

NETWORK SECURITY

INTERNATIONAL SCHOOL OF MANAGEMENT AND TECHNOLOGY



Bisesh Shrestha (HND/ First Semester)

Contents

[Part1 4](#_Toc94282188)

[P1 Identify types of security risks to organizations. 4](#_Toc94282189)

[Content: 6](#_Toc94282190)

[Introduction 6](#_Toc94282191)

[Types of security risk 6](#_Toc94282192)

[Physical risk: 6](#_Toc94282193)

[Malware 6](#_Toc94282194)

[Phishing 6](#_Toc94282195)

[Ransom ware 7](#_Toc94282196)

[Sql injection: 7](#_Toc94282197)

[DDoS 7](#_Toc94282198)

[Man in the middle attack: 8](#_Toc94282199)

[Password attack: 8](#_Toc94282200)

[ENVIRONMENT RISK: 8](#_Toc94282201)

[P2 Describe organizational security procedures 9](#_Toc94282202)

[Risk analysis 9](#_Toc94282203)

[Evaluating the risk 9](#_Toc94282204)

[Develop a system security plan 9](#_Toc94282205)

[Mitigate the risk 9](#_Toc94282206)

[Conclusion 9](#_Toc94282207)

[Part: 2 10](#_Toc94282208)

[P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third- party VPNs. 10](#_Toc94282209)

[Introduction 10](#_Toc94282210)

[Firewall 10](#_Toc94282211)

[Packet filtering firewalls 11](#_Toc94282212)

[Proxy firewalls 11](#_Toc94282213)

[Next-generation firewalls 11](#_Toc94282214)

[Network address translation firewalls 11](#_Toc94282215)

[Stateful multilayer inspection (SMLI) firewalls 11](#_Toc94282216)

[VPN 13](#_Toc94282217)

[P4: Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security 15](#_Toc94282218)

[DMZ 15](#_Toc94282219)

[Static IP 16](#_Toc94282220)

[NAT 17](#_Toc94282221)

[Conclusion 18](#_Toc94282222)

[Part 3: 19](#_Toc94282223)

[P5 Discuss risk assessment procedures. 19](#_Toc94282224)

[P6 Explain data protection processes and regulations as applicable to an organization. 23](#_Toc94282225)

[Conclusion 23](#_Toc94282226)

[Part 4: 24](#_Toc94282227)

[Introduction 24](#_Toc94282228)

[Purpose of bank security policy 24](#_Toc94282229)

[Objectives of bank security policy 24](#_Toc94282230)

[Organizational structure for sunrise bank 25](#_Toc94282231)

[Technical and user documentation 25](#_Toc94282232)

[Technical 25](#_Toc94282233)

[User 26](#_Toc94282234)

[Password policy 26](#_Toc94282235)

[Enforce password history 28](#_Toc94282236)

[Minimum password Age 28](#_Toc94282237)

[Maximum Password Age 28](#_Toc94282238)

[Minimum password length 28](#_Toc94282239)

[Password complexity requirements 28](#_Toc94282240)

[Account lockout policy 28](#_Toc94282241)

[NTFs Security policy: 29](#_Toc94282242)

[Quota Management: 31](#_Toc94282243)

[Encryption 34](#_Toc94282244)

[Firewall Management policy 35](#_Toc94282245)

[P8 List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion. 39](#_Toc94282246)

[Conclusion 40](#_Toc94282247)

[References 41](#_Toc94282248)

# Part1

Before you start the implementation of the IT security measure for the organization, you need to assess the IT security risks in the organization. You need to consider various aspects of risks such as unauthorized access of the system and data, naturally occurring risks, host, application and network risks etc. You are required to consider organizational security procedure such as business continuance, backup/restoration, audits etc. and then produce a report for the CEO of Sunrise Bank containing: 1. Identified security risk types to the organization along with description of organizational security procedure. 2. Develop a proposal of a method to assess and treat IT security risks.

# P1 Identify types of security risks to organizations.

**Report: On the Identification of security risk types to the organization**

**Prepared by: Bisesh Shrestha**

# Content:

* Introduction
* Types of security risk
* Organizational security procedure
* Method to access and treat security risk
* Conclusion

## Introduction

Anything that can harm or steal your data, or allow someone else to access your information without your consent or knowledge, is a security risk on your computer. Malware, a term used to describe some types of harmful software, is one of many things that might harm your computer. Viruses, worms, malware, spyware, and trojan horses are all examples of malicious software that can compromise a computer's security. Risks can arise from both the failure to install computer hardware and the use of unhealthy programming methods. Let's look at these in more detail. The threat to security might be either environmental or physical.

## Types of security risk

## Physical risk:

### Malware

Perhaps the most basic and familiar threat to many users, malware covers a wide range of unwanted programs that can cause any number of issues for a business, from destroying data to sapping resources by turning machines into malware or crypto currency miners. There are a few key categories, such as viruses, which seek to replicate and spread as widely as possible, Trojans, which gain entry to networks by disguising themselves as legitimate applications, and spyware, which looks to monitor an employee's usage to gather sensitive data. Defending against these multitude of threats is no easy task, which is why having strong antimalware tools is paramount. There are hundreds of tools out there claiming to offer protection, but firms need to ensure the solutions they choose can detect even previously unknown malware by spotting their key characteristics - for example, a program that tries to hide once installed. It's also essential this is kept up to date and is able to scan every potential entry point to a network, from emails to USB flash drives.

### Phishing

Phishing is one of the most frequent forms of social engineering attack. It includes sending emails that appear to be from a known and trusted source, generally with a bogus link that urges recipients to submit personal information into an online form. These are commonly used to get access to financial information or login and password combinations, but they may be used for much more - especially with the more targeted ‘spear phishing' variation, which is tailored to an individual receiver. A Snapchat employee, for example, provided crucial payroll information to a fraudster after receiving an email purporting to be from the company's CEO in 2016. The fraudster only had to ask for the information, and the naive employee promptly sent it to them. Effective email security technologies can help lessen the risk of such emails being delivered, but they aren't foolproof. As a result, user education is the most effective strategy to combat this threat. Firms should guarantee their staff are not handing over vital data to anybody who asks for it by educating them to be alert and detect the telltale indications of a phishing effort.

### Ransom ware

Ransom ware is a type of virus that encrypts key data on a system or network and then demands money - generally in the form of Bitcoin or another crypto currency - to decrypt them. This is a pretty straightforward type of attack, but it has the potential to be quite disruptive, as the WannaCry outbreak in 2017 demonstrated. An attack may encrypt certain file types, making it hard to access essential business information, or block vital system files, preventing a computer from starting up at all, depending on the type of ransom ware used.

### Sql injection:

We now know that SQL is used by many website data storage servers. As technology has grown, network security concerns have changed, resulting in the possibility of SQL injection attacks. SQL injection attacks are designed to target data-driven applications by exploiting security flaws in the application software. It has quickly escalated into one of the company's most serious data security issues.

### DDoS

DDoS attacks include an attacker overloading a system - usually a web server - with traffic requests until it can no longer handle the amount of requests it is being requested to send, slow it to a crawl and ultimately taking it down. This is a particularly difficult type of attack to counter since it requires minimal expertise and does not need attackers to enter a company's perimeter. Malware that supply the resources needed to conduct a DDoS attack may be purchased for a few dollars on the dark web. DDoS attacks were once seen to be more of a nuisance than a real danger to businesses. They may take a website down for a few hours, which would undoubtedly affect revenue for digital-focused businesses, but that was about the extent of their influence. The landscape, on the other hand, has changed. Sustained malware attack are larger than ever before, lasting days or weeks rather than hours, and they're increasingly being used as a cover for other operations, such as data theft, rather than as a means of achieving a goal in and of itself. As a result, preventive and corrective steps must be adopted. While firms may take numerous precautions themselves, such as bandwidth buffering, having a DDoS mitigation solution might be the most effective protection. Indeed, in 2018, Github was targeted by a DDoS malware that sent 1.35TB of data every hour - the greatest such assault ever recorded - but owing to its mitigation service, it was able to neutralize the attack in just eight minutes.

### Man in the middle attack:

Man in the middle attack is one of the most horrific threats to the network. An attacker here establishes an independent link to both sender and receiver, decodes their messages one by one, alters those messages and relays back to sender and receiver. All of this happens so quickly that both sender and receiver never get to know that someone is overhearing them. Furthermore it exposes the network to a range of other attacks.

### Password attack:

Passwords can be hard to remember, particularly if you follow the rules to &”strengthen them.” They may also be tricky at input, especially on mobile devices and small keyboards, and difficult and time-consuming to use when using different ones for each account is best practice.

### ENVIRONMENT RISK:

a. Flood and landslide: This form of risk can be seen in companies that are built near landslide areas. Landslides and flooding are more common during rainy seasons.

b. Earthquake: It's a natural calamity. When businesses were built in earthquake-prone areas, there was a greater risk of an earthquake happening. This form of danger is common.

c. Fire: Although it is a human risk, it is assessed as an environmental one. If a company’s building is constructed on a hypertension line, these types of risks are clear, and they have often occurred as a result of employee error.

d. vandalism: Vandalism is such an act which can cause damage to property and organization’s assets. This is an external physical threat.

e. Data Theft: Data theft refers to accessing and getting copies of data without the permission of authorized parties. This could be internal or external.

# P2 Describe organizational security procedures

Your computer network is one of your company's most significant assets. It allows your staff to collaborate on a variety of projects for various corporate divisions and clients, as well as save all of your important company data. To guarantee that your organization's computer network continues to function effectively, you must follow network protection policies and procedures. The process of attempting to support protection in an organization involves a variety of methods. The measures are a risk-mitigation method. The measures that have been announced must have improved risk justification results. These measures will aid you in detecting, assessing, evaluating, and managing risks using the most appropriate techniques. The following are some of the security procedures used by the organization:

Risk analysis: Each risk analysis will include some fundamental risks, but depending on the design, more threats may be added. Unauthorized access, for example, is a common sort of danger. An authorized user's misuse of information (or authority), Unintentional information sharing or data leakage.

Evaluating the risk: After identifying and analyzing the risk you need to evaluate the main risk that can be harmful and dangerous to the computer security. It focuses on avoiding security risk and bugs. It defines, evaluates and implements essential security control.

Develop a system security plan: The System Security Plan (SSP) is the key document of a security plan in which a CSP defines all the security measures in use and their application on the information system When completed, an SSP provides a detailed overview of the security control implementation of a CSP, a detailed system summary including inventory of components and resources and detailed descriptions of the data flows and authorization boundaries of the system.

