a

Security

Adeeb Shaban [18110018]

HTU

FinBank

Table of Contents

[Introduction: 3](#_Toc30249016)

[Identify IT security risks together with proposing methods to assess and treat IT Security Risks: 3](#_Toc30249017)

[Natural causes: 3](#_Toc30249018)

[Human causes: 4](#_Toc30249019)

[Benign intent: 4](#_Toc30249020)

[Malicious intent: 4](#_Toc30249021)

[Social-Engineering: 4](#_Toc30249022)

[Identifying assets: 5](#_Toc30249023)

[Determining the vulnerabilities: 6](#_Toc30249024)

[Estimating the likelihood for risks to happen. 8](#_Toc30249025)

[Security risks treatment 9](#_Toc30249026)

[Risk avoidance: 9](#_Toc30249027)

[Risk transferring: 9](#_Toc30249028)

[Accepting the risk: 9](#_Toc30249029)

[Trying to modify the consiquences 9](#_Toc30249030)

[Trying to modify the likelihood for a risk to happen 10](#_Toc30249031)

[Disaster recovery plan 10](#_Toc30249032)

[Identify the potential impact of incorrect configuration of firewall policies and third-party VPN on IT security. 11](#_Toc30249033)

[Incorrect configuration of Firewalls: 11](#_Toc30249034)

[Incorrect configuration of Third-Party VPNs: 11](#_Toc30249035)

[Discuss risk assessment procedures, and how you can take benefit of the ISO risk management methodology by summarizing it and highlighting its application in IT security. 12](#_Toc30249036)

[Identify and pyritize the assets 12](#_Toc30249037)

[Identification of risk 13](#_Toc30249038)

[Natural Threats 13](#_Toc30249039)

[System failure 13](#_Toc30249040)

[Identification of vulnerability 14](#_Toc30249041)

[Analyze the control 14](#_Toc30249042)

[ISO 31000 risk assesment methodlogy and its application in it security 14](#_Toc30249043)

[Benefits of ISO 31000: (IntechOpen, 2010) 14](#_Toc30249044)

[Priniple of ISO 31000: (IntechOpen, 2010) 15](#_Toc30249045)

[Framework of ISO 31000: (IntechOpen, 2010) 15](#_Toc30249046)

[The process of applying ISO 31000 in IT security includes the following steps: (IntechOpen, 2010) 16](#_Toc30249047)

[Provide ways to improve FinBank IT security via: 20](#_Toc30249048)

[implementing different technologies in network security: 20](#_Toc30249049)

[DMZ 20](#_Toc30249050)

[Static ip 21](#_Toc30249051)

[NAT 22](#_Toc30249052)

[discussing the benefits and justification of using **Network Monitoring Systems**. 23](#_Toc30249053)

[Investigating the ‘**trusted network’** configuration and if it can be part of FinBank IT security solutions. 25](#_Toc30249054)

[Describing organizational security procedures to protect business critical data and equipment. 27](#_Toc30249055)

[Explaining data protection processes and regulations as applicable to an organisation 31](#_Toc30249056)

[Discussing the benefits of IT security audit and its impacts to organizational security. 34](#_Toc30249057)

[Discuss in detail the security impact of any misalignment of IT security with organizational policy. 35](#_Toc30249058)

[Bibliography 39](#_Toc30249059)

[Appendix 1 45](#_Toc30249060)

[designing and implementing a security policy for FinBank. 45](#_Toc30249061)

[Design: 45](#_Toc30249062)

[General: 45](#_Toc30249063)

[RISK ASSESMENT AND RISK: 46](#_Toc30249064)

[SECURITY MEASURE POLICIES 47](#_Toc30249065)

[RISKS AND WEAKNESSES 48](#_Toc30249066)

[Change management (AS, n.d.) 49](#_Toc30249067)

[Implement: 50](#_Toc30249068)

[The responsibilities of employees and stakeholders in relation to security, and their role to implement security audit recommendations. 51](#_Toc30249069)

[List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion. 53](#_Toc30249070)

[Evaluate the suitability of the tools used in an organizational policy. 56](#_Toc30249071)

Introduction:

Working as a junior security coordinator in an IT security consultancy, I will need to provide security consultancy for one of the banks named FinBank, I will need to provide a full plan to asset security rest and treat them, as well as the misconfigurations of the firewall and VPN access. The risk assessment plan will cover all the points to solve any risk that could happen to FinBank, also, I will be improving the security of FinBank by providing ways to enhance the technologies in the network. I will be making a policy that includes all roles of the employees and stakeholders, as well as the recovery plan.

Identify IT security risks together with proposing methods to assess and treat IT Security Risks:

Before talking about IT security risks, we need to know what a **risk** is, and what will it has an impact to the company, and how to control it so we can assess it and treat it. (Pearson, 2015)

A **Risk:** is a potential problem that might happen to the whole system or to the system’s user, and risks can be differentiated according to these three things: (Pearson, 2015)

There are common risks that could happen to companies and banks, risks can be a cause from humans or natural. (Pearson, 2015)

* **Risk impact:** which is the loss that has a negative impact, which could be a lost time, lower quality, lost control and money, and lack of understanding. (Pearson, 2015)
* **The possibility for the risk to happen** which is to measure the risk if it’s possible to happen so we can say we have a problem and start looking for solutions (Pearson, 2015)
* **Risk control:** is the ***actions*** which will reduce, eliminate and manage the risk. (Pearson, 2015)

Also, we need to have an organized process to identify the risks, knowing the impact for every one of them and controlling these risks by applying some actions against these risks, which is called **Risk analysis**. (Pearson, 2015)

Also, we can ***expose the risk*** by multiplying the impact of the risk by its probability. Risk probabilities could change from time to time, so, the plan of the risk analysis should track and plan the possibilities of the risks to happen. (Pearson, 2015)

## Natural causes:

Natural causes can be a risk because it could do a physical harm to the people that work in the company or it could do a physical harm to the devices for example: servers, computers or the building of FinBank. Here’s some examples of the natural causes of threats: (Pearson, 2015)

* Earthquakes.
* Floods.
* Fires.
* Power Failure.
* Overheating.

Human causes:

Human causes have plays big part of the risks that could happen because it could be harmful in two ways:

### Benign intent:

Which is the human error that the harm of it isn’t intentional. There are many examples of human errors for example: one of the employees has left a USB that contains data for FinBank on the floor, which will lead to anybody to steal it. Or for example: somebody has left the door of the room that has the servers and the database of the company. (Pearson, 2015)

### Malicious intent:

Malicious intention is categorized to two different categories: (Pearson, 2015)

#### Random:

Which is in directed threats such as a malicious code that could be for example in an email or in a website that is opened to companies and banks, so this type of threat is intentional and not directed to specific company. (Pearson, 2015)

#### Directed:

Directed threat is the type of threat that is directed to a specific company, in our situation we have the FinBank, so hackers and attackers will plan to steal from FinBank. Also, **Social-Engineering** is type of attacks. Here are some examples: (Pearson, 2015)

### Social-Engineering:

Social Engineering is using malicious activities through human interactions, so it’s a manipulation to trick employees to corrupt security or to get some information about the data. For example: Fishing data, Baiting. (imperva, n.d.)

One of the social engineering methods is the **impersonation** which is stealing the identity of a person by manipulating to gain information, it could be physical, or it could be through social applications such as impersonating through email. (imperva, n.d.)

Here’s some examples of the malicious risks (directed/random) that commonly happen to companies and banks: (Cybershark, n.d.)

* Phishing:This type of attack is trying to take access to the secured network. Phishing uses social sites and uses emails to make a malicious content to these social sites and emails to try and steal information and data of FinBank.
* Malwares:It’s a malicious and harmful program that automatically downloads itself without being noticeable when the user clicks on the malicious link that has the malware.
* DDoS: Distributed Denial of Service:which is the type of attack that has more than one source which purpose is to slow down the servers and crashing it.
* Brute Force and Password Attacks:Which is trying to gain access to a network using a program to get the password.
* Ransomwares:Is a type of malware which while its opened, it locks all system down and do an encryption to the devices so no one can use it, the affected device will be locked until FinBank pays and some hackers wont unlock it even if they paid for them.
* Algorithm Manipulation and IoT:using IoT in banks makes it more vulnerable, so the data would be more vulnerable. Some they will have to use an algorithm and rely on it; hackers would try and get these algorithms and codes and get access to all the data.

These malicious risks could be directed as in a group of people have planned to attack a bank by DDoS attack so there server will be down, or these risks can be random as in some people had put a malware in a website which anyone can view and download the malware and get affected by it. (Cybershark, n.d.)

To apply the risk analysis, we have to consider some steps to continue with the process. Risk analysis could be performed in many ways and steps: (Pearson, 2015)

* **Identifying the assets.**
* **Determining the vulnerabilities.**
* **Estimating the likelihood for risks to happen.**

Identifying assets:

First of all, we have to know what we need to protect. In the IT community, we need to identify the assets of categories, which in our situation is the computing system and not only computing systems. We can identify these assets to different categories such as: (Pearson, 2015)

* Hardware: which includes the hardware components, such as; keyboards, monitors, printers, disks, communication controllers, cables, etc.
* Software: which includes the software components, such as; operating systems, system programs for example; compilers, purchased programs, utility programs for services.
* Data:which includes the stored, printed, archival data and audit records.
* People:which includes the staff that has skills to run the system or some specific programs, also, the guards whom specified to support employees.
* Documentational resources:which includes the documented programs, hardware, procedures of the administration and in addition to the entire system.
* Supplies:which includes the supply resources that is needed for all the company daily, such as; paper, laser cartridges, printer ink, recordable data and media, in addition to the personal needs supplies that includes; power, heating and cooling and shelter.
* Reputation:which are the opinions and thoughts of the company from other companies, people and communities and also can be known as the image of the company.
* Availability:which defines the ability of company to do business and be available and be able to resume the business after accidents.

Every company has its own situations, in this situation, we have the FinBank which will lead to protect different things, also, somethings could be vulnerable to a company and wouldn’t be as vulnerable as to other companies.

Determining the vulnerabilities:

After knowing what we need to protect, we need to determine the vulnerabilities of the assets that was mentioned before, so we need to imagine what damage would happen to these assets and what value they these assets have if happened and what are the sources of damage so we can know what is the nature of vulnerabilities and how we can deal with them. (Pearson, 2015)

There are three important and basic goals of computing security: (Pearson, 2015)

* Confidentiality:means that assets can only be seen by the authorized people.
* Integrity:means that the assets can be modified only by authorized people.
* Availability:means that the assets can be used by authorized people.

And having vulnerability means lack of these three basic goals, so we need to have a well-organized plan to consider these three things with different situations to find the best approaching solutions for what made a lack for a particular thing. To have a well-organized plan we will need to have a relation between these three basic goals of computing security and the security assets because one vulnerability could affect more than one goal of computing security and has more than one of type of damage and loss. (Pearson, 2015)

There are many types of threats that could happen because of some types of vulnerabilities that has different results, here are some of common threats in many companies and banks that have: (security, 2019)

|  |  |  |
| --- | --- | --- |
| Threat | Vulnerability | Results |
| Fire | FinBank lack of fire extinguishers | Damage of devices in FinBank and some human life loss |
| Virus | FinBank has lack of antiviruses software | Most of FinBank’s devices are infected |
| Intruder | No security guards in FinBank | Devices is stolen and broken windows |
| Attackers | No powerful firewalls enough | DDoS attacks |
| Employees | Employees aren’t trained enough and there’s no auditing | Sharing information or changing some data processing application that shouldn’t be changed |

After that, there is some factors we need to consider for the value of the assets and the information of FinBank, firstly we need to know the cost we need to develop our assets, for example: Hardware devices, we need to know how much will cost us to develop them from time to time, also we need to know what would it cost to protect and maintain, for the same example: we should ask ourselves if these hardware devices are worth protecting or maintaining because if the cost of the protection is much more than the cost of these devices then we won’t have any benefit protecting and maintaining. And of course, knowing what would cost us to replace these assets because some assets cannot be replaced for example, the database and even the data, the data of FinBank is irreplaceable. (security, 2019)

Estimating the likelihood for risks to happen.

