Higher Nationals

Internal verification of assessment decisions – BTEC (RQF)

INTERNAL VERIFICATION – ASSESSMENT DECISIONS			
Programme title	BTEC Higher National Diploma in Computing		
Assessor		**Internal Verifier**	
Unit(s)	**Unit 05: Security**		
Assignment title	EMC Cyber		
Student's name	Ryan Wickramaratne		
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	Ryan Wickramaratne (COL 00081762)		
Unit Title	Unit 05: Security		
Assignment Number	1	**Assessor**	Mrs. Ama
Submission Date	17/08/2022	**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** □ M4 □ D2 □

LO4. Manage organisational security.

Pass, Merit & Distinction Descripts **P7** □ **P8** □ **M5** □ **D3** □

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 programme. .
4. I declare therefore that all work presented by me for every aspects of my programme, 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.

17/08/2022

ryandilthusha@gmail.com

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

Assignment Brief

Student Name /ID Number	Ryan Wickramaratne (COL 00081762)
Unit Number and Title	Unit 5- Security
Academic Year	2020/2021
Unit Tutor	Mrs. Ama
Assignment Title	EMC Cyber
Issue Date	
Submission Date	17/08/2022
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 organisational IT security.

LO4 Manage organisational 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 a number of 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).

Grading Rubric

Grading Criteria	Achieved	Feedback
LO1 Assess risks to IT security		
P1 Identify types of security risks to organisations.		
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 thirparty 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 organisational IT security.		
LO3 Review mechanisms to control organisational IT security		
P5 Discuss risk assessment procedures.		
P6 Explain data protection processes and regulations as applicable to an organisation.		
M3 Summarise the ISO 31000 risk management methodology and its application in IT security.		

M4 Discuss possible impacts to organizational security resulting from an IT security audit.		
D2 Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment.		
LO4 Manage organizational security		
P7 Design and implement a security policy for an organisation.		
P8 List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.		
M5 Discuss the roles of stakeholders in the organisation to implement security audit recommendations.		

Acknowledgement

I would like to express my special thanks of gratitude to my programing lecturer Mrs. Ama for providing invaluable guidance and giving immense amount of knowledge to work on this assignment perfectly. I specially thanks her because she helped us in doing a lot of research and I came to know about so many new things about the IT security.

Secondly, I would like to thank my parents and friends who helped me a lot in finalizing this project within the limited time frame.

Executive Summery

This entire assignment is based on assuming the role of External Security Analyst investigate and report on potential cyber security threats to LockHead web site, applications and infrastructure. After the investigation I needed to plan a solution and how to implement it according to standard software engineering principles. The purpose of this assignment is to improve knowledge and skills in Security in Computing.

Assess IT security risks in an organization by identifying types of security risks and proposing a method for assessing and treating IT security risks. Then, describing IT security solutions, including identifying the potential impact on IT security of incorrectly configured firewall policies and third-party VPNs, implementing a DMZ, static IP, and NAT in a network, and implementing network monitoring systems, with supporting reasons.

Following that, Examining control mechanisms for organizational IT security with Managing organizational security through security policies, disaster recovery plans, and IT security audits.

Abbreviations

CIA - Confidentiality, Integrity, and Availability

VPN - Virtual Private Network

SHA - Secure Hash Algorithm

MD5 - Message Direct 5

DoS - Denial-of-Service

DDoS - Distributed Denial-of-Service

2FA - Two-factor authentication

RTO - Recovery Time Objective

IPS- Intrusion Prevention System

CPTED - Crime Prevention Through Environmental Design

SNMP - Simple Network Management Protocol

QoS - Quality-of-Service

DHCP - Dynamic Host Configuration Protocol

GDPR - General Data Protection Regulation

PIPEDA - Personal Information Protection and Electronic Documents Act

NDB - Notifiable Data Breach

CCPA - California Consumer Privacy Act

List of figures

List of Tables

TABLE OF CONTENTS

Activity 1

1.1 Organization security procedure with CIA Triad concept

1.1.1 What is CIA Triad

Information security refers to the methods and techniques used by corporations to protect their information. This also includes policy settings that prevent unauthorized users from accessing company or personal information. Information security protects sensitive data from unauthorized access, modification, surveillance as well as destruction. Information security is concerned with protecting sensitive information such as customer account information, financial information, and intellectual property. This is where CIA triad comes in.

The CIA triad is a well-known information security concept that can help an organization's efforts and policies to keep its information secure. CIA initials stands for Confidentiality, Integrity, and Availability. And these are the three core concepts of information security. Every aspect of the information security program must contain at least one of these concepts.

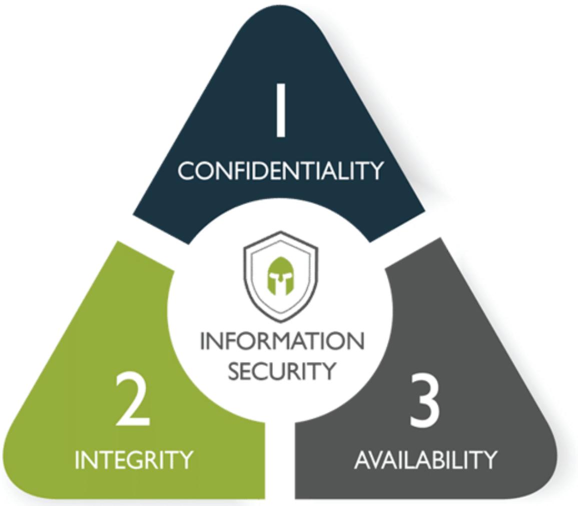


Figure 1. 1 CIA triad with its 3 core concepts

1.1.2 History of CIA Triad

The CIA triad is a concept that evolved over time and has no single inventor. Confidentiality may have been first presented in a study by the United States Air Force as early as 1976. Similarly, David Clark and David Wilson investigated the idea of integrity in their 1987 study "A Comparison of Commercial and Military Computer Security Policies." Despite the fact that finding an initial source is more difficult, the concept of availability became more widely accepted one year later, in 1988. People began to refer to the three principles as the CIA triad by 1998.

1.1.3 Three core concepts of CIA Triad

1) Confidentiality :-

The purpose of the confidentiality principle is to keep personal information private and only make it public and accessible to those who need it to carry out their organizational functions. Only authorized users have access to sensitive or classified information, according to confidentiality. Unauthorized individuals should not have access to data exchanged across the network.

The attacker may attempt to acquire data using various online tools in order to obtain access to personal information. One of the most effective ways to avoid this is to encrypt the data, so that even if an attacker has access to it, he will be unable to decrypt it. A VPN tunnel is another approach to keep data secure. VPN stands for Virtual Private Network, and it improves in the safe transmission of data over a network.

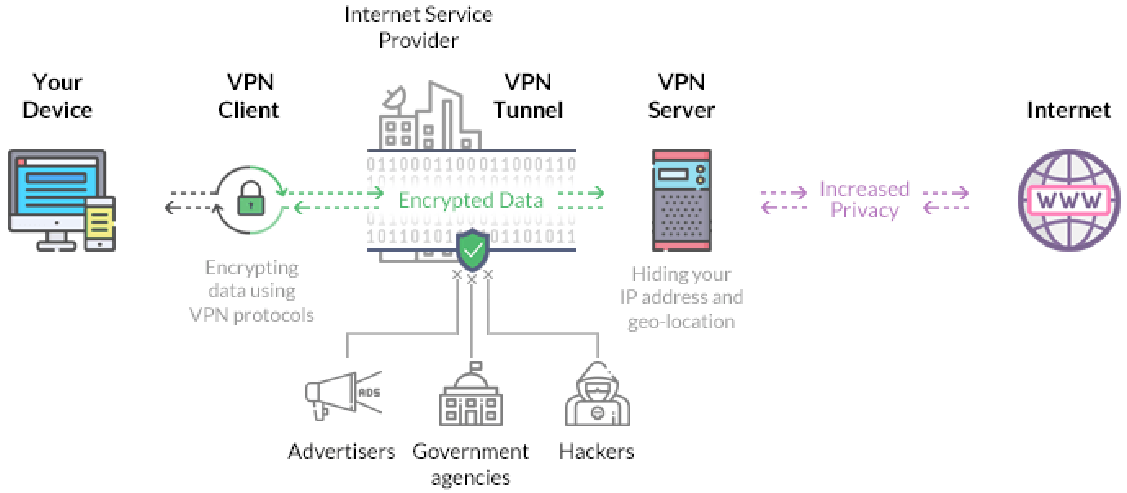


Figure 1. 2 Confidentiality concept figure

2) Integrity :-

The purpose of integrity is to ensure that the data hasn't been modified with in any way. Integrity includes protection against unauthorized data changes (additions, deletions, revisions, and so on). The integrity principle ensures that data is accurate and trustworthy, and that it has not been tampered with in any way, whether accidentally or intentionally.

A hash function is used to determine whether or not data has been modified. A hash function is a mathematical algorithm that turns an input value into a numerical value that has been compressed. There are two common types of hash function. They are SHA (Secure Hash Algorithm) and MD5(Message Direct 5). If we're using SHA-1, SHA is 160-bit hash. And MD5 is 128-bit hash. Other SHA techniques that could be used are SHA-0, SHA-2, and SHA-3.

Assume that Host 'A' intends to communicate data to Host 'B' while maintaining data integrity. A hash function is applied to the data to generate an arbitrary hash value H1 that is then connected to it. When Host 'B' gets the message, the same hash function is applied to the data, giving the hash value H2. If H1 = H2, the integrity of the data has been retained, and the contents have not been modified.

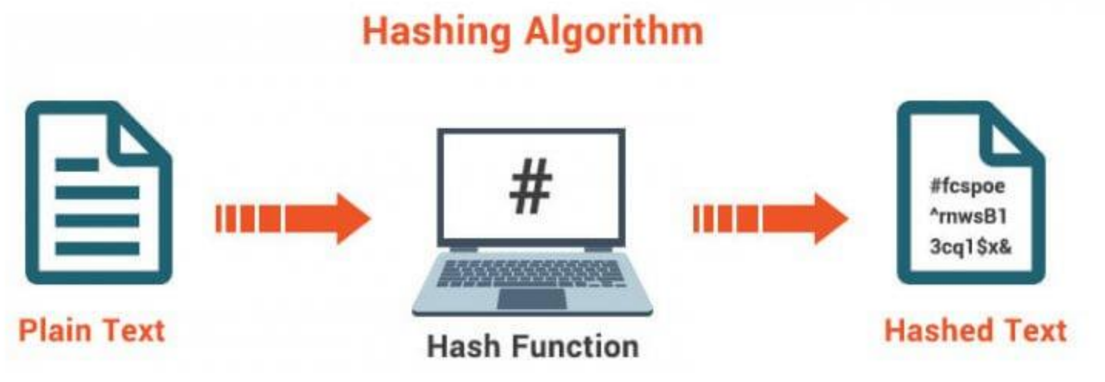


Figure 1. 3 How hashing helps to maintaining integrity concept figure

3) Availability :-

Availability refers to a system's ability to develop software systems and data that are totally accessible when a consumer requests it. This simply means that the network should be accessible to its users at all times. Hence, availability applies to both systems and to data. The purpose of availability is to create technology infrastructure, applications, and data that are accessible when they are needed for a business operation.

To fulfill this purpose the network administrator should maintain hardware, schedule routine upgrades, have a fail-over plan, and avoid bottlenecks in the network to ensure availability. Attacks such as DoS (Denial-of-Service) or DDoS(Distributed Denial-of-Service) can make a network unusable as the network's resources are depleted. Companies and users who rely on the network as a business tool might feel a significant impact. As a result, appropriate precautions should be taken to avoid such attacks.