Mitigate the risk: You can build the infrastructure for IT security but you can’t eliminate all the risks. You repair what happened when a disaster occurs, evaluate why it occurred, and seek toprevent it from happening again or at least make the effects less detrimental.

# Conclusion

In this report, I've identified many types of IT security concerns that the company faces. Because these dangers have caused organizations to fail to accomplish their objectives, it is essential to address them. As a result, I have written on how to address them as well as the many types of organization security policies.

# Part: 2

Once the assessment of the risks and proposal for its remedy has been made you need to describe IT security solution for the organization such as VPNs, firewall, DMZ with a suitable implementation example. You need to:

1. Identify the potential impact to IT security using firewall and VPNs and make aware of the repercussion of incorrect configuration of firewall policies and third party VPNs.

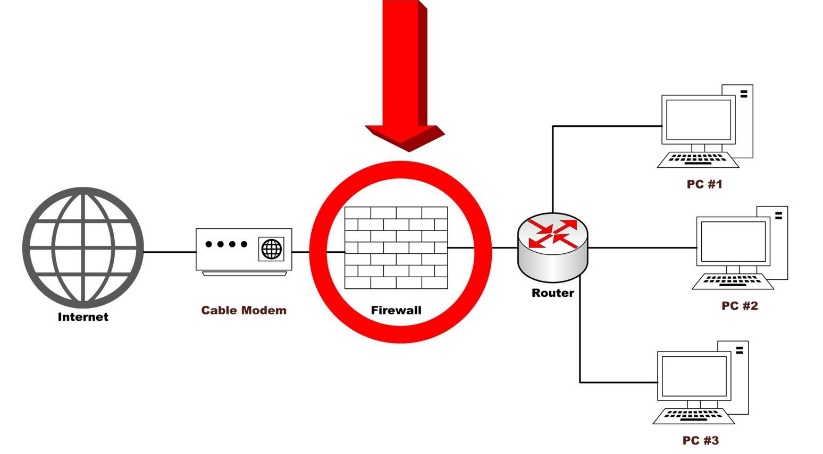
2. Show through an example in simulated environment, how implementing a DMZ, Static IP ad NAT in a network can improve Network Security.

# P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third- party VPNs.

# Introduction

In this part I am going to describe it security solution for the organization sus as VPNs, firewall, dmz with suitable implementation.

## Firewall



A firewall is a network security instrument that monitors incoming and outgoing network traffic and allows or disallows data packet entrance based on security rules. Its primary function is to create a barrier between the internal network and external sources in order to block infections such as viruses and spyware. To prevent attacks, firewalls carefully examine incoming traffic based on previously set rules and filter traffic coming from dangerous or suspicious sources. Firewalls protect traffic passing through ports, which are the points exposed to external sources. There are two types of firewalls:

1. Software Firewall: Software firewalls are programs that are installed on a computer and regulate traffic across port numbers.
2. Hardware firewalls: Hardware firewalls are physical devices that link devices to the gateway.

### Packet filtering firewalls

Packet filtering firewalls are another sort of firewall, and they are the most commonly used. The packets are checked to see if they fit the security rule by looking at their source and destination IP addresses. The packet is permitted to cross into the network if it meets the rule. Stateless and stateful packet filtering firewalls are two types of packet filtering firewalls. Firewalls that are stateless check packets separately and do not have conditions, whereas stateful firewalls maintain information about previously entered packets. Hence stateful firewalls are considered more secure than stateless

### Proxy firewalls

Proxy firewalls sit in the middle of two systems. They normally filter traffic at the application layer, which is the OSI model's seventh layer. When a user sends a request to the firewall, it is analyzed to see if it matches the security rules, and if it does, the service is either blocked or allowed. They commonly use stateful and deep packet inspection to identify malware in FTP and HTTP traffic.

### Next-generation firewalls

Next-generation firewalls, or NGFWs, are a hybrid of traditional firewall technology with intrusion prevention systems that examine encrypted information. Deep packet inspection, which looks at the data in packets as well as the packet headers, is also used by NGFW. This enables packets containing questionable data to be identified, sorted, and blocked.

### Network address translation firewalls

NAT firewalls, also known as network address translation firewalls, allow several devices to connect to the internet using a single IP address and multiple network addresses. Hackers and attackers are unable to monitor IP addresses or obtain information as a result of this. This increases the level of protection against threats. NAT and proxy firewalls are similar in that they function as a barrier between devices and outside traffic.

### Stateful multilayer inspection (SMLI) firewalls

Stateful multilayer inspection (SMLI) firewalls work similarly to NGFW firewalls in that they evaluate the entire packet and allow it to pass if it enters each layer separately. It is mostly related to the network, transport, and application layers, and it filters packets by comparing them to dependable packets.

A firewall can be implemented using pfsense like software. After installing the pfsense the user gets a boot up menu as follows.

If the WAN and LAN IP addresses are not configured through the DHCP the user has to manually add the IP addresses by entering the 2nd option from the above menu.

In this area the interfaces to be configured must be mentioned.

Manually the LAN IP address is given as above:

* Now the IP addresses are assigned properly. So, the user should press enter and give a system reboot. Then through the browser he have to call the pfsense login by entering the assigned IP address (in this case 192.168.0.1).
* As you get this interface the user has to login using the temporary username ‘admin’ and password ‘pfsense’.
* In this menu the user has to add the host name and domain name and perform the basic settings.
* As the password given to everyone is a common one the security level is low in this condition. So, the user can provide a new password according to his preference in the above interface.
* Above is the dashboard of pfsense after configuring basic settings. After configuring the basic settings and password user can add firewall rules which will filter the packets entering into the device or network.
* To create a security rule the user has to go to the rules menu in the firewall settings. Then user will get the following interface.
* By clicking ‘add’ button the user can create a new rule.
* Now in this interface the user can create a block or allow rule and enter the details like IP address, interface type, protocols involved and other basic details about the rule. By clicking ‘save’ the rule will be saved.
* After saving the rule user has to click ‘apply changes’ button to proceed.
* After the settings are properly configured. If the user tries to enter to the site he blocked, it will give the above result which means the user successfully blocked the site with help of firewall.

Although firewall is an important security tool some misconfigurations done can cause attackers to peek in to the data of the organization. According to Wickert (2015), five common firewall misconfigurations are as follows:

* Extensive policy Configurations.

As network administrators tend to set broad rules and work backwards firewalls tend to be with open policies most of time which permits any traffic from source to destination. This is due to work pressures or not giving priority when they create firewall rules. So, the firewall tends to have some loop holes which can allow attackers to peek into organization’s data.

* Risky rogue services and administration services.

Unnecessary keep on running in the firewalls can be very risky. One such wrong practice is dynamic routing and the other is rogue DHCP servers on network distributing IP’s. Because of this availability issues will be formed as an outcome of IP conflicts.

* Authentication mechanisms are not standardized.

Network devices not being configured according to proper standards can be risky. Which will allow weak passwords and anyone will be able to access sensitive data.

So, when considered authentication mechanisms like password they should be up to the standardized levels.

* System testing using production data.

Production data of an organization is a very sensitive kind of data. Most of the organizations have a tendency to test their security systems with their production data which allows the data to be exposed into an unsafe environment. So, it is better to do testing with simulated data.

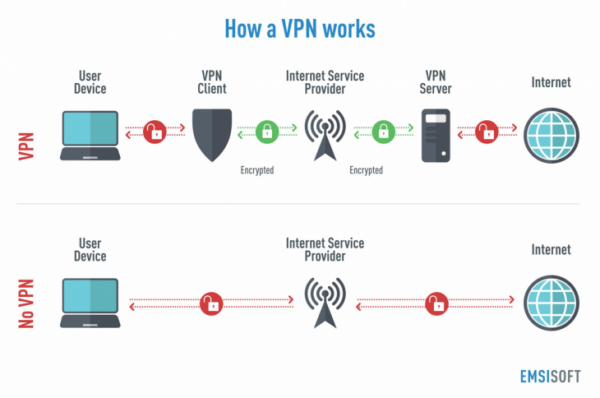
* Security devices with log outputs.

Not analyzing log outputs from their devices is a risky issue. This will keep the administrators blinded from the ongoing attacks and wouldn’t allow any details about the data theft.

So, it is better to effectively configure the firewalls as they can be the main reason for the low security levels of the organization.

## VPN

A VPN, or virtual private network, is an encrypted internet connection between a device and a network (Cisco, 2019). The link's encryption quality allows data to be transmitted safely and prevents unlawful persons from peering into the flow, allowing the user to operate surreptitiously. A virtual private network (VPN) is a secure and private internet connection. The traffic stays private because it is encrypted inside the route between the device and the network. This enables the capacity to securely move data across two networks. Creating an encrypted link via the internet is referred to as tunneling.



Remote access and site-to-site VPNs are the two types of VPNs. Remote access is a VPN connection that allows you to connect your network to an external device, often known as an endpoint. Before connecting to an endpoint, security checks are run to confirm that it is a trustworthy device. Site-to-site a virtual private network (VPN) is a sort of connection that may be used to connect an organization's branches. These connections eliminate the inconvenient complications that arise while building a network between two branches, while also ensuring safety.

VPN, although being one of the safest technologies, has its own set of problems. There are four issues with VPN connections:

* **Rejection of VPN connection.**

The VPN connection may suddenly stop operating without warning. One of the most prevalent VPN issues is the difficulty to connect. In this case, the user should check to see if the routing and remote access service is up and operating. If this is confirmed, the user should attempt pinging the VPN server using the IP address supplied by the VPN client to ensure that TCP/IP communication is working. Alternatively, ping again to see if there's a DNS issue and take necessary measures to fix it.

* **Unauthorized connection getting accepted.**

Unauthorized connections which are approved might compromise security. When viewing a user's properties sheet in the 'Active Directory Users and Computers' interface, the user will notice the Dial In tab, which offers a control option for remote access policy access. The user will be able to connect to the VPN if this option is enabled and the active remote access policy is set to allow remote access.

* **Reaching locations beyond the VPN server is not allowed**.

This is a typical issue that prevents users from accessing networks beyond the VPN server. The source of this problem is that the user is not authorized to access the entire network.