To estimate the likelihood to happen, we need to know the events of risks that could happen, and we need to know the consequences if the risk has happened, as well as the timeline of these likelihood for example: there’s a risk of an earthquake, the likelihood for this to happen is low in a bank in Jordan for example because it’s different between countries. Here I will show the likelihood to the risks I mentioned before: (Sotnikov, 2018)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat | Likelihood | Impact | Vulnerability | Asset | Timeline |
| Malicious threat [DDoS attack]  High | DDoS attacks is newly discovered  Medium | Website resources for FinBank won’t be available  Critical | Firewall has a good DDOS mitigation  Low | Website of FinBank | Could happen at least once or twice per year [depending on the successfulness of FinBank |
| Natural disaster: Flooding  High | This country hasn’t had any floods since 2010  Low | All bank services won’t be available  Critical | Server’s room is in a high point  Low | Servers | Could happen at least once in 10 years |
| System Failure [Overheating]  High | The temperature in the room is high  High | Email, website services will not be available until the problem is solved [2-3 hours]  Critical | The air conditioning system is old  High | Servers | Could happen every week or day |
| Accidental threat [File deletions]  High | Medium | Some data could be lost but could be restored by backups  Low | There are backups taken for the data, and privileges are configured well  Low | Files | Could happen daily |

Security risks treatment

After knowing the likelihood for these risks to happen, now we should know how to treat these risks well. But before, there are some methods to treat the risks because some risks cannot be treated fully. Now, we have some strategies to deal with risks: (Enisa, 2009)

### Risk avoidance:

Which is avoiding risks by changing some requirements for system’s characteristics or for system’s security. For example, we want to avoid the risk of having files deleted by mistake of unintentional human causes, we will need to train the employees well and give them the privileges for the work they need to achieve only, for example: Employees cannot have access to the database of the FinBank, the database administrative will only has the access to it, so, after doing that, the risk of having any files deleted by mistake will be very low and could be 0%. (Enisa, 2009)

### Risk transferring:

Which is giving the risk to different systems, organizations or finding a way so the risk won’t be a reality. As in sharing the risks with other parties that is facing the same risk as in organizational structures to divert the responsibilities and trying to decrease the risk, and if the risk is managed and shared by a group of people, that will acquire a new risk, so the organization should know how to managed if any new risk has appeared to have the effective risk management outcome. For example: there’s some malicious program had appeared newly, the whole organization will try analyzing and find a solution for it, but it will make a new risk as in the cyberhackers will have more than one target to attack. This should be managed properly so none of the risks above will be on reality. (Enisa, 2009)

### Accepting the risk:

Which is accepting and dealing with the risk and knowing what impact it has and be ready for losses that would happen. Accepting the risk is accepting the impact and the consequence of it because sometimes it’s worth taking the risk for the organization to be successful, one the other hand, some risks cannot be worth taking. For example: we have a risk of the overheating, some of the organizations would accept the risk so they won’t have more cost to pay. Accepting the risk comes also with the likelihood to happen, so if the likelihood to happen is **high,** you can’t accept the risk. But if it’s the opposite, you can accept the risk. (Enisa, 2009)

### Trying to modify the consiquences

Which is trying to decrease the harm of the outcome of a risk that had happened, for example: A flooding has happened. The consequence of it is critical is in it has an extreme damage for FinBank, but there’s a backup in another place. Here, you will reduce the consequence of the impact of the risk. (Enisa, 2009)

### Trying to modify the likelihood for a risk to happen

Which is reducing or eliminating the likelihood for the negative outcomes that could happen if FinBank has faced a risk, for example: we have a risk of fire, there is some solutions as having fire extinguishers, but It may be not as effective as finding another solution as in isolating the important devices such as the servers in another place which won’t have any fires. To modify the likelihood, we need to determent the priorities of the assets we have before modifying the likelihood of the risks of it because there are some assets that are more important than other assets. (Enisa, 2009)

### Disaster recovery plan

Also, there are some other ways to treat risks, such as having a backup plan for the data for example if a disaster had happened, as in storing the data in another place where the risk wouldn’t happen. (Bucki, 2020)

This backup plan is called “Disaster Recovery Plan” as in doing a plan to try to reduce the likelihood for a disaster risks to happen and sometimes eliminate these risks, this plan is effective because it’s about implementing the plan before having any risks, this plan can be designed when the organization has started. Here are some of the scope of disasters: (Bucki, 2020)

* The isolated area of the buildings/offices/operators: (Bucki, 2020)
  + In short duration as in the flu bug has infected a department.
  + In extended duration as in water pipes would break over servers or fire might destroy some devices.
* An entire operations/offices/building: (Bucki, 2020)
  + In short duration: Virus attacks.
  + In extended duration: Fire would destroy all the offices and also may be a virus attack too.
* An isolated geographic area: (Bucki, 2020)
  + In short duration: Power failure.
  + In extended duration: Floods or tornados, etc.
* A large geographical area as in a city: (Bucki, 2020)
  + In short duration: Storms.
  + In extended duration: earthquakes, hurricane and wildfires.

To implement this recovery plan, human resources must be considered too in the disaster recovery plan, as well as the property, and the priorities of the assets. There are some solutions such as, having the data backed up from time to time, isolation of some devices as the servers in a place where the risk will be low, as well as having the data stored in more than one offsite locations because if the volume of data is huge, and an earthquake happened for example, it would be the end of the organization. There should always be a plan for anything that might happen, even though sometimes we can’t control any disaster, but we can at least try to reduce the bad outcomes as further as we can. (Bucki, 2020)

Identify the potential impact of incorrect configuration of firewall policies and third-party VPN on IT security.

<https://www.algosec.com/blog/network-security-horror-stories-firewall-misconfigurations/>

Incorrect configuration of Firewalls:

Having your firewall misconfigured has a lot of bad impact, if the firewall isn’t configured properly, the security level/layer will not reach to its fullest. One of the most dangerous outcomes of the misconfigured firewalls is **leaving the ports** open, and that will lead the hackers to gain access to the network, and having the firewall misconfigured will affect the remote control which won’t allow RDP access the servers and will allow hackers to get in through the firewall. Also, having the ports open would allow malicious intent to get into the network too, this is called the egress filtering, which without it would make all the system infected and leave the control servers and contact command with a problem. (algosec, n.d.)

Incorrect configuration of Third-Party VPNs:

Having your third-party VPN not configured properly will lead not to send traffic to trusted and secured resources, also, it might slow the network because the VPN is not configured to reach it’s expected full speed, also its expected for the client for not having an established VPN connection. (Enders, 2012)

Incorrect configuration of third-party VPNs can lead to many security problems. Therefore, it is recommended to configure the VPN with the help of experts. (Enders, 2012)

Incorrect configuration of VPN can’t be aiding a secure network and therefore the threat of data loss can be the result of misconfiguration. (Enders, 2012)

A hacker or unauthorized user can gain the credential information while remote accessing.

Incorrect configuration does not provide strong authentication of the user and can be termed as an insecure network. (Enders, 2012)

As defined, VPN keeps the data shared over the network safe by encrypting it or encapsulation therefore if configured incorrectly, it can lead to the loss of sensitive information as the hacker can steal sensitive information. (Enders, 2012)

If configured incorrectly, one cannot trust the network as it does not control the network traffic and thus anyone can access the data. (Enders, 2012)

Discuss risk assessment procedures, and how you can take benefit of the ISO risk management methodology by summarizing it and highlighting its application in IT security.

Risk evaluation procedures has some steps to be implemented, here are the primary steps of the chance assessment: (CCOHS, 2020)

As mentioned within the first part, property are the matters we want to protect, it can be human resources, facts, hardware devices, software, even the popularity of the company (FinBank).

This part will cover the mechanism to control the organizational IT protection. Here I am going to describe approximately the chance evaluation tactics together with the statistics safety strategies that can be applicable to the organization. In this component I am additionally going to summarize the IOS 31000 danger management method and its software to IT safety. Then we will talk about the possible impacts to the organizational protection because of an IT security audit, and lastly it covers approximately how IT safety can be aligned with organizational policy, detailing the security impact of misalignment.

Risk assessment is the is the system of identity of danger and hazards that have capacity to damage, compare and examine the chance factors which can be concerned in that situation and determine the appropriate manner to take away hazard or manage the risk which cannot be removed (CCOHS).

Here network threat assessment means, figuring out the risk which can harm on the device of FinBank in order I am IT manager of, I actually have assessed the threat of bank and outline of risk assessment is given below.

Identify and pyritize the assets

A screenshot of a cell phone

Description automatically generatedThis is the first step of risk assessment procedures. In FinBank case assets would be servers, information of the clients like contact, critical documents of the partners, trade secret etc. In this step we need to work with the management team and business user to list out all the valuable assets of FinBank. To each asset, we need to gather the following information, as applicable: (CCOHS, 2020)

Most of the organization have the limited budget for the risk assessment, so we need to limit the scope of the project to mission-critical assets. Therefore, we need to state a standard to determine the importance of each asset. Common standards consist of monetary value of asset, legalized standing and importance to the organization. When standard is approved by the management and when it is formally combined with the risk assessment security policy, we have to use it to classify each asset identified as critical, major or minor. (CCOHS, 2020)

Identification of risk

This part of assessment is done in one of the main steps of risk assessment, and we have to determinate the risk and hazards of FinBank. Term risk means that the threat of damage, harm, problem, or any type of other negative occurrence which is caused by external and internal vulnerabilities Risk shows insecurity about deviation from expected things. There are many risks which are originated from different situations. There are lots of risks and threats to FinBank but some of the notable risks are listed below. (CCOHS, 2020)

* + **Unintentional human interface:** without looking on what type of business you are running, this type of threats is always high. Anyone could do a mistake while working, in this case like accidently deleting critical data or files, open on malware links and damaging the hardware of the system. So, we need to always back up the data regularly.
  + **Malicious from human:** This type of risk is also involved in any type of organization; people could steal the hardware and software things of bank. They could delete data, distribute a denial pf services against our website etc. Human could hack our system to steal our data. Not only human could misuse someone’s credentials.

### Natural Threats

Environment can have many security risks to the organizations. Natural disaster can destroy the building and computer system of organization. Which could harm more than hackers. We will not only lose the banks data but the hardware and human resources from these types of risks, so it is very important to think twice about environmental factors before running any business. (Sotnikov, 2018)

### System failure

This is one of the threats which Finbank is facing. System failure depends on the quality of hardware things chosen by the FinBank, for ex: the system which have new and high-quality hardware have the lower chances of system failure. If the equipment is old and low quality, then obviously there would be high chances of system failure. Therefore, FinBank should buy high-quality equipment and it should be replaced in certain time period. (Sotnikov, 2018)

Identification of vulnerability

Now, we need to identify the vulnerabilities. Vulnerability approach weak spot in gadget which risk can go away open to attack. Vulnerability can be identified through the document of auditing, vulnerability analyzing, device and safety evaluation and testing IT gadget (checking out IT device consist of penetration trying out, computerized vulnerability scanning tools and procedure of evaluation of information protection test) etc. We can lessen the vulnerabilities with proper patch management which can be software program base, we need to also consider physical vulnerabilities too. (Sotnikov, 2018)

Analyze the control

In this step we have to analyze the manage both in vicinity and within the making plans stage, to reduce of put off the possible danger which can exploit vulnerability in FinBank system. Control may be applied as technical and nontechnical. Technical approach hardware and software of the computer, information encryption, detection of interruption etc. Non-technical manner safety policies, action of administrative and surroundings and bodily mechanism. Technical and nontechnical manipulate may be in addition categorized as preventive and detective controls. As call implies, preventive manipulate attempts to assault as an instance encryption and authentication devices. Detective controls find out the assault or events through the audit trails and intrusion detection systems. I even have used “Framework” methodology for risk evaluation for Business Bank. (Sotnikov, 2018)

ISO 31000 risk assesment methodlogy and its application in it security

ISO 31000 establishes some concepts that want to be met to do for effective chance management. ISO 3100 of suggestions organize building, making use of and improving, applying and constantly enhancing the molds with the goal is integrating danger management method with the complete admin activities, strategy and planning, management, reporting processes, policies, values and way of life of the organization. (IntechOpen, 2010)

ISO 31000 includes principles and guidelines for managing all types of risk systematically, transparently and reliably as well as in all areas and contexts. ISO 31000 provides general principles and guidelines about risk management. (IntechOpen, 2010)

### Benefits of ISO 31000: (IntechOpen, 2010)

❖ Integrating threat management methods into the organization's preferred management system.

❖ Increase the ability to achieve goals, inspire proactive control, be privy to the need to become aware of and handle dangers inside the organization.

❖ Improve the identity of opportunities and risks; comply with applicable criminal requirements, international rules and standards.

❖ Improve financial reporting, improve governance, enhance stakeholder confidence, establish a reliable basis for selection making and planning.

❖ Improving loss prevention and incident control, minimizing damage.

❖ Improving the resilience of the organization, knowledgeable control stage the tools, tactics and strategies to manage dangers.

❖ Help proactively manage risks in preference to passive handling.

❖ Improve the potential of device control, finance, the foundation of corporate governance.

❖ Improve operational efficiency and implementation results; enhance health, protection and environmental protection.

### Priniple of ISO 31000: (IntechOpen, 2010)

The principle which are made in ISO 31000 give direction on the features of effective and well-organized risk management, collaborating its value and explaining its goal and determination.

* Framework and the processes should be proportionate and customized.
* Human factors influence the risk management methodology.
* Risk management is an part of all activity of the organization.
* Risk management is improved always through experience.
* Risk management considers if there’s any limitation of any available information and data.
* Risk management requires to have a structural and comprehensive ways.
* Risk management requires the involvement of stakeholders.

### Framework of ISO 31000: (IntechOpen, 2010)

The framework of ISO 31000 mirrors a plan, act a cycle and this is common to all the organization system proposals. However, standards state that “This framework is not intended to prescribe a management system, but rather to help the organization to integrate risk management into its overall management system.”

There are some elements of the framework of ISO 31000: (Avalution, 2011)

#### Policy and governance: (IntechOpen, 2010)

Provides the mandate and demonstrate the commitment of the organization. (Avalution, 2011)

#### Program Design: (IntechOpen, 2010)

Design of the framework for managing risk on ongoing basis. (Avalution, 2011)

#### Implementation: (IntechOpen, 2010)

Implementing the risk management structure and program. (Avalution, 2011)

#### Monitoring and Review: (IntechOpen, 2010)

Oversight the management system structure and performance. (Avalution, 2011)

#### Continual improvement: (IntechOpen, 2010)

A picture containing screenshot

Description automatically generatedImprovements for the performance of the overall management system. (Avalution, 2011)

An organization specially those who do not have a prior knowledge of management system, should make to spend significant time starting a robust framework and avoid the need to dive directly into the risk assessment process. Process design is a vital step since the Framework offers the stability and continuousness to contribution in performing a program as opposed to just executing a project. (Avalution, 2011)

### The process of applying ISO 31000 in IT security includes the following steps: (IntechOpen, 2010)

Explain data protection regulations: (IntechOpen, 2010)

General Data Protection Regulation (GDPR): is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). (IntechOpen, 2010)

Business records protection guidelines and procedures need to be created to fit your particular business. Although the General Data Protection Regulations make many modifications to the Data Protection Act concepts, they're consistent with the original ideas and therefore, any coverage that addresses the law Original records is a great vicinity to start.. (IntechOpen, 2010)

It is essential that your policy addresses each of these points and explains how the organization will ensure every point is taken. (IntechOpen, 2010)

That includes how you will ensure data is collected legally, how to update if there are any changes, your business plans to keep data safe from unauthorized access, How to delete data when it is no longer needed and how you will ensure the data is removed from all systems. (IntechOpen, 2010)

GDPR also adds a new principle - that is accountability - so the most important thing is that you articulate your responsibility to enforce these policies for your organization. You will also need to make sure the document explains how you will ensure your entire staff complies with these policies and any processes your business is available if employees do not comply with the policies promulgate. (IntechOpen, 2010)

To establish the risk management, here are some steps that is needed to be implemented:

#### Step 1: ESTABLISH A RISK MANAGEMENT FRAMEWORK

##### Set up context (IntechOpen, 2010)

Enterprises consider outside and internal situations affecting or risking operations of agency.

