDENTIFYING THE THREATS)

Conducted on the company's information assets, you should now be able to properly manage all the threats posed by each of your resources guide you through the creation of a list outlining various potential threats, something that should also be included in the formal security policy.

## PHYSICAL/DESKTOP SECURITY

System Access: best practices for password creation, passwords aging, minimum password length, characters to be included while choosing passwords, password maintenance, tips for safeguarding(any) accounting data; the dangers to each of these issues must be explained in the security awareness program;

Virus Protection: best practices for malicious code protection, how often the system should be scanned, how often, if not automatically, should Live Update of the software database be done, tips for protection against (any) malicious code(viruses/Trojans/worms);

Software Installation: is freeware software forbidden, if allowed, under what conditions, how is software piracy tolerated, are entertainment/games allowed or completely prohibited as well the installation of any other program coming from unknown and untrustworthy sources;

Removable Media(CD's, floppy): "Acceptable Use" measures (perhaps by way of a AUP - Acceptable Use Policy) need to be established, the dangers of potential malicious code entering the company network or any other critical system need to be explained as well;

Encryption: explain when, how and who must encrypt any of the company's data;

System Backups: the advantage of having backups needs to be explained; who is responsible, and how often should the data be backed up;

Maintenance: the risks of a potential physical security breach need to be briefly explained;

Incident Handling: define what a suspicious event is, to whom it needs to be reported, and what further steps need to be taken;

## INTERNET THREATS

Web Browsing: define what constitutes restricted, forbidden and potentially malicious web sites, provide staff members with brief, and well summarized tips for safer browsing, additionally let them know that their Internet usage is strictly monitored in order to protect company's internal systems;

E-mail Use: define the "acceptable use" criteria of the E-mail system, what is allowed and what is not, the company policy on using the mail system for personal messages, etc. Also briefly explain the potential threats posed by (abusing) the mail system and of the potential problems as far as spreading malicious code is concerned; Instant Messaging (IM) Software (ICQ, AIM, MSN, etc.): whether it is allowed or completely forbidden, provide them with short examples of how an attacker might use these programs to penetrate and steal/corrupt/modify company data;

Downloading/Attachments: is downloading allowed or not, useful tips for safer downloading, explanation of trusted and untrustworthy sources, best practices for mail attachments if allowed, discussion of potential threats and dangers, use of virus scanners, etc

## RECEVING THE SECURITY POLICY

In order to reduce the chance of any misunderstanding, your security policy needs to fully outline the responsibilities of each and every one of your staff members. It should clearly state what needs to be protected, how the staff should protect it, and most importantly why it needs to be protected; that way they will be able to understand the importance and distinguish between critical and less critical information assets. The policy needs to be clear, concise and approximately two pages. Don't turn your security policy into a complete security awareness course; each of the elements contained in it should.

Define the purpose of the security policy from the very beginning; does it apply to the information assets of the whole company, or is just created to cover a particular division or department. It is a good idea to provide users with a better understanding of how important information security is to the company, pointing out why there is no such thing as 100% security, but that the risks can be tremendously reduced if everyone realizes that "security is everyone's responsibility".

Each of the assets needs to be precisely described to include, among others, items such as hardware, software, personnel, acceptable Internet use, etc.

If your company has already created a security policy, don't waste valuable time and resources building a new one; just rebuild and update the current one instead, thus saving a lot of research time. You frequently need to monitor and update your security policy as new threats and technologies appear almost every day. Try to always keep up to date with the latest security problems (and the related remedies) in order to have the information assets of your company protected to a reasonable degree.

Your policy must clearly state how the Information Security Office (ISO) can be contacted if there is one, otherwise, a relevant contact person staff need to know with whom they should get in touch when they have questions, doubts, or have detected any suspicious activity. You should at least have a (cell)phone and an e-mail address available for this point of contact.

# THE IMPLEMENT OF THE POLICY

When the security policy is all drawn up, revised, updated and agreed upon, the implementation process will follow. This is usually harder than the creation of the policy itself, due the fact that at this stage you also need to coach and educate your staff to behave in a "secure" manner, following each of the core elements pointed in the formal security policy.

The final version of the security policy must be made available to all of your employees having access to any of your information assets. The policy must be easily obtainable at any time, with a copy placed on the internal network and intranet, if applicable.

A proper implementation requires not only educating staff on each of the core elements flagged as critical in the formal Security Policy, but also changing their role in the effort to protect critical company data.

The next section will aim to guide you through the creation process of a basic Security Awareness Program, along with various innovative and interesting ways of educating your staff, using user-friendly & informal lines of communication between the Information Security Office (ISO) members and your employees.

## CONCLUSION

Security policy is an important concern that must be seriously deliberated. The number of attacks rises day by day as the use of the Internet becomes increasingly popular and more people become aware of some of the vulnerabilities at hand. Security administrators need to watch out continuously for new attacks on the Internet and take the appropriate actions and precautions. This section also explains how to formulate and implement security policies.