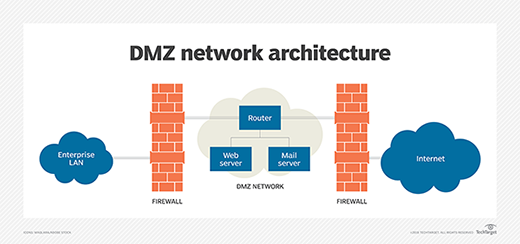
* **Failure to establish a tunnel.**

Even if all of the functions operate, the VPN may not always enable the user to construct a tunnel between the client and the server. This problem exists for two reasons. One or more routers may be involved in the packet filtering process, which may cause IP tunnel communication to be blocked. Another cause is the use of a proxy server between the client and the VPN server. The connection between the device and the internet is NATed by the proxy server, so packets seem to be originating from the proxy rather than the device. This situation may prohibit VPN from establishing a tunnel.

# P4: Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security

## DMZ

The Demilitarized Zone, or DMZ, is a computer security approach that involves creating a tiny sub network between a reliable internal network and an untrustworthy external network. (Webopedia,2019)A DMZ offers an extra layer of security to a company's LAN. While the remainder of the organization's network is safe behind a firewall, a protected and observed network node facing the outside of the internal network can access what is exposed in the DMZ. When a DMZ is correctly set up, it protects the company by allowing it to recognize and handle risks before they reach the inside network and harm important data.



The DMZ network protects the network from malicious sources such as emails, web servers, and DNS servers. They are situated in the monitored sub network to help defend the remainder of the network if they become compromised because to the greater propensity for attack. Because data traveling over the DMZ is not secure, access authorizations to services within the network are strictly regulated. To maintain the safety of the protected zone, hosts in the DMZ and the external network do not communicate with one another. As a result, devices in the protected zone may connect with both internal and external networks, thanks to the firewall, which filters and regulates data flowing between the DMZ and the internal network. While creating a DMZ zone, be sure to include any services that users will need when communicating with them via an external network. Web servers, mail servers, and FTP servers are examples of these services. Web servers are in charge of communicating with an internal database server, which must be located in the DMZ. This protects the database's security, which is responsible for storing sensitive information. Private emails, database login credentials, and personal messages are all stored on mail servers. Email servers are placed in the DMZ zone for this purpose, allowing them to access the email database without being exposed to potentially dangerous traffic. FTP servers enable for direct file communication. Because an FTP server should be isolated from the rest of the system.

There are two ways to create a DMZ. One has a single firewall, whereas the other has two firewalls

Single firewall: A firewall and three network interfaces make up the DMZ. The DMZ is located behind the firewall. The external network is created via a link from the internet service provider, the internal network is connected to the second device, and the DMZ connections are handled by the third device.

Dual firewall: Two firewalls make up the DMZ. The first firewall filters traffic to and from the DMZ, while the second firewall filters traffic from the DMZ to the inner network. This DMZ is more secure since it filters traffic twice, but it is also highly costly to set up.

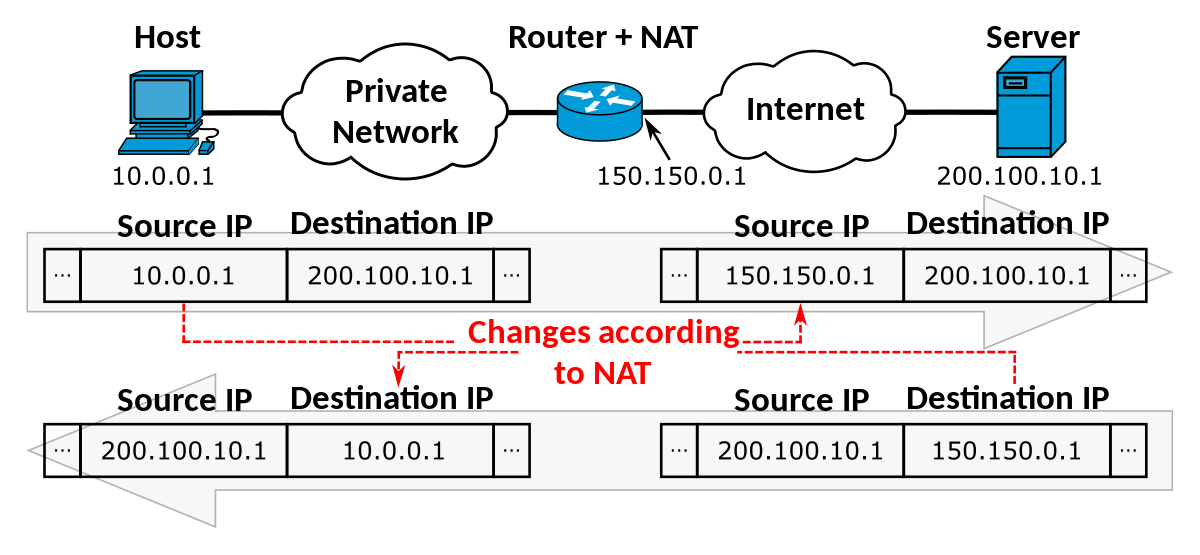
## Static IP

A static IP address is the polar opposite of a dynamic IP address: it is a permanent IP address issued to a device (an IP address which changes). For devices that require regular access, static IP addresses are required. If the computer is set up as a server, such as an FTP server or a web server, they'll be required. This static IP can be used in an organization to share a resource with several devices. Users do not need to continually seek for the IP address if we assign a static IP address to a printer, as they do with a dynamic IP address. Static IP addresses can be beneficial since they provide better security against attacks than DHCP pool addresses. If a hacker or attacker breaks into the pool, all of the IP addresses are revealed. The security level of a static IP address is higher since it is a private address that is difficult to monitor.

If your network doesn't support DHCP, you'll need a static IP address. Then a static IP is the best option. In the event that a DHCP pool assigns an IP address that is already allocated to another device, IP address conflicts may develop, and a static IP address may be the answer. Since a dynamic dress is not very safe and has issues compared to static IP address an organization can use static IP address which allows them to have a problem free network.

## NAT

NAT, or network address translation, is a protocol that allows a LAN (local area network) to utilize one set of IP addresses for internal traffic and another set for exterior traffic (Webopedia.com, 2019). NAT allows a router-like device to function as an agent between the public network and the local network, effectively representing a collection of machines with a single IP address. Static NAT, dynamic NAT, overloading, and overlapping are all examples of NAT. Static NAT is the mapping of an unregistered IP address to a registered address on a one-to-one basis. When a device has to be accessed from a different network, this is handy. Below is how static NAT works.



Dynamic NAT creates a group of registered IP addresses by mapping unregistered IP to registered IP.

Overloading is a sort of dynamic NAT that uses a variety of ports to map several unregistered IP addresses to a single IP address. Despite the fact that all of the devices have the same IP address, they have separate port numbers to distinguish them. As a result, this is referred to as a PAT, or port address translation.

When the IP addresses used on your internal network are registered IP addresses that are also used on another network, the router must have a lookup table of these addresses in order to interrupt them and replace them with registered IP addresses. Internal addresses are translated to registered addresses, and external registered addresses are translated to addresses that are unique to the hidden network.

# Conclusion

We can therefore make our network safe and trusted using distinct policies such as firewall policies and third-party VPN. We may use DMZ, static IP, NAT in a network to enhance network security, not just these policies. Only our company can do all the job securely if our network is steady for a long time, and can manage the organization.

# Part 3:

Once you have identified IT risks and viable security solutions, you need to review the mechanisms to control organizational security. Consider various aspects of network change management, audit controls, disaster recovery plans, Data Protection Acts, Computer Misuse Act,ISO 3001 standards, etc. You need to:

1. Discuss risk assessment procedures and explain data protection processes and regulations as applicable to the organization.

# P5 Discuss risk assessment procedures.

Understanding, managing, limiting, and minimizing risk is what security risk assessment is all about. It's an important part of every company's risk management strategy and data security activities (UpGuard, 2019). Risk assessment is an essential element for firms dealing with information technology and information systems. The key stage in risk assessment procedures is recognizing the threats and dangers the company is now and will face in the future. Risk is a measurement that may be used to calculate the risk of a reputational or financial loss. It can be classified as zero, low, medium, or high. Threats involved, vulnerability degree, and value of information the threat can effect are the three main aspects to consider when assessing a risk. The following equation explains how to calculate risk.

Proper risk assessment allows to recognize, estimate and prioritize risks in organizational operations, assets and individuals. Risk assessment always concerns about facts like,

* Most important assets: Looking through for the most important assets gives an idea about what risks those assets may face. So, to identify the risk we have rank the assets of the organization according to their importance.
* Data breach: Release of confidential information due to a cyber-attack, malware or human errors is referred to as data breach. What kind of data leak could affect the organization’s security the most? Can be identified by observing the data breaching methods.
* Threats and threat sources: In risk assessment understanding threats is a crucial factor but along with it having an idea about what sources allow the threat into the framework allows the organization to manipulate those sources to bring zero threats.
* Exploiting vulnerabilities: In risk assessment understanding external and internal vulnerabilities and impact of them on the organization should be exploited.
* Level of risk: Every organization have a limit on how much risk they can bare. So understanding the level of risk the organization bare allows the administrators to take proper actions to mitigate the risk.

Doing proper risk assessment can bring a lot of advantages to the organization especially in the security sector.

* Cost reduction: Identifying the threats and vulnerabilities beforehand allows the organization prepare themselves to successfully face them with zero risk. Therefore, unnecessary expenses spent on damages can be removed.
* Less data breach and data loss: Data loss or leakage can affect the organization in a massive manner. Risk assessment mitigates the probability of data loss or leakage so the organization will be able to compete better with its rivals,
* Insights to the organization: Observing for the threats can give a better take on the organization which can help to improve the deficient matters in the organization. This also helps in future planning.

Risk assessment can be done in two ways as qualitative risk assessment and quantitative risk assessment. Qualitative risk assessment refers to assessment done in numerical value. Quantitative risk assessment assesses monetary value to each device.

Quantitative loss can be calculate using following equation,

Here SLE (single loss expectancy) means monetary basis loss on a single incident, ARO (Annualized rate of occurrence) means the amount of times the incident occurs annually and ALE (Annualized loss expectancy) means the total monetary basis loss due to the incident annually.