##### Set up risk management policy (IntechOpen, 2010)

Board of administrators develops a chance management policy and publishes this policy to all members and stakeholders.

##### Responsibility (IntechOpen, 2010)

Enterprises determine the powers responsibilities of the individuals of the business inside the software of danger management systems, including:

##### ❖ Identify, evaluate, plan, handle, screen and file risks.

##### ❖ Develop, enforce and keep a chance management framework.

##### Integration of organizational processes (IntechOpen, 2010)

Enterprises integrate risk management content into all strategies of enterprise and see threat management as an integral part of organization methods. Leadership provides resources to enforce risk management programs.

##### Establishing internal reporting and information exchange mechanism (IntechOpen, 2010)

Enterprises set up reporting mechanisms and exchange internal and external records to support and inspire individuals to implement their responsibilities in danger control.

##### Determine risk criteria (IntechOpen, 2010)

Enterprises decide the standards to as a foundation for danger assessment and comparison of modern risks. Also, assessment outcomes in comparison with threat criteria will serve as foundation for deciding to provide sources to prioritize minimizing risks.

#### Step 2: Implementing risk management framework (IntechOpen, 2010)

* **Implementing risk control framework**
* **Monitor and review risk control framework**
* **Continuous development of hazard management framework:**

- Enterprises organize the implementation of threat management frameworks set up above.

- Head of departments will monitor and suggest enhancements to approaches to limit risks.

- Risk management board will reveal and assist the important equipment to put in force the chance management system.

#### Step 3: Identify risks (IntechOpen, 2010)

The head of the department in the organization wishes to perceive the sources of threat, impacted areas, events, reasons and potential effects of the event. As well as applying gear and strategies to pick out risks, constant with goals. And making a hazard list. (Avalution, 2011)

#### Step 4: Risk analysis (IntechOpen, 2010)

Head of risk evaluation branch, chance evaluation and selection of danger handling plan. The method proprietor must bear in mind the purpose and supply of their threat, its superb and negative effects, and the likelihood that these outcomes may additionally occur. (Avalution, 2011)

#### Step 5: Risk assessment (IntechOpen, 2010)

The branch head compares the level of danger seen during the evaluation with the risk criteria recognized in Step 1. Choosing options for risk handling recollect legal, management and different requirements. And risk control board will keep in mind risks (identification, analysis, evaluation) earlier than filing to the Board of Directors for attention and providing resources to address the risks. (Avalution, 2011)

#### Step 6: Risk handling (IntechOpen, 2010) (Avalution, 2011)

##### Selecting options for handling risks (IntechOpen, 2010) (Avalution, 2011)

The method owner chooses one or more options to adjust risks and put into effect these options. Choose the most suitable hazard management choice that entails balancing expenses and implementation compared with the blessings obtained. Risk control board will keep in mind selecting options for hazard management before submitting to the Board of Directors for consideration and decision. And noting other dangers that may arise when coping with dangers.

##### Prepare and implement options for handling risks (IntechOpen, 2010) (Avalution, 2011)

Owners of processes write in writing the way to put in force solution options through risk dealing with plan. Risk management board evaluations and determines the character and volume backlog the danger after it has treated the danger.

#### Step 7: fOLLOWING AND REPORTING (IntechOpen, 2010) (Avalution, 2011)

This step is set tracking and reviewing strategies consistent with the making plans of threat management procedure. And process of imposing hazard management options; imparting a degree of the implementation of risk management system.

#### step 8: reporting the risks: (IntechOpen, 2010) (Avalution, 2011)

This step is about the head of hazard control branch to summarize and file to the general director, board of directors together with hints to improve to minimize risks.

#### Step 9: reviewing and adjusting (IntechOpen, 2010) (Avalution, 2011)

The board of directors should evaluate the consequences of hazard management and evaluation to make the idea of adjustment accordingly. Providing additional sources as needed to cope with outstanding dangers and orienting to cope with dangers according to the generation updates and financial capacity of the enterprise. As well as organizing the implementation for the following years.

Provide ways to improve FinBank IT security via:

implementing different technologies in network security:

### DMZ

Currently for corporations selecting for themselves a security community version is extremely necessary. A precise protection model will help companies to clearly manage and differentiate between network areas in accordance to each function. From then on, according to each region, entrepreneurs can apply rules or set up security strategies for every network place. Therefore, the DMZ model is one of the models which can meet the safety desires for businesses. (Rouse, n.d.)

The DMZ or Demilitarized Zone is one of the security models. Establishing a community vicinity is remoted and separate among the local area community and the internet. In this particular vicinity will store information that allows users from the Internet to get admission to and take delivery of threats and attacks from outside. Services in this location are mainly: Web server services, Mail server, DNS server or FTP server, etc. (Rouse, n.d.)

Understand another way The DMZ network will provide your business an additional protection quarter and, in that place, you will be smooth to control in detecting and minimizing violations or threats earlier than you Bad men get entry to the organization's intranet or places that store valuable facts. (Rouse, n.d.)

#### Implementing dmz solutions

* **Single Firewall:**

Single Firewall is a way Using a firewall located among the inner network, the internet and the DMZ community region ambitions to help technicians easily manipulate and reveal the visitors glide among Network areas, then can save you and monitor network areas from unauthorized access or implement methods to guard the machine and users from attacks. (Rouse, n.d.)

* **Dual Firewall:**

Dual Firewall is the method Using two firewalls, the first Firewall is mediated in the DMZ network region and the Internet place. The other firewall is placed among the DMZ network region and the intranet vicinity, and the alternative Firewall use different types and safety policies, in order to enhance the security of the device due to the fact If we use a common sort of firewall and security policy settings, once hackers can locate a hollow in a firewall, the last firewall will have no impact on protection. But if we use two differing types and protection coverage settings while bad guys can discover safety holes, he's going to spend greater time to invade the second one protection layer. (Rouse, n.d.)

#### Advantages after deploying DMZ:

The DMZ security version turned into created with two main purposes: each as a network location that can offer offerings to users and inner bearing structures, as well as a security protect to defend the organization's intranet systems with the internet. Also, in case you set up the version properly. it will likely be a solid rampart against hazards or restriction strange external access to the inner data system, so as to be useful for preventing data leakage. (Rouse, n.d.)

### Static ip

Static IP addresses or once in a while some humans also name them constant IP addresses. These IP addresses are used to manually install devices compared to addresses which might be set up through the DHCP server. It is known as static due to the fact once it is set to an IP cope with, the assigned tool will now not change, in addition, there is another kind of IP deal with this is in comparison to the province's IP address, that may be a dynamic IP deal with. Any device that is related to a network can be set to static IP addresses which include computers, phones, printers, Routers, moreover, IP address configuration may be achieved by means of gadgets that generate IP addresses (such as routers) or otherwise, manually configure IP addresses on those gadgets. Usually, a static IP address is configured for a server with its own purpose, so that many people can get admission to it without interrupting the get admission to process. In addition, in comparison to static IP addresses, dynamic IP addresses are set via routers automatically which is convenient for configuring IP addresses easily and quickly. However, the dynamic IP address does not work as soon as the server or router fails. For static IP, despite the fact that the configuration is complicated and labor intensive, there are blessings when the router or server dies, the computers within the community still speak normally. (Bruce, 2019) (Techopedia, n.d.)

#### Implementing static ip

When using a network of network devices or computers, the default configuration of the IP address itself means using a dynamic IP. However, you can also set a static IP address for each computer in the same local network to avoid address conflicts between machines. Also, it is possible to change the DNS address to access the web at a fast speed and to some blocked websites such as Facebook. To set up a static IP address, you need to go to the network configuration section of the device. Depends on the device there will be a separate setting. (Bruce, 2019) (Techopedia, n.d.)

#### Advantages after deploying STATIC IP:

Static IP addresses end up quite beneficial when server gadgets are inaccessible. For example, the laptop linked to the document server inside the organization's neighborhood network may be installation to usually connect with the server the use of the server's static IP as opposed to the hostname name. Even if the DNS server is down, computer systems can still access the record server because they may communicate immediately with the document server thru the IP address. You can easily manipulate and control gadgets that are configured with a static IP address, if an attack tool you could effortlessly detect and offer protection and restore measures. (Vaughan-Nichols, 2019)

### NAT

Currently, normal Internet connections apply to NAT technology or also called Network Address Translation. There are some who consider the way NAT network configuration works like a router. Nat also transports packets between different network layers, it transports and changes one or more IP addresses within a packet, and when that packet goes through a router, or some other device. (Rouse, n.d.)

In addition, the NAT network model also acts as a simple firewall. Its mode of operation maintains a data sheet about each packet when shipped over. When a computer connects to a website on the Internet the header of the source IP address is always replaced by Public IP and is set by default on the NAT server, after having a response to NAT based on the information record packets, change the destination IP address to the PC's address in the network and forward it. furthermore, NAT can manage, and filter packets sent to or sent from an IP address, and decide to allow the packet to be accessible or denied. (Rouse, n.d.)

#### Implementing Network NAT

* **Static NAT:** (Wilkins, 2015)

Static NAT is a method to convert a Private to IP Public with an IP connection that has been converted to the Internet, in addition it's miles often referred to as NAT 11. At each session, there is most effective one facts packet. Are connected out to exchange information, and next packages need to queue as a way to hold repeating the conversion and outward cycle. However, this NAT method is very costly due to the fact the cost of renting and shopping for a public IP address isn't always cheap, whereas usually a network machine has many IP addresses. Static NAT models are commonly configured for an organization's servers, similarly we need to observe which Interface side is Inside and Interface which is Outside to apply to the Interface Router.

* **Dynamic NAT**: (Wilkins, 2015)

Dynamic NAT is a technique that allows to transform all Private IP addresses to IP Public to connect to the Internet. Depending on the number of public IPs used, at each session it's going to correspond to that quantity of IPs linked to the Internet, as an instance a enterprise that hires a huge variety of Public IPs including a hundred IP addresses. When setting up a static NAT technique, there could be one hundred IP addresses converted to Private IP (one hundred computers) linked to the Internet through NAT. In addition, this technique helps to address Public deal with to apply for network system than static NAT, but if the range of Host and Public IP variety is simply too different, the overall performance will not be much advanced This method is still not suitable for large networks.

#### Advantages After Deploying NAT (EDUCBA, n.d.)

One of the main benefits of NAT deployment is that you can use a large number of private IP addresses with more. A class A network address, And when an enterprise uses a private IP address even if the business changes the service provider, you don't have to You have to re-set the address for each device in the organization's local network, you just need to reset NAT on the firewall to the same public IP address. High security for the organization's intranet system by controlling and managing private IP addresses from outside networks.

### discussing the benefits and justification of using **Network Monitoring Systems**.

There are some tools that is used to monitor network system:

#### NMap (Ferranti, 2018)

NMap stands for network mapper, it is one of the open source packages which paintings as a scanner for auditing network. Some time we ought to audit the community of our device it'd assist at that time. It is likewise used to discover the host and services on network through building map of the network by transporting special packets to targeted host and evaluating the reply. In bank scenario we can experiment the network device of bank using this software program, so we are able to discover the possible safety threats and also, we are able to audit the network to discover he modern-day scenario of the community.

Some of the notable advantages of NMap are listed below: (Quora, 2018)

- NMap assist to pass firewall or IDS.

- It enables to scan or to discover the different kinds of vulnerabilities in network

- NMap also assist to send well-crafted packets to the target device

- It also enables to test the range of IPs

- Perform fast DNS lookup.

#### Honeypot

Honeypot is decoy server of computer device, which is installation to hit upon, gather records concerning to an attacker. In different words, it studies about hacking attempts who are trying to benefit unauthorized access to the facts the main characteristic of honeypot is that it identifies all of the malicious activities completed over the internet. Honeypot can set up inside. Using honeypot software, we can detect the information of attacker in case its attacker attack on device and also, we are able to find out the malicious activities completed over the community, with its supply and vacation spot port number. (Murali, 2015)

Some of the fantastic intention or benefits of getting honeypot in gadget is listed below: (Murali, 2015)

- Honey device collect the actual or real records of attackers an also offer analyst with rich supply of worthwhile facts.

- It can gather all of the malicious hobby even the encrypted facts too.

- It additionally decreases fake positives. This means regular cyber safety exposure technology produce alert that incorporate a vital quantity or fake positive, however honeypot lower this quantity, for there is no motive for legitimate users to use them.

- Honey is value effective, to look for attackers they don’t need excessive performance resources to process large volumes of network traffic, the motive behind is that it simplest interacts with malicious actions.

#### Wireshark

In widespread Wireshark is open supply protocol or community analyzer which is to be had for free. This era will attempt to seize the packets of the community and it will attempt to display the info of facts packet as could as possible, so that network administrator should found packets transmit time, its supply and destination, kind of protocol and header facts. In other word it indicates what really happens in network. Wireshark is also used for analyzing the troubleshooting and additionally used to check the faults and failures. Using this software, we will capture the packets of the network and we can see the details of each facts packets wherein we have doubt. (Jose, 2016) Some of the notable advantages of Wireshark are listed below: (Jose, 2016)

- With the help of Wireshark, we will capture the facts packets on remote system, using primary system we are able to analyze the statistics packets in real time. This facility of work throughout the device advantages the community administration and additionally for troubleshooting.

