Higher Nationals

Internal verification of assessment decisions – BTEC (RQF)

INTERNAL VERIFICATION – ASSESSMENT DECISIONS			
Programme title	BTEC Higher National Diploma in Computing		
Assessor	Mr. Isura Kulathilake	**Internal Verifier**	Mr.Lakindu Premachandra
Unit(s)	Unit 05: Security		
Assignment title	EMC Cyber		
Student's name	Ranudi Gayathmie Kariyapperuma		
List which assessment criteria the Assessor has awarded.	**Pass**	**Merit**	**Distinction**

INTERNAL VERIFIER CHECKLIST		
Do the assessment criteria awarded match those shown in the assignment brief?	Y/N	
Is the Pass/Merit/Distinction grade awarded justified by the assessor's comments on the student work?	Y/N	
Has the work been assessed accurately?	Y/N	
Is the feedback to the student: Give details: • Constructive? • Linked to relevant assessment criteria? • Identifying opportunities for improved performance? • Agreeing actions?	Y/N Y/N Y/N Y/N	
Does the assessment decision need amending?	Y/N	

Assessor signature		**Date**	
Internal Verifier signature		**Date**	
Programme Leader signature (if required)		**Date**	

Confirm action completed			
Remedial action taken Give details:			
Assessor signature		**Date**	
Internal Verifier signature		**Date**	
Programme Leader signature (if required)		**Date**	

Higher Nationals - Summative Assignment Feedback Form

Student Name/ID	Ranudi Gayathmie Kariyapperuma KIR/X -00104243		
Unit Title	Unit 05: Security		
Assignment Number	3	Assessor	
Submission Date	18.05.2023	Date Received 1st submission	
Re-submission Date		Date Received 2nd submission	

Assessor Feedback:

LO1. Assess risks to IT security

Pass, Merit & Distinction Descripts   P1 □   P2 □   M1 □   D1 □

LO2. Describe IT security solutions.

Pass, Merit & Distinction Descripts   P3 □   P4 □   M2 □   D1 □

LO3. Review mechanisms to control organisational IT security.

Pass, Merit & Distinction Descripts   P5 □   P6 □   M3 □   M □   D2 □

LO4. Manage organisational security.

Pass, Merit & Distinction Descripts   P7 □   P8 □   M5 □   D □

Grade:	Assessor Signature:	Date:
Resubmission Feedback:		
Grade:	Assessor Signature:	Date:
Internal Verifier's Comments:		
Signature & Date:		

* Please note that grade decisions are provisional. They are only confirmed once internal and external moderation has taken place and grades decisions have been agreed at the assessment board

Pearson

Higher Nationals in

Computing

Unit 5: Security

General Guidelines

1. A Cover page or title page – You should always attach a title page to your assignment. Use previous page as your cover sheet and make sure all the details are accurately filled.
2. Attach this brief as the first section of your assignment.
3. All the assignments should be prepared using a word processing software.
4. All the assignments should be printed on A4 sized papers. Use single side printing.
5. Allow 1" for top, bottom , right margins and 1.25" for the left margin of each page.

Word Processing Rules

1. The font size should be **12** point, and should be in the style of **Time New Roman**.
2. **Use 1.5 line spacing**. Left justify all paragraphs.
3. Ensure that all the headings are consistent in terms of the font size and font style.
4. Use **footer function in the word processor to insert Your Name, Subject, Assignment No, and Page Number on each pag**e. This is useful if individual sheets become detached for any reason.
5. Use word processing application spell check and grammar check function to help editing your assignment.

Important Points:

1. It is strictly prohibited to use textboxes to add texts in the assignments, except for the compulsory information. eg: Figures, tables of comparison etc. Adding text boxes in the body except for the before mentioned compulsory information will result in rejection of your work.
2. Carefully check the hand in date and the instructions given in the assignment. Late submissions will not be accepted.
3. Ensure that you give yourself enough time to complete the assignment by the due date.
4. Excuses of any nature will not be accepted for failure to hand in the work on time.
5. You must take responsibility for managing your own time effectively.
6. If you are unable to hand in your assignment on time and have valid reasons such as illness, you may apply (in writing) for an extension.
7. Failure to achieve at least PASS criteria will result in a REFERRAL grade .
8. Non-submission of work without valid reasons will lead to an automatic RE FERRAL. You will then be asked to complete an alternative assignment.
9. If you use other people's work or ideas in your assignment, reference them properly using HARVARD referencing system to avoid plagiarism. You have to provide both in-text citation and a reference list.
10. If you are proven to be guilty of plagiarism or any academic misconduct, your grade could be reduced to A REFERRAL or at worst you could be expelled from the course

Student Declaration

I hereby, declare that I know what plagiarism entails, namely to use another's work and to present it as my own without attributing the sources in the correct way. I further understand what it means to copy another's work.

1. I know that plagiarism is a punishable offence because it constitutes theft.
2. I understand the plagiarism and copying policy of the Edexcel UK.
3. I know what the consequences will be if I plagiarize or copy another's work in any of the assignments for this program. .
4. I declare therefore that all work presented by me for every aspects of my program, will be of my own, and where I have made use of another's work, I will attribute the source in the correct way.
5. I acknowledge that the attachment of this document, signed or not, constitutes a binding agreement between myself and Pearson UK.
6. I understand that my assignment will not be considered as submitted if this document is not attached to the main submission.

ranudigk@gmail.com 18/05/2023

Student's Signature: **Date:**
(*Provide E-mail ID*) **(*Provide Submission*
***Date*)**

Assignment Brief

Student Name /ID Number	Ranudi Gayathmie Kariyapperuma KIR/X -00104243
Unit Number and Title	Unit 5- Security
Academic Year	2020/2021
Unit Tutor	Mr. Isura Kulathilake
Assignment Title	EMC Cyber
Issue Date	10.04.2023
Submission Date	18.05.2023
IV Name & Date	

Submission Format:

The submission should be in the form of an individual written report written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using Harvard referencing system. Please provide in- text citation and an end list of references using Harvard referencing system.

Section 4.2 of the assignment required to do a 15 minutes presentation to illustrate the answers.

Unit Learning Outcomes:

LO1 Assess risks to IT security.
LO2 Describe IT security solutions.
LO3 Review mechanisms to control organizational IT security.
LO4 Manage organizational security.

Assignment Brief and Guidance:

Scenario

'EMC Cyber' is a reputed cyber security company based in Colombo Sri Lanka that is delivering security products and services across the entire information technology infrastructure. The company has several clients both in Sri Lanka and abroad, which includes some of the top-level companies of the world serving in multitude of industries. The company develops cyber security software including firewalls, anti-virus, intrusion detection and protection, and endpoint security. EMC Cyber is tasked with protecting companies' networks, clouds, web applications and emails. They also offer advanced threat protection, secure unified access, and endpoint security. Further they also play the role of consulting clients on security threats and how to solve them. Additionally, the company follows different risk management standards depending on the company, with the ISO 31000 being the most prominent.

One of the clients of EMC Cyber, Lockhead Aerospace manufacturing which is a reputed aircraft manufacturer based in the US, has tasked the company to investigate the security implications of developing IOT based automation applications in their manufacturing process. The client has requested EMC to further audit security risks of implementing web based IOT applications in their manufacturing process and to propose solutions. Further, Lockhead uses ISO standards and has instructed EMC to use the ISO risk management standards when proposing the solution.

The director of the company understands such a system would be the target for cyber-attacks. As you are following a BTEC course which includes a unit in security, the director has asked you to investigate and report on potential cyber security threats to their web site, applications, and infrastructure. After the investigation you need to plan a solution and how to implement it according standard software engineering principles.

Activity 01

Assuming the role of External Security Analyst, you need to compile a report focusing on following elements to the board of EMC Cyber';

1.1 Identify the CIA Triad concept and evaluate why and how the CIA Triad could be utilize to EMC Cyber in order to improve the organization's security.

1.2 Identify types of security risks EMC Cyber is subject to its present setup and the impact that they would make on the business itself. Evaluate at least three physical and virtual security risks identified and suggest the security measures that can be implemented in order to improve the organization's security.

1.3 Develop and describe security procedures for EMC Cyber to minimize the impact of issues discussed in section (1.1) by assessing and rectifying the risks.

Activity 02

2.1 Identify how EMC Cyber and its clients will be impacted by improper/ incorrect configurations that are applicable to firewalls and VPN solutions. IT security can include a network monitoring system. Discuss how EMC cyber can benefit by implementing a network monitoring system with supporting reasons.

2.2 Explain how the following technologies would benefit EMC Cyber and its Clients by facilitating a '**trusted network**'. (Support your answer with suitable examples).

i) DMZ

ii) Static IP

iii)NAT

2.3 Identify and evaluate the tools that can be utilized by EMC cyber to improve the network and security performance without compromising each other. Evaluate at least three virtual and physical security measures that can be implemented by EMC to uphold the integrity of organization's IT policy.

Activity 03

3.1 Discuss suitable risk assessment integrated enterprise risk management procedures for EMC Cyber solutions and the impact an IT security audit will have on safeguarding organization and its clients. Furthermore, your discussion should include how IT security can be aligned with an organizational IT policy and how misalignment of such a policy can impact on organization's security. (This can include one or more of the following: network change management, audit control, business continuance/disaster recovery plans, potential loss of data/business, intellectual property, Data Protection Act; Computer Misuse Act; ISO 31000 standards.)

3.2 Explain the mandatory data protection laws and procedures which will be applied to data storage solutions provided by EMC Cyber. You should also summarize ISO 31000 risk management methodology.

Activity 04

4.1 Design an organizational security policy for EMC Cyber to minimize exploitations and misuses while evaluating the suitability of the tools used in an organizational policy.

4.2 Develop and present a disaster recovery plan for EMC Cyber according to the ISO/IEC 17799:2005 or similar standard which should include the main components of an organizational disaster recovery plan with justifications. Discuss how critical the roles of the stakeholders in the organization to successfully implement the security policy and the disaster recovery plan you recommended as a part of the security audit.

(Students should produce a 15 minutes PowerPoint presentation which illustrates the answer for this section including justifications and reason for decisions and options used).