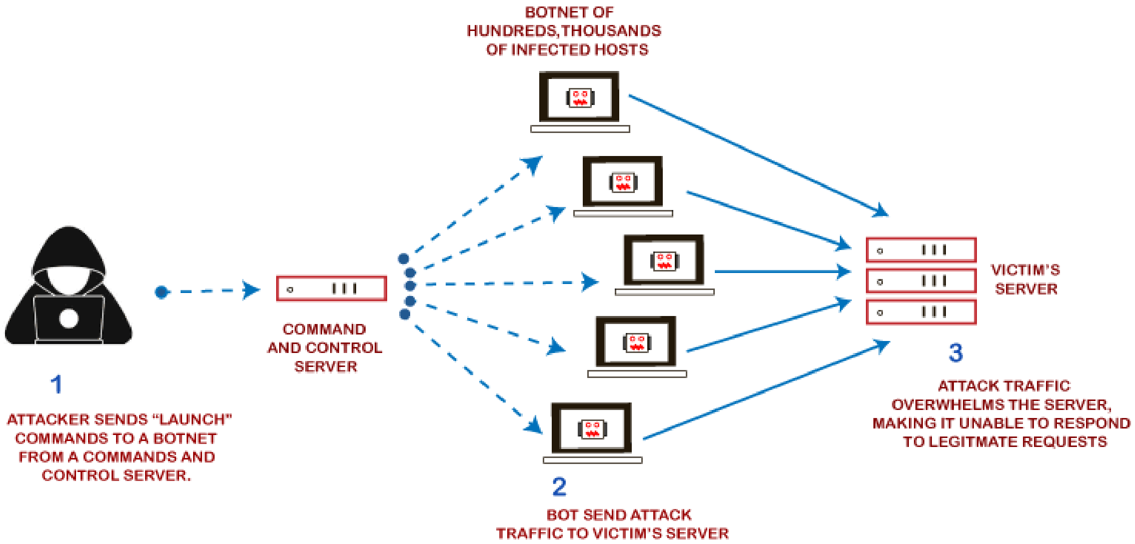

BOTNET OF
HUNDREDS,THOUSANDS
OF INFECTED HOSTS
1
ATTACKER SENDS "LAUNCH" COMMANDS TO A BOTNET FROM A COMMANDS AND CONTROL SERVER.
COMMAND AND CONTROL SERVER
2
BOT SEND ATTACK TRAFFIC TO VICTIM'S SERVER
VICTIM'S SERVER
3
ATTACK TRAFFIC OVERWHELMS THE SERVER, MAKING IT UNABLE TO RESPOND TO LEGITMATE REQUESTS

Figure 1. 4 How DoS attacks makes unavailable networks concept figure

1.2 How CIA Triad could be utilized to IRONONE Cyber in order to improve the organizational security

As I explained above with each letter signifying a core principle in Information Security. Within information security, the three key principles are confidentiality, integrity, and availability. Hence, The relevance of the CIA triad security model speaks for itself. The CIA triad is essential in keeping data safe and secure in the face of expanding cyberthreats. When a security incident occurs, such as data theft or a security breach, it is determined that an organization failed to implement one or more of these concepts properly.

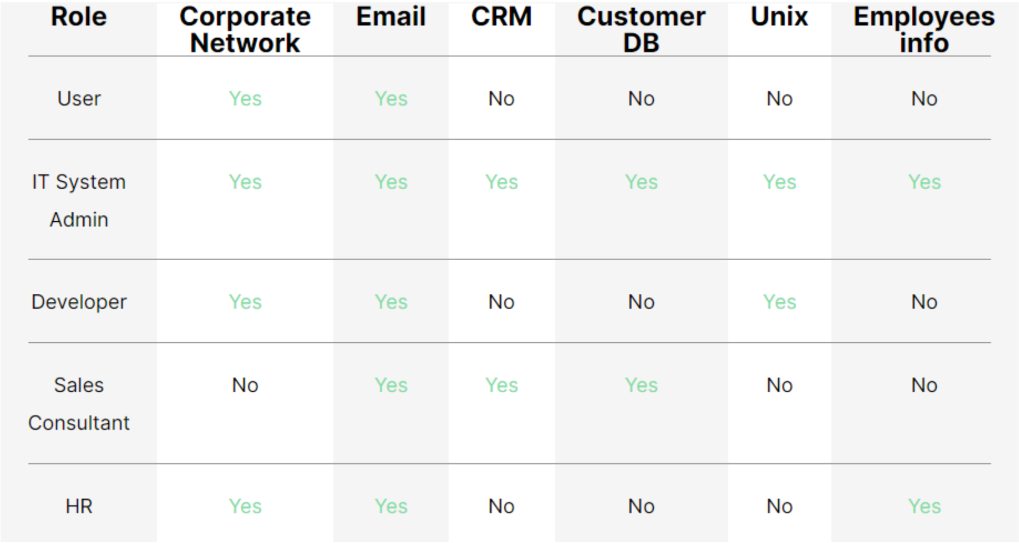
Hence, Integrating the three concepts of the CIA triad as one interconnected system, rather than three separate concepts, this can help IRONONE Cyber to deliver more secured system within Lockhead Aerospace organization. IRONONE Cyber can concern to installing these three concepts in the Lockhead Aerospace framework then it can assist in the creating this organizational security policies without having no issues. When evaluating needs of security implications, the triad answering how much security is being provided in those three key areas of this organization. Hence, it's clear the CIA triad is important for information security, and it helps this organization stay compliant with complicated regulations while also ensuring business continuity.

1.3 How to use CIA Triad’s Confidentiality to improve the security

1.3.1 Role-Based Access Control (RBAC)

RBAC (role-based access control), often known as role-based security, is a system access control mechanism. It consists of granting permissions and privileges to allow authorized users access. Role-based access control is used by most large firms to give their employees different levels of access depending on their positions and responsibilities. Hence this can be assigned to Lockhead Aerospace framework too.

This safeguards sensitive information and ensures that employees only have access to the information and activities they require to complete their jobs. Every person in an organization is given a role-based access control role. The role defines which permissions are granted to the user by the system. Some employees may be allowed to create and change files, while others may simply be allowed to view them.



Role	Corporate Network	Email	CRM	Customer DB	Unix	Employees info
User	Yes	Yes	No	No	No	No
IT System Admin	Yes	Yes	Yes	Yes	Yes	Yes
Developer	Yes	Yes	No	No	Yes	No
Sales Consultant	No	Yes	Yes	Yes	No	No
HR	Yes	Yes	No	No	No	Yes

Figure 1. 5 Role-Based Access Control sample table

1.3.2 Data Encryption

Data encryption is the process of transforming readable data (plaintext) into an unreadable, encoded format (ciphertext). Data that has been encrypted can only be viewed or processed after it has been decrypted with the use of a decryption key or password. The decryption key should only be accessible to the data sender and receiver. Most security solutions require data encryption to prevent hackers from gaining access to critical information. However, encryption should not be the main security method.

Techniques and Technologies of Encryption

Column level encryption :- Column level encryption encrypts individual data columns within a database. Each column has its own encryption key, which provides flexibility and security.

Field-level encryption :- Encrypting data in specific data fields is known as field-level encryption. Sensitive fields can be marked by creators so that data entered by users in certain fields is encrypted. Social security numbers, credit card details, and bank account details are examples that can use Field-level encryption.

Transparent data encryption :- Transparent data encryption assists in the encryption of a database as a whole. The database's encryption is transparent to the apps that use it. The database's backups are additionally encrypted, preventing data loss in the event that backup media is stolen or compromised.

Hashing :- Hashing is the process of converting a long string of characters into a shorter, fixed-length key or value that closely resembles the original. In password systems, hashing is broadly utilized. A hash is created when a person creates a password for the first time. When the user returns to the site, their password is compared to the unique hash to see if it is correct.

Symmetric key encryption :- A private key is applied to data in symmetric key encryption, modifying it such that it cannot be read without being decoded. If the user or application provides the key, data is encrypted when saved and decrypted when retrieved. Because the key must be sent from sender to recipient, symmetric encryption is considered inferior to asymmetric encryption.

Asymmetric encryption :- Two encryption keys are used in asymmetric encryption: private and public. A public key is one-of-a-kind and may be retrieved by anyone. A private key is a secret key that only one person has access to. In most circumstances, the encryption key is the public key, while the decryption key is the private key.

1.3.3 Passwords

Passwords are an essential component of data and network security. Passwords secure user accounts, but a poorly designed password could put the entire network at danger if it is compromised. As a result, a company should take the necessary precautions to ensuring that strong, secure passwords are created and kept safe at all times. Passwords ensure that only those who are permitted have access to computer systems. Passwords also assist in determining who is responsible for all transactions and other changes to system resources, such as information.

To access any shared computer information system, users must be verified as valid users by entering a valid password. Each user is responsible for selecting, keeping secure, and updating passwords that are necessary for identification. A good password is simple to remember but difficult for others to guess.

1.3.4 Two-factor authentication

Two-factor authentication can protect a number of online checkpoints, including administrator access to entire websites and applications and remote access to corporate - wide web applications,

Two-factor authentication can help with security in three ways:

1) After a breach, two-factor authentication helps to reduce vulnerability. Due to the required second form of authentication, even if one account is compromised, all others are safe.
2) Some 2FA (two-factor authentication) types tell users ahead of time if suspicious activity is detected, such as an attempt to get into an account.
3) User data is less likely to be compromised in the long run. Traditional credentials can be misplaced, stolen, forgotten, or hacked. But 2FA relies on something that can only be presented by an authorized user.

1.3.5 Biometric Verification

Biometric authentication is a type of security that depends on an individual's unique biological traits to verify that he is who he claims to be. Biometric authentication technology matches biometric information captured with data in a database that has been verified as valid. Biometric Data can be obtained and screened using the following methods.

- scanners for fingerprints
- Recognition of the retina and iris
- voice recognition
- recognition of faces
- Detecting aliveness

1.4 How to use CIA Triad's Integrity to improve the security

1.4.1 Data validation

Data validation, commonly referred to as input validation, is a way of verifying that incoming data is free from errors before it is processed. To verify that data entering a system is relevant, correct, and secure, data validation uses one or more checks, procedures, and rules. It's crucial to ensure that the data processes aren't tampered with. Before the user validates the data, it is critical to identify the standards and essential attributes that are significant to the organization. The following are some of the best input validation techniques.

- Before receiving any input, validate it on the server.
- Making use of a whitelist. Whitelist validation involves specifying precisely what is allowed and not authorized. Regular expressions are an excellent technique for defining an application's whitelist.
- During input validation, identify special characters and escape them consistently.
- Set the minimum and maximum lengths for the input data.

1.4.2 Remove Duplicate Data

Sensitive data from a secure database might easily find on a document, spreadsheet, email, or shared folders, where it can be accessed by personnel without proper access. Cleaning up stray data and removing duplicates is a great thing. Tools can help small businesses without a dedicated team clear up duplicate files on a hard disk or in the cloud. The following are some of the best tools that can clean up duplicate files on a hard drive or cloud.

- Clone Files Checker
- Duplicate Images Finder
- Easy Duplicate Finder
- Duplicate Cleaner

- CCleaner

1.4.3 Back up Data

Data backup is a copy or archive of essential information kept on personal devices, such as a computer, phone, or tablet, that is used to restore that original data in the case of a data loss. Hard drive malfunctions, ransomware attacks, and even human mistakes or physical theft can all result in data loss. Whatever the disaster, a data backup could provide the relief user need to restore the data on the devices. It's usually kept in a safe, off-site place, such as the cloud, away from the originating device.

Data backups are an important element of the process, in addition to removing duplicates to maintain data protection. Backups are essential and go a long way toward preventing irreversible loss of data. We should back up important data and information as often as possible. When it comes to ransomware assaults, it's important to remember that backups are essential. Just make sure our backups aren't encrypted as well.

1.4.4 Access Controls

Access control is a crucial part of data security since it determines who has access to and uses organization data and resources. Access control policies ensure that users are who they say they are and have proper access to company data through authentication and permission. Physical access to campuses, buildings, rooms, and datacenters can also be restricted using access control.

Individuals with unauthorized access and malicious intent within an organization might cause serious data damage. worse case is an outsider can pretend to be an insider. A very successful access control system is establishing a minimal privilege format that is accessible only to those that require data access. Most of times physical access to the server is often neglected. The most important servers should be isolated and anchored to the floor or wall. Only those who need access should have an access key, ensuring that the server keys are retained safe.

1.4.5 Keep an Audit Trail

Audit trails is a procedure of recording of a series of events and actions in chronological order. Systems and application processes can both have audit trails. The audit trails keep track of how systems work as well as what users do while they're using them. When audit trails are combined with the right tools and procedures, they can discover security breaches. They can detect whether sensitive data has been tampered with, as well as system performance issues and application weaknesses.

It's essential to be able to track out the source of a data breach if data integrity is to be maintained. An audit trail, often known as a breadcrumb trail, provides an organization with the information it needs to trace the root of an issue. An audit trail usually includes the following.

- It is necessary to generate audit trails automatically.
- The audit trail should not be accessible to users, nor should they be able to alter it.
- Every action is tracked and recorded, including create, delete, read, and edit.
- Every event is also associated to the user, allowing them to see who has accessed the information.
- Every event is time stamped so we can see when it happened.

1.5 How to use CIA Triad's Availability to improve the security

1.5.1 Data Redundancy

The most fundamental step we can take to improve data availability is to make sure our data is redundant, or that we have numerous data sources available. That way, if one of the disks, servers, or databases hosting our data crashes, the availability of our data will not be harmed.

The difficulty with redundancy is finding the correct balance of redundancy and cost-effectiveness. The number of copies of a database or data server that can operate at the same time is limited in a world where finances are a concern. For each data source, we can make an informed decision about how much redundancy to apply. It can be done by analyzing data such as how frequently a certain server or database malfunctions, as well as determining the importance of various data workloads.