- Wireshark can study the encapsulation approach of different network information pocketing protocols, not simplest this it could additionally work with the wide range of community variability.

#### ZMap

Zmap is one of the loose and open source network security scanners which was evolved as a quicker alternative to NMap vulnerability protection tools. The main motive in the back of designed of this device is to studies statistics security. It may be used for both white and black hat purposes. This device enables to discover the vulnerabilities and their impact over the internet, not simplest this it also enables to pick out the affected device with the assist of 1 gigabit consistent with 2nd of network bandwidth. It also can experiment the complete IPV4 deal with space inside hour on single port. We can research about statistics of security the usage of Zmap software program over the network. Some of the advantages of Zmap is given below: (J.Halderman, 2013)

- Zmap can scan the entire public IPV4 address space within forty-five minutes. (J.Halderman, 2013)

- It may be used for vulnerability detection as well as exploitation. (J.Halderman, 2013)

- Zmap has also used to look a weak public key in HTTPS website logs.

Using these kinds of tools, it will benefit to:

Protecting your network towards attackers. Network tracking structures are able to perceive suspicious traffic, thereby empowering owners to behave fast. A community tracking carrier is capable of provide an extensive assessment of an SMB's complete IT infrastructure, in order that nothing is missed. Today, exploits are more sophisticated and advanced, and are able to target a gadget in a variety of ways. Monitoring antivirus and firewall solutions separately may additionally leave safety gaps. (Koshan, 2016)

Keeping informed without in-residence employees. A community tracking carrier will send indicators and facts to an SMB proprietor as troubles arise. Otherwise, an SMB might also want to either attempt to display their network security themselves or hire a full-time IT employee -- which might be very costly. Data breaches may be greater negative and pricier the longer they go without being detected. (Koshan, 2016)

Optimizing and monitoring your network. Many small business proprietors are aimed towards speedy growth. This growth cannot be viable if components in their IT infrastructure are over-confused or slowed. Network monitoring services will map out the infrastructure of a small business, showing an SMB proprietor region of improvement and any problems that currently need to be addressed. (Koshan, 2016)

Remotely connecting for your infrastructure. Network monitoring offerings are capable of be accessed from anywhere inside the world, permitting an SMB owner to still behavior business whether they may be at home, on the office, or traveling abroad. This can be absolutely essential while you are running with a small amount of staff members or while you simply want to finish obligations on your very own. (Koshan, 2016)

A network monitoring provider will be capable of alert small business owners to any threats or records breaches, a good way to act unexpectedly to secure their own digital belongings and to protect themselves and their customers. Small enterprise proprietors are frequently the maximum vulnerable due to the fact they cannot devote the time or the assets to coping with their personal IT infrastructure; a community monitoring carrier will fill that hole and extra. (Koshan, 2016)

### Investigating the ‘**trusted network’** configuration and if it can be part of FinBank IT security solutions.

In general, a relied-on network is that community where network devices of community are related to each different and which can be only access through the authorized community users, and it must also allow for only stable data to be transferred. A depended-on network is a community controlled by using a network administrator or network administrator to ensure privacy and safety facts aren't leaked. Basically, this is the community that the community administrator tries to defend and determine the safety parameters for the same. Therefore, it could be stated that reliable networks are within security. The trusted community may be a part of an IT security answer and should put into effect the subsequent features: (Naturez-Vous, n.d.)

- Should have robust authentication mechanisms. When user attempt to authenticate community, it should require login so that it could most effective use by way of authenticating users.

- Should have strong statistics encryption method enabled. It way that Data have to be encrypted in order that secure statistics cannot be interrupted and transferred to unauthorized users.

- Should be protected using Firewalls. The computers and servers on the depended-on community should include hardware like a firewall, that is a software program or piece of hardware that allows display for safety.

- The trusted network can also use a virtual personal community (VPN) for enhanced security. Both server and pc of user have to have geared up with VPN (digital personal community) which could allow for remote work and also secure the transferred data.

#### benefits of trusted network:

There are so many advantages of the implementation of the trusted network in any organization, and it could be the part of the IT security solution due to many benefits offered by it. The benefits of having the trusted network on organization is discussed below: (Naturez-Vous, n.d.)

* Trusted network has private network so only authorized used can access the permitted data. The network is private which means it secure data transmission.
* The data in trusted network are encrypted so they are more secure, only the authorized person who have the decryption key can access it. Because of this reason trusted network is considered to be fruitful to security solution.
* In trusted network access is limited so unauthorized users cannot access the network. The trusted network gives access permission only to those who have the permission to access it, so it is considered as the IT security solution.
* It also helps to the administrator to look after all the activities on the network. The administrator could easily monitor all the activities of the users on the network.

The main aim of any organization is to increase the profit of business. We can increase the profit only if we could increase the number of customer and the number of customers will only increase when they are satisfying with our service. The main service of bank is to secure customer financial things. If attacker have hacked our system, then it could leave negative impact in the market. (Naturez-Vous, n.d.)

Trusted community plays vital function in our bank (FinBank). The different sorts of additives like VPN, firewall, encryption, authentication, security gear could certainly help to electricity the security of FinBank that can be bear in mind as the IT safety solution. Because I am IT manager of FinBank, I have carried out all the policy, software program and hardware gear so there's easy operation and paintings is done thinking about the clients’ satisfaction. All the devices are appearing very well, and network machine of FinBank have all the pleasant of depended on network. There aren't any severe attack and all the minor assault or threats and tackling very well. The statistics are very secure as it ought to be and transmitted facts transmitting very thoroughly and accurately. In conclusion community machine of FinBank is secure. After all of the feasible threats are identified, we've applied a few IT solutions. We have applied firewall, DMZ (Dematerialized zone), static IP and NAT to enhance the quality of community safety of FinBank. Not handiest this we've additionally applied some network protection monitoring gear consisting of honeypot, Wireshark, Nmap and ZMap. At final we have investigated how relied on community may be a part of the IT solutions. (Naturez-Vous, n.d.)

### Describing organizational security procedures to protect business critical data and equipment.

According to protection experts, the defense systems of some companies currently exist too many holes. A Director of the Network Management and Security Training Center shared, many groups do no longer know they may be having safety holes, even those which have been exploited through hackers for a long term without discovering. Moreover, cybercriminals have become extra informed and wiser and attacks are growing at a higher price than the capacity of agencies and groups to preserve up. Currently, traditional techniques which include anti-malware, viruses are no longer sufficient to steady your data. Organizational administrators want to consolidate community protection techniques by applying protection methods and policies or using automation as a more defensive tool. Automation is turning into a effective and efficient system to respond right away when issues occur. So how to defend your business towards security risks. Following a sequence of methods to help groups protect themselves from unsecured safety issues. (crane, 2019)

#### Evaluate network security risks

Assessing community protection risks is an extremely critical activity for every company, and business. The assessment of network protection will help to defend the intranet system, information and files of enterprises.. (Abernathy, 2019)

The assessment of community protection dangers is commonly completed by way of the network protection department of the enterprise or through the advice of community protection specialists. They have sufficient expertise and experience to show you the potential dangers to enterprise information that you can't know.. (Abernathy, 2019)

The system safety evaluation is normally divided into two activities: (Abernathy, 2019)

- Scan the system vulnerability: Scanning machine vulnerabilities is a way to identify all protection vulnerabilities, viruses, and malicious code that may attack and potentially have an effect on the entire machine.

- System intrusion testing: Network security engineers and experts will act as hackers, then proceed to invade the system from outdoor and inside. The reason of that is to discover vulnerabilities in addition to potential risks that have an effect on the website machine, intranet system.

After performing threat identification, you need to apply safety features to the organization's gadget. It will assist you to know precisely the safety risks that can have took place for your organization's machine. Thereby making use of measures to restore the device or enforce security measures appropriate to the model, finance and necessities of the business. (Abernathy, 2019)

#### Training staff on security related issues

One of the most dangerous matters with corporation security is the human factor. Therefore, the software of schooling measures, improving the information of employees in the organization on information protection is one of the leading and handiest measures to ensure facts protection in the organization. Organizations want to plot to train records safety classes for groups and community security periodically. It is one of the essential regulations to decrease the dangers in protecting businesses, in addition to the use of security offerings or security professionals from out of doors or growing safety guidelines. records and paintings processes, application of control requirements and facts safety warranty including ISO 27001, PCI DSS. (D, n.d.)

#### Encrypt data information

Encryption is the procedure used to turn information from one form to every other and prevent unauthorized humans from getting access to that records. Encryption itself does not save you the statistics from being stolen, something that the records cannot be used, can't read or apprehend as it has been converted. For example, if you have a letter of love that you want to send for your colleague within the subsequent room, there is a lot of folks who can see the letter before the woman you like. Even if you already delivered the letter to her, it's far still viable that the other individual will dig up the letter and examine it. In order for the confession to be safe and confidential, you need to encrypt the letter in a way that best you and the other female understand, others who observe it simplest see a gaggle of unknown characters. Encryption will bring more safety for statistics, particularly in modern day Internet age, when records must undergo many transfer stations earlier than attaining the destination. Without encryption, the potential of your facts to be stolen by a person in the transmission manner and taking gain of it to do horrific things is totally present. (Rouse, n.d.)

#### Policies to Set up a secure password

Finding a great password and implementing password measures on computers is an essential and necessary problem for organizations. A properly password ought to be a password with a certain amount of complexity - which includes duration and kind of characters - to make passwords more tough to guess than password criminals. Setting up an awesome password policy for your corporation can help prevent an attacker from playing the role of a legitimate person and thereby save you facts loss, sensitive data disclosure. (Brecht, 2019)

We want to create password management regulations as follows: (Brecht, 2019)

- Character period guaranteed: The longer your password, the more secure your site (the minimum variety of characters is 12). We strongly propose trying to add greater characters, including numbers, symbols, capital letters, and lowercase letters. This honestly helps prevent password guessing. Therefore, the longer the password, the harder it is to crack.

- The more complicated the password, the better: A precise password need to consist of a aggregate of numbers, special symbols, uppercase letters and lowercase letters. This virtually helps save you password guessing programs from being available.

- Password used must be unique: You should now not use your password again. If one in all your debts is attacked, statistics is leaked, the account ought to be quarantined.

- Change password periodically. In addition, the new password does no longer fit 2-3 previous passwords. This is to save you your password from being uncovered when a person follows

#### Applying two-layer security

Whether your statistics is encrypted, or you've got a strong password set, you can nevertheless lose your password while it isn't as secure as a wireless community in a cafe or network in public places. To be able to defend your records yourself, you need to use password protection over 2 layers. This manner that similarly to the password, you need other facts to use. (Afonin, 2019)

2-layer protection is the quality way to protect you from network attacks which include phishing (stealing user account information, financial institution accounts, credit score cards, etc., spoofing login pages (like Internet banking) as well as other methods of appropriating accounts. Not most effective that two-layer safety (together with entering the activation code dispatched on your phone) will make hackers unable to faux you as unauthorized get admission to enterprise intranet systems. Therefore, the second affirmation steps have become extra important, and extra and extra groups are the usage of double-layer security, specifically for far off workers. (Afonin, 2019)

#### Divide the network into separate zones

Dividing an agency community from a total community to a separate place will assist you easily control and manage the employer's community. In addition, inside the case of network safety problems, applying separate network areas will help isolate and limit the harm of network safety threats consisting of leakage of business records or infection. Malicious code, etc. From there you will control and save you connections from unsafe network regions to secure network regions. (Murashka, 2019)

#### Use antivirus software

The use of anti-virus software is likewise certainly one of the critical measures in preventing and preventing the dangers of viruses and malware assaults the gadget. Any computer in use is likely to be inflamed with a virus. Viruses often spread thru the roads along with Internet, email, USB drive, hard drive, CD. Viruses frequently seem new variations each hour and every minute. There are many one-of-a-kind forms of viruses and specific tiers of vandalism. When infecting a laptop, the virus can slow down the computer, harm the inflamed files, cause records loss, and motive gadget errors. Types of adware and spyware use victims' computers to illegally advertise, ship spam, motive soreness to users, motive records insecurity, steal personal records, account facts, Credit card numbers. Some viruses take advantage of victims' computer systems to create botnets, to attack different server systems and web sites inflicting unintended outcomes and damages. Therefore, using anti-virus software is crucial for defensive the safety of your network. (Educheer, n.d.)

In addition, you may additionally ask third birthday party protection experts or protection services. Here they can provide expert advice or prevention methods, as nicely as a way to solve safety problems for the device. (Educheer, n.d.)

#### Update regular patches

Currently there are numerous new ways of attack, therefore, no machine can say is constantly safe. Therefore, updating the operating machine or software patches is a vital job to help guard and save you the hazard of assaults on the corporation device. Of course, to make sure the best stage of protection for the system, enterprises need to deploy a couple of security solutions simultaneously and combine unique security policies. (Oracle, 2020)

For example: your neighbor is burgled by using a thief, stealing all his property. The reason is determined due to the fact the layout window isn't guaranteed, and the reduce thief is easy to break into the interior. So, this residence window has a disorder that the landlord does not know. On your side, you find out that your private home window is the same layout. That means day after today the thief can enter your house in the same way. You determine to continue to repair the disorder by way of reinforcing the window firmly and better. Similarly, for software, the illness is known as a "gap" and the correction of the defect is "patch update". (Oracle, 2020)

Therefore, updating the device patches is also one of the measures that you need to recollect when shielding the protection machine for businesses. (Oracle, 2020)

#### Firewall

Firewall is a method that is implemented to the community to save you unauthorized get admission to, to shield internal facts sources and to restrict outside intrusion into the machine. In addition, it protects certain pc networks or servers towards malicious get right of entry to and intrusion from outside, together with websites inflamed with malware or vulnerable network deal with ports. (tutorialspoint, n.d.)