TABLE OF CONTENTS

Table Of Figures 13

Acknowledgement 15

Assess Risks To It Security.. 16

Identify Types Of Security Risks To Organizations.. 16

Definition Of Security In It Industry 16

Security Types 16

Security Attacks 18

Types Of Security Risks For Companies.. 20

Threats.. 20

1. Malware Attacks 22

2. Social Engineering Attacks.. 22

3. Supply Chain Attacks 23

4. Man In The Middle Attack 23

5. Denial Of Service Attack 23

6. Injection Attacks 23

2. Organizational Risks 24

Cia Triad Concept 24

Cia Main 3 Principles.. 25

3.2 Importance Of Applying Cia Triad Concept To Emc Cyber......................... 26

Organizational Security Procedures... 26

1.Security Procedures That Should Have In An Organization. 26

It Security Solutions.. 28

The Potential Impact To It Security Of Incorrect Configuration Of Firewall Policies And Third Party Vpns.. 28

1. Firewalls.. 28

Implementing A Dmz, Static Ip And Nat In A Network Can Improve Network Security 33

1. Dmz 33

2. Static Ip 34

3. Ntp 35

Discussion Of Risk Assessment Procedures. 37

Data Protection Processes And Regulations As Applicable To An Organization. 38

Designing And Implementing A Security Policy For An Organization 40

The Main Components Of An Organizational Disaster Recovery Plan, Justifying The Reasons For Inclusion 41

1. Disaster Recovery Plan 41

1.3 Disaster Recovery Plan 42

Disaster Recovery Plan For Emc Cyber 43

A Method To Assess And Treat It Security Risks 48

It Security Risks And Solutions To Reduce It 50

Three Benefits To Implementing Network Monitoring Systems. 51

The Iso 31000 Risk Management Methodology And Its Application In It Security 52

The Components Of Iso 31000 52

The Framework 52

The Process 53

Possible Impacts To Organizational Security Resulting From An It Security Audit 54

The Roles Of Stakeholders In The Organisation To Implement Security Audit Recommendations. 55

Roles And Responsibilities 56

References 57

- **TABLE OF FIGURES**

Figure 1 IT Security (Https://Www.Exabeam.Com) --------------------------------- 17

Figure 2 Active Attacks Vs Passive Attacks (Https://Intellipaat.Com) ------------ 18

Figure 3 What Is A Security Risk(Https://Www.Wealthmanagement.Com) ---- 19

Figure 4 Organizational Risks (Https://Evacuteer.Org) ------------------------------ 24

Figure 5 CIA Triad Concept (Https://Websitesecuritystore.Com)------------------ 25

Figure 6 Security Procedures In Organization (Https://Linfordco.Com) ---------- 27

Figure 7 Firewalls (Https://Forumautomation.Com) --------------------------------- 29

Figure 8 VPN (Www.Kaspersky.Com)-- 32

Figure 9 Disaster Recovery Plan Slide 1 (Made By Author) ------------------------ 43

Figure 10 Disaster Recovery Plan Slide 2 (Made By Author) ---------------------- 43

Figure 11 Disaster Recovery Plan Slide 3 (Made By Author) ---------------------- 44

Figure 12 : Disaster Recovery Plan Slide 4 (Made By Author)--------------------- 44

Figure 13 Disaster Recovery Plan Slide 5 (Made By Author) ---------------------- 45

Figure 14 Disaster Recovery Plan Slide 6 (Made By Author) ---------------------- 45

Figure 15 Disaster Recovery Plan Slide 7 (Made By Author) ---------------------- 46

Figure 16 Disaster Recovery Plan Slide 8 Made By Author) ----------------------- 46

Figure 17 Disaster Recovery Plan Slide 9 (Made By Author) ---------------------- 47

Figure 18 Network Monitoring System (Www.Wallarm.Com) -- 52

Figure 19 ISO 31000 Risk Management System (Https://Iso-Docs.Com/) ------- 53

LIST OF TABLES

Table 1 : Risk Assessment (Made by Author) ____________________________ 37

Table 2 : Policy table (Made by Author) ________________________________ 40

Table 3 : Disaster Recovery Plan (Made by Author) ______________________ 42

Table 4 : Organizational security risks and Solutions to reduce it ____________ 49

Table 6 : IT security Risks and Solutions to reduce it _____________________ 50

ACKNOWLEDGEMENT

At last author would like to share the experience while doing the project. Author learns many new things about the Security topics. The best thing which author can share is that author developed more interest in this subject. This Module gave author a real sight about the Security .

A very special thanks to Mr Isuru Kulathilake who teach us this subject and Author thanks for who helped author to do this kind of project. Thank you!

- **ASSESS RISKS TO IT SECURITY**

- **IDENTIFY TYPES OF SECURITY RISKS TO ORGANIZATIONS.**

Aircraft Manufacturer Company is a Client of EMC Cyber and need a good Security System to secure the data in the Company. So, in the EMC Company reporter found security risks in this company and reporter reports the risks and the solutions for it. There are multiple kinds of risks in this company, so the reporter reports few of them in this report. Before talking about the risks author will firstly explain about what Security is and how to secure them.

- **DEFINITION OF SECURITY IN IT INDUSTRY**

Security is an important part in the IT field because there can be various kind of data protection issues in IT Field. Security means that secure company or humans' information from threats that occur in IT field. Some information has that are very sensitive data that should keep protective in a computer also that data also don't even share with other people such as passwords.

- **SECURITY TYPES**

People should be aware that there are mainly 4 types of Information Technology Security, so now author will explain them.

- Network Security

In small space or a large space like office use computers and make a network to communicate with each other so it is very easy to share data but there is also have a risk because it opens for threats to get important information about companies or personal life.

So, in every Company should monitor their network usually, refresh the passwords and also should maintain and monitor the internet access. Companies should always implement firewalls and antivirus protections for their network to prevent threats.

- Cloud Networking

Clouds is a platform that can store data safely. So, when choosing a cloud user should choose a trust worthy platform that has a minimum of risk. In cloud-based platforms there has a usually safe instructions that need to be applied when user get into clouds. So, when a user needs to protect the cloud system it is good that Acorn's cloud protects.

- Application Security

In apps also need to be secure because even in the apps also may have risk to the devices so it is better to have trustworthy brand to install apps. Whether it is used in network or the cloud.

For an example when people play games sometimes when the game is over it will pop up an advertisement to click when user click the advertisement it can be a virus so then it can spread all over your device and get your important details through your device. So, people should be aware when using applications and also need to apply safe guard for every application in the device.

- Internet of Things Security

Internet of things means that devices that connected to the Internet. In internet there should always protect the devices that connected because it can easily get threats. It is important to have a security risk assessment to find vulnerabilities in users' device and network.

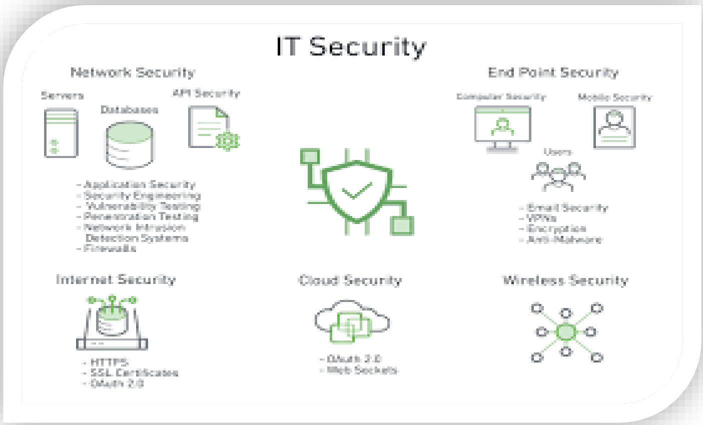


Figure 1 IT Security (https://www.exabeam.com)

- **SECURITY ATTACKS**

A security attack means that damaged the important information system that needs a user. In security attack it is mainly divided into 2 parts. that are called as,

- Active Attacks
- Passive Attacks

Active Attacks	Passive Attacks
Active attacks are the attackers that change the content of information.	Passive attacker will look after the information or copy the content of the information.
Victims get the information that it has an attack.	Victim doesn't know even it had a attack.
System Resources can be change.	System Recourses are not changed.
Can be easily caught.	Difficult to identify what happened.
The time of period is short	Time of period id high.

Table 1: Active attacks vs Passive Attack

Figure 2 Active Attacks vs Passive Attacks (https://intellipaat.com)

DEFINITION OF IT SECURITY RISK.

As a Wise Man told that "I really think that if we change our own approach and thinking about what we have available to us, that is what will unlock our ability to truly excel in security. It's a perspectives exercise. What would it look like if abundance were the reality and not resource constraint?" — Greg York

So, the author think that a Security risk means that for an example A suspicious person log into another computer of a company and try to harm the company data or collect the important data from the computer without knowing others that means there has a Security risk. There are many ways to attack companies like that.

Figure 3 What is a Security Risk(https://www.wealthmanagement.com)

- **TYPES OF SECURITY RISKS FOR COMPANIES**

There are various kinds of risks in companies so EMC Cyber Company should always update all kinds of security Risks and how to solve the risks. Now the author will clarify the types of security risks.

- Vulnerability

Vulnerability is a weakness of an IT system. Attackers always looked after a vulnerability to make a successful attack. To make a Successful software or Successful system developer should always take the bugs of a system and have to do a patch or mitigation on them. There are some categories of vulnerabilities.

1. Program Flows

Program flows means that programs that do un necessary stuff even developer doesn't ask to do.

2. Zero day

Zero day means that hackers or developers found vulnerabilities in a system but even now developers don't find a solution to fix it.

3. Features

In a system there are some features that people misuse them, and these kinds of things are vulnerabilities.

4. User Errors

As an example, some users are using simple passwords for important systems and it can be easily gotten by the hackers. That kinds of things are called as user errors.

- **THREATS**

In RFC 4949 explain what threat is,

A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

So as the above-mentioned author explains, a threat is a harmful thing that happens to a computer or organization. So, in threats also it is divided into 3 main categories as,

- Natural Threats

Natural threats are that happens naturally like floods, tsunamis, tornados. etc...

- Intentional Threats

This threat means that someone purposely harms a computer organization. Information. Examples like computer crimes and credit card theft.

- Unintentional Threats

This threat happens accidently like deleting some important **information** on the computer by mistake. In computer threats there are many types of it. Like,

- **1. MALWARE ATTACKS**

In malware attacks their main types:

- Viruses

Viruses means that spreads between computers and damage the data and software.

- Worms

Spreads all over the network immediately

- Trojan

This malware threat is coming like a game, apps, email attachments if user click will spread in the computer.

- Adware – It means that the treat is coming as an advertisement.

- Spyware – Collect user activity data without user knowing.

- **2. SOCIAL ENGINEERING ATTACKS**

In this Attacks attacker tricking users providing something important to user then when user fell it user unintentionally put users' sensitive data and attacker get them.

- Baiting

this type of threats is coming as a gift card or something that valuable for victim and victim give them sensitive information to the attacker.

- Phishing

Phishing threat is coming as an email to attack victim.

- Vishing
- Smishing
- Tailgating

- **3. SUPPLY CHAIN ATTACKS**

A supply chain attack is a new attack for software developers and vendors. In this attack the attacker distribute malware in a source code.

- **4. MAN IN THE MIDDLE ATTACK**

- Main in the middle attack is involves communication in between an application example for that are,
- Wi-Fi eavesdropping.
- Email Hijacking
- DNS spoofing
- IP spoofing

- **5. DENIAL OF SERVICE ATTACK**

- Denial of Service Attack is target in a large volume of a system.

  - HTTP flood DDOS
  - SYN flood DOOS
  - UDP flood DDOS
  - ICMP flood
  - NTP amplification

- **6. INJECTION ATTACKS**

- Injection Attack means that directly applies malware attack to the code of web application.