When performing risk assessment, we have to drill down into the lowest segments of the organization. Similarly, a better understanding about the data and infrastructure of the organization is needed. According to UpGuard (2019), risk assessment can be performed in eight steps as follows.  
**Step 01: Determine the value of information.**

Any organization's information is critical. Understanding the value of the organization's information is a critical component. Because it is linked to elements like legal, financial, and profitability, the sensitivity level of information can be quite important. When determining the information value, we must consider the penalties associated with losing or exposing information, the value of the information to the organization's competitors, scratch and backups of the information or the ability to recreate the information in the event of an emergency, the cost associated with the recreation, the impact of losing data on day-to-day business operations, and the damage to the organization's reputation.

**Step 02: Identifying and ranking the organizations assets.**

Every object and person may have a different worth. As a result, prioritizing and evaluating the item based on its worth is critical. It can help the assessor get a better picture of which assets require more care than others. Otherwise, the assessor will have to evaluate every single facility, data, employee, and piece of office equipment. The assessor creates a list of assets based on their priority and inspects factors such as software and apps throughout this procedure. Hardware, data, interfaces, and users, asset purpose, functional and non-functional needs, security policy and architecture, and information storage and flow.

**Step 03: Recognizing threats.**

Threat is something which can cause to exploit a vulnerability to crack to the security and endanger the system. There are two types of threats as logical threats and physical threats. Logical threats are malware and hackers.

- Malware are malicious programs or files which can cause harm to user and his data. Virus, Trojan horses, worms and spyware are examples for malware. To minimize we can use virus guards and other mechanics.

- Hackers are is an expert programmer who uses his knowledge to break into computer systems and sometimes harm or manipulate the data according to his preference.

Physical threats are natural disasters, system breakdowns, human blunders, data breach and data loss.

- Natural disasters like flood, earthquakes and lightening can cause threat to the organization assets which can loss important data. If the threat is high in the current place, we can consider shifting to a safer place or placing the backup server in a safer place.

- System breakdown can loss data which can harm the normal routine of the business. Here we can consider whether the equipment we are using of a of high quality or can they tolerate the failures.

- Human blunders can cause to threat the security of the organization. We have to check whether proper training is given to employees on using and handling the systems. And check whether backup procedure is working well and passwords are managed.

- Data breach and data loss can harm the functions of the organization. So, it is better to tighten the security of data storage and keep them confidential.

In above manner the assessor should recognize the threats and list them down along with their impact on the organization and think of ways to try to minimize them.

**Step 04: Vulnerability recognition.**

Vulnerability is a type of flaw that compromises an organization's security. By reviewing vulnerability analysis or audit data, the assessor should be able to spot the flaws. In addition, the assessor should consider the potential harm to the organization's data and how to avoid vulnerabilities.

**Step 05: Evaluate and implement new controls.**

Threats and weaknesses are addressed by controls. There are two sorts of controls: preventative and detective. Preventive controls work to prevent dangers from occurring, whereas investigative controls work to identify threats and weaknesses. The assessor should go over the current controls in place at the organization and look for any loopholes, as well as evaluate their effectiveness. If the current security measures are insufficient to limit the risk, the assessor might look for and install new controls in the future.

**Step 06: Measure the impact and possibility of some situations on per year basis.**

When it comes to risk assessment, probability is important. The assessor must consider how frequently such risks might occur in a year and how much money the firm would lose as a result of those events. For example, if the company suffers a data breach, the damage might be $5 million each year. Because of this analysis, the company can forecast how much money it will require each year to attain break-even profitability.

**Step 07: Rank risks according to the cost of prevention and value of information.**

The threats are ranked according to their risk level in this stage. High-risk risks require urgent attention, medium-risk risks may be given a limited amount of time to take action, and low-risk risks can be taken later. This may enable top managers and accountable individuals to respond to threats while taking into account organizational rules, legal considerations, and laws.

**Step 08: Documenting the risk assessment report.**

Finally, the assessor must write a report that details the risks, vulnerabilities, and countermeasures. Aside from the current facts, the assessor might offer his opinions on the issues. This report will assist management in making right and effective decisions about the organization's security sector.

A business may execute a thorough risk assessment approach and strengthen security by following the procedures outlined above.

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

To retain the organization's goodwill in front of consumers, partners, and other relevant persons, any type of business need a set of data protection laws and regulations. As a result, various laws and regulations need be enacted to this end. GDPR, or General Data Protection Regulation, is a set of rules governing data protection. The following are the rules:

* Data should be attained and processed justly and legally.
* Data must be attained for a definite and legal purpose and shall not be processed in any manner incompatible with that purpose.
* Data should be suitable, appropriate and not unnecessary for those purposes.
* Data should be precise and kept up to date.
* Data should not be kept longer than is required for that purpose.
* Data should be processed in accord with the data subject rights.
* Data should be kept safe from illegal access, unintentional loss or devastation.

Risk management is a technique for identifying dangers and risks and controlling them with precise controls and procedures. In 2009, the ISO organization, which is best recognized for giving product quality certificates, launched a risk management system. This approach is made up of two parts: a framework and a process. In operations, the framework directs the organization's structure and risk management. Through the management system, the framework assists the company in assimilation of risk management. The following pieces make up the framework. (2011, Avalution)

* Policy and Governance: Runs the instructions and determines the pledge of the organization.
* Program Design: Total framework for management of risks is designed as per a current basis.
* Implementation: Executing the planned structure.
* Monitoring and Review: Constant track the performance and check for loop holes.
* Continual Improvement: Make changes to improve the quality of risk management procedure.

# Conclusion

The risk that is seen in the organization can be identified, analyzed and evaluated according to the risk Assessment procedure.

# Part 4:

**Lastly you will produce technical and user documentation which will be given to the company for the management of organizational security. You have to design and implement a security policy for the bank which will**

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

# Introduction

In this part I am going to design and implement a security policy for an organization and also I am going to list the main components of an organizational disaster recovery plan, justifying the reasons for inclusion.

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

By designing and implementing network security policies, all types of networks may be protected from external attacks. Proper network security policies bridge the gap between an organization's stated security goals and its actual security needs for users and administrators. If a company decides to use a set of security technologies without at least establishing an implicit security policy, the network security strategy will be meaningless.

## Purpose of bank security policy

The purpose of sunrise bank is:

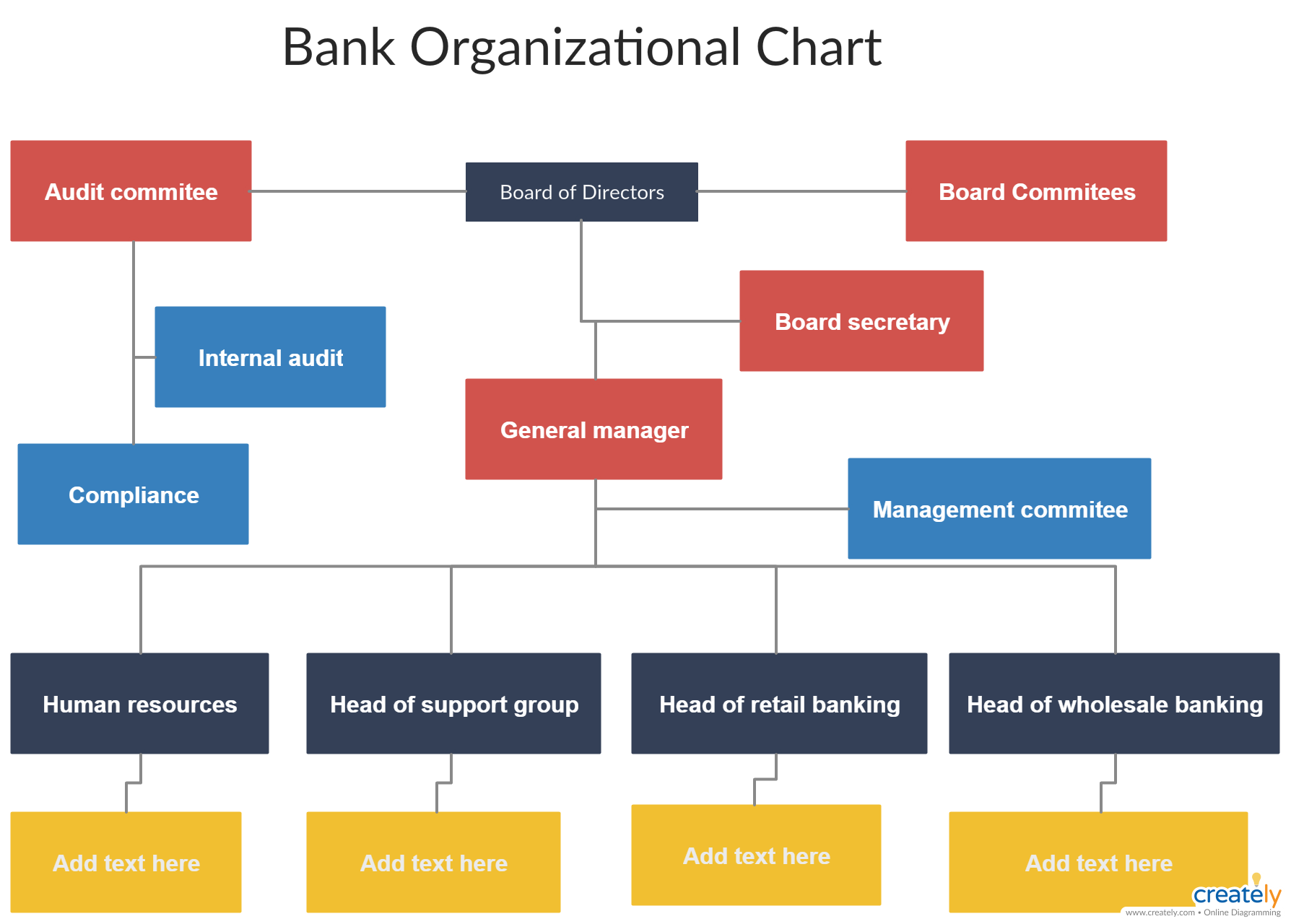
* It's important to understand the risks and threats that the bank’s information system faces.
* It is necessary to evaluate the risks and their possible exposures.
* An adequate information security system, as well as administrative, technological, and physical security measures, must be established to reduce such recognized risks, threats, and exposures.

## Objectives of bank security policy

The objectives for designing and implementing security policies are described below: -

* Protect the bank’s system from unauthorized access to our client details, which could cause significant harm or inconvenience to any customer.
* Establish a policy standard for the management and control of risks that have been established.
* Ensure that customer information collected, processed, and retained by the bank is kept confidential, safe, and accurate.
* Ensure that customer and bank information is safeguarded against security threats.
* Software and hardware components that comprise the bank&#39;s information technology are secured.