You can locate them anyplace a community is used, which include at home, school, or business. When a firewall is used, it continuously video display units all incoming and outgoing traffic. That will make a firewall use a traffic analysis device and also can be installation to dam the threats you discover. (tutorialspoint, n.d.)

At above we just speak some strategies to defend our corporation from the security threats. There are different some method or we can say the methods that's quite much like above strategies. Let’s see, other security applicable business technique followed. It includes: (tutorialspoint, n.d.)

##### Business Continuance

Business continuity is the capacity of an agency to maintain basic capability for the duration of and after a disaster. The Business Continuity Plan establishes chance management tactics and approaches designed to prevent disruption of mission-critical offerings and to re-set up the full functionality of the organization as quickly and easily as possible. Today's groups face unheard of exposure. The frequency and severity of weather-related events look like increasing, and reliance on complex technologies and deliver chain networks is increasing. With these two trends, businesses are more susceptible to loads of current and emerging dangers. Developing a business continuity method and coping with these dangers is fundamental to the survival of any organization. (KENTON, 2019)

##### Backup/restoration of data:

Data backup is the procedure of copying data so that you can get a duplicate set after a statistics loss occasion. Data healing is a process of retrieving inaccessible, misplaced, corrupted, damaged or formatted statistics from secondary storage, removable media or files, when the information saved in them can't be accessed in a everyday way. Today, many sorts of facts backup services help companies and organizations protect data and ensure that critical data is not lost in the event of natural disasters, theft or other styles of emergencies. (boun, n.d.)

##### Access Control Policy:

The get entry to manipulate coverage application prevents unauthorized access and use of your company's records. Access control rules and procedures ensure the security, integrity and availability of statistics. The system of get right of entry to control regulations applies to all business records and all storage get right of entry to methods. (bizmanualz, n.d.)

##### Disaster control policy:

A disaster recovery policy should start at the business level and determine which applications A disaster recuperation policy need to start at the commercial enterprise degree and decide which applications are the most crucial to going for walks the company. (Campbell, n.d.)

Recovery techniques define an organization’s plans for responding to an incident, while disaster healing plans describe how the business enterprise should respond. (Campbell, n.d.)

Issues like Budget, Resources (humans and bodily facilities), management's position on risks, technology, data, suppliers are considered in figuring out a recuperation strategy. (Campbell, n.d.)

### Explaining data protection processes and regulations as applicable to an organisation

In general information safety refers to the technique of safeguarding or conservation of vital facts from loss, hack, misuse and corruption. (Rouse, n.d.)

Data are very crucial matters for any employer and organization. In those days massive range of humans and businesses are developing and storing facts in database at extraordinary rates, so the importance of records technique and policies has been increased. There is undertaking that unauthorized individual can access critical facts. (Rouse, n.d.)

When we make the statistics protection method and rules, it must be creating to suit for business or groups. Our information protection process needs to be acquired and managed pretty and lawfully. It should be relevant, adequate and also want to hold update. It should be safe in order that we can avoid unauthorized access, loss and destruction. The point of all records safety procedure is to safe the facts. There are many approaches of records safety and description of each is given below: (Rouse, n.d.)

#### Data backup

In general records backup is the process of copying or duplicating or archiving the data to allow repair them in case records loss. Data may be loss from many methods like laptop viruses, failure of hardware, report corruption, fire, environmental elements etc. Data loss can lead to massive loss of monetary lost, so solid statistics backup is very vital for every corporations or company. There are several statistics backup services that are helping entrepreneurs and agencies by way of securing the critical statistics. (Winston, 2018)

#### NTFS security

NTFS stands for brand new technology report gadget. It is the standard record structure which is particularly for the Windows NT operating gadget. It is especially used to improving and store documents on the hard disk. (Techopedia, n.d.)

NTFS authorizations are on hand to drives which are formatted with NTFS. It can affect neighborhood user alongside with network users and they may be primarily based on authorization granted. Administrator can use this service to monitor or manipulate documents, folders and item on the network as a security type, administrator can manipulate over man or woman customers and group customers. (Techopedia, n.d.)

Some of the blessings of NTFS are given below: (Techopedia, n.d.)

- It can restore or retrieve the consistency file gadget in case of electricity loss of failure in gadget.

- Only set customers and groups can get admission to a permitted files and folders.

- NTFS assist quotas, it means reveal over the handy storage space on force or partition.

- Another characteristic is that it keeps the deleted, changed and brought log on tough power.

#### Raid 5

RAID stands for redundant array of unbiased disks mode. RAID consist minimum of three tough disk drives and it haven't any maximum. RAID five is considered as taken into consideration one in every of the most solid RAIDS because of the truth on this RAID data parity is spread all over drives; due to this you will reconstruct records in case of failure in disk. Currently raid five is one in all the maximum generally used methods. (Rouse, n.d.)

A main advantage of raid five is that its combined disk stripping and parity. The word stripping is the machine of storing the consecutive components of records in all drives, which allow us to higher overall performance and throughput. Only disk striping cannot make tolerant of any array fault, disk stripping blended with parity and that provide reliability and redundancy. (Rouse, n.d.)

#### Antivirus

At Business Bank, I suggest Kaspersky anti-virus software. Who has the first-rate patron in a long time? It is extraordinarily useful while considering the cash maintaining area. The usefulness of Kaspersky Anti-Virus combines continuous security, vicinity and expulsion of infections, Trojans, worms, spyware, adware, keyloggers, risky machines and self-dialers. Dynamic, and find out and evacuate rootkits. It also carries programmed upgrades without delay from Kaspersky Security Network. (Detectives, 2020)

#### BCP

The commercial enterprise continuity plan also known as "BCP" is the development of an technique by recognizing the dangers and vulnerabilities and risks of an agency to ensure non-public and belongings security and compliance. suitable for operating in debates. The continuous enterprise arrangement consists of the possible risks, how the risks have an effect on the activities, implement safety and techniques to lessen those hazards, Test strategies to verify that they work and now and then approaches are guaranteed. (KENTON, 2019)

#### Encryption

There are many forms of protection innovations which might be accessible, but encryption is one of the applications that ought to know every day of the client. There are five varieties of encryption, for example:(Allan, n.d.)

##### Triple DES

Triple DES was designed for the first standard (Data Encryption) to be replaced, in the end hackers located a way to restore it without any difficulties. At any time, Triple DES is the most broadly used and widely used symmetric symmetry as part of a business.(Allan, n.d.)

##### RSA

RSA is an open-key encryption and encryption of standard statistics transmitted over the Internet. This is also one of the procedures of PGP and GPG. With 3 DES distinctions, RSA is taken into consideration a deviation calculation the usage of several keys.(Allan, n.d.)

##### Blowfish

Blowfish is supposed to replace some other DES calculation. This symmetric encryption separates the messages into 64-bit squares and the person digit.(Allan, n.d.)

##### AES

Advanced encryption fashionable calculation (AES) is the certainty of the United States government and plenty of associations. Although the special 128-piece AES kind also uses the 192 and 256-piece key encryption for substantial application purposes.(Allan, n.d.)

#### General Data Protection Regulation (GDPR):

GDPR is a law in EU regulation on information protection and prolateness for all individuals inside the European Union (EU) and the European Economic Area (EEA). (Middleton-Leal, 2018)

Business data safety policies and procedures have to be created to suit your specific enterprise. Although the General Data Protection Regulations make many adjustments to the Data Protection Act standards, they're consistent with the unique principles and therefore, any policy that addresses the law Original records is a superb region to start. (Middleton-Leal, 2018)

It is important that your policy addresses each of these factors and explains how the organization will ensure every factor is taken. (Middleton-Leal, 2018)

That includes the way you will ensure data is amassed legally, the way to update if there are any modifications, your enterprise plans to keep data safe from unauthorized access, How to delete data when it's miles not needed and the way you will make certain the statistics is removed from all systems. (Middleton-Leal, 2018)

GDPR also adds a new principle - that is accountability - so the most important thing is that you articulate your responsibility to put into effect these rules for your organization. You will also need to ensure the record explains how you will ensure your complete employees complies with these regulations and any tactics your enterprise is available if employees do not comply with the policies promulgate. (Middleton-Leal, 2018)

### Discussing the benefits of IT security audit and its impacts to organizational security.

Information Technology Audit (IT) is an audit an organization of IT systems, management and operation and related processes. IT audits can be done in relation to regular financial audits or selected audits. As the records, services and activities of many organizations often highly computerized, need to evaluate IT controls in the audit process these organizations. (Ocharo, 2018)

Many users rely on IT without knowing how the computers work. A computer error could be repeated indefinitely, causing more extensive damage than a human mistake. (Ocharo, 2018)

* IT audit is important because it gives assurance that the IT systems are adequately protected, provide reliable information to users and properly managed to achieve their intended benefits. (Ocharo, 2018)
* IT audit could also help to reduce risks of data tampering, data loss or leakage, service disruption, and poor management of IT systems. (Ocharo, 2018)
* Crime prevention. IT security audit prevent crime. It will help the system to be the most secure, prevent hackers from exploiting vulnerabilities and security weaknesses of the company system. At the same time, it also offers solutions to fix the fastest problems (if any problems occur), to ensure data integrity. (Ocharo, 2018)
* Enhances IT governance, IT auditing serves an important function in ensuring all your business laws, regulations and compliance are met by all employees and of course the IT department. This in turn improves IT governance, because IT management generally has a strong understanding of the organization's controls, risks and values. It includes leadership, organizational structure and processes that ensure that the organization's IT maintains and broadens its strategies and goals. Deep network penetration testing also improves IT management of any company. (Ocharo, 2018)

### Discuss in detail the security impact of any misalignment of IT security with organizational policy.

Business alignment is the manner of describing a era tactic that targets to backing enterprise method. The term alignment is criticized as being susceptible and passive sounding. In general, alignment is challenges of an organization. To improve the commercial enterprise alignment corporation, have to make investments time and resources. No strategies and strategy can assure the success of development of enterprise alignment security, instead different styles of interrelated moves are had to be identified to improve the commercial enterprise alignment. Gartner has diagnosed seven domains which are applicable to enhance the commercial enterprise alignment, and they are indexed below: (Scholtz, 2009)

#### Culture

In this domain, agency broaden the organizational way of life wherein IT professionals, mangers and users can choice approximately information risk. (Scholtz, 2009)

#### Planning

The records protection enterprise tactical and plan give lots risk for aligning the resultant projects and activities to actual commercial enterprise necessities. For example, the primary strategies are to leverage planning precept in protection scheduling practices. (Scholtz, 2009)

#### Processes

Accepting the strategic procedure technique like ISMS set by means of ISO 27001, to the safety control program, it creates a capacity to asses, develop and put in force security answers as and while required through the commercial enterprise in preference to applying a “one size suits all” manage baseline. (Scholtz, 2009)

#### Communications

This domain describes that, most important aim needs to be expanded protection associated carrier level metrics which can be comprised in formal provider level agreements (SLAS) among IT, customers and service providers. (Scholtz, 2009)

#### Capabilities

This domain describes that once in a while business alignment requires abilities which are not usually associated with statistics security specialists like architecture practice, communications talent of the person, information of business and marketing talents. (Scholtz, 2009)

#### Technology

The way or method in which safety technology is utilized may have a important impact on how security is perceived through customers of the era. The fulfillment incorporated IT carrier transport strategy, such as that prescribed by means of ITL v3, will rely on how security controls are technically integrated with IT services. (Scholtz, 2009)

#### Relationships

This domain describes about the importance of creating and maintaining effective family members with different roles and individual inside the business enterprise. Alignment is depending upon the cooperation and backing of key influencers, decision maker and different stakeholders. (Scholtz, 2009)

#### Security impacts of misalignment

Misalignment between IT security and organizations policy is can lead to lot of IT security threat, and the risks that can occur from misalignment between IT security and organization policy. (Scholtz, 2009)

#### Internal Risks

The following are the possible internal security dangers that occurred due to misalignment among IT security bank policy. (Robert S. Kaplan, 2012)

#### Theft by employee

Hardware and software can be stolen with the aid of the worker, so it is also the one of the human risks for employer. To avoid this kind of threat from the business enterprise we should practice fallowing guidelines and regulation: (Robert S. Kaplan, 2012)

- The use of biometrics identification

- The employees of the company must be secretly watched.

- Organization must aware or encourage worker for enterprise success.

#### Weak access control

Weak access manage is one the main inner security hazard of organization. In this kind of risks authorization and accounting are at excessive hazard. The susceptible access manipulate can result in hacking users account and hacking the database of the organization. To save you susceptible access control, we need to fallow the below listed rules: (ISMS.online, 2013)

- User account password has to be robust

- Password have to be in encrypted form

- Password must be lengthy having special individual like \*,.@ etc.

- Access manipulate must be sturdy having the high privacy, countability and integrity.

#### Privilege abuse

Organization should not give all of the permission and authority for employee over resources due to the fact they can misuse the sources deliberately and by chance which can damage on the popularity of the organization. The following policies and regulation may be applied for this: (HASSAN, n.d.)

- The historical past of the worker has to be checked before proving the energy to them.

- Regular training need to be provided for them.