Main types of Injection Attacks are,

  - SQL injection
  - Code injection
  - OS Command injection
  - LDAP injection

- **2. ORGANIZATIONAL RISKS**

Even EMC Cyber company may have organizational risks. It is better to know organizational risks to prevent from them. the risks are,

- Business Risk
- Economic Risk
- Financial Risk
- Health & Safety
- Risk Identification
- Human Error
- Credit Risk
- Country Risk

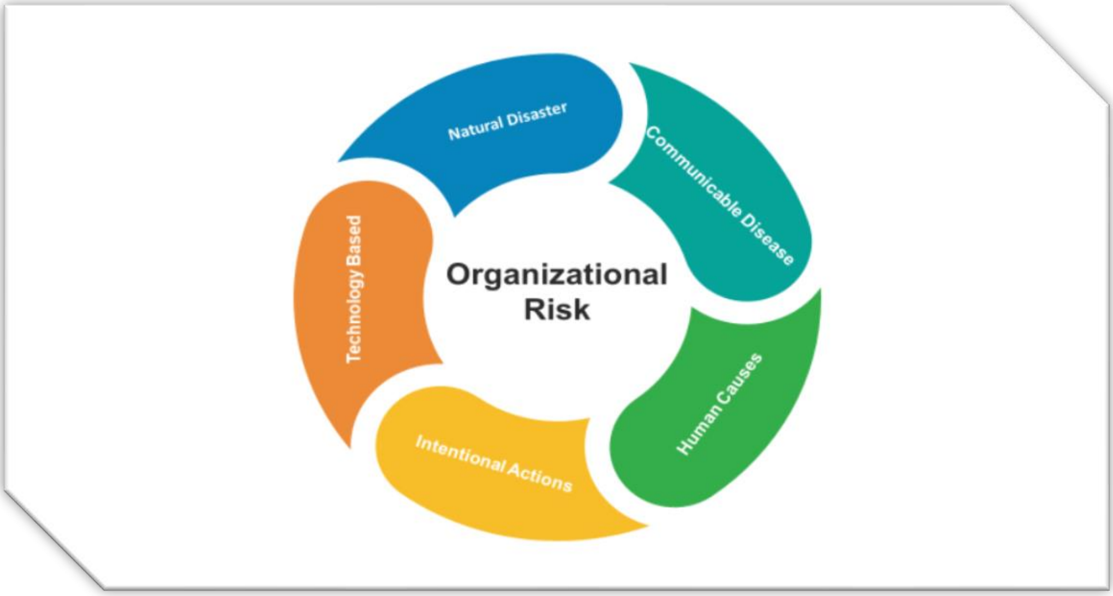


Figure 4 Organizational Risks (https://evacuteer.org)

- **CIA TRIAD CONCEPT**

CIA Triad is a popular information security model. This concept was started in 1998. CIA Triad is a very important concept because there are three principles known as,

- Confidentially
- Availability
- Integrity

For an example for begin a fire there should be main three elements that are oxygen, Fuel, heat if one of those were missing then it will not begin a fire so this example equal to CIA concept if the one of the principles were missing then it can't be a successful Defense mechanism.

- **CIA MAIN 3 PRINCIPLES**

1. Confidentially

In CIA Concept the C letter is known as Confidentially. Protect information and for look the protect. Information can get access only to the authorized ones. In Companies identify sensitive data as employee data, accounts etc... To secure data it is better to implement security mechanisms like passwords, encryptions etc...

2. Integrity

In CIA concept I stand for Integrity. So, in this principle authorized person can change the data under this concept. For an example In a Company when a data that should be change then as a authorized The person supervisor will change it but if the person that is under the supervisor can't change data. If that person changes it will not be accepted. Also, the data can be changed when transmitting data when storing data and when use data.

3. Availability

Letter A in CIA concept called Availability. Information should always be available for access to authorized users when needed. To make it more efficient organizations can use servers, applications and redundant networks.

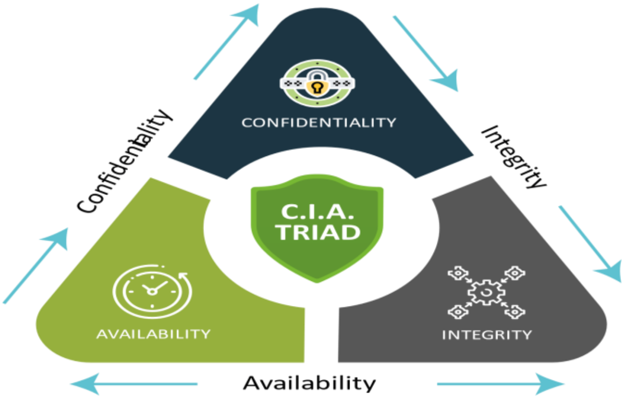


Figure 5 CIA triad Concept (https://websitesecuritystore.com)

- **3.2 IMPORTANCE OF APPLYING CIA TRIAD CONCEPT TO EMC CYBER.**

Using CIA concept is very important because EMC Cyber also can secure data more efficiently using this, Method. Mainly 3 elements that are confidentiality, integrity and availability have power to secure very Important data. Also, EMC can introduce the CIA concept to EMC clients that other companies also can save the data Secure in this concept. In confidentiality can protect data an allows to look authorized users unauthorized users can't get any information in confidentiality part, in integrity part only authorized person can change data and in availability information should always available when needed them.

- **ORGANIZATIONAL SECURITY PROCEDURES.**

For organization security procedures the organization have to have steps and tasks for ensure the security of organization. To take security procedures organization should have to look after policies of organization.

A security Procedure means a set of security that can be implemented to a Organization to secure the important information in an organization. Organizations can take any security procedures based on their company rules and regulations. In an organization there should be security physically and internally on devices. In EMC Cyber also can take some of these security procedures to make more secure the organization. So now the author will discuss what kind of security procedure that should have to make in an organization.

- **1.SECURITY PROCEDURES THAT SHOULD HAVE IN AN ORGANIZATION.**

COMMON SECURITY PROCEDURES

- Emergency Procedures

Emergency Procedures means when them has an evacuation, lockdowns, and first aid like any crisis organization have to have procedure what can do next moment these risks are coming as unexpected way in life.

- Security Training

In security Training helps individually understand about the security procedures correctly. Security training is provided through classes and online resources. This is great starting points to improve their business security in work place.

Technical Security Procedures

- Access Control

Access control is a security measure that restricts or manages people's access to particular places. Physical barriers like locks, gates, fences, and security personnel can be used to implement these, as well as electronic systems like key cards or biometric scanners. Access control is frequently used in conjunction with other security measures including alarm systems and CCTV surveillance.

- CCTV Monitoring

CCTV surveillance is a form of security that employs cameras to keep an eye on local activity. They are capable of keeping an eye on both public and private areas, and they can be stationary or movable. This piece of technology is frequently used in conjunction with other security tools like access control and alarm systems.

- Alarm Systems

Alarm systems are a form of security that employ sensors to find irregularities or breaches.

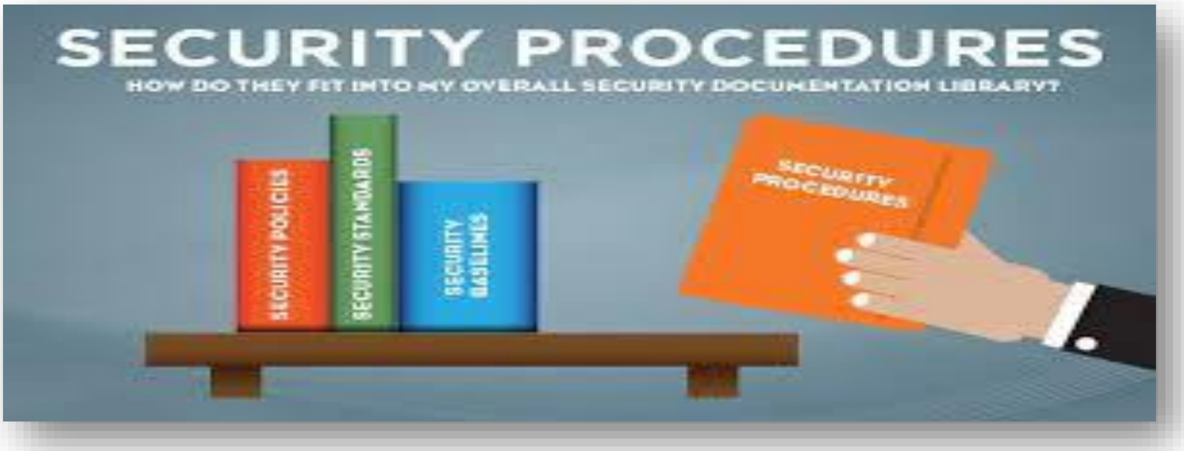


Figure 6 Security Procedures in organization (https://linfordco.com)

- **IT SECURITY SOLUTIONS**
- **THE POTENTIAL IMPACT TO IT SECURITY OF INCORRECT CONFIGURATION OF FIREWALL POLICIES AND THIRD PARTY VPNS.**

- **1. FIREWALLS**

Firewalls are a defense like a wall. This is a network security model. On a set of rules firewalls monitor network traffic that incoming and outgoing through the network system and give the permission to enter the data or block the data. The important of firewall is that viruses or malware can’t go through a firewall to attack a computer.

1.1 HISTORY OF FIREWALL.

- Gen 1 Virus

The beginning of Firewall is in the late 1980s. It was built on virus focused. In the Time period was the internet was found after building these firewalls then businesses focused on developing anti- virus software.

- Gen 2 Network

This was built in the 1990s. This was built to prevent the internet from attack. In This generation had the advanced firewall.

- Gen 3 Application

In this generation hidden security flaws can also capture and also because of this IPS was started build that time period.

- Gen 4 Payload

This generation was found for highly invasive and to trace hard attacks. These Specific attacks were happening in the 2019 – 2010 time.

- Gen 5 Mega

In 2017 this was launched, and this was the threat prevent measures that global recognized.

TYPES OF FIREWALLS

Basically, there are 3 types of firewalls. These are known as,

- Packet filtering firewalls
- Application-level firewalls
- Circuit Level Gateway

- Packet Filtering Firewalls

In Packet filtering firewalls are applied set of rules on each incoming packets. Incoming packets are known as data that coming like a packet. If the packets obey the rules, it can go forward but if packets don't obey the rules, it will drop out.

- Application -level Firewalls

This Firewall is known as proxy servers. Application-level firewall is more secure than the packet filtering firewall and it is controlled by TCP/IP protocols. (Telnet, Smtp, Http, Ftp etc.)

- Circuit Level Gateways

In Circuit level gateways It uses 2 main TCP Connections. One connection is in between the gateways and the Internal Hosts, and the other connection is between the External Host and the Gateway. Between the internal host and the Gateway connection is called as Inside connection and between the gateway and the external host connection is called as Outside connection. It is faster than the previous two firewalls.

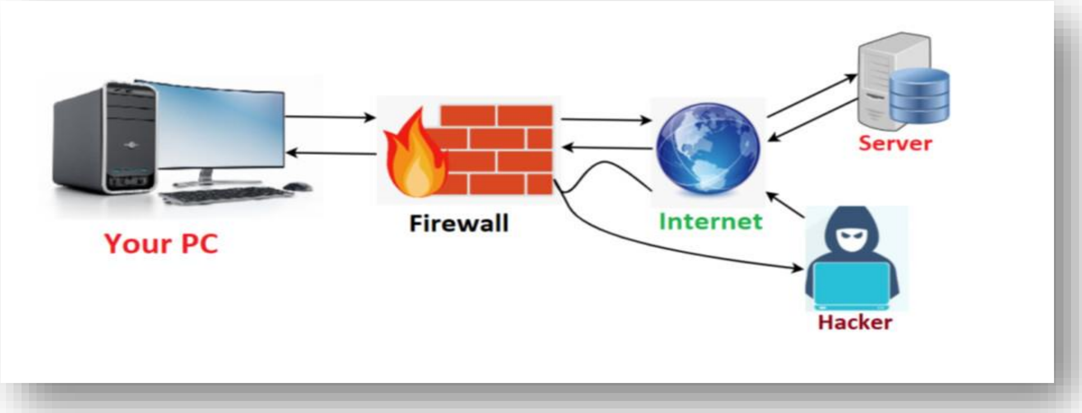


Figure 7 Firewalls (https://forumautomation.com)

1.3. Common Firewall Configuration mistakes

Gartner said that 99% of firewall breaches are caused by configuration errors. A wrong configuration can affect. the whole organization system. If a firewall was damaged attackers can easily get into their network and can easily access it. The mostly common mistakes are known as,

- Relaying on Import/Export

When a user designs a new network replacing a firewall with another firewall configuration is a mistake. It may be a priority of user's organization. If the firewalls don't exact same then there has a huge mistake. If it happens then there will be a suspicious traffic in network system.

- Using Broad Policies

These firewalls are open policies, so the IT personals do not untouched them. organization adjust these broad policies later but, in many times, they never visit that rule sets then broad policies will open to the unauthorized people then these people can get the organization stuff easily.