1.5.2 Automate Failover

Data redundancy is good, but data redundancy combined automated failover is much better. That's because, as the name implies, automated failover means that if a component of our system fails, a backup component takes over automatically. Automated failover reduces or eliminates data availability disturbance by reducing the requirement for a human engineer to detect a problem and switch to a backup system.

Automated failover can be configured with a number of monitoring and management tools for virtual servers and databases. System designers build failover capability in servers, backend database support, and networks that require constant availability and excellent reliability.

1.5.3 Avoid single points of failure

Another straightforward action we can take to improve data availability is to avoid single points of failure, which are infrastructure components or applications that can make our data unavailable if they fail. Although the concept is similar to that of redundancy mentioned before, there are several differences between redundancy and reducing single points of failure.

For example, even if we have a redundant storage system consisting of numerous servers and disks, we are still at risk of them being unavailable if the network router on which they depend malfunctions. Our router would be your single point of failure in that situation. By ensuring that not all data goes through a single router, a high availability structure eliminates this risk.

1.5.4 Keeping Software-Defined infrastructure

Data availability is supported by software-defined infrastructure and storage. That's because data storage infrastructure and file systems are easier to move around and scale when they're designed in software rather than physically connected with the hardware that supports them.

Software-defined environments can be as simple as a virtual server and virtual disks, which provide storage that is independent of any particular hardware. There are other more sophisticated approaches to software-defined infrastructure, such as utilizing GlusterFS or Ceph as a file system. However, taking use of software-defined infrastructure and storage to enhance the data availability effectively. Obviously, not every form of data workload can be transferred to a software-defined environment. Furthermore, certain software-defined environments are more complex.

1.5.5 Establish and stick to Recovery Time Objective (RTO)

The period of time organization can continue to run if data availability is disrupted is referred to as the Recovery Time Objective. Depending on the business, the amount of data they collect, and other considerations, they may be able to function for days without data, or they may only be able to function for an hour before suffering massive commercial impact. If the business is a chain of coffee shops, restoring data immediately may not be as important. retrieving data quickly could be crucial if it is a bank and it is dependent on digital data for nearly all of their operations.

We don't want to wait for a data interruption to see how long our business can operate without its data. We must ensure that we can recover from a disaster within the timeframe indicated by our RTO in order for RTO to be useful.

1.6 Vulnerability

1.6.1 What is Vulnerability

A vulnerability is a recognized weakness in an asset (resource) that one or more attackers can exploit. To put it another way, it's a well-known problem that enables an attack to proceed. For instance, if we forgot to disable a team member's access to external accounts, alter logins, or wipe their names from company credit cards after they resign, we leave our organization vulnerable to both intentional and unintentional threats.

On the other hand, the majority of vulnerabilities are targeted by automated attackers rather by humans on the other side of the network. Vulnerability testing is necessary for keeping the security of our networks. With identifying weaker points of a system, we can build a strategy for quick response.

As a security analyst, I should be aware that small & mid organizations are more susceptible to cyber-attacks. Because few businesses can afford a full-fledged IT/security department, security processes are less likely to be implemented. Because few businesses can afford a separate IT/security department, making it more vulnerable to attackers. In order to detect and respond to all risks, organizations need be aware of their threats and vulnerabilities.

1.6.2 Types of security Vulnerabilities that would affect the company

System misconfigurations :-

Network assets with vulnerable configurations or different security policies cause system misconfigurations. For system misconfigurations a popular tactic cybercriminals use is to probing networks and gaps that can be attacked. Because the possibility of network misconfigurations increases as more businesses use digital solutions. It's essential to cooperate with experienced security specialists when adopting new technology.

Out of date or unpatched software :-

Malicious actors might use unpatched vulnerabilities to launch attacks and steal sensitive information. Cyber adversaries will scan networks for unpatched systems they may compromise, similar to how system misconfigurations are exploited. To minimize this risk, develop a patch management schedule that ensures all new system patches are applied as soon as they are released.

Missing or weak authorization credentials :-

Attempting to force their way into a network by assuming employee credentials is a typical strategy used by attackers. Employees should be trained on security best practices so that their login credentials are not easily exploited to acquire network access.

Malicious insider threats :-

Employees having access to critical systems can provide information that allows attackers to enter a network, whether unintentionally or maliciously. Internal threats are hard to detect because all acts taken by employees will seem to genuine. To prevent these threats, we can consider to investing in network access control solutions and segment our network based on employee seniority and expertise.

Poor data encryption :-

Attackers can eavesdrop communication between systems on networks that lack or have insufficient encryption, resulting in a breach. Cyber attackers can steal essential information and insert false information onto a server when weakly or unencrypted communication is disrupted. This can compromise a company's cybersecurity ongoing effectiveness and result in large costs from government regulators.

Zero-day vulnerabilities :-

Zero-day threats are software flaws that are known to the malicious user and has yet to be discovered by an organization. Because the vulnerability has not yet been reported to the system vendor, there is no known fix. These are especially troublesome because there is no way to protect against them until the attack is completed. To reduce the risk of a zero-day attack, it's critical to stay alert and constantly monitor company systems for vulnerabilities.

1.6.3 Vulnerability Management

The process of identifying, classifying, minimizing, and resolving system vulnerabilities is known as vulnerability management. To support our organization to implement a vulnerability management program, we can follow 3 key steps.

1. Identify vulnerabilities
2. Evaluate vulnerabilities
3. Address vulnerabilities

1) Identify vulnerabilities

The procedure of identifying and documenting vulnerable gaps in network operations is known as vulnerability identification. This is often accomplished through the use of vulnerability scanners, which check network systems for misconfigurations, inappropriate file system structures, and other issues on a regular basis.

The results of the scanners are then compared to databases of known security intelligence. It is vital that the scanner is configured properly and up to date in order to provide reliable search results. It is essential that a test-run be performed during off-peak hours so that we can assess the accuracy of the data and make any improvements.

2) Evaluate vulnerabilities

Soon after the identifying of vulnerabilities, a cybersecurity vulnerability assessment is being used to evaluate the risk they cause to business. We can assign risk levels to detected vulnerabilities using vulnerability assessments, allowing us to prioritize corrective measures. Effective assessments can help with compliance by ensuring that vulnerabilities are fixed before they are attacked.

3) Address vulnerabilities

Once the risk level of a vulnerability has been evaluated, the vulnerability must be addressed. The following are the several approaches of dealing with a vulnerability.

- Remediation :- Vulnerability remediation includes repairing or fixing a vulnerability completely. Because it reduces danger, this is the preferable method of treating vulnerabilities.
- Mitigation :- Mitigation is the process of reducing the chances of a vulnerability being exploited. Vulnerability mitigation is frequently used to buy time before a suitable patch has become released.
- Acceptance :- When a company determines that a vulnerability creates a low risk, it is acceptable to take no action to resolve it. This is also acceptable when the expense of correcting the vulnerability is higher than the cost of exploiting it.

1.7 Threat

1.7.1 What is Threat

The potential circumstance in which an attacker exploits the vulnerability is referred to as a threat. The threat will almost always include an exploit, as this is a frequent approach for hackers to get their hands on sensitive information. After determining which flaws will produce the most profit, a hacker may deploy many attacks at the same time. While nothing tragic has yet occurred, it can provide insight to a security department as to whether or not specific security measures should be implemented.

Professional spies, computer hackers, terror organizations, hostile nation-states, criminal groups, solo hackers, and dissatisfied workers are all potential threats. These malicious attackers can steal information or get access to a person's financial accounts by using sensitive data. Cyber security professionals are important for keeping private information safe, among other possibly harmful behaviors.

1.7.2 Main types of network threats that would affect the company

- External threats :- Threats from outside organizations or persons attempting to get access to a network are known as external threats.
- Internal threats :- Malicious insiders, such as dissatisfied or poorly screened personnel who work for someone else, provide an internal threat. These are extremely common. According to Forrester, insiders such as employees and third-party partners were engaged in 46 percent of breaches in 2019.
- Structured threats :- Attacks carried out in an organized way by attackers who know what they're doing and have a specific purpose in mind. For example, state-sponsored attacks come within this category.
- Unstructured attacks :- Attacks that are disorganized, often by amateurs with no clear purpose in mind.

1.7.3 Difference between a Threat and a Vulnerability

If attackers throw rocks at a wall, a vulnerability is a weak spot in the wall, a place where they can smash a window or take out a loose rock and gain access. And the attackers are the threat to the wall. Simply said, vulnerabilities are weaknesses in the systems that attackers can take advantage of. The threat is a harmful act intended on stealing or causing damage to a network or system.

Threat and vulnerability both terms are referred to danger, damage, and harm. They both relate to a security risk. As we saw a threat is someone or something that has the potential to create problems or harm. Vulnerability is the characteristic or state of being exposed to the risk of being attacked or damaged in some way, whether physically or emotionally. The primary distinction between threat and vulnerability is this.

Table 1. 1 Difference between a Threat and a Vulnerability

Threat	Vulnerability
This could be a person or a thing which likely cause damage or danger.	This refers to being open to attack or damage.
This is a danger posed by someone else.	This is a flaw or a weakness.
Threat can be identified but cannot be controlled.	Vulnerability can be identified and can be controlled.

1.7.4 How to identify threats and vulnerabilities

- Watch own network :- The most crucial step in identifying threats and vulnerabilities is to ensure that they are visible. We want to be able to look at our defenses through the perspective of an attacker, identifying network flaws and vulnerabilities that are most capable of damaging the organization.

- Take advantage of threat intelligence :- We need to figure out what kinds of attacks are being carried out and which hazards the organization might face. We can safeguard our organization from dangers before they happen by knowing the possible threats.

- Penetration test :- We need to figure out where our defenses give way under pressure and which employees are most likely to click a malicious link in an anonymous email. We won't know unless you put your defenses to the test, and penetration testing is the most effective way to do so.

- Manage permissions :- By segmenting our system and controlling permissions, we can ensure that not every employee has access to every aspect of it. We can manage who sees what and keep our network safe from data breaches and harmful insiders.

- By using a firewall :- Internally and externally, there's no reason not to utilize firewalls. Unauthorized users are prevented from connecting to the network via firewalls. They also keep track of traffic across the entire network.

- Constantly monitor the network :- In order to be effective, security must be continually monitored. Once we've established our controls, make sure they're checked and updated on a regular basis to catch any new vulnerabilities or threats to our network.

1.8 Risk

1.8.1 What is Risk

Risk is the probability of being exposed, losing vital assets and sensitive information, or suffering reputational damage as a result of a network attack or breach. Risk is the probability of being exposed, losing vital assets and sensitive information, or suffering reputational damage as a result of a network attack or breach. Security must remain a top priority across industries, and organizations should seek to create a security risk management strategy to defend against any kind of threats. Followings are examples of risk.

- Financial losses.
- Privacy invasion.
- Damage to reputation.
- Legal implications.
- Even death is a possibility.

1.8.2 3 main components of Risk

Threat, vulnerability, and consequence are the three components that typically describe cybersecurity risk.

- Threat :- Social engineering attacks, DDoS attacks, and advanced persistent threats are just a few examples of threats. Threat operators are often linked to nation-states, insiders, and criminal organizations, and are driven by monetary gain or political ambitions.
- Vulnerability :- A vulnerability is a flaw, weakness, or error in cybersecurity that can be exploited by attackers to gain unauthorized access. Vulnerabilities can be exploited in a number of different ways, which is why vulnerability assessment is so important for remaining one step ahead of cybercriminals.
- Consequence :- The actual harm or losses that happen as a result of a network interruption are referred to as the consequence. In most cases, when a company works to solve the problem, it will suffer both direct and indirect consequences. The effects of an attack may have an influence on an organization's finances, operations, reputation, and regulatory compliance status, depending on the nature of the attack.

1.8.3 Types of security Risks that would affect the company

Third-party vendor risk :-

Third- and fourth-party vendors help organizations to outsource specific company functions, reducing costs and improving operational efficiency. Inside access to an organization's most sensitive information, including customers' personal information, is common among these vendors. It is important for organizations to have complete and ongoing awareness of all entities in their network. Third-party risk management enables firms to take advantage of vendor benefits while maintaining security.

Employees and contractors as insider threats :-

Insiders with network access, such as employees and contractors, play a key role in sustaining an organization's cybersecurity posture, as said before. As a result, cybersecurity education and social engineering training are essential. Insiders should be able to recognize various risks and hazards and know what to do after they've been identified. Insiders can take proactive efforts to limit risk after they have a thorough awareness of the numerous dangers, they should be aware of.

A Zero Trust Security approach should be implemented by organizations. This is a security strategy that is based on the idea that access should be granted based on the job function of each user or device. This reduces the number of opportunities for insiders to take advantage of their access controls unintentionally or intentionally.

Lacking compliance measures :-

More regulatory compliance standards, such as PCI, HIPAA, and GDPR, are being implemented as data privacy becomes a growing issue for customers. While these policies are necessary to evaluate and implement, it's necessary to keep in mind that complying to them does not guarantee that an organization is safe from attackers.