**PART 1.6:-**

# IT SECURITY CAN BE ASSOCIATE WITH ORGANIZATION POLICY

## PASSWORD/PIN POLICY

Developing a password and personal identification number policy helps ensure employees are creating their login or access credentials in a secure manner. Common guidance is to not use birthdays, names, or other information that is easily attainable.

## DEVICE CONTROLS

Proper methods of access to computers, tablets, and smartphones should be established to control access to information. Methods can include access card readers, passwords, and PINs.

Devices should be locked when the user steps away. Access cards should be removed, and passwords and PINs should not be written down or stored where they might be accessed.

Assess whether employees should be allowed to bring and access their own devices in the workplace or during business hours. Personal devices have the potential to distract employees from their duties, as well as create accidental breaches of information security.

## INTERNET/WEB USAGE

Internet access in the workplace should be restricted to business needs only. Not only does personal web use tie up resources, but it also introduces the risks of viruses and can give hackers access to information.

Email should be conducted through business email servers and clients only unless your business is built around a model that doesn't allow for it.

Many scams and attempts to infiltrate businesses are initiated through email. Guidance for dealing with links, apparent phishing attempts, or emails from unknown sources is recommended.

Develop agreements with employees that will minimize the risk of workplace information exposure through social media or other personal networking sites, unless it is business-related.

## ENCRYPT AND PHYSICAL SECURITY

You may want to develop encryption procedures for your information. If your business has information such as client credit card numbers stored in a database, encrypting the files adds an extra measure of protection.

Key and key card control procedures such as key issue logs or separate keys for different areas can help control access to information storage areas.

If identification is needed, develop a method of issuing, logging, displaying, and periodically inspecting identification.

Establish a visitor procedure. Visitor check-in, access badges, and logs will keep unnecessary visitations in check.

## SECURITY POLICY REPORTING REQUIREMENTS

Employees need to understand what they need to report, how they need to report it, and who to report it to. Clear instructions should be published. Training should be implemented into the policy and be conducted to ensure all employees understand reporting procedures.

## EMPOWER YOUR TEAM

One key to creating effective policies is to make sure that the policies are clear, easy to comply with, and realistic. Policies that are overly complicated or controlling will encourage people to bypass the system. If you communicate the need for information security and empower your employees to act if they discover a security issue, you will develop a secure environment where information is safe.

**PART 2:-**

**PART 2.1, 2.3:-**

# DESIGN AND IMPLEMENT A SECURITY POLICY FOR eBay ORGANIZATION

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in eBay if its security is compromised. For this it is important to formulate a security policy.

* **Confidentiality-** Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.
* **Integrity-** Information should not be altered during its transmission over the network.
* **Availability-** Information should be available wherever and whenever required within a time limit specified.
* **Authenticity-** There should be a mechanism to authenticate a user before giving him/her an access to the required information.
* **Non Reputability-** It is the protection against the denial of order or denial of payment . once a sender sends a message the sender should not be able to deny sending the massage. Similarly the recipient of massage should not be able to deny the receipt.
* **Encryption-** Information should be encrypted and only by an authorized user.
* **Auditability-** Data should be recorded in such a way that it can be audited for integrity requirements.

# MEASURES TO ENSURE SECURITY

* **Encryption-** It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and only the specified receiver can decrypt the data using the same or a different secret code.
* **Digital Signature-** Digital signature ensures the authenticity of the information. A digital signature is an e-signature authenticated through encryption and password.
* **Security Certificates-** Security certificate is a unique digital id used to verify the identity of an individual website or user.

# SECURITY PROTOCOLS IN INTERNET

The popular protocols used over the internet to ensure secured online transactions.

## SECURE SOCKET LAYER (SSL)

It is the most commonly used protocol and is widely used across the industry. It meets following security requirements.

* Authentication
* Encryption
* Integrity
* Non-reputability

"https://" is to be used for HTTP urls with SSL, where as "http:/" is to be used for HTTP urls without SSL.

## SECURE HYPERTEXT TRANSFER PROTOCOL (SHTTP)

SHTTP extends the HTTP internet protocol with public key encryption, authentication, and digital signature over the internet. Secure HTTP supports multiple security mechanism, providing security to the end-users. SHTTP works by negotiating encryption scheme types used between the client and the server.

## SECURE ELECTRONIC TRANSACTION

It is a secure protocol developed by MasterCard and Visa in collaboration. Theoretically, it is the best security protocol.

* **Card Holder's Digital Wallet Software −** Digital Wallet allows the card holder to make secure purchases online via point and click interface.
* **Merchant Software −** This software helps merchants to communicate with potential customers and financial institutions in a secure manner.
* **Payment Gateway Server Software −** Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.
* **Certificate Authority Software −** This software is used by financial institutions to issue digital certificates to card holders and merchants, and to enable them to register their account agreements for secure electronic commerce.