## Organizational structure for sunrise bank



## Technical and user documentation

### Technical

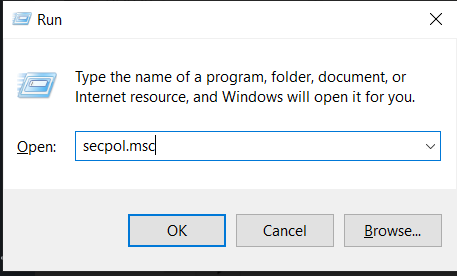
Technical documentation is the documentation that explains how a product or service works. When the network is provided by the Internet Provider, we have an excellent management of organizational security, comparable to our bank, which incorporates our finest security measures. After getting internet from the network, we installed firewalls, followed by a router with firewall for filtering Internet protocol as it flows via a server and to the client. In the context of server, we have Web server, Active Directory Server, Print Server, Database Server, DHCP Server, DNS Server, and more servers to govern every client activity. On the client side, we have numerous Switches that send the various securities strategies to the customer. We have numerous VLANs that encompass diverse departments such as General Banking, Human Resources, and Information Technology in the context of the customer.

### User

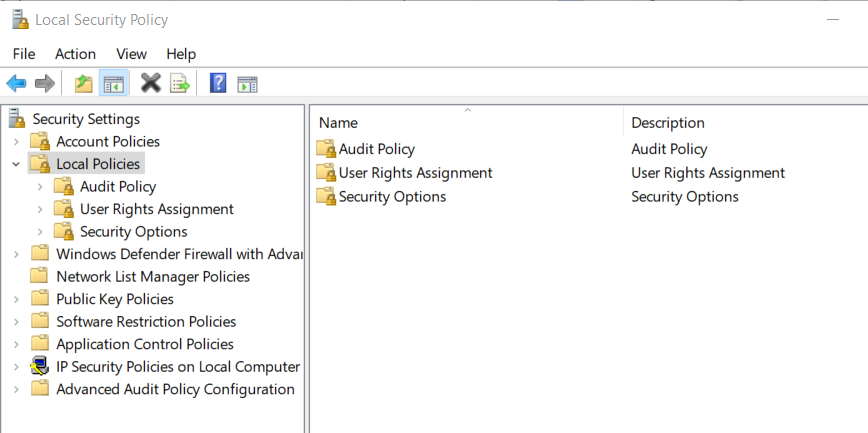
We are unable to provide such information on the organization's security rules in this scenario since user documentation necessitates several user guides for organizational security policies. As a result, we now have an application or software that consumers may utilize to do routine banking chores. Users can gain access to certain rights in order to use certain policies, such as mobile banking for general banking such as money transfers, for various payments of the bank's various facilities, for the creation of a user to be a part of the bank, and for learning and achieving the bank's various features.

## Password policy

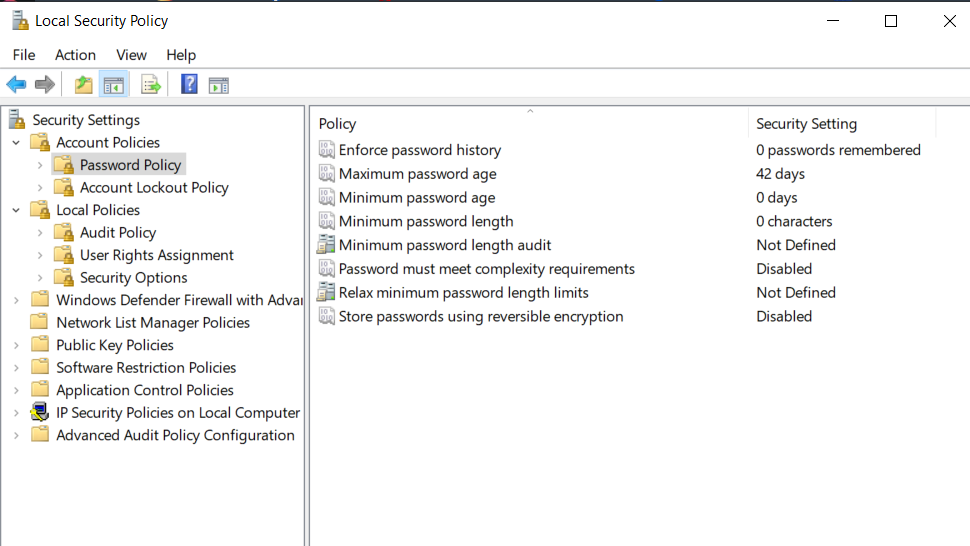
Step1: At first we need to open secpol.msc and then press ok



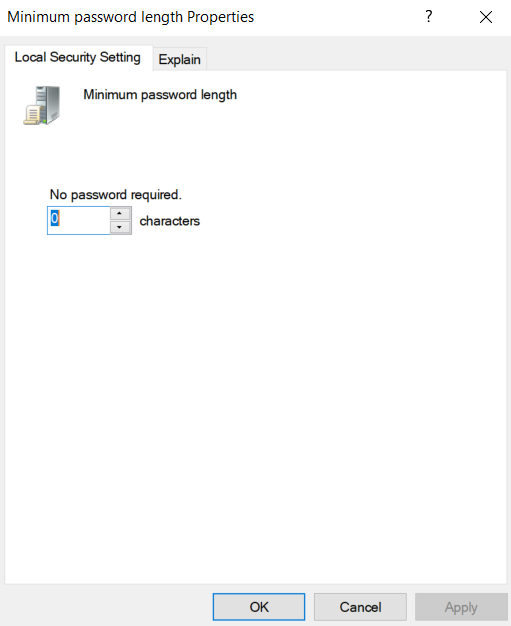
Step2: We may establish several security policies such as password policy, account lockout policy, audit policy, and so on after entering the local policy configuration panel. I'm going to set up a password policy here.



Step3: When we click on the password policy we can see the multiple options are visible such as minimum password age, length, and password complexity etc.



Step4: To set the minimum password length requirement, just choose the option and enter the appropriate length value.



As illustrated in the above diagram, there are several practices to consider when implementing our bank's password policy, including minimum password age, maximum password age, password length, password complexity requirements, and so on. For our bank, the following are the ideal password practices:

Enforce password history: This policy determines how often old passwords may be reused. In our bank network, we're attempting to prohibit users from using many popular passwords. We'll make it hard for users to change their passwords immediately quickly in order to prevent our bank staff and clients from evading the Enforce Password History environment. To establish how long a password must be stored, we'll use a minimum password age policy. A client can only use a store password once in our bank network, which means that once he uses it, it will expire and he will not be able to use it again.

Minimum password Age: This policy specifies how long users or staff of our bank must keep a password before updating it. This policy will be implemented at our bank to deter users from evading the password system by creating a new password and then reverting to the old ones. Ten days will be the minimum password age. In our bank system, if a password change is necessary in an emergency, our bank network administrator will change the password.

Maximum Password Age: This policy specifies how long our bank clients' passwords will be valid before they must be updated. For the sake of our bank's security, we shall give a shorter term. Because our bank places a premium on security, we'll establish a maximum password age of 42 days, as shown in the figure above.

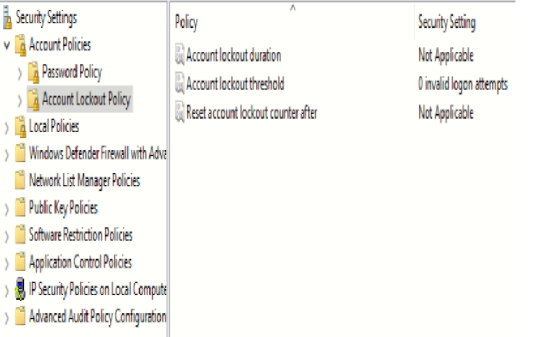
Minimum password length: This controls how long a password must be. We'll use at least eight characters for the purpose of our bank's convenience, as long passwords are often more difficult to decipher than short ones. We can increase the minimum length to 14 characters if we wish to boost security, but most bank users will have passwords that are at least 8 characters long.

Password complexity requirements: This is an important feature to have in all user accounts. In these instructions, we'll utilize this function to make it obligatory to use a secure password:

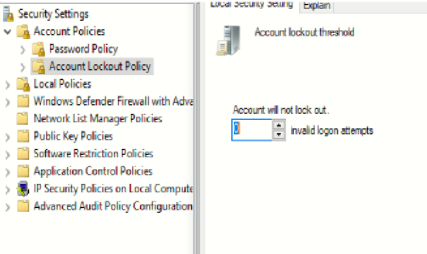
* The length of a password must be at least 8 characters.
* The password should not contain the username or his first name.
* The password must contain lowercase letters, capital letters, digits, and symbols.

## Account lockout policy

Step1: We must go to the account policies section and click on the account lockout policy.



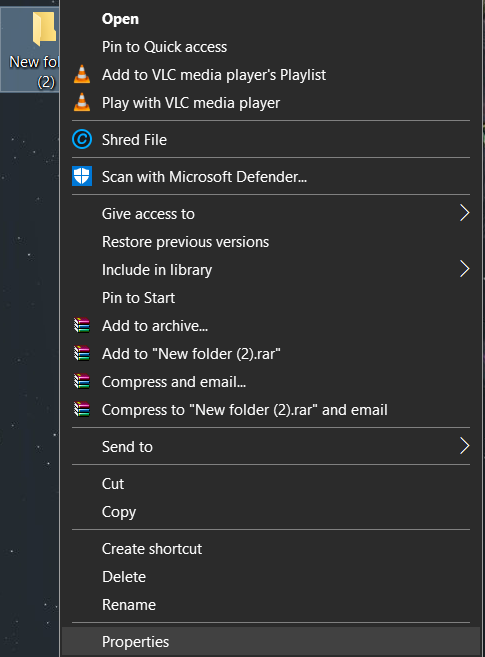
Step2: We may set the value and implement the changes after opening the account lockout threshold.