- Forgetting outbound rules

People think that if configure only inbound rules can be secure the network system but the outbound rules also important to a network system. If not, threats can pull users data to external location and lack of configuration of outbound policies can have IP spoofing attacks that hackers store illegal data on users' network and also if it wasn't fix it might be a problem for the organization.

- Neglecting Security Features

This means that user not using all the security features. There lots of securities in firewalls such as GEO-IP configuration that means can block web traffic from entire countries and content filtering can stop problematic websites and SMTP protection likewise.

- VPN

Virtual Private Network, or VPN for short, is the ability to create a secure network connection when utilizing public networks. VPNs enable user to utilize public Wi-Fi hotspots securely, safeguard user online identity by obscuring user IP address, and establish an encrypted tunnel for users' data.

THE TYPES OF VPN S

- Access VPNs

These VPNs are intended to give faraway workers or lone users secure access to a private network over the internet. Users can safely connect from a distance to a company network or internal resources. To secure the connection and guarantee anonymity, remote access VPNs often employ authentication and encryption mechanisms.

- Site-to-Site VPN

Site-to-Site VPN, often referred to as a Router-to-Router VPN, is a method for using the internet to link together various networks or locations. It creates secure communication between the local networks of various sites, such data centers or branch offices. Site-to-Site VPNs give businesses the ability to link geographically separated networks as if they were on the same local network by establishing a virtual private network.

- Intranet VPN

An intranet virtual private network (VPN) connects various networks or devices inside a private network. Between several devices or subnets inside the same company, it enables safe data transfer and communication. For internal use, intranet VPNs offer a private and secure network infrastructure.

- Extranet VPNs

used to provide safe connections between several businesses or business partners. It enables secure access to particular resources or services on the private network for authorized users from outside organizations. Through the use of extranet VPNs, trustworthy parties may communicate in a safe and regulated manner while being isolated from the public internet.

THE BENEFITS OF VPN

- dependable encryption
- covering up your whereabouts
- Availability of regional connections
- Transferring data securely

Figure 8 VPN (www.kaspersky.com)

- **IMPLEMENTING A DMZ, STATIC IP AND NAT IN A NETWORK CAN IMPROVE NETWORK SECURITY**

- **1. DMZ**

Demilitarized Zone" is what DMZ stands for. A DMZ is a distinct and segregated network segment that lies between an organization's intranet and its external network, which is typically the internet, in the context of computer networks and cybersecurity. The main goal of a DMZ is to offer an extra layer of protection by separating the internal private network from any externally accessible systems or services. The internal network's critical data and resources are shielded from potential internet assaults by the DMZ, which serves as a buffer zone. Web servers, email servers, and other public-facing applications are examples of servers or services that are frequently found in the DMZ.

BENEFITS OF DMZ

In terms of security and operational effectiveness, DMZ (Demilitarized Zone) implementation in a network architecture offers a number of advantages. Here are a few major advantages of utilizing a DMZ

- **Improved Network Security**

A DMZ's main advantage is its increased network security. You can separate public-facing servers and services from the internal network by putting them in the DMZ. This separation lowers the danger of unwanted access or assaults by preventing direct access to sensitive data and essential systems.

- **Controlled Access**

For external organizations to access certain services located in the DMZ, the DMZ serves as a controlled entry point. It enables enterprises to specify and apply stringent security and access requirements. By limiting access, possible security lapses or harmful activity's effects are lessened.

- Network segmentation:

The DMZ divides the internal network from the external network. The lateral movement of attackers is restricted by this segmentation inside the network. Even if an attacker succeeds in breaching the DMZ, they will encounter more obstacles while trying to access the inside network, buying more time for discovery and reaction.

Network traffic going to and coming from the DMZ may be carefully watched and documented. Security tools can be implemented to analyze the traffic and find any malicious activity or unauthorized access attempts, such as firewalls and intrusion detection systems (IDS). This monitoring capability improves the overall security posture and helps with forensic investigation and incident response.

- Scalability and Flexibility

Organizations may simply grow and add new services thanks to the DMZ design.

- **2. STATIC IP**

An IP address that doesn't change over time and remains constant is known as a static IP address. It is given to a machine, such a computer, server, or network router, and is continuous, allowing other machines to connect to it using the same IP address constantly.

2.1 Benefits Of Static IP

- **Fixed Address**

A static IP address guarantees that the given IP address won't change over time. This is especially helpful if you need to host services or equipment like web servers, email servers, or remote access systems that need a constant and predictable address. It enables consumers to connect to these services with confidence using a known IP address.

- **Reliable Remote Access**

Having a static IP address makes it easier to access devices or services remotely. You can connect to the device immediately using its fixed IP address rather than continuously looking for the device's changing IP address. For things like remote desktop access, VPN connections, or accessing security cameras, this is very helpful.

- **Services that require hosting**

A static IP is necessary for hosting services like websites or gaming servers. It makes it possible for users to continually access your services without being interrupted by shifting IP addresses. For a consistent and ongoing online presence, this is essential.

- **DNS Management**

Since a domain name is normally linked to a static IP address, you may set up DNS (Domain Name System) records to connect your domain to the fixed IP. This makes it simpler for people to locate and utilize your services by ensuring that your domain name continuously links to the right IP address.

- **3. NTP**

Network Time Protocol is known as NTP. It is a protocol used to synchronize computer and network clocks over the internet or within a network. NTP's main objective is to guarantee that devices have correct and synchronized time information, which is essential for many network processes and applications

Benefits of NTP

- **Time Synchronization**

Devices can synchronize their clocks to a shared time reference via NTP. Regardless of differences in their internal clocks or network delay, it makes sure that various devices within a network or across networks retain constant time.

- **Client-Server Architecture**

The client-server architecture used by NTP. Both NTP clients (devices that need correct time) and NTP servers (devices that supply accurate time) are used in the time synchronization process. NTP clients ping NTP servers to get precise time readings.

- **Stratum Levels**

Based on stratum levels, NTP arranges time servers into a hierarchical framework. Lower stratum numbers signify servers that are closer to the primary time source. A stratum level represents the distance from the reference clock. Stratum 1 servers have direct access to a very precise.

- **Redundancy and fault tolerance**

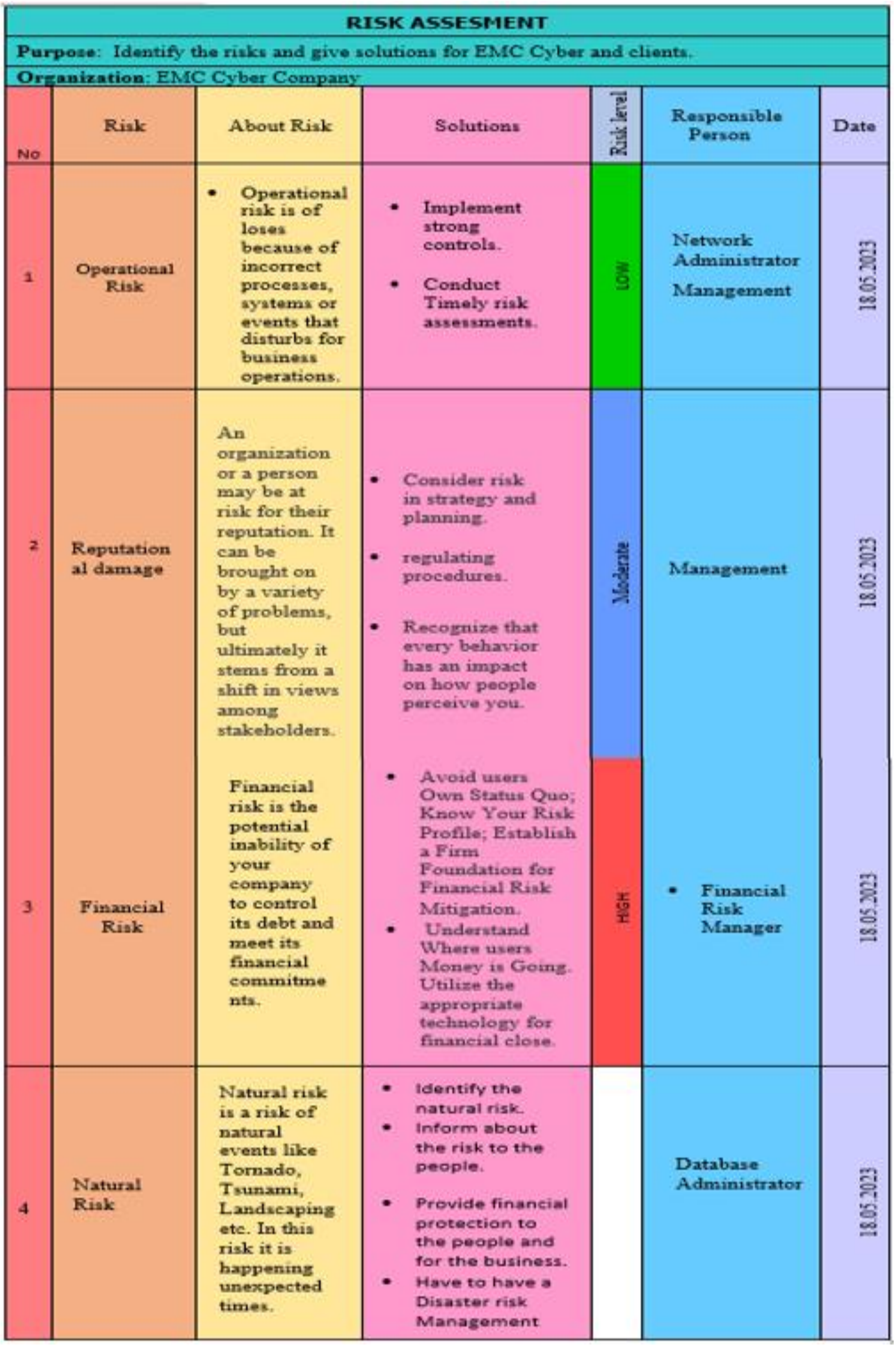
For redundancy and fault tolerance, NTP permits the use of several time servers. To assure accuracy and dependability, clients can connect to several servers and compare the time information collected from various sources.

NTP includes authentication measures to guarantee the authenticity and integrity of time information. NTP authentication (NTPAuth) and other protocols that make use of cryptographic keys can help stop time spoofing and unauthorized time source modification.

- **Applications and Importance**

For many network applications and services, precise time synchronization is essential. It is necessary for financial transactions, distributed systems, network log analysis, file synchronization, authentication protocols, and event coordination across remote systems.

- **DISCUSSION OF RISK ASSESSMENT PROCEDURES.**



RISK ASSESMENT						
Purpose: Identify the risks and give solutions for EMC Cyber and clients.						
Organization: EMC Cyber Company						
No	Risk	About Risk	Solutions	Risk level	Responsible Person	Date
1	Operational Risk	• Operational risk is of loses because of incorrect processes, systems or events that disturbs for business operations.	• Implement strong controls. • Conduct Timely risk assessments.	LOW	Network Administrator Management	18.05.2023
2	Reputational damage	An organization or a person may be at risk for their reputation. It can be brought on by a variety of problems, but ultimately it stems from a shift in views among stakeholders.	• Consider risk in strategy and planning. • regulating procedures. • Recognize that every behavior has an impact on how people perceive you.	Moderate	Management	18.05.2023
3	Financial Risk	Financial risk is the potential inability of your company to control its debt and meet its financial commitments.	• Avoid users Own Status Quo; Know Your Risk Profile; Establish a Firm Foundation for Financial Risk Mitigation. • Understand Where users Money is Going. Utilize the appropriate technology for financial close.	HIGH	• Financial Risk Manager	18.05.2023
4	Natural Risk	Natural risk is a risk of natural events like Tornado, Tsunami, Landscaping etc. In this risk it is happening unexpected times.	• Identify the natural risk. • Inform about the risk to the people. • Provide financial protection to the people and for the business. • Have to have a Disaster risk Management		Database Administrator	18.05.2023

Table 1 : Risk Assessment (Made by Author)

Risk assessment is needed to make sure the safety of organization. It recognizes and judge and arrange the risk in work. It results a good safe working place.