Conventional point-and-time assessments are no longer sufficient as institutions can slip in and out of the audit. An effective cybersecurity approach must include the ability to consistently monitor the whole network environment for noncompliance.

Intellectual property and sensitive information that has been improperly secured :-

Companies are collecting more client data than ever before in today's digital age. Such sensitive data enables businesses to improve consumer experiences and guide future decisions, but it also exposes them to significant danger, particularly if key information or intellectual property is not adequately protected. Organizations should evaluate their industry's data protection standards to ensure that appropriate security measures are in place.

1.8.4 Key differences between a Vulnerability, Threat, and a Risk

Table 1. 2 Key differences between a Vulnerability, Threat, and a Risk

	Vulnerability	Threat	Risk
Definition	Vulnerabilities in a security program are flaws or gaps that can be exploited by threats to gain unauthorized access to an asset.	Threat is defined as anything that can take advantage of a vulnerability, either intentionally or unintentionally, to do harm or destroy an asset.	Risk refers to the possibility of an asset being lost, damaged, or destroyed as a result of a threat exploiting a vulnerability.
Learning Key	A vulnerability is a gap or weakness in a security system's defenses.	A threat is what a security system is attempting to defend against.	The intersection between threat and vulnerability is risk.
Examples	Employee IDs that have been dismissed are not completely removed from the system.	Connecting to the company's network and gaining access to confidential information	Unauthorized exposure of confidential business in customer information.
	Improperly maintained fire-fighting equipment	Fire	Lead to loss of life, data, and infrastructure.

Hence, Risk can also be defined as following.

Risk = Threat x Vulnerability

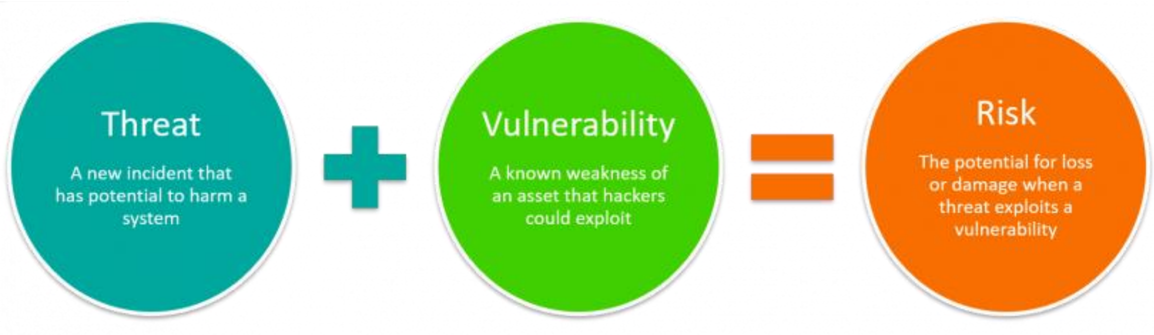

Threat
A new incident that has potential to harm a system
Vulnerability
A known weakness of an asset that hackers could exploit
Risk
The potential for loss or damage when a threat exploits a vulnerability

Figure 1. 6 The intersection between threat and vulnerability is risk

1.9 Countermeasure

1.9.1 What is Countermeasure

Security countermeasures are safeguards that are used to secure the confidentiality, integrity, and availability of data and information systems. Adding extra security measures, eliminating unnecessary services, and restricting access can all help to improve overall security. Some examples for countermeasure are as following.

- IPS (Intrusion Prevention System)
- Security awareness training
- Security Guard
- Firewall
- Anti-Virus

The purpose of countermeasures is to prevent or reduce the loss of unavailability caused by attacks exploiting their underlying vulnerability. There are 3 types of countermeasures. They are as following. The following 3 types of countermeasures must be implemented together to establish a layered and efficient security system. Hence, against all threat situations, no single security countermeasure is sufficient.

- Hi-Tech
- Lo-Tech
- No-Tech

As a countermeasure we can use good password protection for access to a computer system as well as the BIOS of the machine are also useful countermeasures against cyber-criminals with physical access to the machine. Another option is to utilize a bootable bastion host that runs a web browser in a known safe and secure environment.

1.9.2 Types of security countermeasures

Hi-Tech Systems :-

All electronic systems are classified as hi-tech systems. Alert system Controllers, Camera Systems, Communications Systems, Integrated Security Systems, Specialized Detection Systems, and Computerized Systems are examples of these types of systems. Hi-tech systems are used to automate repetitive tasks, monitor continually without error, and report to and assist security personnel in communication and coordination.

Hi-Tech systems are increasingly being utilized to handle massive amounts of data that humans could never handle cost-effectively. Examples for Hi-Tech systems are as following.

- Smart surveillance data analysis that analyzes a video scene for unwanted behaviors
- Multiple credential techniques are used in integrated systems. Face recognition and a card reader are two examples.
- Weapons screening that is automated
- Package X-ray screening to allow automatic access to a high-security area.

Since security programs are increasingly focusing on high-tech systems, they should be the last element considered. An effective Security Program is built on a foundation of low-tech and no-tech elements. But Hi-Tech elements on the other hand, enhance the capabilities of Lo-Tech and No-Tech elements.

Lo-Tech Systems :-

Physical security features known as Lo-Tech are among the most cost-effective security measures that may be used by any firm. Some examples of low-tech Lo-Tech Systems are as following.

- Barriers and locks.
- Fencing and lighting.
- Safety signs.
- Other Physical Obstructions.
- Crime Prevention Through Environmental Design (CPTED) measures.

Lo-Tech elements are efficient because, in most circumstances, they are a one-time investment that continues to perform without fail on a daily basis. By using Lo-Tech elements people are directed to controlled access points, Visitors have been made aware of security policies, Unauthorized people are not allowed in and with unexpected barriers intruders have been stopped.

No-Tech Systems :-

Security elements with no technology are known as no-tech elements. Because of their active nature, No-Tech elements are among the most effective. Every encounter with a Security Officer leaves an unforgettable impression. But the same impression cannot be taken from card reader contact. But users are more motivated to criticize or complain to Security Officers than they are to criticize or complain about technology. Some examples of low-tech No-Tech Systems are as following.

- A thorough risk assessment.
- Procedures and policies.
- Programs for Security Guards
- Security Training and Awareness
- Interaction with law enforcement.
- Investigations.
- Dogs and other non-technological projects

1.9.3 Security Countermeasures Layering

Layering indicates that an asset is secured from the outside in by many layers of countermeasures. A threat actor must overcome a number of security aspects in order to get access to a valuable asset such as the Information Technology Server Room. For certain types of security countermeasures, the more layers there are, the less likely it is that a threat action would succeed.

Mixed-technology approaches should be used by layers. The threat actor first encounters the outside wall, next the lights, then perimeter sensor systems, then camera systems, then entrance detection, then more camera systems, then motion alarm systems, then access control and finally the Server Room controls. Likewise, there should be Mixed-countermeasure types approaches to be it more secure system. If the threat actor encountered all of these countermeasures on the way out, we must limit the chances of a successful exit and undetected escape for security countermeasures even more.

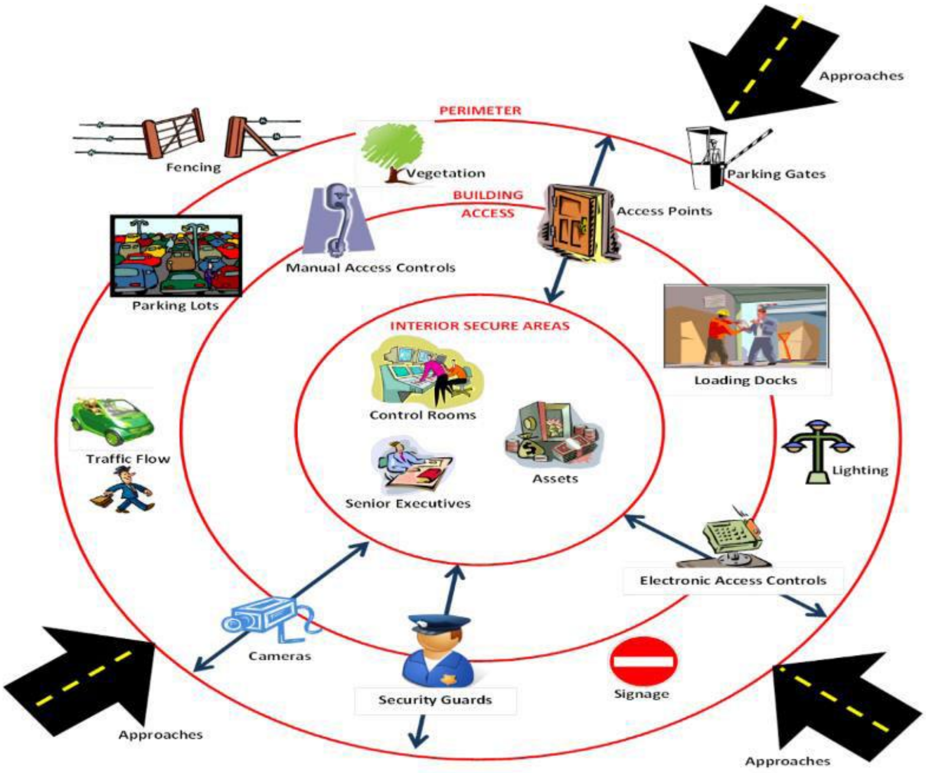


Figure 1. 7 Layers of security countermeasures

1.10 Common types of security Threats with their Countermeasures (Mitigation of IT security risks)

1.10.1 Malware :-

Malware is also known as malicious software. Malware is a file or program that infects, investigates, steals, or performs nearly any action that an attacker desire. Malware is often supplied over a network. And, because malware comes in so many different forms, there are a variety of ways to infect computers. Malware usually has one of the following goals, despite its diverse types and capabilities.

- Allow an attacker to use an infected computer via remote control.
- Send spam to unsuspecting targets from the infected system.
- Examine the local network of the affected user.
- Steal confidential information.

Most Common Types of Malwares with their Countermeasures

1) Virus :-

Viruses are a type of malware that can infect any computer or a system. A virus is a type of malicious software that is attached to a document or file and uses macros to execute its code and spread from one host to another. The virus will remain inactive once downloaded until the file is opened and used. Viruses are created to cause a system's ability to function to be disrupted. Viruses can thus cause significant operational problems and loss of data.

Countermeasures for Virus →

An enterprise-level antivirus solution can assist users defend against viruses by allowing them to secure all devices from a single location while keeping central management and visibility. The user must run complete scans on a regular basis and keep antivirus programs up to date.

Getting a free copy of a game, film, or software that everyone else has to buy for can be tempting. However, downloading a cracked or pirated version of software may put the system or device at risk. It's easy for a cybercriminal to put a virus into a free application because there's no virus prevention integrated into what's being downloaded. There may not even be any free software available, only a virus. When downloading something for free, be careful. Use antivirus protection if users download pirated materials, which is not recommended.

2) Worms :-

Worms are malicious programs that duplicates and quickly spread to any device on a network. Unlike viruses, the worms do not require host programs to spread. Before multiplying and spreading at an exponential rate, a worm infects a system via a downloaded file or a network connection. Worms, like viruses, can cause a device's operations to be severely disrupted and data to be lost.

Types of Worms that can be seen today →

- Internet worms :- An internet worm uses the LAN to jump from one device to another. It infects one computer before spreading to other vulnerable devices linked to the same internet connection.
- Email worms :- An email worm tries to act as an attachment in an email. If the attachment contains more than one file extension, such as ".mp4.exe," we can determine it's a worm, although this isn't always the case. The ILOVEYOU worm is an example of an email worm.
- File-sharing worms :- Anyone may believe they're downloading a media file or a software installer, but it could actually be a computer worm that begins to work as soon as it hits their system.
- Instant messaging (IM) worms :- IM worms, like email worms, disguise themselves as attachments or links shared via instant messaging networks. They may even include creative clickbait headlines such as "This will blow your mind" or "You've won the prize" in order for IM users to accidentally download the worm by clicking on them.