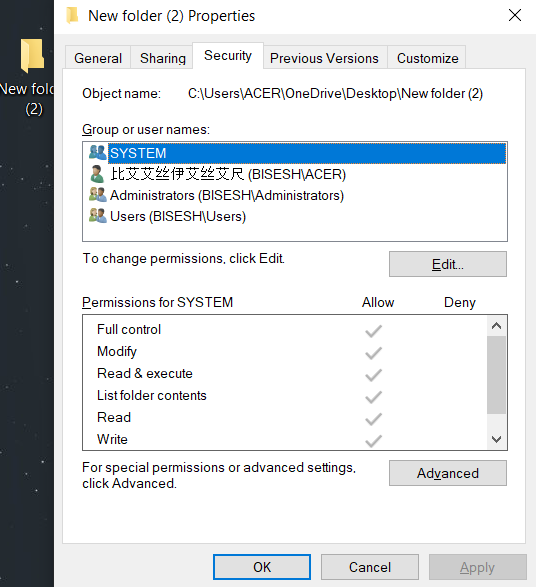
## NTFs Security policy:

The security of NTFs is achieved by granting access to the folder to just a few persons. This is applied in those folders that are visible to other department employees. This is also included on each computer to prevent employees from accessing information from other departments.

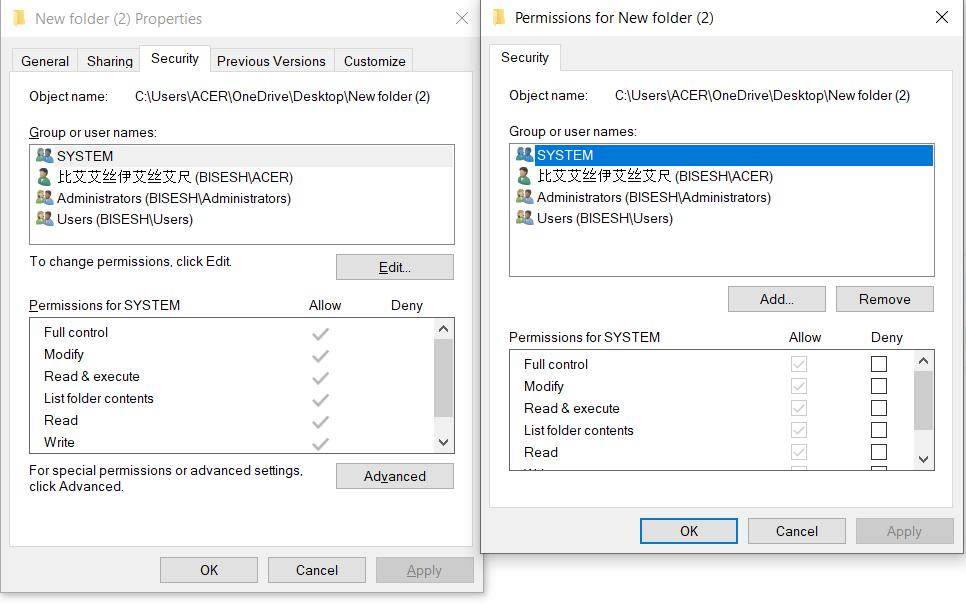
Step1: Right-click any file or folder to which you want to apply NTFs, then select Properties from the right menu.



Step2: Go to Security



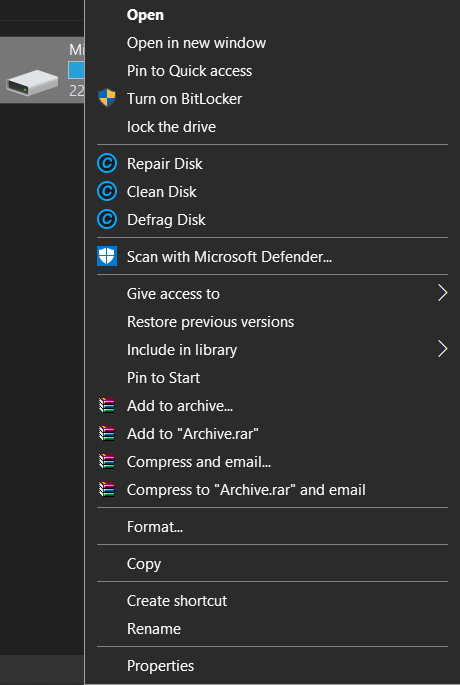
Step3: Select Edit and choose whom to give permission to access the folder.



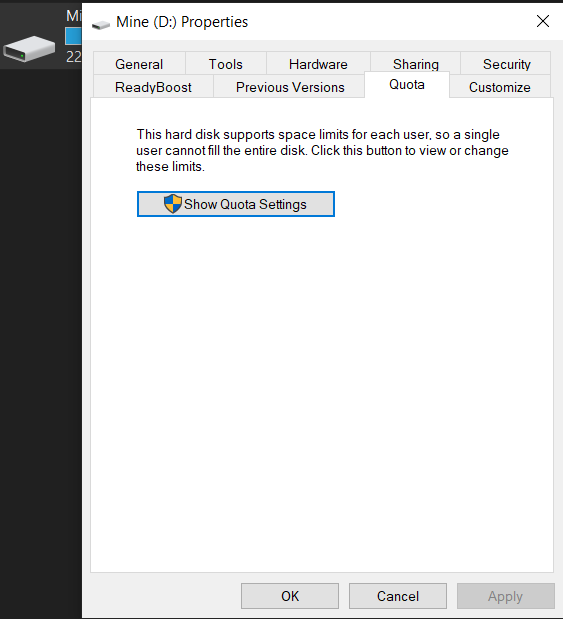
## Quota Management:

Administrators grant quota management rights, which restrict the amount of storage space available to users, workgroups, and other groups. Setting a quota protects a server or share from getting overburdened with data while still allowing users to store files. It essentially entails each user sharing storage.

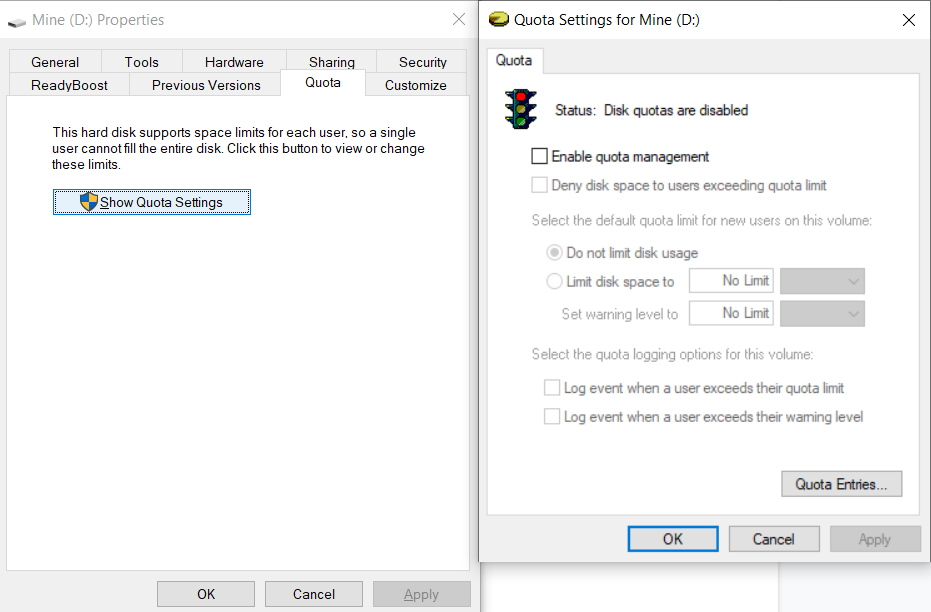
Step1: Administrators grant quota management rights, which restrict the amount of storage space available to users, workgroups, and other groups. Setting a quota protects a server or share from getting overburdened with data while still allowing users to store files. It essentially entails each user sharing storage.



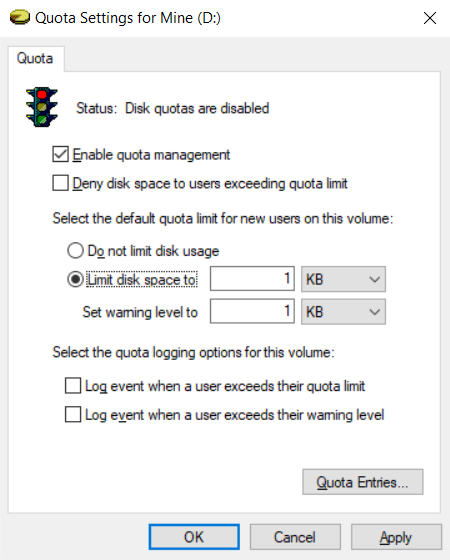
Step2: You can see “Quota” right above. Click there.



Step3: This will appear. Click on “Show Quota Settings”

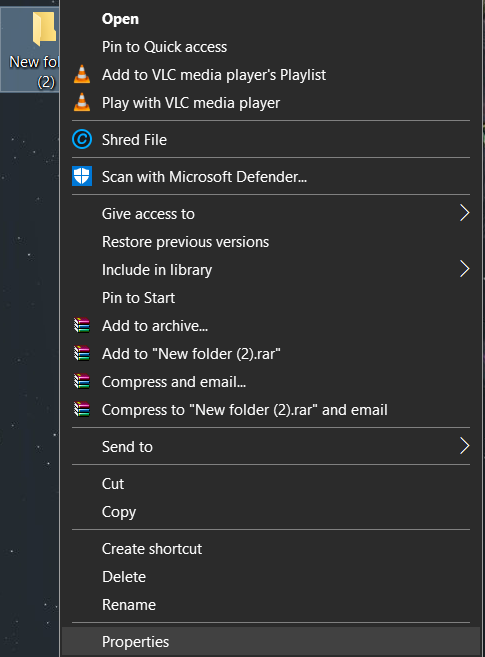
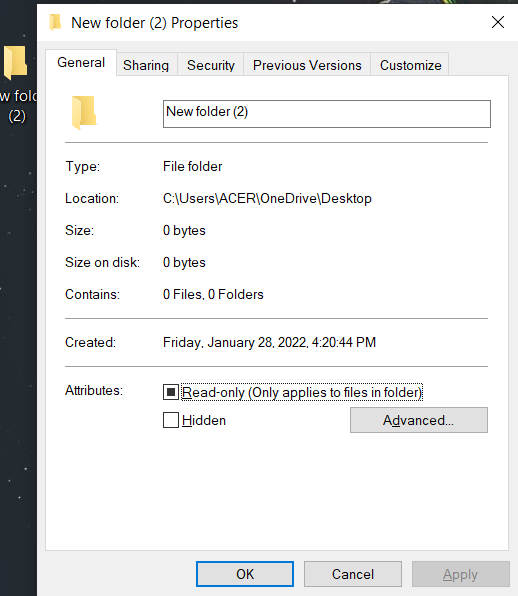


Step4: When you enable quota management, the options listed below will become available for usage. Set a disk space limit and a warning level that suits your needs. Finally, click >>Apply.