The risk assessment,

- Recognized the danger
- Evaluate the danger
- Control the risk

- **DATA PROTECTION PROCESSES AND REGULATIONS AS APPLICABLE TO AN ORGANIZATION.**

Data Protection process and regulations play a key role in the security of an organization. It takes actions to stop the Threats and protects confidential information from damaging or destroying Data.

- Data protection – it guards your data from losing through backup and recovery.
- Data security - To protect against viruses or spyware. It provides internal and external threats.
- Data Privacy - To control entries to the data.

Regulations that commonly Applicable

- Data Protection standards:

When managing personal data, organizations must abide by the basic data protection standards. Generally speaking, these principles include getting valid and fair permission for data gathering, restricting data collection to what is required, guaranteeing accuracy and data quality, putting in place suitable security measures, and protecting data integrity and confidentiality**.**

- General Data Protection policy (GDPR):

The GDPR is a thorough data protection policy that is applicable to businesses that manage the personal data of people living in the European Union (EU). It lays forth particular demands on data controllers and processors, such as the need for legal justifications for processing, individual rights (including the right of access and the right to be forgotten), notification of data breaches, and data transfer procedures.

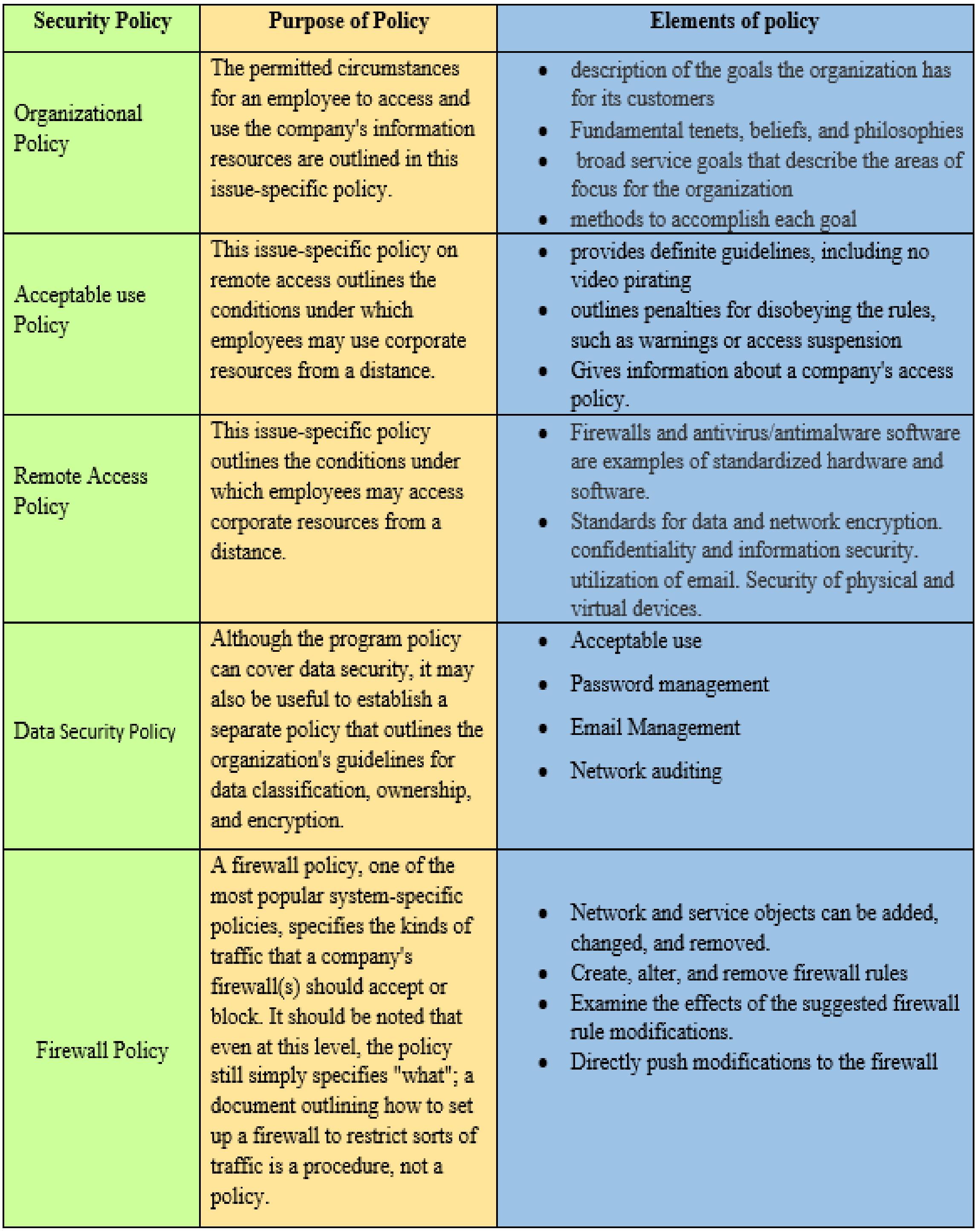
- Data Security Measures

To safeguard personal data from unauthorized access, disclosure, alteration, or destruction, organizations must put in place the proper organizational and technological security measures. This might include actions like employee training on data protection procedures, access controls, safe storage, routine security assessments, and encryption.

- Consent and Privacy Notices

It is frequently necessary to get individuals' lawful consent before processing their personal data. The aim of data processing, the categories of data being processed, the rights of persons, and any third parties with whom data may be shared must all be made explicit in privacy statements that are simple to read.

- **DESIGNING AND IMPLEMENTING A SECURITY POLICY FOR AN ORGANIZATION**



Security Policy	Purpose of Policy	Elements of policy
Organizational Policy	The permitted circumstances for an employee to access and use the company's information resources are outlined in this issue-specific policy.	• description of the goals the organization has for its customers • Fundamental tenets, beliefs, and philosophies • broad service goals that describe the areas of focus for the organization • methods to accomplish each goal
Acceptable use Policy	This issue-specific policy on remote access outlines the conditions under which employees may use corporate resources from a distance.	• provides definite guidelines, including no video pirating • outlines penalties for disobeying the rules, such as warnings or access suspension • Gives information about a company's access policy.
Remote Access Policy	This issue-specific policy outlines the conditions under which employees may access corporate resources from a distance.	• Firewalls and antivirus/antimalware software are examples of standardized hardware and software. • Standards for data and network encryption. confidentiality and information security. utilization of email. Security of physical and virtual devices.
Data Security Policy	Although the program policy can cover data security, it may also be useful to establish a separate policy that outlines the organization's guidelines for data classification, ownership, and encryption.	• Acceptable use • Password management • Email Management • Network auditing
Firewall Policy	A firewall policy, one of the most popular system-specific policies, specifies the kinds of traffic that a company's firewall(s) should accept or block. It should be noted that even at this level, the policy still simply specifies "what"; a document outlining how to set up a firewall to restrict sorts of traffic is a procedure, not a policy.	• Network and service objects can be added, changed, and removed. • Create, alter, and remove firewall rules • Examine the effects of the suggested firewall rule modifications. • Directly push modifications to the firewall

Table 2 : Policy table (Made by Author)

- **THE MAIN COMPONENTS OF AN ORGANIZATIONAL DISASTER RECOVERY PLAN, JUSTIFYING THE REASONS FOR INCLUSION.**
- **1. DISASTER RECOVERY PLAN**

A disaster recovery plan outlines procedures that uniformly govern how a certain business reacts to disruptive events including cyberattacks, natural disasters, and power outages. The plan is a formal document that outlines how to reduce catastrophe scenarios' consequences, aid the business in minimizing damage, and swiftly resume operations. Organize your strategy according to the area and the kind of catastrophe to guarantee efficacy, and include clear, step-by-step implementation instructions that stakeholders can readily follow.

1.1Steps of Disaster Recovery Plan

- Create a disaster recovery with the team.
- List all names and contact details
- Consider a chain at command
- Determine the risk assessment
- Make a b Plan
- Protect Company details
- Test the system

1.2 Importance of Disaster Recovery Plan

- Can prevent data loss
- Minimize downtime
- Maintain customer satisfaction

- **1.3 DISASTER RECOVERY PLAN**

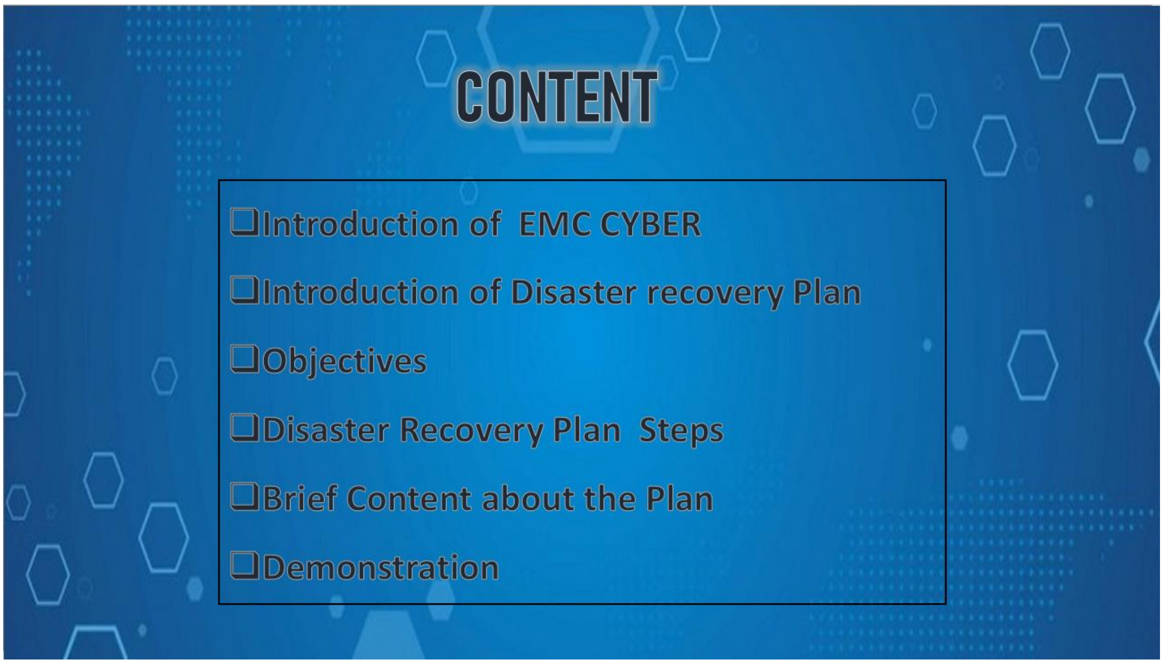
Threat	Vulnerability	Responsible person	Solutions
Malware	**HIGH**	Network Engineers	• Protect important business procedures and sensitive information. • preserve the confidence of your clients, partners, and stockholders. • Avoid significant financial losses from damage or ransom payments.
Cloud Security	MEDIUM	Network Engineers	• Recognize the risks and obligations • Provide staff with training on cloud security • . Encrypt your data • . Install a monitoring system
‘ Ransomware	HIGH	Unit Maintainer	• Make use of security software • Know the risks posed by ransomware: • Utilize safe networks: • Train your staff:
Data Loss	MEDIUM	Database Engineers	• Create a device security policy • back up user data, • encrypt sensitive data • Use software • establish a password policy • train user team • Improve the equipment.