Examples of Worms →

- Morris Worm :- The Morris worm was the very first computer worm to cause harm in the actual life. This worm was accidently produced by a computer science student in 1988, and it crashed many of the 6,000 systems it infected.
- WannaCry/WannaCryptor Worm :- In 2017, the WannaCry worm encrypted Windows users' files and demanded a payment in exchange for them. It was a ransomware-spreading worm.
- ILOVEYOU/Love Bug/Love Letter Worm :- In the year 2000, the ILOVEYOU worm spread through emails disguised as a love letter attachment. Over 10 million machines were affected.
- Nimda Worm :- Nimda was the very first computer worm to alter existing websites so that malicious downloads could be offered. It started spreading in LANs when massive emails were sent out.
- Code Red Worm :- The Code Red worm used infected computers to launch a DDoS (distributed denial of service) attack against the White House in the United States. The White House and its web servers were forced to change IP addresses as a result of the attack.
- Jerusalem/BlackBox worm :- This was a form of computer worm that consumed computer resources. It removed any application that was running on Friday the 13th of any year when it was triggered. It also repeatedly infected .exe files until they became too big for the computer to handle.
- MSBlast/Blaster Worm :- When the Blaster was first activated, it displayed two messages: "I simply want to say LOVE YOU SAN" and "billy gates why do you make this possible? Stop making money and fix your program!!" However, as a side effect, computers were forced to shut down.
- Sobig worm :- From Sobig.A to Sobig.F, there would be various versions of the Sobig worm. It was disseminated as an email attachment with subject lines like "Thank You" and "Re: Details." The worm search for better targets after infecting a machine by sending 20 or more emails to the user's contacts.

Countermeasures for Worms →

Users should avoid using public or unsecured Wi-Fi networks, as they might act as a route for worms to spread. If they must use public Wi-Fi, they should utilize a VPN to protect their network traffic. Because many worms get access through phishing emails. Hence, email education is also essential. If a device on the network is infected, the firewall prevents the worm from spreading to other devices. Hence, an antivirus with a firewall integrated in is perfect against worms.

In order to get access to devices, computer worms may install adware into legitimate websites. An ad that claims user has won something or that the machine has a virus is an example of adware. To avoid software vulnerabilities, keep the operating system and applications up to date. Enable automatic updates if at all possible.

Do not use default passwords for anything, especially in network configuration, because certain worms infect numerous devices using default credentials. For novice users can utilize the password strength test and the password guide to develop better, stronger passwords. Finally, encrypt essential files to safeguard sensitive information on the devices and keep them safe from malware attacks.

3) Trojan Virus :-

A trojan program basically acts as a genuine program, but it is actually malicious. Trojan viruses are viruses that are camouflaged as important applications. However, after the Trojan virus has been downloaded, it can obtain access to sensitive data and change, block, or erase it. This can be extremely damaging to the device's functioning. Trojan viruses, unlike other viruses and worms, are not designed to multiply themselves.

Types of Trojan Virus that can be seen today →

- Backdoor Trojans :- This sort of Trojan allows hackers to remotely access and control a machine.
- Exploit Trojans :- These Trojans inject code onto a machine that is specifically designed to attack a vulnerability in a certain software program.
- Rootkit Trojans :- These Trojans are designed to prevent malware from being discovered once it has infected a system, allowing it to do the most harm possible.
- Banker Trojans :- This type of Trojan is designed to steal personal information used in online banking and other operations.
- DDoS Trojans :- These are Trojans that are programmed to carry out Distributed Denial of Service (DDoS) attacks. This disables a network or machine by flooding it with requests from many sources.

Examples of Trojan Viruses →

- Zeus :- Zbot is another name for this. Zeus is a popular Trojan malware package with a range of variations that may be used to carry out a series of attacks.
- Wirenet :- Wirenet is a password-stealing Trojan that was one of the first to targeting Linux and OSX users, many of whom were moving from Windows due to security problems.
- Mobile banking Trojans :- Webroot has identified a variety of Trojans designed to steal login credentials or replace legitimate apps with malicious ones in mobile banking apps.

Countermeasures for Trojan Virus →

The most straightforward strategy to avoid trojans is to never download or install software from an unknown source. Instead, make sure that staff only download software from trusted developers and app marketplaces that company has approved. Individuals can add an extra layer of security by using security software such as antivirus, anti-malware, and firewalls.

4) Spyware :-

Spyware is malicious software that operates in the background on a computer and sends information to a remote user. Rather from just interfering with a device's functionality, spyware targets sensitive data and can provide remote access to attackers. Spyware is frequently used to steal personal or financial information. A keylogger is a sort of spyware that captures user keystrokes in order to leak passwords and personal information.

Types of Spywares that can be seen today →

Spyware is typically divided into four categories.

- Trojan spyware invades computers with Trojan malware, which then installs the spyware program.
- Adware may track user activities in order to sell the information to marketers or offer misleading malicious advertisements.
- A website can use tracking cookie files to follow user throughout the internet.
- System monitors track everything that happens on a computer, including keystrokes, websites viewed, emails, and more. This is where keyloggers are usually found.

Each type collects data for the author or a third party, which is then used to the attacker's advantage. The less dangerous varieties will just monitor and provide personal information to the attacker, similar to tracking cookies. System monitors and adware are considerably more dangerous, as they can collect data and make changes to the system that expose users to other risks.

Countermeasures for Spyware →

Antivirus software, like other malware, can assist in the detection and removal of spyware. There are several sorts of anti-virus software to choose from, depending on company budget and requirements. Anti-tracking browser extensions can also be used to prevent spyware from following users from one website to the next.

Also, make sure the browser and device are both up to date on a regular basis it good defend against Spyware. Only a recent update may be able to fix a flaw that leaves the device vulnerable to spyware. It is also important to be cautious when downloading files from file-sharing platforms. These downloads are frequently infected with spyware and malware.

Don't click on pop-ups that appear on the screen, no matter how inters looking they are. Users can also use a pop-up blocker to avoid ever having to deal with them. Finally, do not download materials from unknown email addresses. Even better, do not open the emails at all. It is better to remove them.

5) Adware :-

Adware is malicious software that collects data on computer activity in order to serve users with relevant advertising. While adware is not always harmful, it might cause problems for the user's system in rare circumstances. Adware can redirect the user's browser to dangerous websites and possibly contain Trojan horses and spyware. Furthermore, high levels of adware can significantly slow down a user's Computer. Because not all adware is dangerous, it's critical to have protection that checks these programs frequently and effectively.

Examples of Adware →

- Fireball :- The adware was created by a Chinese agency to take control of the browser and convert the user's homepage to a fake search engine called Trotux. The first and most visible sign of a Fireball infection should be this. In the second sign of infection, the user is unable to modify the default search engine or homepage settings. Trotux collects information about the websites that a user visits in order to create a profile of him and send him annoying advertisements while he is browsing.
- DollarRevenue :- Who created DollarRevenue and for what reason is currently unknown. It was developed by DollarRevenue's creators to install a browser toolbar that would track all web searches. Its primary goal was to collect and steal personal information. DollarRevenue is easily identified by its false ad pop-ups. The adware bombards our device with advertising full of errors, grammar mistakes and unregistered brands as soon as we click anywhere on the page.
- Gator :- The alligator icon in the system tray gave Gator its name, but no one knows who made it or why. Gator operated by taking down genuine advertisements from websites and replacing them with its own. Gator became a full-fledged spyware program at one time when it began recording people's browser history and financial details. Gator's popularity peaked with Windows XP, and fortunately, Gator infections in later Windows versions are quite rare.

Countermeasures for Adware →

To begin with, users should always keep an up-to-date antivirus product installed on their computer. Antivirus software is the first line of defense against all forms of computer threats, and it does help to filter out the most of harmful and suspicious applications.

When it comes to avoiding adware and malware attacks in general, user behavior is also essential. This means just downloading and installing programs from reputable websites, such as the software developers' official websites, rather than torrent and file-sharing sites. Users should avoid using key generators or downloading cracked or pirated software. Users are frequently asked to install adware on websites that offer unlicensed online sports or movie streaming, as well as games, movies, music, and other pirated content.

The more people that do things that aren't necessarily lawful, the more likely they are to encounter adware. Users should read the installation prompts carefully while installing genuine freeware apps and uncheck third-party advertising elements if they don't want them. It's best to check the most recent user evaluations before installing browser extensions and add-ons from the official sources.

6) Ransomware :-

Ransomware is a type of malicious software that acquires access to sensitive data on a computer, encrypts it so that the user cannot access it, and then demands a money payment in exchange for the data's release. Ransomware is frequently used in phishing scams. The user downloads the malware by accessing a fake link. The attacker then encrypts data that can only be decrypted with a mathematical key that they know. The data is decrypted once the attacker receives money.

Examples of Ransomware →

- Bad Rabbit :- On infected websites, Bad Rabbit spreads via a fake Adobe Flash update. Users are routed to a payment page demanding 0.05 bitcoins when the ransomware attacks a machine
- Cerber :- Cerber uses a sophisticated phishing effort to target cloud-based Microsoft 365 subscribers, affecting millions of people.
- CryptoLocker :- The first CryptoLocker botnet was shut down in May 2014, but not before extorting roughly $3 million from victims.
- CryptoWall :- Soon after the death of the first CryptoLocker, CryptoWall emerged. CryptoBit, CryptoDefense, CryptoWall 2.0, and CryptoWall 3.0 are some of the variations that have appeared since its first release in early 2014. CryptoWall, like CryptoLocker, is spread by spam or exploit kits.
- Crysis :- Crysis ransomware uses a strong encryption method to encrypt files on fixed, removable, and network drives, making it impossible to crack in a reasonable period. It's usually spread by emails with attachments that have a double-file extension, making the file appear to be non-executable. It can also be camouflaged as a legitimate application installer, in addition to emails.
- Jigsaw :- Jigsaw encrypts files and deletes them one by one until a ransom is paid. After the first hour, the ransomware deletes a single file, then more and more each hour until all remaining files are erased at the 72-hour point.

Countermeasures for Ransomware →

The first step is to never click on any unsafe links. Clicking on links in spam messages or on unfamiliar websites should be avoided. When users click on malicious links, an automated download may begin, potentially infecting the machine.

Then do not respond to a call, text message, or email from an unknown source asking for personal information. Cybercriminals launching a ransomware assault may try to gather personal information ahead of time, which can then be used to customize phishing messages to specific victims. When you have any doubts about the message's authenticity, user can contact the sender directly.

Email attachments can also be used to deliver ransomware to a device. Any attachments that appear to be suspect should be avoided. Pay close attention to the author and double-check that the address is right to ensure that the email is trustworthy. To view attachments, never open them if they ask to run macros. If the attachment is contaminated, opening it will activate a malicious macro that will allow malware to take control of the computer.

Never download software or media files from unknown sites to reduce the chance of installing ransomware. For downloads, stick to sites that have been verified and are trustworthy. The trust seals can be used to identify certain types of websites. Make sure the page visiting uses "https" instead of "http" in the URL bar of the browser. In the URL bar, a shield or lock icon might also signify that the page is secure. Also, be cautious when downloading files to any mobile device. Depending on their device, users can trust the Google Play Store or the Apple App Store.

7) Fileless Malware :-

Fileless malware is a sort of memory-resident malware. It is malware that functions from a victim's computer's memory rather than data on the hard drive, as the name indicates. The software also vanishes when the target Computer is rebooted, making investigations more difficult.

Countermeasures for Fileless Malware →

Organizations must look beyond signature-based solutions to fight against fileless malware attacks.They should concentrate on tools that can detect malicious behavior on the network and practice good cybersecurity hygiene, such as timely patching of publicly disclosed vulnerabilities.

Developers can help protect against fileless malware assaults by including security into their programs from the beginning. Bugs and vulnerabilities will always remain in software, but if security is prioritized throughout the development process, they can be reduced and detected before being exploited by attackers.

Antivirus software struggles to fight against fileless malware since there is no executable file. To combat it, ensure that users only have the rights and privileges they require to perform their tasks. This will make it more difficult for criminals to use fireless malware to steal employee credentials and access sensitive data. Additionally, for those who do not require Windows programs such as PowerShell, disable them.

8) **Malicious Bots :-**

A bot is a computer program that automates a process and does not require human interaction. A computer infected with a malicious bot can distribute the bot to other computers, forming a botnet. This bot-infected network can then be managed and utilized by hackers to launch large-scale attacks, frequently without the device owner being aware of its role in the attack. Bots are capable of large-scale attacks, such as the 2018 distributed denial of service (DDoS) attack that knocked out the internet for the majority of the Eastern United States.

Types of Malicious Bots that can be seen today →

- File-sharing Bots :- The user's query terms is taken by these bots. Consider a well-known film or an album by a well-known performer. They react to the query by saying they have the file and provide a link to download it. The unknowing user clicks on the link, downloads and opens it, and unintentionally infects their machine.
- Spam bots :- These bots send unwanted direct messages, flooding inboxes with spam, and interrupting chats. These bots are used by certain pushy advertisers to target individuals based on demographic data acquired from the user's profile. These bots are usually easy to recognize because they usually provide a link to click on along with an attractive message to encourage people to click.
- Zombie Bots :- This is a computer that has been compromised as part of a botnet, together with hundreds or thousands of other computers. These computers are used to organize large-scale attacks in which all of the zombie computers work together to carry out the botnet owner's commands. These bots are more difficult to spot and harder to kill. Often, victims of this form of infection are unaware that their computers have been infected.