#### System Risks

System threat refers to the harm to the physical or hardware equipment of the organization. This could be the reason of misalignment between IT security and organization. The possible system dangers to the enterprise are described below: (Arshad, 2012)

##### Failure of equipment

When any hardware gadget stopped to paintings that is known as the failure of the device. So, to limit those sorts of chance ordinary test and preserve of the physical gadget need to be achieved. (Arshad, 2012)

##### Power fluctuation

When the energy is surged which stopped to carry out the electronic gadget, so that is also one of the gadget dangers that any enterprise can faced. For this form of threat wiring of the electronic device need to be completed properly, and surge protector ought to be established. (Arshad, 2012)

##### External risks

Any form of chance that are from out of doors the corporation are external dangers. There are different kind of external threat and a number of the tremendous external risks are described below: (Arshad, 2012)

**- Hacking:** (Arshad, 2012)

Hackers can theft very touchy data, financial information such as financial institution information and fee card information, they can also disturb on trading.

Hacking can damage recognition of any company and erode the trust of clients. This could potentially lead to loss of customers; decrease in income and lack of sale. The damage of recognition also outcomes on dating of business enterprise with partners and 0.33 parties who're vested in company. We can minimize the hacking by way of following activities: (Arshad, 2012)

- Install firewall and list out IP to prevent DOS attack

- Information must be encrypted

- Third birthday party protection tools should be established, and employee must be limited to use it.

**- Phishing:** (Arshad, 2012)

It is the manner to obtain the information of customers from internet by themselves (clients). The criminal sends an e mail to consumers which is alleged to be form her bank of organization but when they click the link and input his/her facts, criminal gets all that information, so phishing is also one of the human risks to community security. We can aware employees about the policies and law of the enterprise website to decrease those varieties of dangers.

**- Malicious threat:** (Arshad, 2012)

This threat can harm the safety gadget of the company. Viruses of the computer, trojan, trojan horse and adware are a number of the instance of malicious danger. Actually, those are the software which can be particularly developed to damage, disturb the protection system of the computer. Not handiest this they also perform unlawful activities on hosts, software and pc. They also can trade the operation of the computer. Some of the sign of malicious are that computer work slowly, files are grown to be corrupted, use of storage increased. To limit these forms of threat we can hooked up antivirus software program at the operating device, and after its miles set up it must be update time to time to restore new issues and viruses.

Misalignment have negative effect on IT protection, but good news is that it may be clear up once we've got the proper tools and tactics. (Arshad, 2012)

# Bibliography

Abernathy, R., 2019. *Security Assessment and Testing.* [Online]   
Available at: http://www.pearsonitcertification.com/articles/article.aspx?p=2931575&seqNum=2

Adrian Duigan, N., 2003. *10 steps to a successful security policy.* [Online]   
Available at: https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html

Afonin, O., 2019. *You Lost Your Second Authentication Factor. Now What?.* [Online]   
Available at: https://blog.elcomsoft.com/2019/04/you-lost-your-second-authentication-factor-now-what/

algosec, n.d. *Network Security Horror Stories: Firewall Misconfigurations.* [Online]   
Available at: https://www.algosec.com/blog/network-security-horror-stories-firewall-misconfigurations/

Allan, M., n.d. *6 Types Of Encryption That You Must Know About.* [Online]   
Available at: https://www.goodcore.co.uk/blog/types-of-encryption/

Arshad, A. R. A. a. Y., 2012. *Understanding Components of IT Risks and Enterprise Risk Management.* [Online]   
Available at: https://www.intechopen.com/books/risk-management-for-the-future-theory-and-cases/understanding-components-of-it-risks-and-enterprise-risk-management-a-literature-review

AS, C., n.d. *security policy.* [Online]   
Available at: https://kodu.ut.ee/~mroos/turve/turvapoliitika/secpolicy.html

Avalution, 2011. *THE BASICS OF ISO 31000 – RISK MANAGEMENT.* [Online]   
Available at: https://avalution.com/the-basics-of-iso-31000-risk-management/

Beal, V., n.d. *DRP - disaster recovery plan.* [Online]   
Available at: https://www.webopedia.com/TERM/D/DRP.html

bizmanualz, n.d. *IT Access Control Policy Procedure| ITSD106.* [Online]   
Available at: https://www.bizmanualz.com/business-procedures/it-procedures/it-access-control-procedure

boun, c., n.d. *Secondary Storage.* [Online]   
Available at: https://www.cmpe.boun.edu.tr/~say/c150/intro/lit3.html

Brecht, D., 2019. *Password Security: Complexity vs. Length.* [Online]   
Available at: https://resources.infosecinstitute.com/password-security-complexity-vs-length/

Bruce, J., 2019. *What Is a Static IP Address? Here’s Why You Don’t Need One.* [Online]   
Available at: https://www.makeuseof.com/tag/static-ip-address-advantages-disadvantages/

Bucki, J., 2020. *Disaster Recovery Planning and Risk Management.* [Online]   
Available at: https://www.thebalancesmb.com/disaster-recovery-planning-and-risk-management-2533585

businessdictionary, n.d. *risk.* [Online]   
Available at: http://www.businessdictionary.com/definition/risk.html

Buzdar, K., 2017. *Deploy a Read-Only Domain Controller (RODC) on Windows Server 2016.* [Online]   
Available at: https://www.itprotoday.com/windows-78/deploy-read-only-domain-controller-rodc-windows-server-2016

Campbell, J., n.d. *DISASTER RECOVERY AND BUSINESS CONTINUITY.* [Online]   
Available at: https://www.pefservices.com/disaster-recovery-business-continuity/

CCOHS, 2020. *Risk Assessment.* [Online]   
Available at: https://www.ccohs.ca/oshanswers/hsprograms/risk\_assessment.html

Cerini and Associates, L., 2018. *10 Key Elements Of A Disaster Recovery Plan.* [Online]   
Available at: https://medium.com/@cerini3340/10-key-elements-of-a-disaster-recovery-plan-cf91cae6bf9f

CompareCamp, n.d. *AVG Antivirus Review.* [Online]   
Available at: http://comparecamp.com/avg-antivirus-review-pricing-pros-cons-features/

crane, C., 2019. *What is Cybercrime?.* [Online]   
Available at: https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know/

Cybershark, n.d. *Why Is It Important to Address Cybersecurity Threats?.* [Online]   
Available at: https://www.blackstratus.com/cybersecurity-threat-detection/

Detectives, S., 2020. *Kaspersky Antivirus Review 2020 — Is Kaspersky REALLY Russian Spyware?.* [Online]   
Available at: https://www.safetydetectives.com/best-antivirus/kaspersky/

Dewan, C., n.d. *IronWASP: An Introduction.* [Online].

D, V., n.d. *Objectives of Employee Training.* [Online]   
Available at: http://www.economicsdiscussion.net/human-resource-management/employee-training/objectives-of-employee-training/31634

EDUCBA, n.d. *What is NAT?.* [Online]   
Available at: https://www.educba.com/what-is-nat/

Educheer, n.d. *Anti Virus Software Spyware Security Information.* [Online]   
Available at: https://educheer.com/essays/anti-virus-software-spyware-security-information/

Enders, R., 2012. *How can incorrectly configuring VPN clients lead to a security breach?.* [Online]   
Available at: https://searchnetworking.techtarget.com/answer/How-can-incorrectly-configuring-VPN-clients-lead-to-a-security-breach

Enisa, 2009. *Risk Treatment.* [Online]   
Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment

Ferranti, M., 2018. *What is Nmap? Why you need this network mapper.* [Online]   
Available at: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html

Golding, S., 2015. *Key Elements of a Disaster Recovery Plan (DRP).* [Online]   
Available at: https://trilogytechnologies.com/key-elements-of-a-disaster-recovery-plan/

HASSAN, W., n.d. *Contingency Plans: 6 Reasons Why Every Business Should Have Them.* [Online]   
Available at: https://tweakyourbiz.com/global/contingency-plans

Hope, C., 2017. *Disk quota management.* [Online]   
Available at: https://www.computerhope.com/jargon/d/diskqm.htm

imperva, n.d. *Social Engineering.* [Online]   
Available at: https://www.imperva.com/learn/application-security/social-engineering-attack/

IntechOpen, 2010. *The Role of Standardization in Improving the Effectiveness of Integrated Risk Management.* [Online]   
Available at: https://www.intechopen.com/books/advances-in-risk-management/the-role-of-standardization-in-improving-the-effectiveness-of-integrated-risk-management

ISMS.online, 2013. *What is the objective of Annex A.9.1 of ISO 27001:2013?.* [Online]   
Available at: https://www.isms.online/iso-27001/annex-a-9-access-control/

J.Halderman, 2013. *ZMap: Fast Internet-Wide Scanning and its Security Applications.* [Online]   
Available at: https://www.academia.edu/23324082/ZMap\_Fast\_Internet-Wide\_Scanning\_and\_its\_Security\_Applications

Jose, A., 2016. *What is exactly wireshark?.* [Online]   
Available at: https://www.quora.com/What-is-exactly-wireshark

KENTON, W., 2019. *Business Continuity Planning (BCP).* [Online]   
Available at: https://www.investopedia.com/terms/b/business-continuity-planning.asp

KerioControl, 2019. *Application awareness in Kerio Control.* [Online]   
Available at: https://manuals.gfi.com/en/kerio/control/content/content-filtering/application-awareness-in-kerio-control-1900.html

Kirvan, P., 2009. *Including employees in your disaster recovery plan.* [Online]   
Available at: https://searchdisasterrecovery.techtarget.com/tip/Including-employees-in-your-disaster-recovery-plan

Koshan, M., 2016. *The Advantages to Using a Network Monitoring Service - CWPS.* [Online]   
Available at: https://www.cwps.com/blog/the-advantages-to-using-a-network-monitoring-service

Larue-Langlois, R., 2018. *8 Best Network Configuration Tools and Software.* [Online]   
Available at: https://www.addictivetips.com/net-admin/network-configuration/

Mark Talabis, J. M., 2012. *Information Security Risk Assessment.* s.l.:s.n.

Middleton-Leal, M., 2018. *What is GDPR: 10 Frequently Asked Questions.* [Online]   
Available at: https://blog.netwrix.com/2018/02/06/what-is-the-general-data-protection-regulation-gdpr-10-frequently-asked-questions/

Murali, M., 2015. *How does a Honeypot work?.* [Online]   
Available at: https://www.quora.com/How-does-a-Honeypot-work

Murashka, U., 2019. *3 Levels of Corporate Network Security.* [Online]   
Available at: https://www.scnsoft.com/blog/3-levels-corporate-network-security

Naturez-Vous, n.d. *Naturez-Vous.* [Online]   
Available at: https://naturez-vous.com/trusted-network-solutions-environment-technologies/

Netwrix, n.d. *Network Security Best Practices.* [Online]   
Available at: https://www.netwrix.com/network\_security\_best\_practices.html

Ocharo, H., 2018. *The Importance of Information Systems Audit.* [Online]   
Available at: https://www.linkedin.com/pulse/20140620054920-64969119-the-importance-of-information-systems-audit

Oracle, 2020. *13 Operating System Updates.* [Online]   
Available at: https://docs.oracle.com/cd/E27363\_01/doc.121/e27511/ftr\_os\_update.htm#OPCFG5318

Pearson, 2015. *Higher Natinals on Computing Core Text book.* United kingdom: s.n.

Quora, 2018. *What is the advantage and disadvantage of Nmap (network mapper)?.* [Online]   
Available at: https://www.quora.com/What-is-the-advantage-and-disadvantage-of-Nmap-network-mapper

Robert S. Kaplan, A. M., 2012. *Managing Risks: A New Framework.* [Online]   
Available at: https://hbr.org/2012/06/managing-risks-a-new-framework

Rouse, M., 2011. *content filtering (information filtering).* [Online]   
Available at: https://searchsecurity.techtarget.com/definition/content-filtering

Rouse, M., n.d. *Data protection.* [Online]   
Available at: https://searchdatabackup.techtarget.com/definition/data-protection

Rouse, M., n.d. *DMZ(networking).* [Online]   
Available at: https://searchsecurity.techtarget.com/definition/DMZ

Rouse, M., n.d. *Encryption.* [Online]   
Available at: https://searchsecurity.techtarget.com/definition/encryption

Rouse, M., n.d. *Network Address Translation (NAT).* [Online]   
Available at: https://searchnetworking.techtarget.com/definition/Network-Address-Translation-NAT

Rouse, M., n.d. *RAID 5.* [Online]   
Available at: https://searchstorage.techtarget.com/definition/RAID-5-redundant-array-of-independent-disks

Rouse, M., n.d. *Wireshark.* [Online]   
Available at: https://whatis.techtarget.com/definition/Wireshark

Scholtz, T., 2009. *Seven ways to align security with the business.* [Online]   
Available at: https://www.computerweekly.com/opinion/Seven-ways-to-align-security-with-the-business

Scripto, D., 2013. *Use PowerShell Functions to Authorize DHCP Servers.* [Online]   
Available at: https://devblogs.microsoft.com/scripting/use-powershell-functions-to-authorize-dhcp-servers/

security, M. o. I., 2019. *Fundamentals of Information Systems Security/Information Security and Risk Management.* [Online]   
Available at: https://en.wikibooks.org/wiki/Fundamentals\_of\_Information\_Systems\_Security/Information\_Security\_and\_Risk\_Management#Confidentiality

Sotnikov, L., 2018. *How to Perform IT Risk Assessment.* [Online]   
Available at: https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/

Srivastava, K., 2010. *Disaster: Challenges and perspectives.* [Online]   
Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3105552/

STEVENS, M., 2016. *9 Critical Responsibilities Of The Cybersecurity Manager.* [Online]   
Available at: https://www.bitsight.com/blog/responsibilities-cybersecurity-manager

Techopedia, n.d. *New Technology File System (NTFS).* [Online]   
Available at: https://www.techopedia.com/definition/24482/new-technology-file-system-ntfs

Techopedia, n.d. *Security Policy.* [Online]   
Available at: https://www.techopedia.com/definition/4099/security-policy

Techopedia, n.d. *Static Internet Protocol (IP) Address (Static IP Address).* [Online]   
Available at: https://www.techopedia.com/definition/9544/static-internet-protocol-ip-address-static-ip-address

tool, C., n.d. *Identifying and Analyzing Stakeholders and Their Interests.* [Online]   
Available at: https://ctb.ku.edu/en/table-of-contents/participation/encouraging-involvement/identify-stakeholders/main

tutorialspoint, n.d. *Network Security – Firewalls.* [Online]   
Available at: https://www.tutorialspoint.com/network\_security/network\_security\_firewalls.htm

UCLA, n.d. *TOP 10 IT SECURITY RECOMMENDATIONS.* [Online]   
Available at: https://www.it.ucla.edu/security/resources/security-best-practices/top-10-it-security-recommendations

Vaughan-Nichols, S. J., 2019. *Static vs. Dynamic IP Addresses.* [Online]   
Available at: https://www.avast.com/c-static-vs-dynamic-ip-addresses

Watts, S., 2018. *IT Disaster Recovery Planning: How To Craft A Plan For Your Organization.* [Online]   
Available at: https://www.bmc.com/blogs/disaster-recovery-planning/

Wilkins, S., 2015. *Network Address Translation (NAT) Implementation Methods.* [Online]   
Available at: http://www.pearsonitcertification.com/articles/article.aspx?p=2447202

Winston, E., 2018. *Data backup.* [Online]   
Available at: https://www.quora.com/What-is-%E2%80%9Cdata-backup%E2%80%9D

Appendix 1

designing and implementing a security policy for FinBank.