Table 3 : Disaster Recovery Plan (Made by Author)

- **DISASTER RECOVERY PLAN FOR EMC CYBER**

DISASTER RECOVERY PLAN FOR EMC CYBER

Figure 9 Disaster Recovery Plan slide 1 (made by author)



CONTENT

❑Introduction of EMC CYBER

❑Introduction of Disaster recovery Plan

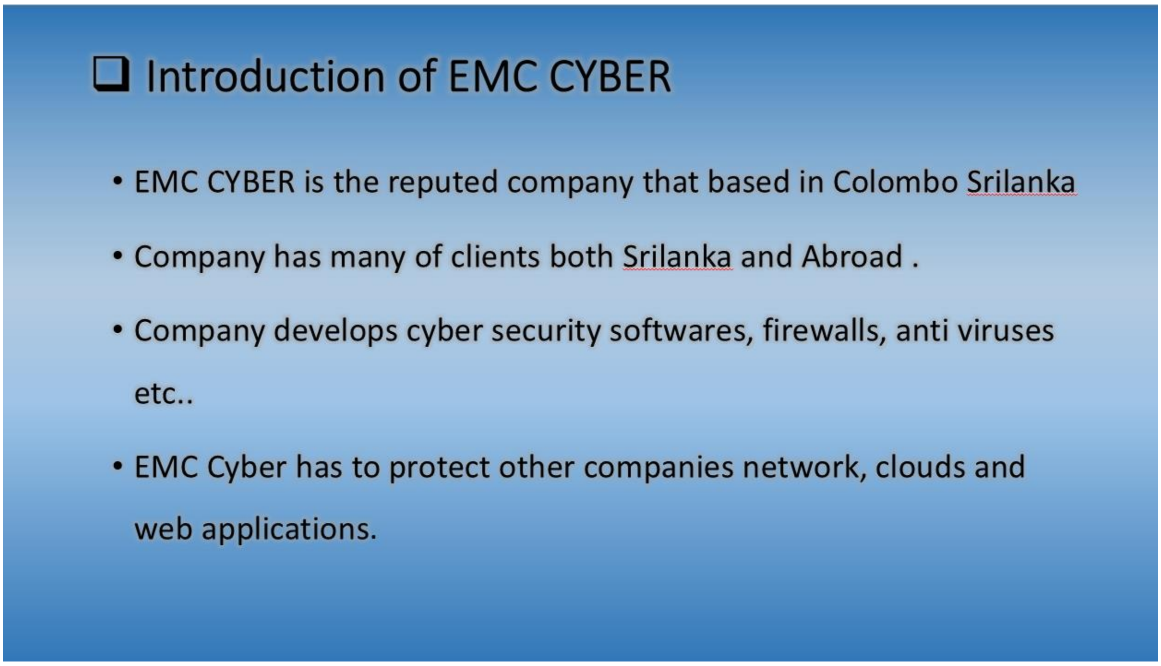
❑Objectives

❑Disaster Recovery Plan Steps

❑Brief Content about the Plan

❑Demonstration

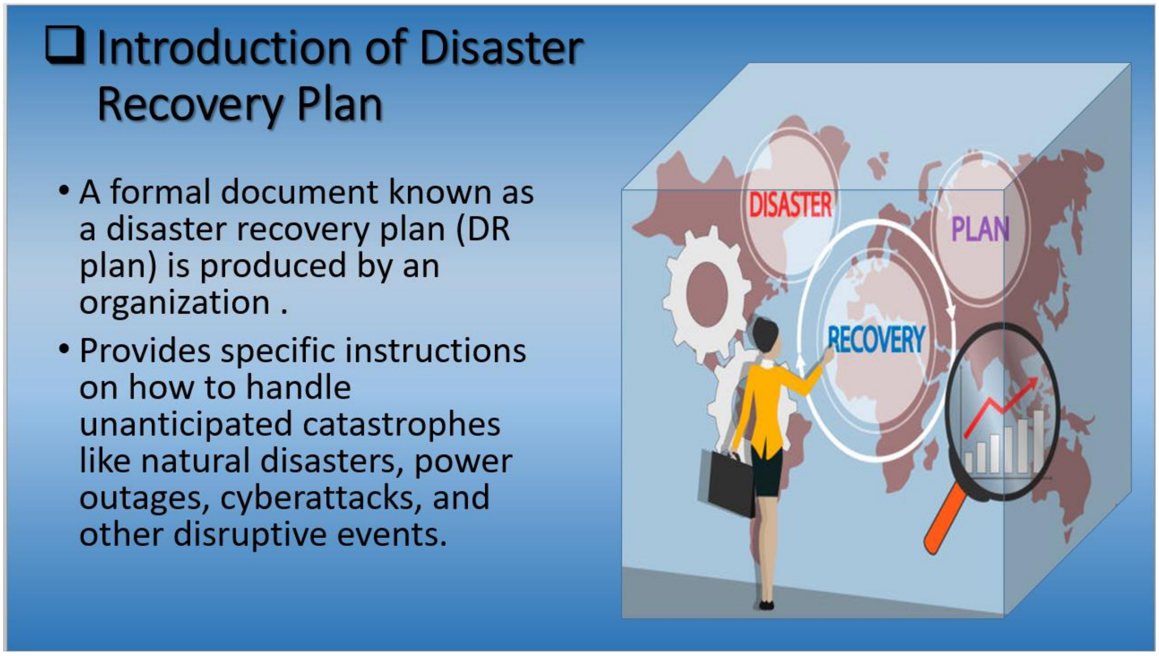
Figure 10 Disaster Recovery Plan slide 2 (made by author)



❑ Introduction of EMC CYBER

- EMC CYBER is the reputed company that based in Colombo Srilanka
- Company has many of clients both Srilanka and Abroad .
- Company develops cyber security softwares, firewalls, anti viruses etc..
- EMC Cyber has to protect other companies network, clouds and web applications.

Figure 11 Disaster Recovery Plan slide 3 (made by author)

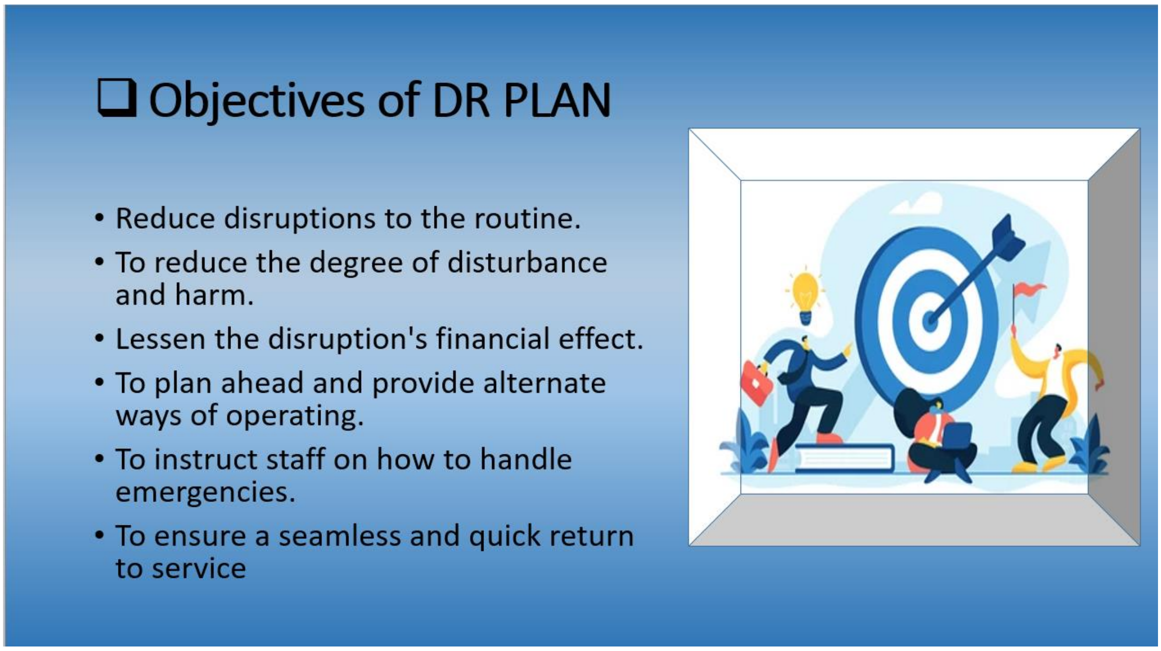


❑ Introduction of Disaster Recovery Plan

- A formal document known as a disaster recovery plan (DR plan) is produced by an organization .
- Provides specific instructions on how to handle unanticipated catastrophes like natural disasters, power outages, cyberattacks, and other disruptive events.

DISASTER
PLAN
RECOVERY

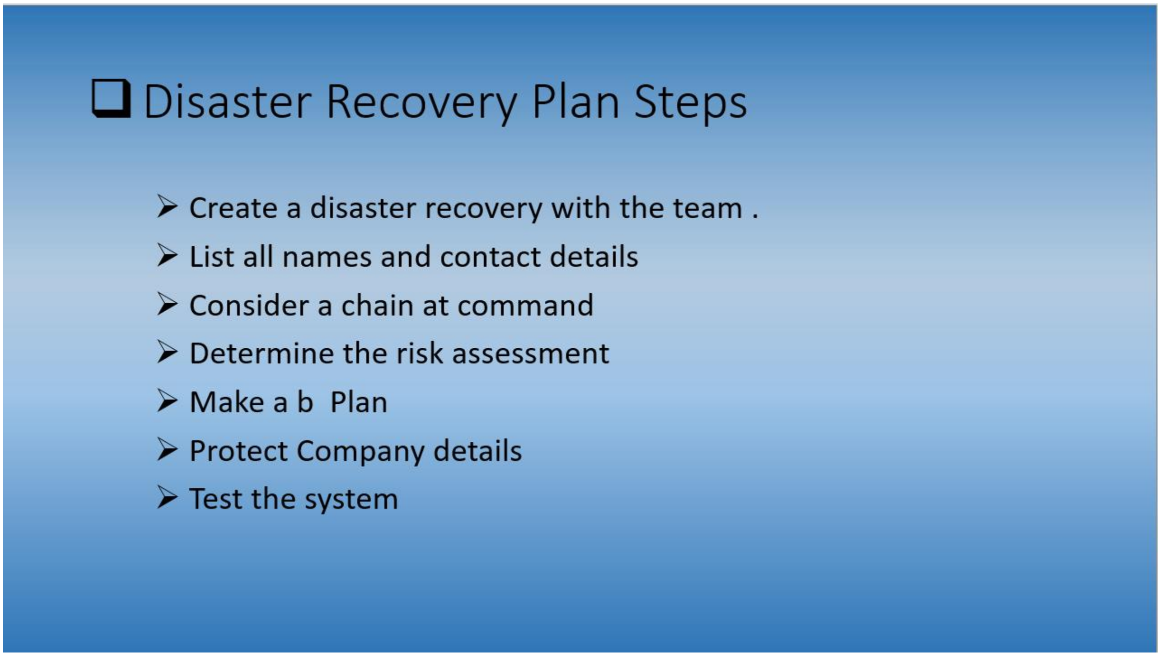
Figure 12 : Disaster Recovery Plan slide 4 (made by author)



❑ Objectives of DR PLAN

- Reduce disruptions to the routine.
- To reduce the degree of disturbance and harm.
- Lessen the disruption's financial effect.
- To plan ahead and provide alternate ways of operating.
- To instruct staff on how to handle emergencies.
- To ensure a seamless and quick return to service