Countermeasures for Malicious Bots →

For beginners, in addition to any existing anti-virus software, consider using a second opinion scanner. Many anti-virus applications are incapable of detecting botnet-related software. Malwarebytes is a well-known example of bot detecting software of this type.

Secondly, keep an eye on the records. Staying proactive and alert to the website will boost the chances of being able to react before any significant damage is done. In recent years, new tools have developed to make this work easier and more user-friendly. These tools allow users to pinpoint any IP that is acting aggressively or abnormally.

One method of controlling bots is to apply tools that help determine whether traffic is coming from a human or a bot. For example, CAPTCHAs can be added to forms to prevent bots from flooding the site with requests. This can assist in identifying and distinguishing between good and bad traffic.

Activity 2

2.1 VPN

2.1.1 What is VPN

VPN (Virtual Private Network) refers to the ability to establish a secure network connection when using public networks. VPNs encrypt the internet traffic and conceal the identity online. This makes it more difficult for third parties to track someone online activities and steal information. The encryption happens in real time. When we connect to the internet, our ISP usually configures our connection. It tracks us using our IP address. Our network traffic is routed through the servers of our Internet service provider, which can log and display everything we do online.

Our ISP may appear to be trustworthy, but it may share our browsing history with advertisers, law enforcement, or the government, as well as other third parties. ISPs can also be targeted by cybercriminals: if they are hacked, our personal and private information may be compromised. This is especially important if we use public Wi-Fi networks frequently. We never know who is watching our internet traffic or what they are trying to steal from us, such as passwords, personal information, payment information, or even our entire identity.

2.1.2 Impact of not having proper policies and configurations for VPN

Our data could be vulnerable to outsiders :-

Our data is vulnerable to theft by hackers if we do not use a VPN. For example, if we use public Wi-Fi, someone else on the network might be able to access our data. A VPN encrypts our data so that no one else can read or access it. If we use a weak password or click on a malicious link, we may also be hacked. We can also protect ourselves by employing a VPN, creating strong passwords, and taking precautions when clicking on links. VPNs are used by both consumers and businesses to protect their data because anyone's privacy can be compromised. Banks and other financial institutions, for example, use VPNs to protect their consumers' data from theft. Put another way, the company we work for that has sensitive data, our company use a VPN to protect their information from unauthorized access.

Furthermore, by safeguarding our data, we can improve our security and reduce our chances of becoming a victim of identity theft. When someone steals our personal details, such as our name, Social Security number, or credit card details, this is referred to as identity theft. This information can be used to open new accounts, make purchases, or even obtain a loan in our name. When we use a VPN, our data is encrypted, making it much more difficult for someone to steal it.

Figure 2. 1 Stealing data by hacker

We data could be spied by the government :-

The government may be spying on our online activity if we do not use a VPN. In some countries, the government monitors all online activity. A VPN encrypts our data, making it impossible for the government to see what we are doing. In this case, a VPN creates a secure tunnel between our device and the internet. This way, even if the government is watching our every move, they won't be able to see what we're up to. A VPN can also be used to access websites and services that are restricted in our country.

In China, for example, the government restricts access to many websites, including Google, Facebook, and Twitter. A VPN allows us to bypass such restrictions and freely use the web. We can also unblock geo-restricted source material on Netflix, BBC iPlayer, and other streaming services by changing the location of our PC with a VPN. This way, no matter where we are in the world, we can watch our favorite shows and movies. It also gives us access to censored news websites and social media platforms.

Figure 2. 2 US protest against government to stop mass spying

We could face lag of internet speed :-

Our ISP may reduce our internet speed if we do not use a VPN. ISP is an abbreviation for Internet Service Provider. If our VPN ISP believes we are using too much data, they can throttle or slow down our bandwidth. This is usually done to reduce network congestion or to save money on bandwidth costs. A VPN encrypts our data, making it impossible for our ISP to see what we're doing. This means they won't be able to throttle our bandwidth, and we'll be able to use our internet connection at full speed.

We could be tracked by advertisers :-

Advertisers may track our online activity if we do not use a VPN. Advertisers collect data about our online behavior using cookies and other tracking technologies. This information is then used to display targeted advertisements to us. A VPN encrypts our data, making it impossible for advertisers to track us. This means that we will only see advertisements that are relevant to us and will not be bombarded with advertisements for things we are not interested in.

(StefanCoders, n.d.)

2.2 Firewall

2.2.1 What is Firewall

A firewall is a network security tool that keeps track of and filters incoming and outgoing network traffic in accordance with previously established security policies for an organization. A firewall, at its most basic, is a barrier that sits between a private internal network and the public Internet. The primary function of a firewall is to allow non-threatening traffic in while keeping dangerous traffic out.

A firewall is an essential component of any security architecture because it removes the confusion from host-level protections and transfers them to our network security device. Firewalls, particularly Next Generation Firewalls, are focused on blocking malware and application-layer attacks. When combined with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can detect and respond to outside attacks across the entire network quickly and seamlessly. They can set policies to better defend our network and perform quick assessments to detect and shut down invasive or suspicious activity, such as malware.

2.2.2 Impact of not having proper policies and configurations for Firewall

Data can be vulnerable to Cyber Criminals :-

Not having a firewall is equivalent to leaving our front door open. It's as if we're encouraging criminals to break into our network, which they will. A company that does not have a firewall is vulnerable because anyone can gain access to their network, and they have no way of monitoring potential threats and untrustworthy traffic.

Outdated firewalls can also allow various security threats to infiltrate the computer system, such as hacking (unauthorized access by third parties), malware emergence, and phishing. This obviously has the effect of lowering the quality of data handled by the system, resulting in identity theft and a loss of trust in the organization.

Figure 2. 3 Cyber Criminals stealing open data

Company could have severe losses :-

Now, if we believe that our small business does not need to be concerned because the data, we generate has no value outside of our organization, we should think again. Our data is valuable, and cybercriminals are aware of this. According to the Ponemon Institute, the average cost of a data breach is $4.24 million per incident, a 10% increase over last year's $3.85 million.

Firewalls' primary responsibility is to inspect the data that flows into and out of computer systems and networks. Firewalls that are no longer in use lose their strength and vitality. This significantly slows data movement into and out of the system. This reduces productivity in the workplace where the system is used.

Without a firewall, we give attackers complete access to our data. They have the option of stealing our data, leaking it to the public, encrypting it and holding it for ransom, or simply deleting it. Failure to protect our network with a firewall is not only a costly error; it can also cost to our business.

Network Downtime :-

Without a firewall, one of the worst-case scenarios is complete network failure. Malicious criminals can effectively shut down our business if we do not provide adequate protection. And this can have disastrous consequences for our company. Not only can you lose data, but it can also take days or even weeks to get your systems back up and running. Crashes are frequently caused by a failure to keep the firewall up to date. Regular software upgrades and virus scans should be performed on a firewall. Crashing renders the entire computer system inoperable.

According to a GE Digital study, unplanned downtime can cost a company more than $250,000 per hour on average. Some industries reported average costs of over $25,000 per minute. When we consider the impact of downtime on productivity, morale, and customer trust, it's only a matter of time before the damage becomes irreversible.

(Technology, n.d.)

2.3 Importance of Network Monitoring

2.3.1 What is Network Monitoring

IT teams can gain insights into their networks using network monitoring tools. These insights enable teams to examine metrics such as network performance, security, and efficiency. Monitoring tools, such as network performance monitors (NPMs), analyze the network using a variety of monitoring methods. Most tools use a variety of network monitoring techniques to provide users with valuable performance data.

Some monitoring programs focus purely on one or two network monitoring techniques, while others include a much broader range. Regardless, when it comes to how their monitoring tools analyze their networks, businesses have a lot of options.

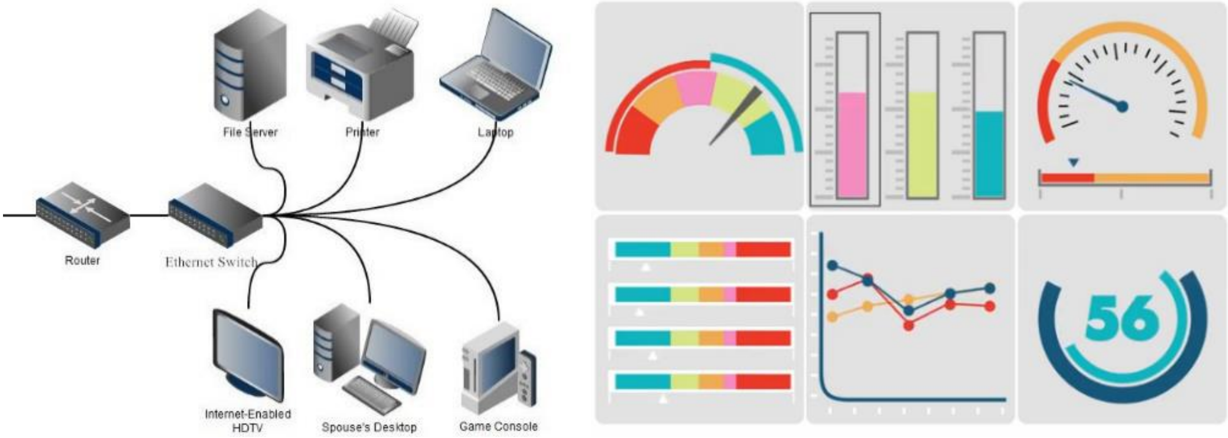


Figure 2. 4 Network Monitoring

2.3.2 Techniques and Protocols of network monitoring

Ping monitoring :-

Pings on the network are one of the oldest monitoring techniques, but they are still widely used by NPMs today. The monitoring tool sends a packet (or several packets) to a node or device and waits for a response. If the target node responds with a "all-clear" message, the monitor knows the node is operational. If no response is received, it sends out more pings in an attempt to get the node's attention. If these pings still yield no results, the monitoring tool notifies the user. Pings are a simple monitoring technique, but they are an excellent way for businesses to determine whether or not devices are currently operational.

SNMP monitoring :-

The majority of modern devices are SNMP, or Simple Network Management Protocol, compliant. Monitoring tools and nodes can communicate with one another using the device protocol known as SNMP. The system uses agents inside of devices to transmit data to network administrators and monitoring software. Devices can send traps when important network events take place, and an SNMP manager can poll them to find out their current status. The communication between NPMs that support SNMP monitoring is standardized, centralizing, and makes monitoring operations simpler.

Log file monitoring :-

Devices on a network typically generate log files as they operate. These log files contain basic information about the device, including any errors. While not as sophisticated as other methods, some tools monitor log files for device-reported issues. Log files are simple text files that may contain keywords like "error" or "critical" that indicate a node problem. Monitoring tools look for these keywords and report on anything out of the ordinary.

NetFlow monitoring :-

NetFlow systems use packet traps to examine traffic that flows through a specific network segment. NetFlow probes collect traffic data and forward it to a monitoring tool for analysis. To determine how data moves through the network, the analysis examines network traffic flow and volume. In order to ensure that data and information are moving along the network path without any slowdowns, flow-based monitoring systems, such as NetFlow, analyze the communications between devices.

SQL query monitoring :-

SQL queries can be used to monitor databases connected to a network. These queries request data from the database, such as the number of data requests, transmissions, and so on. A monitor can use this information to determine whether or not the database is performing adequately. If the database is performing slowly, the monitoring tool can detect it and notify the network team.

Syslog :-

The System Logging Protocol (Syslog) is a standard message format that network devices can use to communicate with a logging server. It was created specifically to make network device monitoring simple. A Syslog agent can be used by devices to send out notification messages under a variety of conditions. These log messages contain a timestamp, a severity rating, a device ID (including IP address), and event-specific information. Despite its flaws, the Syslog protocol is widely used because it is easy to implement and fairly open-ended, allowing for a variety of proprietary implementations and thus the ability to track almost any connected device.

(Hein, 2019)

2.3.3 Benefits of network monitoring for EMC Cyber

Keeping full network visibility :-

We cannot fully comprehend the performance of our network unless we have complete network visibility. EMC Cyber company must be able to monitor and analyze common performance metrics as well as observe every bit of traffic that passes through their network. Any network monitoring tool that is worthwhile will provide comprehensive monitoring capabilities that ensure no part of their network is left in the dark. That way, there won't be any performance issues lurking somewhere on their network.

Identifying security threats :-

While network monitoring solutions are mainly meant for performance monitoring, they can also assist EMC Cyber in detecting security threats in their system. Some malware and viruses are designed to remain on a network after gaining access without doing anything; others may perform small actions that are undetectable to the human eye. Network monitoring solutions will monitor a network for unusual and suspicious network traffic (indicating that a security threat is consuming network resources) and notify their company of the issue.