In general security policy refers to the documentation, which is written, and it outlines how we can protect the organization or company from the threats, including the computer security threats and it also include how to handle such situations when they occur. Security policy should identity the assets of company along with their possible threats to the assets. The company needs to update the security policy to the employees and also the policies need to be updated regularly. As I am IT manage of FinBank, I have made some security policies for FinBank and description of each is given below: (Techopedia, n.d.)

Design:

### General:

#### Subject:

This security coverage involves the safety of my organization. It includes security objectives, suggestions for their achievement, and overall safety management approach and implementation of rules on key protection mechanisms. (AS, n.d.)

The protection policy is for all subdivisions of my employer and regulates interactions and relationships with the subsequent subjects: (AS, n.d.)

-partners, clients and subcontractors

- country agencies

- media and public

#### Goal of security policy

The protection coverage establishes the recommendations and procedures within the scope of property that corporation employees are required to recognize and follow as a primary manner of achieving safety goals. Security coverage is the bottom for planning, design, execution and management of safety. (AS, n.d.)

#### Security Objectives

-Security of assets need to be maintained to the quantity that corporation may want to function usually and without interruptions inside the case of maximum in all likelihood threats, to obtain its enterprise goals. (AS, n.d.)

- Security measures must be economically justified and their disruptive effect to Yellow Chicken operations and staff ought to be as small as possible. (AS, n.d.)

- Asset availability, integrity and confidentiality need to conform to an average level of protection. (AS, n.d.)

- Compliance to the safety legislation (together with copyright, private information, kingdom laws and rules and workers health and protection necessities and fire safety necessities) need to be ensured. To meet this requirement, some objects and methods ought to be included with measures above the average stage of protection if needed. (AS, n.d.)

- Due to contractual and similar relationships with partners, safety features above the common degree ought to be used to fulfill the necessities of objects and approaches in which appropriate. When making ready the contracts, resource costs for additional protection ought to be taken into account and the safety measures must be economically justified. (AS, n.d.)

#### Principles of security

Assets utilization permissions are granted to the employees on the basis of work-associated needs. For any asset is some person accountable for it. (AS, n.d.)

### RISK ASSESMENT AND RISK:

#### MANAGEMENT 2.1 Acceptable residual risk

Acceptable residual threat is determined once a year. (AS, n.d.)

#### Testing of security conformance

- External audit is performed while necessary, however now not less often than as soon as each 3 years. (AS, n.d.)

- Security Council performs an internal audit to check the conformance to baseline protection at the least once a year. (AS, n.d.)

- Security Council member check the conformance of safety to the safety policy at random at the least once a month. (AS, n.d.)

#### Insurance

Under the prevailing conditions, insurance isn't economically justified for organization. (AS, n.d.)

### SECURITY MEASURE POLICIES

The implementation and control of primary security mechanisms ought to comply with the following rules and guidelines. (AS, n.d.)

#### Access policy

- IT role set must have as a minimum 3 ranges for access to records: no get right of entry to, read-best, read-write. (AS, n.d.)

- IT person roles are defined with the aid of IT gadget capabilities and from the structure of IT control. (AS, n.d.)

- Access to sources is function-based, in keeping with task requirements. (AS, n.d.)

#### Cryptography policy

- The minimum acceptable key period for symmetric encryption is 256 bits. (AS, n.d.)

- The minimal allowable key duration for the use of an asymmetric cryptographic gadget is 1024 bits. (AS, n.d.)

- All confidential facts on computers being carried outdoor the enterprise perimeter (laptops, computer systems of domestic people), all confidential statistics on hard disks ought to be encrypted. Encryption keys have to be duplicated in a secure backup. (AS, n.d.)

- For accessing inner community sources across the public network and for the transmission of confidential data across public community, only stable connections should be used: VPN connections, SSL / HTTPS connections, and encrypted mail messages. (AS, n.d.)

#### Password management

Password help to hold the pc secure. This coverage can be implemented to all of the computers of every department. The age of the password is set to set new password after that set certain days. If the password is very simple then there is hazard that unauthorized character can wager the password, so permitting the complexity of the password should be enabled so it will assist to steady the consumer’s laptop via making password complexity. (AS, n.d.)

#### Quota management policy

Disk quota management permission are given with the aid of the administrator in which administrator set restrict at the user, workgroup or the storage space. By placing quota coverage, we are able to prevent a server from becoming the total of facts, however it gives permit to keep files. In well-known quota reveal over storage space. (Hope, 2017)

#### Firewall policies

Firewall is a network safety device which is used to avoid unauthorized get admission to to or from personal community or intranet. (AS, n.d.)

All the messages which can be entering and leaving the personal network of bank is filtered by way of firewall due to the fact they pass via firewall, using this technology we are able to block every of the messages which did now not meet specified protection criteria. Firewall can be hardware and software or aggregate of both. Hardware firewall may be purchased stand-alone but normally they may be observed in routers. (AS, n.d.)

#### Removal policy

- To delete state secret or especially confidential records from disk, stable deletion must be used. (AS, n.d.)

- All unnecessary paper documents with confidential statistics should be destroyed with a shredder. (AS, n.d.)

- Retired and / or discarded from archive storage media must be destroyed physically. (AS, n.d.)

#### Work environment

- No real information should be used for trying out and demos. (AS, n.d.)

- New software need to be tested before use and showed to be suitable. (AS, n.d.)

#### Legality policy

- All assets have to be obtained legally. (AS, n.d.)

- All uses of the assets have to be legal. (AS, n.d.)

### RISKS AND WEAKNESSES

For planning, implementation and control of protection, the following dangers will be taken into consideration typical, and safety measures must be based totally on this selection. (AS, n.d.)

#### Spontaneous risks: (AS, n.d.)

- Fire

- Thunderstorm

- Water and fire extinguishing damages, consisting of typhoon water, emergency pipelines, etc.

- Human error

- Fluctuations in power pleasant and simple blackout

- Hardware error

- Interruption of external communications

- Loss of staff

#### Attacks: (AS, n.d.)

- Theft

- Viruses

- Penetration into the internal network from public community

- Distributed Denial of Service (DDoS)

- Sniffing of an internal pc network

- Interception of oral communication

- Workers' deliberate safety breaching behavior, inner attacks

### Change management (AS, n.d.)

#### Security monitoring (AS, n.d.)

##### Operative monitoring (AS, n.d.)

- Security officers need to evaluate audit logs at least as soon as a week.

- On security incidents, possible safety needs modifications need to be identified.

- On good sized technical, organizational, criminal or other inner or external modifications, feasible security need changes need to be identified.

##### Random security checks (AS, n.d.)

In subunits, the statistics protection has to be randomly checked at least as soon as each month.

##### Regular review of security (AS, n.d.)

Must be achieved at the least as soon as a year.

#### Security policy modification: (AS, n.d.)

- The protection coverage is changed, if so, required by using the security tracking results.

- The protection coverage is amended, if they want arises from the appearance of a new version of baseline protection directory. Security Council makes the amendments in all cases, in no later than one week.

- Security changes because of security coverage adjustments are completed within one month.

Implement:

* **Identify risks:** (Adrian Duigan, 2003)

Through the use of monitoring or reporting equipment, it is the first-class way to pick out risks. Internet safety products and plenty of firewall providers permit time to assess their merchandise. Such merchandise can be useful when the usage of these assessment tiers to assess risk if it affords reporting information.

* **Learn from others:** (Adrian Duigan, 2003)

There are many types of privateness regulations, so it's miles critical to look what other companies like yours are doing. In addition, you may take the time to speak to income representatives from special protection software program providers. They are constantly happy to offer information.

* **Make sure the policy conforms to legal requirements:** (Adrian Duigan, 2003)

One way to minimize the felony duties that you could incur within the event of a protection breach is to have a feasible protection coverage documented and implemented specifically. You may must comply with positive minimum standards to make sure the privacy and integrity of your data, depending in your data, jurisdiction and location, in particular if your enterprise you keep non-public information

* **Level of security = level of risk:** (Adrian Duigan, 2003)

In addition to preventing bad guys, you do not have any problems with proper use because you've got a dedicated team of workers. A written code of behavior is the most important in such cases. Make sure you don’t overprotect yourself because immoderate safety may be a hindrance to easy commercial enterprise operations.

* **Include staff in policy development:** (Adrian Duigan, 2003)

The leaders above have to propagate and attract employees to take part within the manner of determining appropriate use. No one needs a coverage dictated from above. Keep employees knowledgeable when guidelines are developed, and tools are implemented. They will tend to adhere greater if people recognize the want for a responsible prolateness policy.

* **Train employees:** (Adrian Duigan, 2003)

This is one of the most useful periods. Because it not handiest helps you inform employees and facilitates them understand policies, but also lets in you to talk about the real meaning of the coverage. End customers will often ask questions or give examples in a education forum and this may be very rewarding. Because these questions will help you become aware of extra detailed rules and improve it to be more beneficial.

* **Get it in writing:** (Adrian Duigan, 2003)

Make sure all participants have read, signed and understood the policy. For large companies, use automated gear to assist electronically distribute and track document signatures. Some equipment even offers puzzle mechanisms to test user policy knowledge.

* **Set clear penalties and enforce them:** (Adrian Duigan, 2003)

There is a clean set of tactics in region that spell out the penalties for violations inside the safety policy. Security coverage is not a fixed of voluntary guidelines however a situation of employment. Then enforce them. A protection coverage with chaos compliance is nearly as bad as there may be no policy at all.

* **Update employees:** (Adrian Duigan, 2003)

People come and go. Databases are created and destroyed. Because the network itself is continually developing so the safety coverage is a dynamic file. Keeping the up to date safety policy is tough enough, but one factor is even greater hard, is to preserve employees aware about any adjustments that may affect their everyday activities. To succeed, open communication is the key.

* **Install the tools you need:** (Adrian Duigan, 2003)

Customizable units of policies for Internet content material and e-mail protection products can make certain that your policy, no matter how complex, is adhered to. One of the most effective purchases you have made is probably to put money into equipment to put in force protection guidelines.

### The responsibilities of employees and stakeholders in relation to security, and their role to implement security audit recommendations.

Stakeholder audit is a crucial thing of the continuing strategic improvement process. Your organization may advantage from stakeholder audits in other ways. Stakeholder audits are a mandatory thing of a hassle management program, they're part and part of top governance, and they are the important thing to collaboration. (tool, n.d.)

A crucial way wherein audits offer fee to stakeholders is thru assessing inner manage and making suggestions for improvements. (tool, n.d.)

Identifying of key stakeholders and their interests is important in: (tool, n.d.)

- Ensuring the fulfillment of an inner audit function.

- Ensuring internal audit efforts are appropriately aligned with the wishes of their employer.

Benefits of stakeholder plans: (tool, n.d.)

- Keeps you contemporary with emerging issues, risks, priorities

- Demonstrates how inner audit adds value

- Markets the contribution and services of inner audit (tool, n.d.)

**- Role of administrators: responsible for maintaining, configuring and retaining the operation of computer systems, servers or organizations.** (tool, n.d.)

**- Role of customers: folks who have interaction with organizations, who offer feedback, requests and comments to enhance and troubleshoot the more complete system.** (tool, n.d.)

**- Role of branches: branches will support each other for safety audits to enhance agency security.** (tool, n.d.)

**- Role of business partners: as a second birthday party to paintings with companies and help safety audit agencies, the two units will work together to comply with protection policies.** (tool, n.d.)

#### Recommendations:

Administrators/branches offer solutions and implement the following security measures: (UCLA, n.d.)

* **Application Visibility**: Reduce productivity losses, compliance issues, threat spread andrisk of data leakage (KerioControl, 2019)
* Encrypt company laptop hard disks: Less sensitive data can be stored on a laptop that can be encrypted to increase security.
* **Web Content Filtering:** Web content filtering solutions continually update thesewebsites and push these updates to your filter according to the schedule that administrators can define**.** (Rouse, 2011)
* **Network Security Analysis:** Scanning network rings and network devices allows you tothoroughly examine vulnerabilities in your environment.
* **Malware Scans:** Malware includes viruses, adware, spyware, worms, Trojans, SPAMand other active malicious content. Administrators can detect all this with products and eliminate threats to the enterprise intranet. (UCLA, n.d.)
* **Threat Security:** Stop bad apps. Scanning allowed applications for all types of threats.Do it at multi-Gbps speeds. (UCLA, n.d.)
* UTM multi-purpose firewall solution (Benefits - Protecting system ports (ports), preventing risks from the Internet environment.
* Anti-intrusion and anti-denial of service (DDoS) solutions (Benefits - Specialized equipment to prevent DDoS attacks.) (UCLA, n.d.)
* Network security and encryption solutions (Benefits - Dedicated solutions to protect connections between websites within the system, especially suitable for businesses with many branches and high security requirements on the road transmission. (UCLA, n.d.)
* Solution to detect security vulnerabilities (Benefits - Identify, monitor and offer solutions to address security vulnerabilities across the network, servers, operating systems, databases and applications.) (UCLA, n.d.)