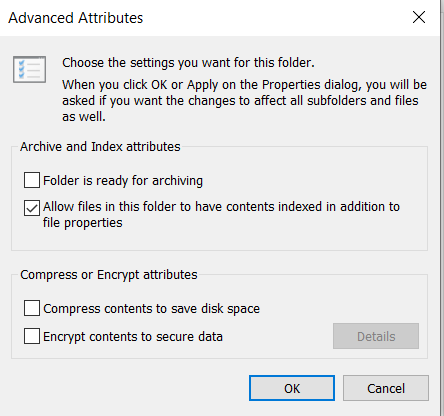


## Encryption

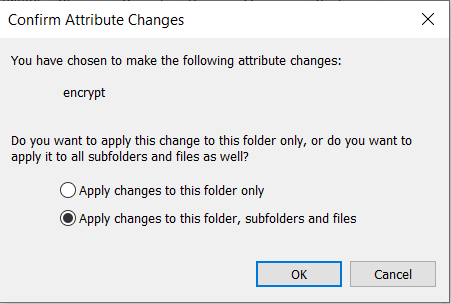
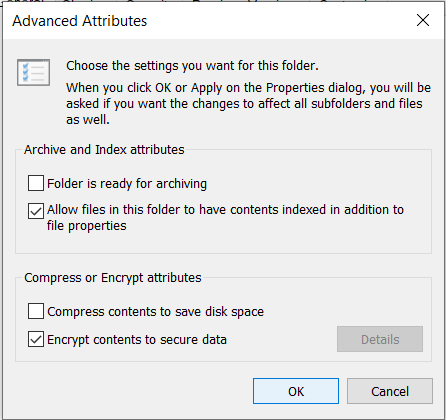
Step1: Right click on the file which is need to be encrypted and go to the properties



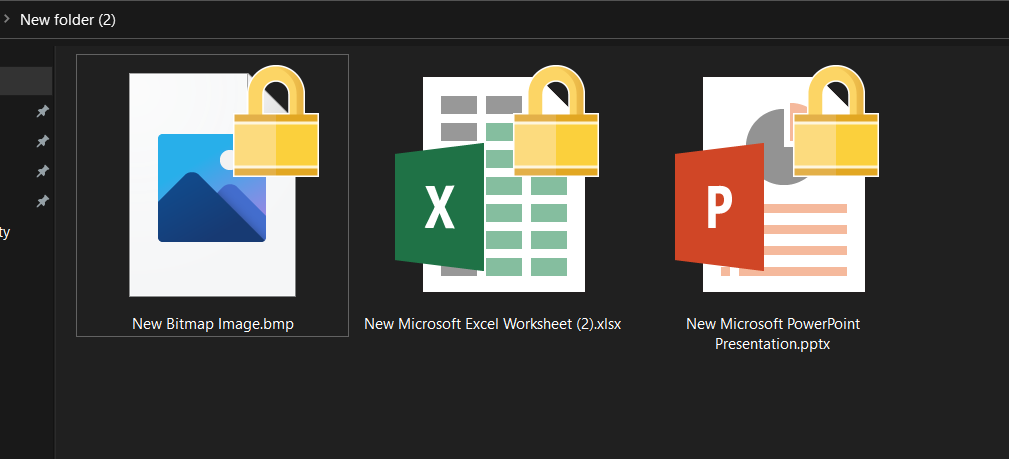
Step2: Once the property is open click on advance option and check into the Encrypt content to source data. And click OK.



Step3: Once we click on the ok button the confirmation tab is open. Click on Apply changes to this folder, subfolders and files and click ok.



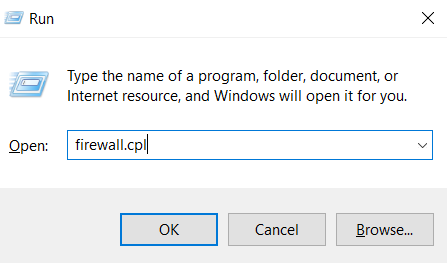
Step4: Once we click on ok then in the folders or in its subfolder this symbol is visible. For opening this file we need to enter specific key

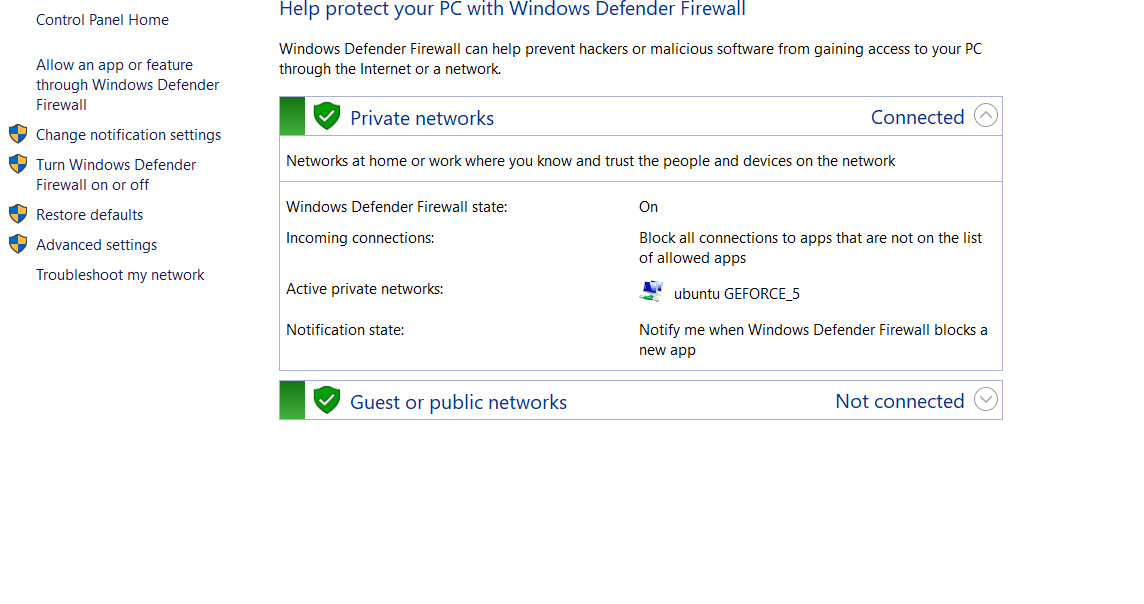


## Firewall Management policy

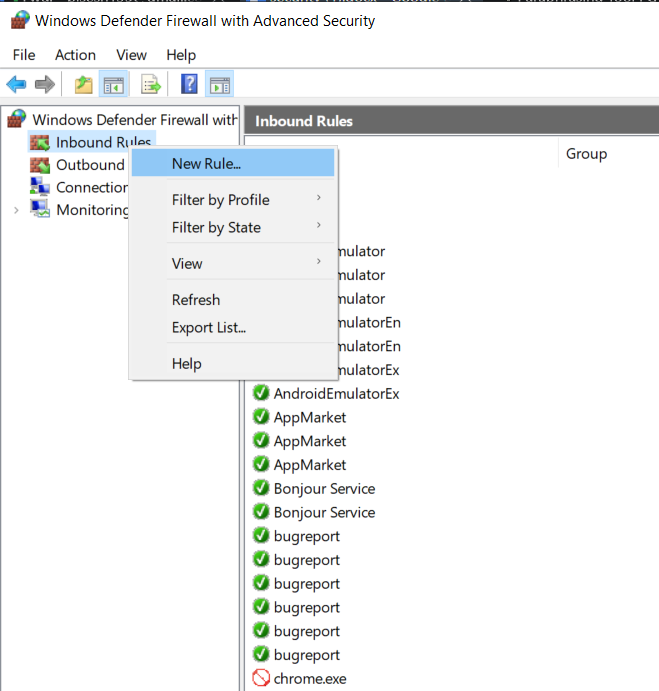
"A firewall is a network security device that enables or denies network access to traffic flows between an untrusted zone (such as the Internet) and a trusted zone (such as a private or corporate network.") It acts as a network demarcation point since all communication must travel through it, and it is where traffic is granted or refused access. To implement access restrictions, they employ a positive control model, which stipulates that only traffic described in the security policy is allowed into the network; all other traffic is denied.

Step1: Go to run and type firewall.cpl and time ok

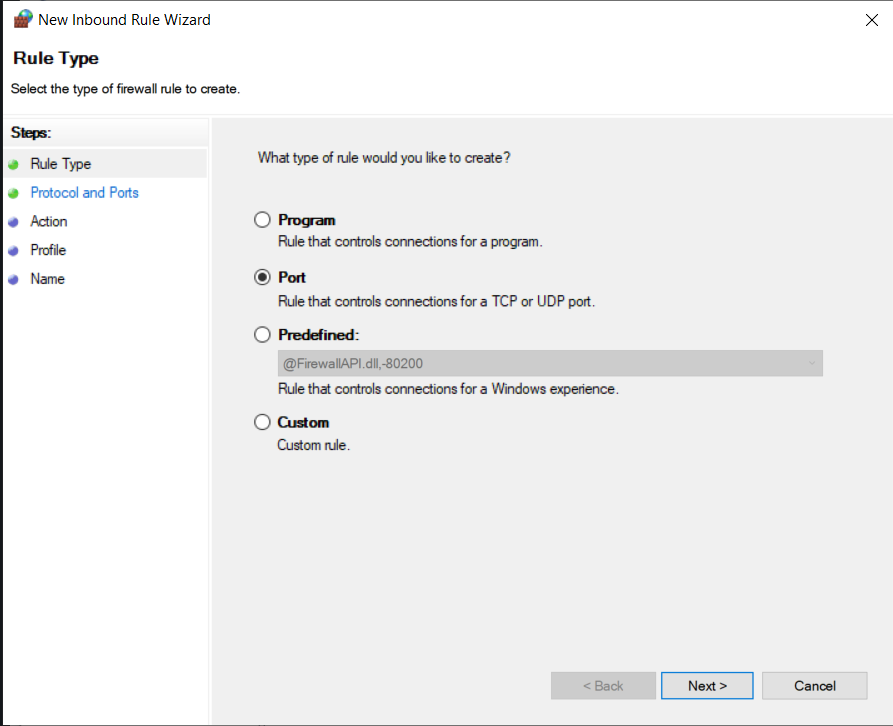


Step2: When the firewall is turned on, select the Advanced option. 