Predicting and avoiding network outages :-

Even with the most powerful network monitoring solution, EMC Cyber can never guarantee 100 % service uptime. However, they can assist EMC Cyber in preventing unexpected network outages. A key function of network monitoring solutions is to look for network traffic that indicates a device or network failure is about to occur. This allows the enterprise to correct any unexpected downtime in advance, allowing them to maximize uptime wherever possible.

Monitoring bandwidth usage :-

Most network administrators consider bandwidth usage to be one of the most important performance metrics to monitor. EMC Cyber company would prefer to use as much bandwidth as possible while ensuring that all services run efficiently. A network monitoring solution will track bandwidth usage, notify their network when it reaches critical levels, and make sure that quality-of-service (QoS) protocols are running properly.

Changes to a network or device are tested :-

When we make changes to our network or a device, we must test it to ensure that it is functioning properly. If a device is added or reconfigured incorrectly, it can disrupt the rest of our network. EMC Cyber can use network monitoring tools to test new or updated hardware and connections to see if they will cause problems before they negatively impact their network.

Producing network performance reports :-

A network monitoring solution continuously tracks performance data and displays it visually on their dashboard. Monitoring tools can also generate reports that EMC Cyber enterprise can review and convert into a variety of printable file formats. EMC Cyber company can specify whether the solution generates these reports on a weekly, monthly, quarterly, or other basis.

Identifying performance issues that occur outside of business hours :-

Performance issues can arise at any time, even when no one is present to address them. If a problem occurs after business hours, EMC Cyber enterprise must be notified; network monitoring tools continuously monitor a network, which means they can detect these issues for EMC Cyber. However, a solid network monitoring solution will not immediately send out alerts for these issues because those alerts may be lost by the time the EMC Cyber team returns to work. The solution should ideally delay the alert until a time specified by the network administrator.

2.4 DMZ

2.4.1 What is DMZ

DMZ is an abbreviation for "Demilitarized Zone." This term was borrowed from the Korea Demilitarized Zone (DMZ). When the Korean War ended in 1953, a cease-fire was established, and a demilitarized zone (DMZ) was established. In any case, according to the ceasefire agreement, no military troops or weapons will be deployed within this buffer zone. In the networking world, a DMZ is a network that is only lightly protected. It is still a part of our company's LAN network, but it is less secure than the internet, where critical and sensitive data is stored.

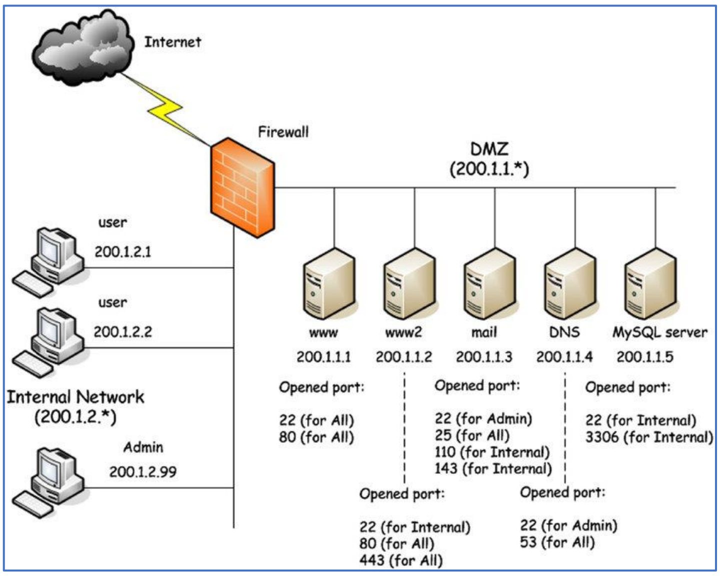


Figure 2. 5 DMZ illustration

A DMZ Network is a defensive line network that provides protection and secures a company's internal local-area network from non - trusted traffic. A common DMZ is a subnetwork that connects the public internet to private networks. A DMZ's ultimate objective is to permit a company to access non - trusted networks, such as the internet, while keeping its private network or LAN secure. In the DMZ, organizations typically store external-facing services and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers.

These servers and resources are isolated and have limited LAN access to ensure that they can be accessed via the internet but not the internal LAN. As a result, a DMZ strategy makes it more difficult for a hacker to gain direct internet access to an organization's data and internal servers.

(Fortinet, n.d.)

A DMZ is a "wide-open network," but it can be protected through various design and architecture approaches. A DMZ can be designed in a variety of ways, ranging from a single firewall to dual or multiple firewalls. The majority of modern DMZ architectures make use of dual firewalls, which can be expanded to create more complex systems.

- Single firewall: Three or more network interfaces are required for a DMZ with a single firewall. The first is the external network, which connects the firewall to the public internet connection. The second is the internal network, and the third is linked to the DMZ. Various rules monitor and control traffic allowed to access the DMZ, as well as limiting connectivity to the internal network.
- Dual firewall: In general, deploying two firewalls with a DMZ among them is a more secure option. The first firewall only allows traffic from the outside world into the DMZ, while the second only allows traffic from the DMZ into the internal network. To gain access to an organization's LAN, an attacker would have to compromise both firewalls.

2.4.2 How DMZ is useful for trusted network

Access control can be enabled using DMZ. Companies can provide users with access to services from outside their network's boundaries via the public internet. The DMZ allows access to these services while also implementing network segmentation to make it more difficult for unauthorized users to gain access to the private network. A proxy server may be included in a DMZ, which centralizes inner traffic flow and simplifies tracking and recording of that traffic.

And also, DMZ can prevent network reconnaissance by acting as a buffer between the internet and a private network. This prevents attackers from conducting reconnaissance work in search of potential targets. Servers in the DMZ are publicly accessible but are protected by a firewall, which prevents an intruder from seeing inside of the company's network. Even if a DMZ system has been compromised, the internal firewall keeps the private network secure and makes external reconnaissance difficult.

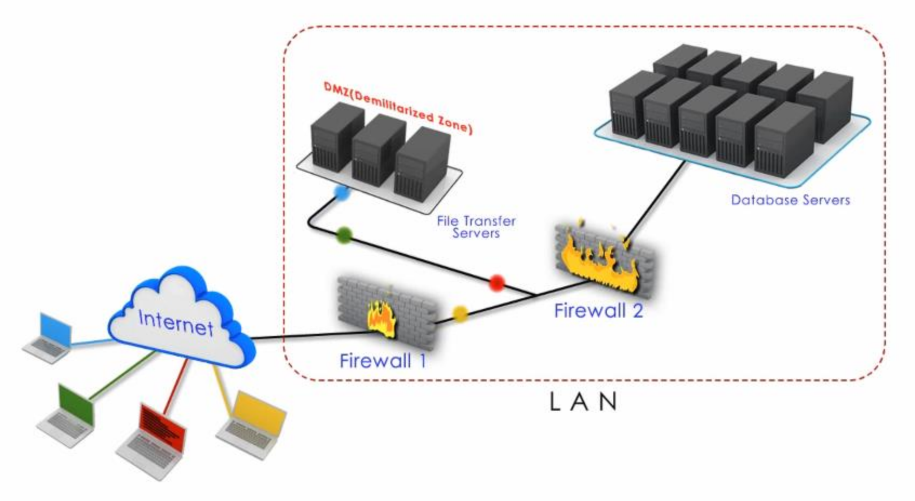


Figure 2. 6 Network reconnaissance by DMZ

DMZ can also improve network trust by preventing Internet Protocol (IP) spoofing. Attackers try to gain access to systems by sending fake an IP address and trying to impersonate an authorized device connected to a network. A DMZ can detect and prevent such attempts while another service confirms the credibility of the IP address. In addition to network segmentation, the DMZ offers a place for traffic organization and public services access that is separate from the internal private network.

2.5 Static IP

2.5.1 What is Static IP

The Internet Protocol (IP) addresses for each host on the network of your company are dynamically assigned using the Dynamic Host Configuration Protocol (DHCP). A host can be any device that allows access to a network in this DHCP definition. Desktop computers and laptops, thin clients, and personal devices are a few examples. DHCP ensures that each of these devices receives an IP address.

And there are two ways that a computer can be assigned an IP address.

1) Static IP
2) Dynamic IP

A static IP address is a 32-bit address assigned to a computer as an internet address. This number is typically provided by an internet service provider in the form of a dotted quad.

An IP address (internet protocol address) is a device's unique identifier when it connects to the internet. Computers use IP addresses to find and communicate with one another on the internet, much like people use phone numbers to find and communicate with one another over the phone. An IP address can reveal details such as the hosting provider and geographical location.

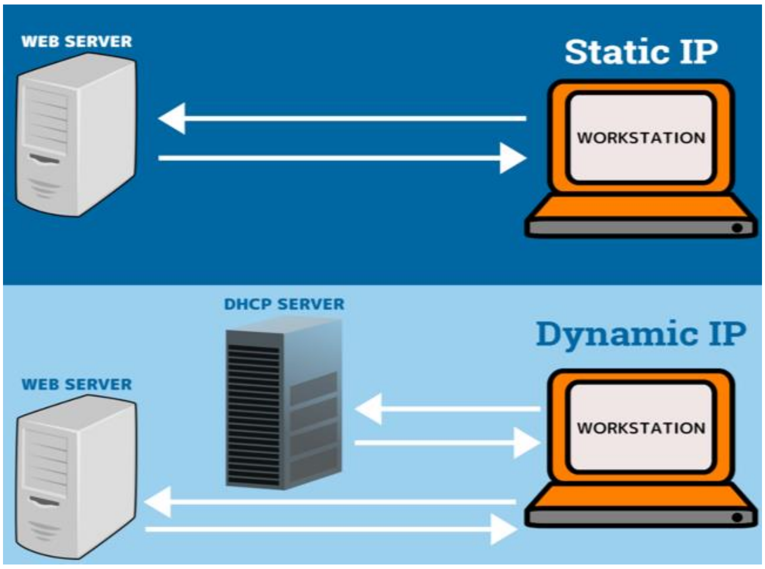
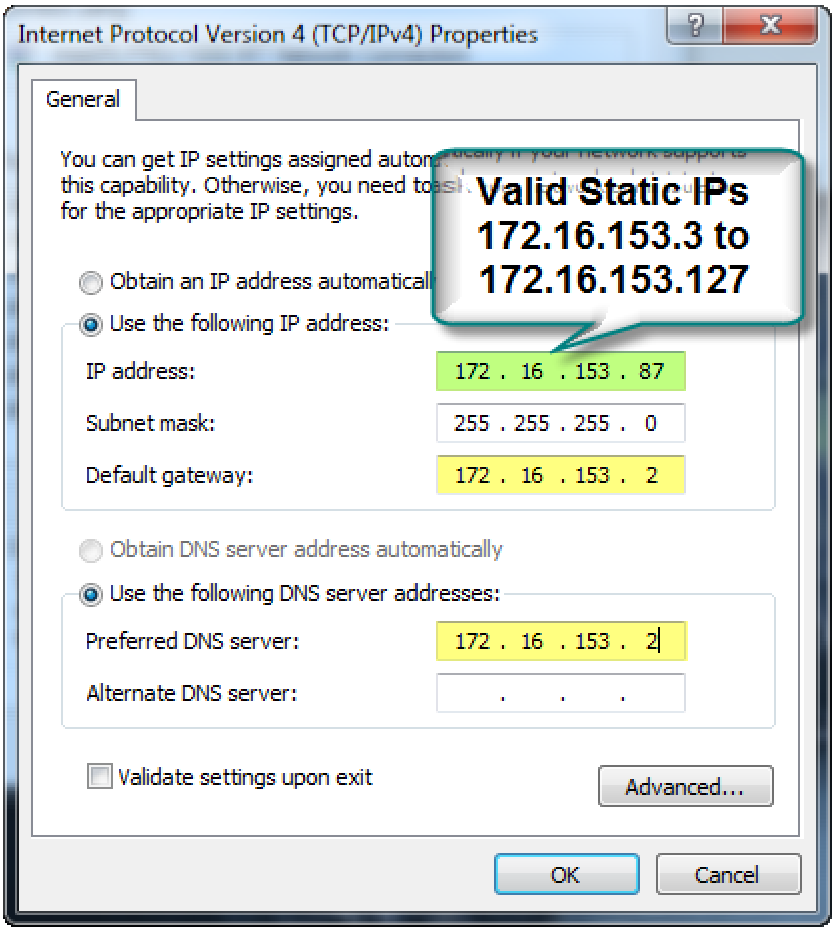


Figure 2. 7 Difference between Static IP and Dynamic IP

When a user wants to go to facebook.com, their computer asks a domain name system (DNS) server, which is similar to a telephone information operator, for the correct dotted quad number. The DNS system converts a domain name into an IP address, which is required to identify a device using a network protocol. In this case, the DNS server will associate the quad number, which is analogous to a phone number for facebook.com, and our computer will use the response to connect to the facebook.com server.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned autom... this capability. Otherwise, you need to ask ... for the appropriate IP settings.