Customers using the service include survey and evaluation of the following information: (Netwrix, n.d.)

* Data backup and recovery system
* Network transmission speed and stability
* Basic network devices (Routers, Switches, ...)
* Software support tools and network security devices (Firewalls, attack detection and prevention systems, VPN systems, etc.)
* Model of integrated system connection.

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

DRP stands for disaster recovery plan. In general, it is a plan or strategy for business continuousness in such time when disaster destroy the certain part of all the business resources like IT equipment including data records, physical hardware and space of and organization. The goal of DRP (disaster recovery plan) is to resume the normal computing capabilities in short time as could as possible. The successful DRP take step to prevent the possibility disaster from occurring. When DR plan is to be implemented it should be audit and plan so that there is no any fault on our plan. Disaster recovery plan involve the employee from management level to entry level. (Beal, n.d.) (Watts, 2018)

As I am IT supervisor of Finbank my activity is to secure community safety of financial institution and to secure statistics and facts from theft, hack and loss. There are different kinds of risks that can damage or disaster the safety coverage of FinBank. Here hazard means danger of damage, harm, hassle or any sorts of negative occurrence. There isn't any organization and agency which are safe from information disaster and pc protection danger. In the case of FinBank there are different kinds of threats that may smash information and safety policy of financial institution inclusive of failure in DHCP, earthquake, fireplace these sorts of natural catastrophe things can also spoil the organizational facts and records and protection coverage. As I am IT supervisor of FinBank, I have made some recovery plan against disaster and description of every is given below: (Beal, n.d.) (Watts, 2018)

#### Communication plan and role assignment

When it involves a disaster, communique is critical. A plan is critical because it places all employees on the same page and makes certain to truly define all communique. No depend how many employees you have, preserving in contact is extremely beneficial to constructing a believe network to your business. Make sure you may contact every other, irrespective of in which you are; make sure the disaster may be treated as soon because it happens. Remote employees or staff need to also recognize the tiers of disaster healing plan for procedural purposes, to ensure that everybody sings from the equal hymn. (Watts, 2018)

#### Outline a disaster recovery plan protocol for employees

Disaster recovery plans have to include an employee’s safety and security protocol in case of different disasters for example; fire, intruder. Define roles to different types of disaster and making sure that every employee understood the protocol. (Kirvan, 2009)

Also, we need to make sure and to realize the positions and priorities of employees while assigning their roles. Asking workforce to assist with the company's recovery plans to expand when their houses and families are stricken by disasters. Focusing your disaster healing plan protocol on getting local employees to protection and searching at the function of remote workers can assist with greater time-consuming tasks. (Kirvan, 2009)

#### Backup data

Make a listing of information, software program that wishes to be backed up, classified in line with importance, storage time, backup time, backup approach and device recuperation time from facts save. Data requirements of important records technology systems have to be subsidized up all through the day. (Cerini and Associates, 2018)

Data of important information technology systems have to be backed up to outside storage media (consisting of magnetic tape, difficult disk, optical disc or other storage media) and safely stored and saved one after the other from Area to conduct backup. Check and restore backup data from outside storage media at the least each six months. (Cerini and Associates, 2018)

#### Take inventory of all assets

Digital stock: make inventory of hardware and software applications, prioritized so as of importance. Each party must have a supplier's technical guide agreement linked to the proper contact information, to allow easy reference when needed. (Mark Talabis, 2012)

- Physical assets: statistics generation device, communique devices and system for the operation of statistics era systems.

- Information assets: records and records in digital shape and documents are expressed in paper files or other means.

- Software assets: device software, utility software, databases, application applications and development tools.

The unit makes a listing of all IT assets, reviews and updates this listing at least as soon as a year. (Mark Talabis, 2012)

#### Monitoring and logging operations of information technology systems

Recording and archiving logs on the operation of information technology systems and users, arising errors and unsafely incidents of the information technology system. Log data must be stored online for at least three months and backed up for at least one year. Take measures to monitor, analyze diaries, risk warnings, process and report results. Protection of logging and log information functions, anti-forgery and unauthorized access. (STEVENS, 2016)

System administrators and users must not delete or modify the system log to record their own activities. Time synchronization between information technology systems. (STEVENS, 2016)

#### Time recovery

Performing business impact analysis will help you solve any vulnerability within the restoration model and perceive the key factors of your IT infrastructure. This means you could create the perfect recuperation timeline on your business.

Every second counts to ensure that crucial systems can be restored as quick as possible. Determining the desirable healing time that statistics should be restored after a catastrophe presents the most time that disaster have to be addressed. It also facilitates you discover any vulnerabilities in your disaster restoration process because if the deadlines aren't met, there may be a potential problem. (Golding, 2015)

#### Disaster recovery plan against environmental factors

Environmental factors can destroy the organization’s property. Landslide, earthquake, flood, fire and fire this kind of things can be disaster threats for any organization. They can cause property damage not only this they can cause injury and death. (Beal, n.d.) (Watts, 2018) (Srivastava, 2010)

When we lost the data, information from these types of factors then we have to recover the data for this we need a disaster recovery plan to be implemented. Some of the disaster recovery plan against the environmental factor for FinBank is given below: (Beal, n.d.) (Watts, 2018) (Srivastava, 2010)

* Since natural disaster are unpredictable and cannot be avoid organization should try to lower the damage. First, build the earthquake resistant building, and building should be in such area where possibility of landslide and flood is very low, and it should be away from ocean so there is no chance of Tsunami, also company should have the fire extinguisher.
* Data backup is one of the main effective disaster recovery plans. Data backup help to resume or data and information when we lost it, so we have to keep the backup of data daily. Data backup could be one site storage or off-site storage. We can also keep the back up of data in cloud storage.
* The data backup center should keep far away from the current working area, so that when natural disaster hit in that place our backup could be safe.

#### Recovery plan when domain is hacked

We can use the RODC (read only domain controller) when area is hacked. According to IT pro “Read Only Domain controller (RODC) is a sort of domain controller which holds a examine only partition of energetic listing area services database”. (Buzdar, 2017)

RODC is in particular use in branch office to provide handiest study authentication. In case if our domain is hacked and should lose the statistics then we are able to get better the facts from the RODC. (Buzdar, 2017)

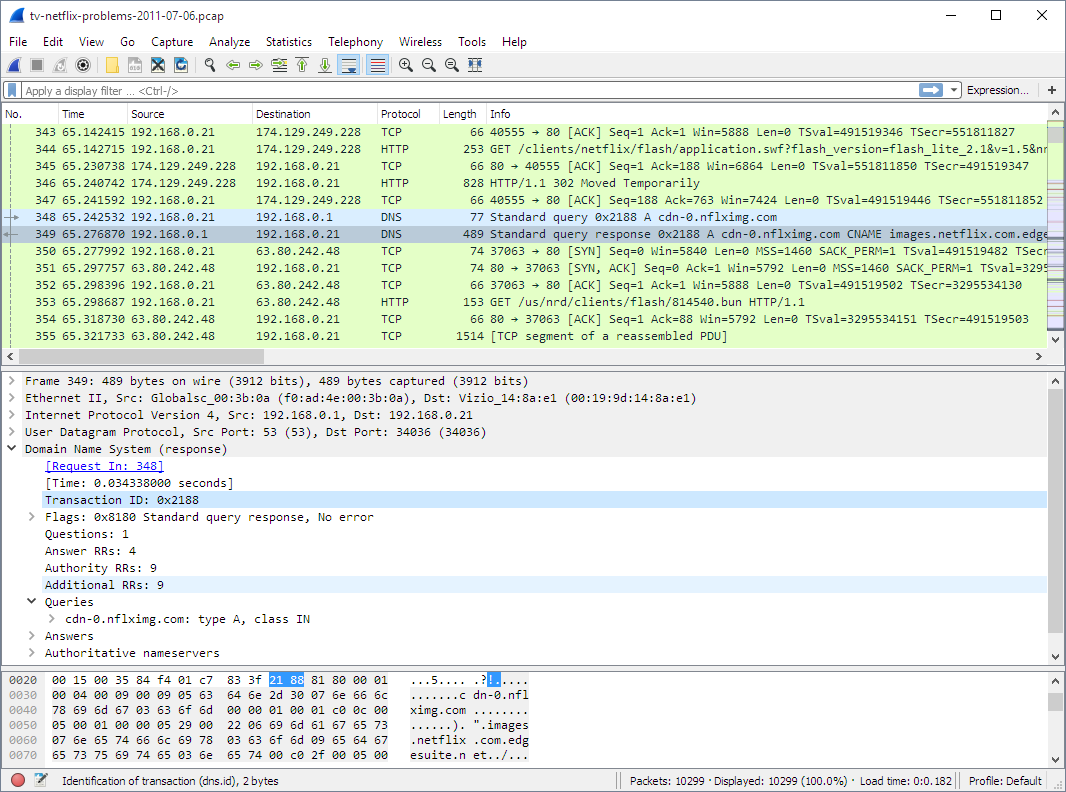
#### DHCP fail

When DHCP server fail or crashed user can’t access the email, the internet stops to work and also some apps no longer work. It is because of the DHCP server crash. In bank case if this happen then bank have to stop their services. To overcome from this problem, we can use DHCP console and PowerShell. (Scripto, 2013)

### Evaluate the suitability of the tools used in an organizational policy.

#### Wireshark

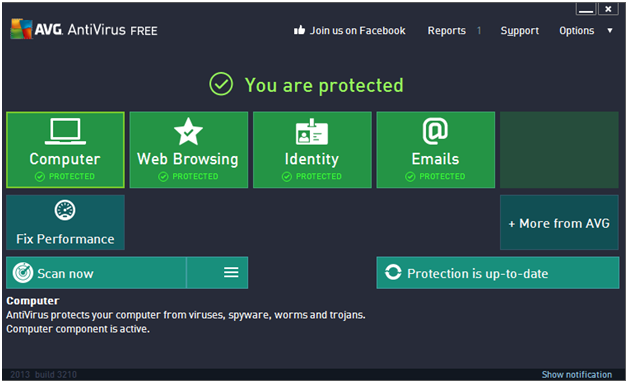
**Wireshark** is used as a tool to make analysis of network traffic. It will allow you to capture traffic and decodeeach package, showing you exactly what it has. Its task is to try to capture network packets and trying to show that packet data as possible. (Rouse, n.d.)



#### AVG Antivirus

**AVG Antivirus** is a tool to prevent viruses and malware to protect all important data on the system, while enhancing the performanceof your computer. (CompareCamp, n.d.)

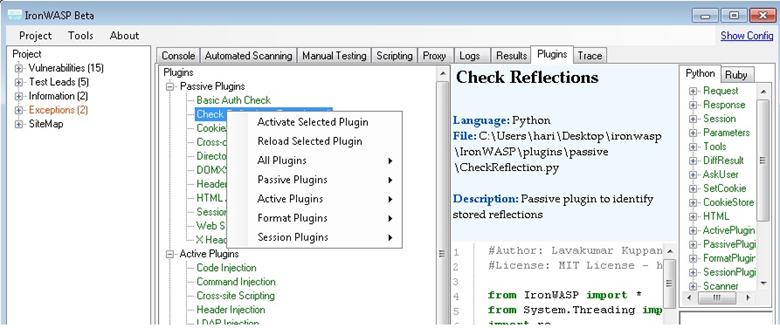
* **Protect the network through link scanning:** It provides intelligent protection mode that allows users to share files securelyon multiple environments. It supports keeping the network safe from cyber threats, ensuring that companies and employees will be able to access the Internet safely. (CompareCamp, n.d.)
* **Email Shield technology:** It also provides email protection technology that automatically scans email and deletes content thatcontains malware or any security threats. It blocks suspicious and dangerous email attachments. (CompareCamp, n.d.)
* **Improve features:** Scan PC performance issues, ensuring the best performance and stability for your PC. (CompareCamp, n.d.)
* **Get real-time security updates:** Monitor computer at all times and alert when there are potential threats. (CompareCamp, n.d.)



#### IronWASP

IronWASP (Iron Web Application Advanced Security Testing Platform) is an open source tool used for web application vulnerability trying out. It is designed in such a manner that customers having the right know-how can create their very own scanners using this as a framework. IronWASP is built the usage of Python and Ruby and customers having knowledge of them could be able to make full use of the platform. However, IronWASP gives with lots of features are easy to understand. This tool will help us protect network security of organization: (Dewan, n.d.)

* Static analysis, to scan compiled binaries to find weaknesses in web, mobile and desktop applications as well as micro services.
* Software component analysis, to identify vulnerabilities in open source components.
* Web application scanning, an Internet security test helps inventory, scan and monitor all publicly facing web applications.
* Time protection, to protect against application layer attacks in real time.



#### SoladWinds Network Configuration Manager

**SolarWinds Network Configuration Manager** will let you make certain that all tool configurations are standardized. It will allow you to push bulk configuration modifications to hundreds of network devices. It will hit upon unauthorized changes that is a sign of malicious configuration tampering. This tool let your speedy recover from errors with the aid of restoring previous configurations. You also can use its trade management features to quickly identify what has changed in the configuration document and highlight adjustments. Furthermore, this tool will let you display compliance and skip auditing as required via integrated industry standard reports. (Larue-Langlois, 2018)

A screenshot of a cell phone

Description automatically generated