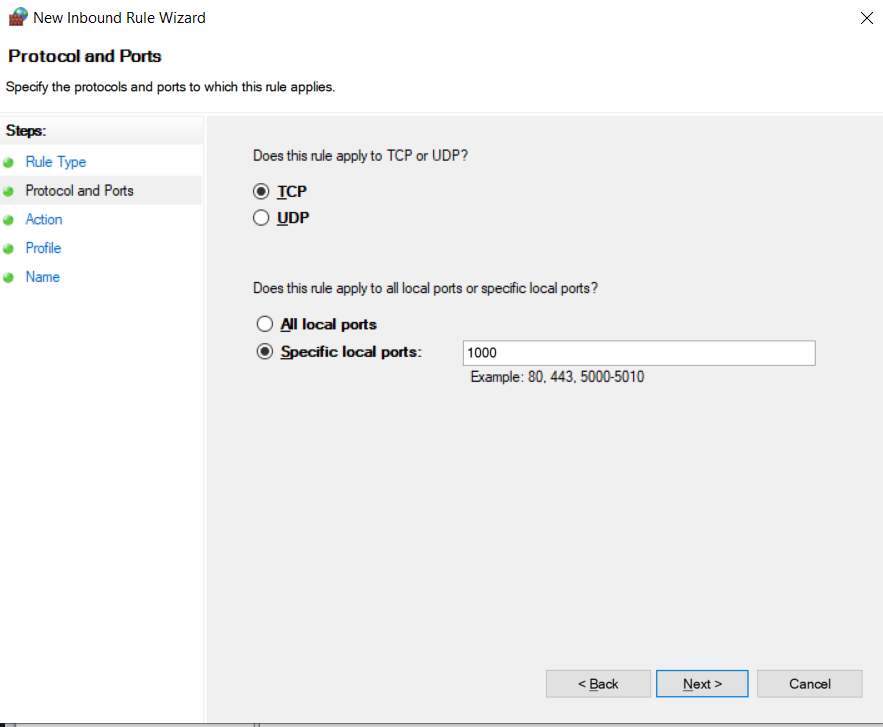
Step3:When the firewall's advanced security is open, right-click on the inbound rule and choose "new rule."



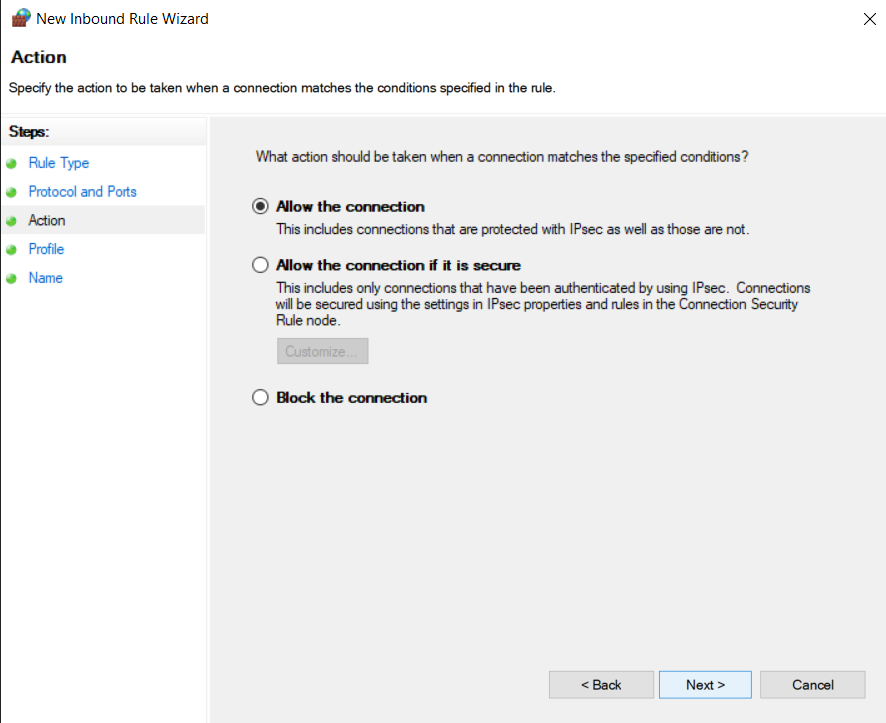
Step4:select the port option and click next



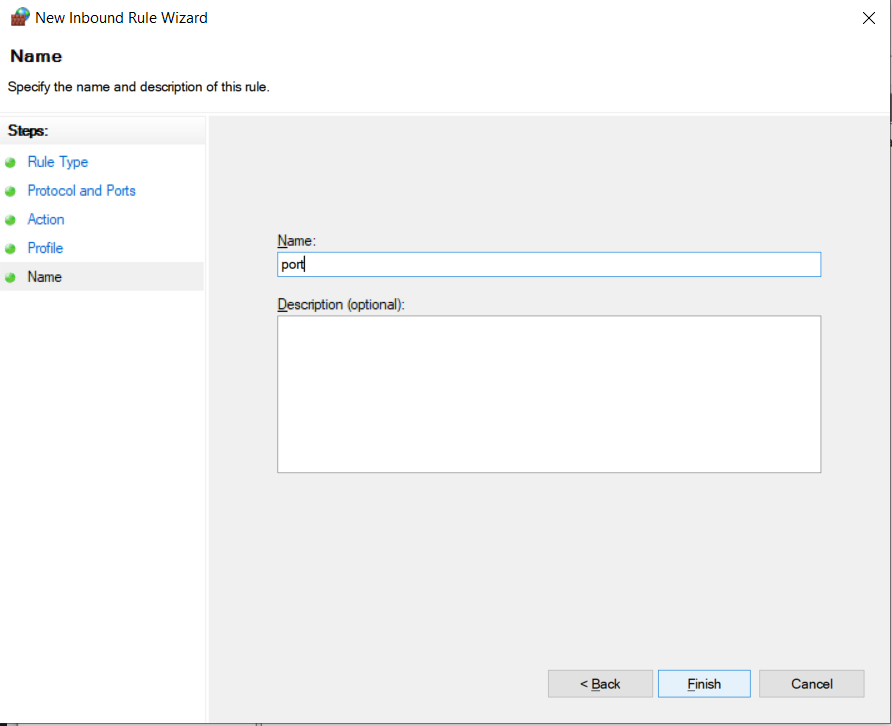
Step5:select tcp option and specific local policy and set a range of port for implementing inbound rule



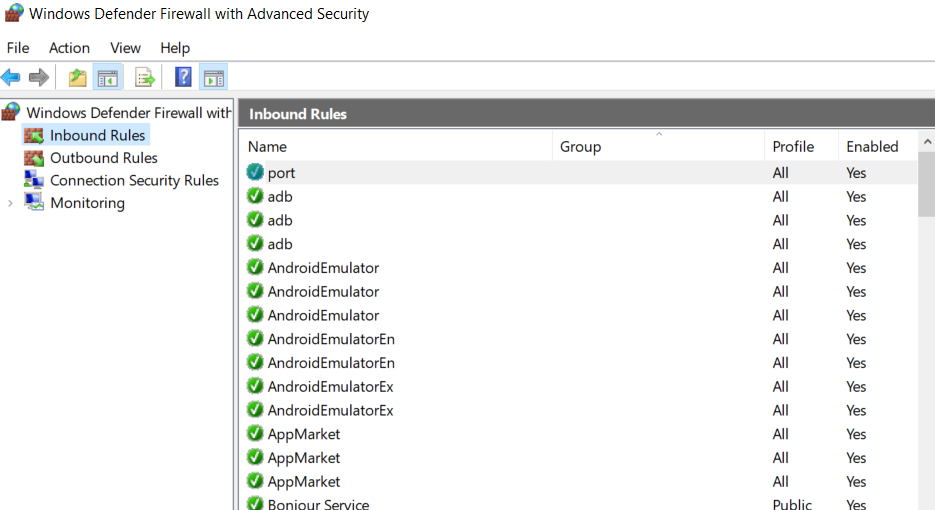
Step6: click on allow the connection if we want to allow connection otherwise click on block connection and click next



Step7: name the port and click finish



Step8:see if it is created or not



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

A disaster recovery plan outlines how to carry on with business operations even after a disaster. Any company will experience a bad circumstance at some point throughout its existence, and in order to properly deal with the crisis, the company must have a strategy. Natural disasters, technical failures, and human participation are all examples of disasters. The following details should be included in your disaster recovery plan:

**How long a data loss or system dropdown can be tolerated**.

If a system dropdown or data loss how long the operations of the business will have to be halted and how can we recover should be planned. This allows the organization to be ready for any disaster condition.

**Responsibilities should be shared**.

Responsibilities should be shared so that only one or two won’t be responsible for the whole organization. Like daily backups in each sector should be assigned to persons from those sectors. If so after a system outage if the data cannot be recovered he will be responsible not the whole team.

**Communication plan**

Proper communication plan should be created. During a disastrous situation communication is a vital part. If the phone and email services dropdown some other communication methodology should be implemented so the staff can know about the ongoing situation.

**Backup plan**

Backup plan of the organization should be a very effective one. Employees should be trained for daily, monthly or weekly backup procedures. Apart from the server in the work site there should backup server in a geographical location which has less tendency for destruction due to natural disasters.

**Handling sensitive information**

Sensitive information should be handled carefully. If demolishing them they should be in such a manner that they can’t be recovered. And they should be stored with password protection

# Conclusion

Data can be broken at any time due to the unpredictability of environmental dangers such as natural catastrophes. As a result, we should create and implement a recovery strategy to reduce data loss in the case of a natural disaster. To keep the organization's data secure and improve its security, firewalls, encryption, local policy, group policy, and other measures are utilized. Whether small or large, the security approaches employed to strengthen the bank's security have their own level of involvement.

# References

<https://www.insightsforprofessionals.com/it/security/types-of-security-threat>

<https://blog.panoply.io/top-cloud-security-threats-risks-and-concerns>

<https://www.cisco.com/c/en/us/products/security/what-is-it-security.html>

<https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>

<https://www.getkisi.com/blog/7-tips-prevent-cloud-security-threats>

<https://www.mimecast.com/content/cloud-based-spam-filtering/>

<https://www.upguard.com/blog/cyber-security-risk-assessment>

<https://www.cwps.com/blog/cloud-computing-security-issues>

<https://www.forcepoint.com/cyber-edu/firewall>

<https://www.comptia.org/content/guides/what-is-network-address-translation>