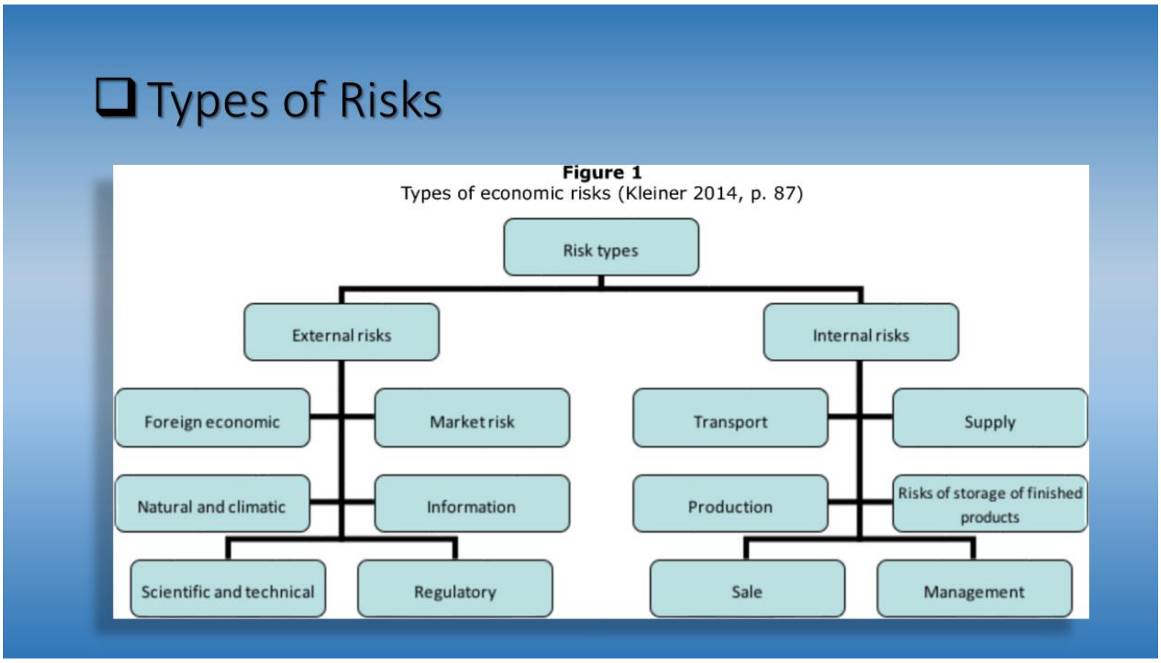
Figure 13 Disaster Recovery Plan slide 5 (made by author)



❑ Disaster Recovery Plan Steps

- ➢ Create a disaster recovery with the team .
- ➢ List all names and contact details
- ➢ Consider a chain at command
- ➢ Determine the risk assessment
- ➢ Make a b Plan
- ➢ Protect Company details
- ➢ Test the system

Figure 14 Disaster Recovery Plan slide 6 (made by author)



❑ Types of Risks

Figure 1

Types of economic risks (Kleiner 2014, p. 87)

Risk types

External risks

Internal risks

Foreign economic

Market risk

Natural and climatic

Information

Scientific and technical

Regulatory

Transport

Supply

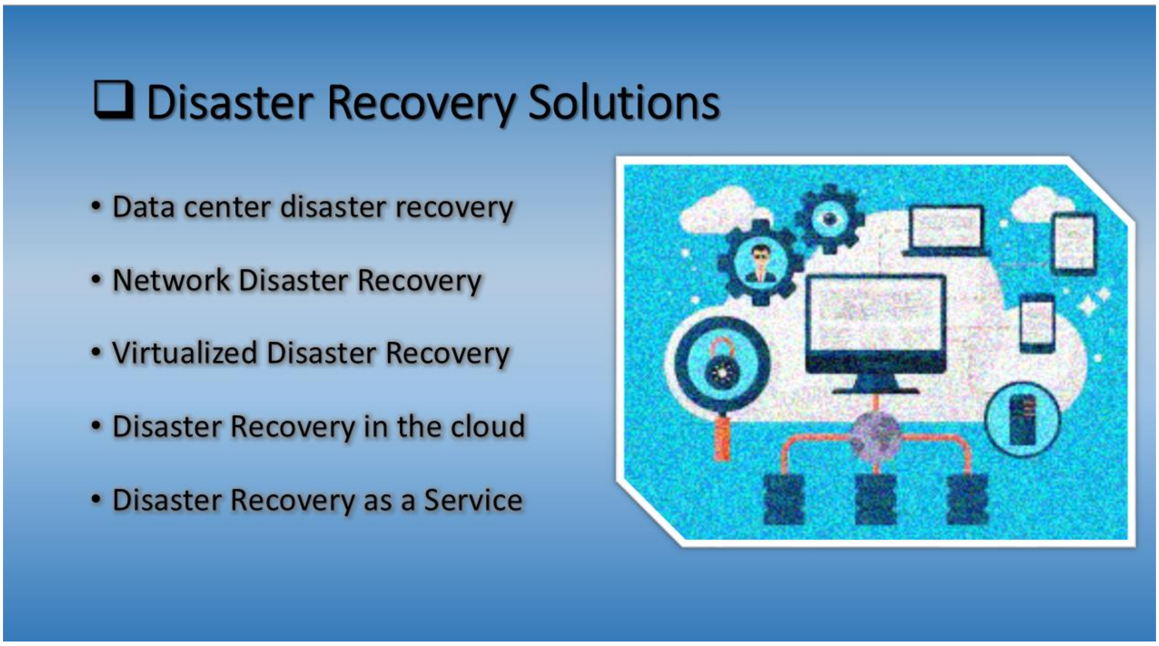
Production

Risks of storage of finished products

Sale

Management

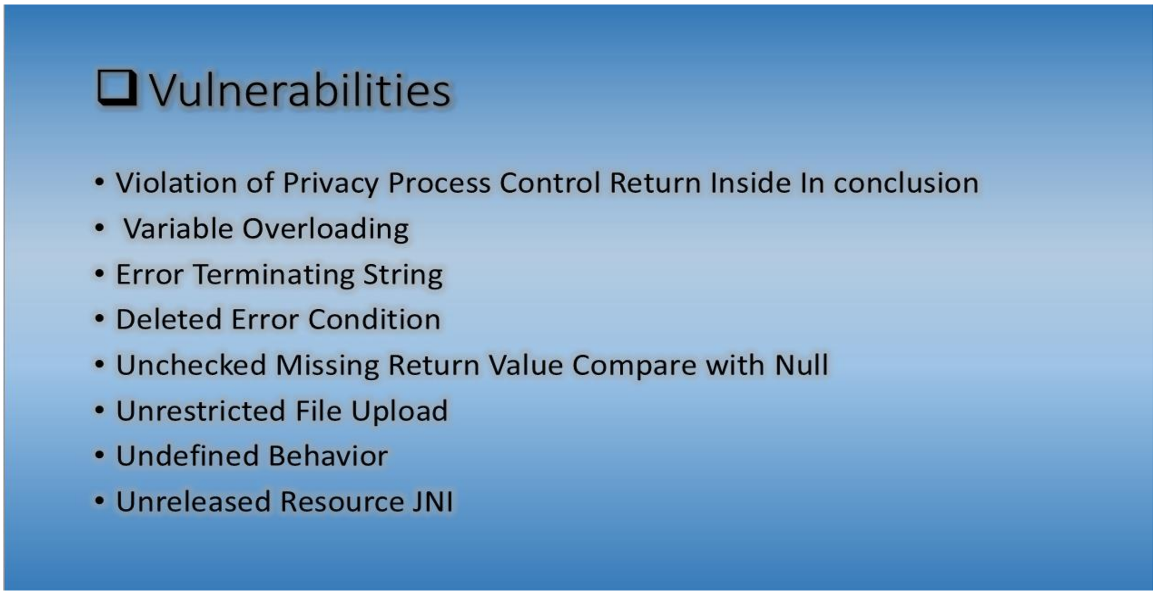
Figure 15 Disaster Recovery Plan slide 7 (made by author)



❑ Disaster Recovery Solutions

- Data center disaster recovery
- Network Disaster Recovery
- Virtualized Disaster Recovery
- Disaster Recovery in the cloud
- Disaster Recovery as a Service

Figure 16 Disaster Recovery Plan slide 8 made by author)



❑ Vulnerabilities

- Violation of Privacy Process Control Return Inside In conclusion
- Variable Overloading
- Error Terminating String
- Deleted Error Condition
- Unchecked Missing Return Value Compare with Null
- Unrestricted File Upload
- Undefined Behavior
- Unreleased Resource JNI

Figure 17 Disaster Recovery Plan slide 9 (made by author)

- **A METHOD TO ASSESS AND TREAT IT SECURITY RISKS**

ORGANIZATIONAL SECURITY RISKS AND SOLUTIONS TO REDUCE IT

Risk	Definition	Solutions
Operational Risk	A risk of system mistake, Human instruction and also technical issues in organization called as an operational risk.	Need to have a strong relationship between business to business. Implement a plan of risk management. Need to have backup plans. Obey the rules and regulations of the organization correctly. Train the employees about the risks and how to reduce it.
Natural risk	Natural risk is a risk of natural events like Tornado, Tsunami, Landscaping etc. In this risk it is happening unexpected times.	Identify the natural risk. Inform about the risk to the people. Provide financial protection to the people and for the business. Have to have a Disaster risk Management plan.
Security Risk	Security risk means an organization that could have a risk of financial. Also, for the can have security risks.	Identify the risk in the organization. (Network, Servers, Data centers etc.) Create risk profiles. Measure risks in the organization. Apply mitigating controls for each risk in the organization.
Environmental Risk	Environmental risk known as the environmental issues like pollution, noises, climate changes etc..	Identify the Environmental risk and the sources that harm. Research the harm that costs.

Business Risk	Business risk means when forcedly business reaching downwards in business.	Identify the risk that negatively effect in an organization. Then identify if there had a risk who or what could be harmed. Develop risk Document. Then evaluate controls for risk.
Liquidity Risk	The risk of being unable to buy or sell assets in each size over a given period without adversely affecting the price of the asset.	Identify the cash flow of the organization and improve it. Improve risk reporting abilities. Identify the balance sheet and improve it.

Table 4 : Organizational security risks and Solutions to reduce it

- **IT SECURITY RISKS AND SOLUTIONS TO REDUCE IT**

Risk	Solutions
• Ransomware	• Need to have a good, educated employees. • Upgrade all software's. • Secure network system. • Need to have a backup data always.
• Malware	• Install anti-virus software's. • Must use secure methods to protect the devices. • Update software. • Apply emails security protections. • Need to look always for suspicious activity.
• Phishing	• Install Firewalls. • When there has a pop-up link don't need to click such links. • Install an anti-phishing tool. • Don't give any personal details
• Denial of service attack	• Need to have high level network security. • Monitor warning signals. • Monitor of Network traffic.
• Insider Threat	• Need to apply advanced passwords as a security method. • Monitor all endpoints of device and have to monitor mobile devices. • Enable supervision. • Apply secure backups.

Table 5 : IT security Risks and Solutions to reduce it

- **THREE BENEFITS TO IMPLEMENTING NETWORK MONITORING SYSTEMS.**

In these days there are lots of things connected to the internet. Most of employees work remotely and uses own devices to access company networks but then the security risk of the company is increased. Because of that it is important to understand benefits about the network monitoring systems.

If an outage happens it takes a long time to recover and in that time period, the company can lose staff time and also can lose the productivity. So, it is better to have a network monitoring system to prevent such disasters.

Allocate resources most effectively.

In a company the workloads and projects are very heavy, and it is very complex. So, it teams can't do the work without any work managed also It teams can't spent time for any other works. So, by implementing the network monitoring system then can understand what's the problem and can place protective measures and fix it.