**PART 2.3**

# RESPONSIBILITIES OF EMPLOYEES AND STAKEHOLDERS IN RELATION TO SECURITY

* **Executive Management:** Assigned overall responsibility for information security and should include specific organizational roles such as the CISO (Chief Information Security Officer), CTO (Chief Technology Officer), CRO (Chief Risk Officer), CSO (Chief Security Officer), etc. These executive level roles generally are responsible for overseeing the enterprise information security strategy that ensures information assets are protected.
* **Information System Security Professionals**: Responsible for the design, implementation, management, and review of the organization’s security policies, standards, baselines, procedures, and guidelines. Examples of these roles can include but are not limited to the following IT security manager, IT Risk management manager, Compliance manager, IT security analyst, etc.
* **Data Owners:** Owners (data owners, information owner, system owners who have budgetary authority); responsible for:
  + Ensuring that appropriate security—consistent with the organization’s security policy—is implemented in their information systems.
  + Determining appropriate sensitivity or classification levels.
  + Determining access privileges.
* **Data Custodians:** A function that has “custody” of the system/databases, not necessarily belonging to them, for any period of time. Usually network administration or operations (those who normally operate the systems for the owners).
* **Users:** Responsible for using resources and preserving availability, integrity, and confidentiality of assets; responsible for adhering to security policy.
* **IT Auditors:** Responsible for:
  + Providing independent assurance to management on the appropriateness of the security objectives.
  + Determining whether the security policy, standards, baselines, procedures, and guidelines are appropriate and effective to comply with the organization’s security objectives.
  + Identifying whether the objectives and controls are being achieved.

# ROLES OF STAKHOLDERS IN THE ORGANIZATION TO IMPLEMENT SECURITY AUDIT RECOMMENDATIONS

Stakeholders have many important questions to ask as expectations change for internal audit functions. Do we have the specialized skills and capability to address the most relevant organizational risks? Have we embedded analytics in everything we do? And most importantly: does our internal audit department have the impact we expect?

Through the years, there is a reluctant acceptance that internal audit does not enjoy as much influence as it could. Many heads of internal audit are challenged in securing the types of skills and capabilities they need to be highly effective. Others say internal audit is not positioned properly within their organization to have the maximum possible impact. And, too often, internal audit is reduced to a compliance function, unable to focus on the greatest opportunities and risks.

Oftentimes, internal audit departments do not have the right skills and capabilities to undertake the kinds of activities to be relevant and impactful within their organization. Co-sourcing, for instance, is a popular option. “Our research shows that co-sourcing to get the specialized skills that are needed will continue to be the most prevalent model,”. “Additional alternative resourcing models such as guest auditor programs and rotation programs were highlighted in the research.”

Though many internal audit departments are embracing analytics to drive deeper insight and provide greater foresight, others are barely scratching the surface. “Many internal audit departments would say that they're using analytics. “In our research, one of the findings was that most heads of internal audit would rate their capability from an analytics standpoint at the basic level, meaning they're just using analytics in simple profiling and sampling. In the many follow-up discussions that we've had with heads of internal audit, they're just not aware of the more advanced analytics and predictive tools that leading internal audit departments are using to provide greater value, to provide deeper insight, and to provide foresight to their stakeholders.”

Another challenge hindering analytics adoption is data quality, which nearly half of the respondents cited as one of their biggest barriers to using analytics. Addressing data quality begins with developing a roadmap. “Determine where we, as internal audit, want to be from an analytic standpoint in terms of our capabilities, the tools that we use, how we use it in our methodology and approach, and then put a plan in place to get there, notwithstanding any concerns that may exist with respect to data.”

# REFERANCE

<https://www.securityinfowatch.com/home/article/10541925/identifying-and-defining-security-stakeholders?fbclid=IwAR3uMevGFatLB2YKGTtXgOUtlhFcRdD1xhtgyDZBlVhrnkQlCpUGjgw8Sc4>

<https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1124&context=ism&fbclid=IwAR3sLPalmfHvmUPISvDxZqFquPYT7k30o-JveqIn2yuEQk95HtlTGqrcQTY>

<https://www.iso.org/iso-31000-risk-management.html#:~:text=ISO%2031000%2C%20Risk%20management%20%E2%80%93%20Guidelines,a%20process%20for%20managing%20risk.&text=Using%20ISO%2031000%20can%20help,use%20resources%20for%20risk%20treatment>.

<https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_73/rzauf/rzaufdefine.htm>

<https://www.techopedia.com/definition/29406/data-protection>

<https://nces.ed.gov/pubs98/safetech/chapter3.asp>

<https://reciprocitylabs.com/resources/what-is-security-by-design/>

<https://www.ebay.com/help/policies/default/ebays-rules-policies?id=4205>

<https://pages.ebay.com/securitycenter/protect_your_information.html#protect_account_info>

<https://one.comodo.com/blog/cyber-security/it-security.php>

<https://www.difenda.com/blog/what-is-the-cia-triangle-and-why-is-it-important-for-cybersecurity-management#:~:text=Confidentiality%2C%20integrity%2C%20and%20availability%2C,most%20important%20components%20of%20security>.

<https://www.loop54.com/blog/top-5-security-threats-facing-e-commerce-today>

<https://blog.i2owater.com/next-generation-network-monitoring>