Issues can Fix Quickly

For a Company There are lots of issues not only one. Companies should always have to fix all issues for the Company growth. So, it is very important to implement a network monitoring system because it can quickly identify the main reason and can take the steps to fix it quickly. If there is an issue in network system like traffics likewise this method can help to fix it. This method can also identify the security vulnerabilities.

Enhance Customer Satisfaction

When a customer needs the information's about the company or something it should be appear when its needed. Then the customer will satisfy about the product. By having a network monitoring system can easily resolve any issues and can build the loyalty among customers. Also, Company can search about the customers feedbacks through social media posts about the company. That's how enhance the customer satisfaction through the network monitoring system.

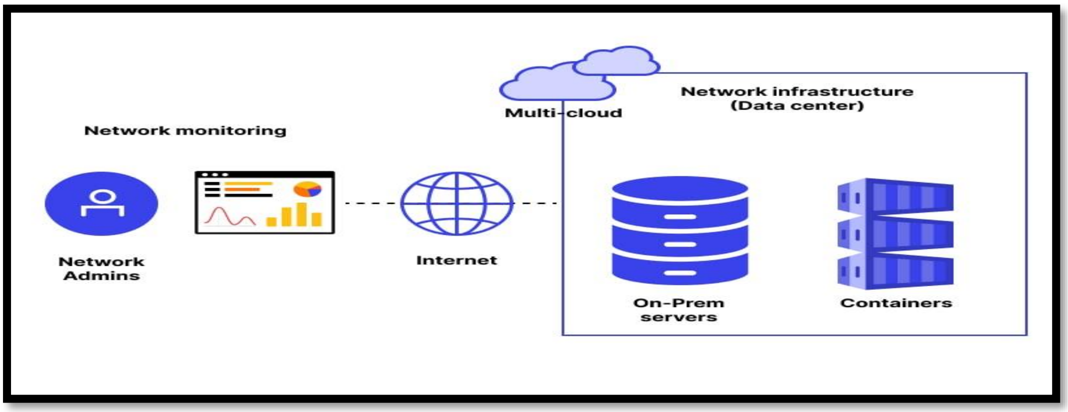


Figure 18 Network monitoring system (www.wallarm.com)

- **THE ISO 31000 RISK MANAGEMENT METHODOLOGY AND ITS APPLICATION IN IT SECURITY**

ISO stands for International standard organizations. ISO 13000 Risk Management means a guideline that give a structural approach how to manage a risk management system. This was published in 2009. There are two scopes that connects with risk management systems. That are known as,

- A risk management framework
- A risk management process

- **THE COMPONENTS OF ISO 31000**

In ISO 13000 there are two key components that are known as ,

- The framework
- The Process

- **THE FRAMEWORK**

This creates all management system and help to discover the risks. This is known as cycle like plan, do, check to the all-management system.

The major components of frameworks are,

Government policy

- It means that begin the mission and then it will appear about the organization commitment

Program design

- Design a program framework for continuous improvement.

Implementation

- Implement the risk management framework and program it correctly.

Monitoring and Evaluation

- monitoring the management system's effectiveness and organizational structure

Continuous Enhancement

- Check overall management system performance.

- **THE PROCESS**

Early on in the Process, regular communication is essential for grasping the interests and concerns of stakeholders and so validating the Process's emphasis. Later, consistent communication helps to explain the rationale behind decisions and the reasons the company needs certain risk solutions.

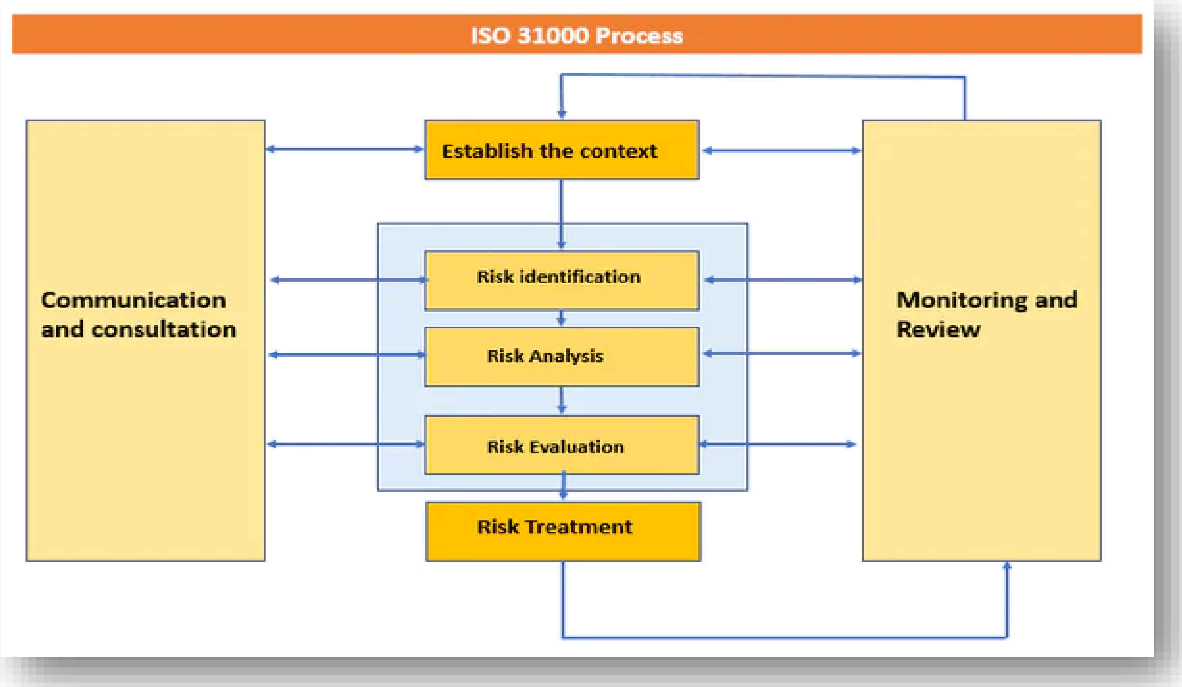


Figure 19 ISO 31000 Risk Management System (https://iso-docs.com/)

- **POSSIBLE IMPACTS TO ORGANIZATIONAL SECURITY RESULTING FROM AN IT SECURITY AUDIT**

DEFINITION OF AN IT SECURITY AUDIT

An organization's established security procedures are evaluated as part of an information security audit. It is a procedure that assesses how well the defensive systems put in place counter threats. Network assessments, vulnerability scans, penetration tests, and other procedures are frequently included in information security audits to assist identify weaknesses and security gaps in IT systems. An administrative, physical hardware, software application, and network inspection are all included in the audit. In this way, the evaluation procedure may assist a business or organization in understanding the state of its security.

TYPES OF IT SECURITY AUDITS

Its security audit types can be divided into two categories. That are known as,

Approached Based

In approached based category there are 3 types of Audits.

- Black box audit

  In this category auditor only knows the publicly available information regarding the organization.

- White box audit

  In this audit the auditor will provide the details of the organization that to be audited.

- Grey box audit

  This audit gathered the information and saved in that time also its provide the beginning of the audit and proceed it.

Methodology Based

- Penetration Test

In this method auditor tries to interrupt the organization Framework.

- Compliance Audits

Only certain can check if the organization observe security standards

- Risk Assessment

Analysis of various types of resources that can be threaten to the organization

IMPORTANCE OF AN IT SECURITY AUDIT FOR AN ORGANIZATION

- safeguards a company's important data assets.
- keeps the company in compliance with several security certifications.
- discovers security flaws before hackers do.
- updates the company on security precautions.
- determines the weak points in the physical security.
- aids in creating new security rules for the firm.
- enables the company to be ready to act quickly in the event of a cybersecurity compromise.

• THE ROLES OF STAKEHOLDERS IN THE ORGANISATION TO IMPLEMENT SECURITY AUDIT RECOMMENDATIONS.

Some significant people are directly or indirectly involved in the success of a firm. These people, also known as stakeholders, create strategies and procedures to carry out commercial tasks and generate customer confidence.

- **ROLES AND RESPONSIBILITIES**

Owners

A company's assets and business may be subject to the owner's sole control. A business may have a single owner or numerous owners, depending on the corporate structure and incorporation. Major company decisions are made by these owners, and they also negotiate contract conditions with other parties. They also decide on the manufacturing method and the available goods and services. Owners may also collaborate on the development of the company's growth and sales plans with other stakeholders including the board, consultants, and staff. Owners of the firm are personally accountable for its success and design the objectives to do so.

Managers

For the purpose of coordinating staff operations, managers interact closely with senior management. They supervise teams and departments to make ensuring that their operations follow the mission and rules of the business. These individuals manage teams and assign work while ensuring that staff members have access to the tools, they need to complete their assignments. Additionally, they determine project deadlines, assess employee performance, and deliver crucial reports to top management. Managers may work alongside senior executives and participate in the decision-making process, depending on the firm structure.

There are 3 levels of managers in a Company.

- Senior Manager
- Middle-tier managers
- Lower managers

Employees

For the purpose of completing tasks and achieving organizational goals, businesses add workers to their workforce. Employees are valuable to the company because their quality affects productivity and efficiency over time. They also play a significant role in the success of the company by finishing projects and interacting with consumers and other stakeholders. The business offers perks, pay, and other forms of payment in return for the services that employees give.

To assist employees in honing their skills, a corporation may also provide personal development programs like workshops and training. Employees provide feedback that can affect decision-making even if they may not directly participate in the decision-making process. Additionally, it's critical for companies to foster an environment that is welcoming to their employees since doing so influences customer satisfaction, brand perception, and productivity.

Labor Unions

An organization that often stands up for workers' rights at work is a labor union. Because they develop the regulations that define the benefits, working conditions, and compensation for employees in both private and public enterprises, labor unions are crucial to business. In some cases, they may also represent workers in employee-related matters and assist them in negotiating employment agreements. In cases of policy infractions, labor unions may impede operations, thus it's critical for businesses to keep good ties with them.

- **REFERENCES**

Anon., n.d. *Blue pencil.* [Online] Available at: https://www.blue-pencil.ca

Anon., n.d. *Risk.Net.* [Online] Available at: https://www.risk.net

Hell, M., 2021. *debricked.* [Online] Available at: https://debricked.com/
[Accessed 29 07 2021].

lint, T., 2023. *Kacher Group.* [Online] Available at: https://www.tkg.com/insights/learn/4-types-information-technology-security
[Accessed 24 january 2023].

Grading Rubric

Grading Criteria	Achieved	Feedback
LO1 Assess risks to IT security		
P1 Identify types of security risks to organizations.		
P2 Describe organizational security procedures.		
M1 Propose a method to assess and treat IT security risks.		
LO2 Describe IT security solutions		
P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.		
P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.		
M2 Discuss three benefits to implement network monitoring systems with supporting reasons.		
D1 Evaluate a minimum of three of physical and virtual security measures that can be employed to ensure the integrity of organizational IT security.		
LO3 Review mechanisms to control organizational IT Security		
P5 Discuss risk assessment procedures.		
P6 Explain data protection processes and regulations as applicable to an organization.		
M3 Summarize the ISO 31000 risk management methodology and its application in IT security.		
M4 Discuss possible impacts to organizational security resulting from an IT security audit.		
D2 Consider how IT security can be aligned with organizational policy, detailing the security impact of any misalignment.		
LO4 Manage organizational security		

P7 Design and implement a security policy for an organization.		
P8 List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion.		
M5 Discuss the roles of stakeholders in the organization to implement security audit recommendations.		
D3 Evaluate the suitability of the tools used in an organizational policy.		