○ Obtain an IP address automaticall...

● Use the following IP address:

IP address: 172 . 16 . 153 . 87

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 172 . 16 . 153 . 2

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 172 . 16 . 153 . 2

Alternate DNS server: . . .

□ Validate settings upon exit

Valid Static IPs 172.16.153.3 to 172.16.153.127

Figure 2. 8 Configuring Static IP

2.5.2 How Static IP is useful for trusted network

Static IP may provide a higher level of security. Despite the fact that a static IP address creates a fact, and a dynamic IP address creates change, we have an advantage when using this option over a DHCP address assignment. When we use a static IP address, our company network gains an extra layer of protection against security issues that may arise on the network.

Additionally, it greatly reduces the possibility of misplacing an important message. If we use a dynamic IP address instead of a static IP address for the server, we may not receive all messages sent to us. When the dynamic IP address changes, any messages sent to the old address are lost until the DNS records are updated. This is never an issue with a static IP address. Because our address remains constant, we will always be aware when someone attempts to contact us.

One of the most common use cases is to use a firewall to restrict network access to your internet-facing services, allowing only whitelisted IP addresses to connect to the service. Only with static IP can you create an indefinitely valid firewall rule.

One of the most common security use cases in Static IP is restricting network access to our internet-facing services via a firewall, so that only whitelisted IP addresses can connect to the service. Only with static IP can we define an indefinitely valid firewall rule. When using a dynamic IP address, however, the firewall rule becomes obsolete whenever the IP address changes. As a result, a whitelist update is required (which implies extensive manual work in large networks). Hence, Static IP offer better protection against network security issues than DHCP address assignment.

2.6 NAT

2.6.1 What is NAT

NAT is an acronym which stands for Network Address Translation. And this is a service used in routers to convert one set of IP addresses to another set of IP addresses. And the NAT service exists to assist maintain the limited number of IP version 4 public IP addresses that are available around the world. When engineers designed the IP version 4 address, they had no idea how massive the internet would grow.

Because, despite the fact that there were over 4 billion IP version 4 addresses available, the developers believed that this would sufficient. But they were definitely mistaken. To avoid a shortage of public IP version 4 addresses, engineers developed private IP addresses and network address translation. There are now two sorts of IP version 4 addresses. These are public and private IPV4 addresses.

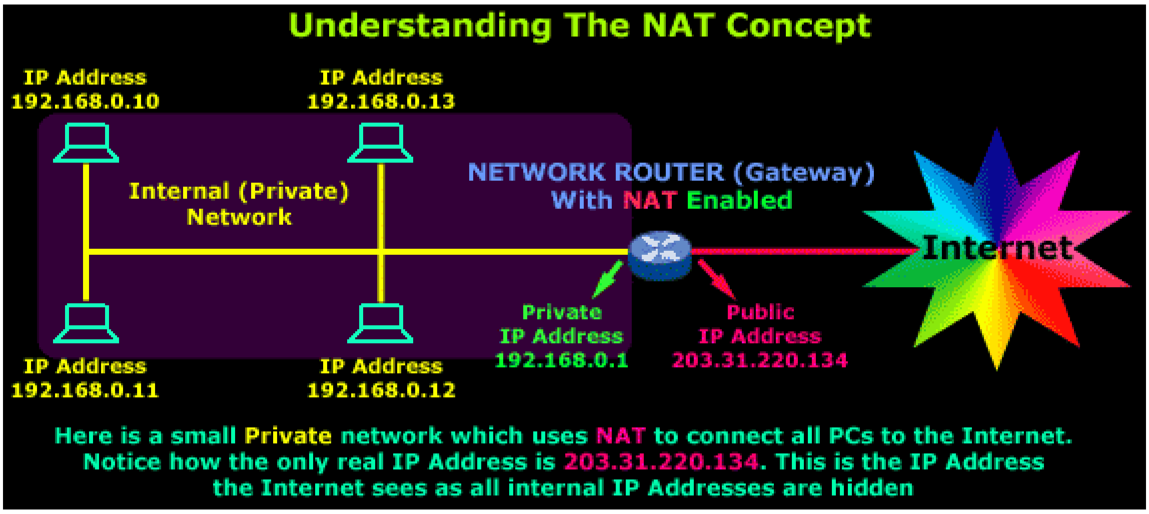

Understanding The NAT Concept
IP Address 192.168.0.10
IP Address 192.168.0.13
Internal (Private) Network
NETWORK ROUTER (Gateway) With NAT Enabled
Internet
Private IP Address 192.168.0.1
Public IP Address 203.31.220.134
IP Address 192.168.0.11
IP Address 192.168.0.12
Here is a small Private network which uses NAT to connect all PCs to the Internet. Notice how the only real IP Address is 203.31.220.134. This is the IP Address the Internet sees as all internal IP Addresses are hidden

Figure 2. 9 NAT diagram

On the Internet, public IP addresses are publicly registered. If we wish to use the internet, we must have a public IP address. There are around 4 billion accessible public IP addresses. As a result, they are limited.

Private IP addresses, on the other hand, are different. Private IP addresses are not made public. As a result, users cannot immediately connect to the internet using a private IP address. Private IP addresses are only used for internal purposes, such as within a home or business. They are not utilized on the open Internet. Below table shows the difference between Private and Public IP addresses.

Table 2. 1 Private IP addresses vs Public IP addresses.

Private IP	**Public IP**
Use within LAN network.	Use in public network.
Assigned by LAN admin.	Assigned by service provider.
These are unique in LAN.	These are unique in Globally.
No cost associated (Free of charge)	Cost is associated.
Range → Class A 10.0.0.0 to 10.255.255.255 Class B 172.16.0.0 to 172.31.255.255 Class C 192.168.0.0 to 192.168.255.255	Range → Class A 1.0.0.0 to 9.255.255.255 111.0.0.0 to 126.255.255.255 Class B 128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255 Class C 192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

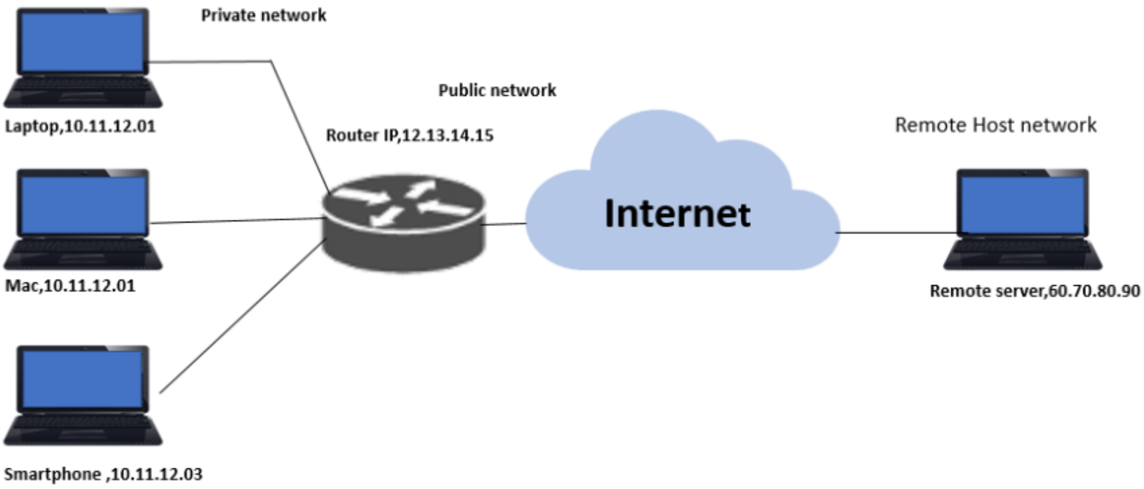


Figure 2. 10 How NAT works

We can already contact your internet service provider and get these extra public IP addresses for all of our devices. But that would be more expensive, unnecessary, and, more significantly, a waste of public IP addresses. And, let's face it, if every device in the globe had its own public IP address, we'd have run out of them by now.

Instead, we can have our router assign Private IP addresses to the devices in our house or business. When our devices need to connect to the Internet, NAT in the router will translate their private IP addresses to the single public IP address that we have been assigned. This, once again, is what NAT does. It converts one set of IP addresses to a different set of IP addresses. So, it not only turns private to public, but also public to private.

Because if a computer on the internet wishes to communicate with a computer on this private network, the public IP address must be translated by NAT to that computer's private IP address. We will no longer require NAT or private IP addresses in the future. This is due to the new generation of IP addresses known as IP version 6. With IPv6, every device on the planet will have its own public IP address.

As a result, IP address translation is unnecessary. This is due to the fact that IP version 6 can generate over 340 undecillion IP addresses. So, the number 340 has 36 digits after it. So, with such a large number, we will never run out of IP addresses. So, with such a large number, we would never run out of IP addresses.

2.6.2 How NAT is useful for trusted network

NAT can improve security by enforcing boundaries. The corporate LAN's private IP addresses cannot be routed from the outside owing to NAT. Because external systems don't know which computer to contact even if they have the ability to bypass the firewall, this enforces network boundaries and forces traffic to flow through the network firewall. NAT ensures that all inbound and outbound traffic can always be inspected before being routed to its destination by forcing traffic to flow through a next-generation firewall (NGFW).

If NAT is enabled on our network, then our local area IP address (also known as our private IP address) is masked. This means that no one from the outside can easily determine which IP address is linked to our PC or local side computer system. When attackers attempt to target our PC from the outside world to attack, this will help in terms of network capabilities.

If our network is Nat enabled, they cannot determine our machine's IP address. They could only see the Public IP address. Because of network address translation, the private IP address is hidden. However, NAT is not a completely secure mechanism that improves the security of our network. That is why we are including a Firewall in addition to NAT.

Furthermore, NAT improves privacy. NAT obscures an organization's internal network structure from the outside world. External systems are seeing a single IP address or a set of regularly changing ones, which makes it difficult to map an organization's internal network for use in subsequent attacks.

2.7 Ensure the integrity organizational IT security by evaluating physical and virtual security measures

2.7.1 What Is Data Integrity

The process of maintaining and ensuring the accuracy and consistency of data throughout the data lifecycle is known as data integrity. The goal is to ensure that our data is reliable, accurate, and stored in the best possible way, and that it does not change when we modify, transfer, or delete it.

We can divide data integrity into two parts for better understanding:

1. Physical Data Integrity : Physical data integrity is concerned with how data is stored and accessed in our company (using on-premise servers or the cloud databases you are remotely connected to). Our main concerns in this section are ensuring the physical security of devices and having a disaster recovery plan.
2. Virtual Data Integrity : Virtual Data Integrity is really about preventing human error from causing data integrity to be lost.

2.7.2 Methods of ensuring data integrity in the company with physical and virtual security measures

1. Data Entry Training

The way I see one of the most significant challenges that businesses face in maintaining data integrity is that their employees are unaware of how to do so. As a result, providing data entry training to them may be the best way to get started. So, I recommend to begin by training our employees on how to enter and maintain data and entrusting them with the responsibility of maintaining data quality. It will ensure that everyone on our team is working hard to maintain data integrity.

2. Validating Input and Data

As I see this is critical, especially if our data comes from an unknown source, such as an end-user, another application, or third-party sources. To ensure the accuracy of the data inputs, I recommend we must verify and validate them. Aside from that, we must validate data on a regular basis to ensure that data processes are not corrupted.

3. Removing Duplicate Data

Duplicate data is one of the leading causes of data integrity breaches because it frequently causes ambiguity and led directly to malicious errors. Recognizing and removing duplicate data on time is therefore critical. While large companies have dedicated staff for this purpose, if we are a small organization without dedicated resources for this role, we can use duplicate file cleaners. Some of them are BleachBit, FSlint, and GDuplicateFinder.

The best thing about the tools on this list is that they are all open source, which means user can not only use them for free but also receive community support.

4. Backing Up Data

Even if we take the necessary precautions to maintain data integrity in our organization, we cannot risk losing permanent data. As a result, I would recommend that we make regular backups of our data. We must understand that, in the event of a cybersecurity attack, data backup will play a critical role in restoring normal function and preserving data integrity.

We must also proceed cautiously when selecting a cloud storage and backup solution for our organization. Most providers are not what they claim to be and making the wrong choice can put us in danger. Amazon Web Services (AWS), the cloud computing service of Amazon.com, is the largest cloud service provider globally, in my opinion. The company offers over 200 fully featured services from its data centers, including compute, storage, and database.

5. Using Access Controls

When there is no access control in our organization, the chances of a data integrity breach increase tenfold. It frequently leads to individuals with no organizational access and malicious intent gaining access to our data and causing significant harm to the organization. That is why we must implement access control in our organization. Implement a least privilege model and restrict access to only those users who require it to maintain high-level control and data integrity.

6. Keeping an Audit Trail

It is critical to identify the source of any data breach. That is why maintaining an audit trail is critical to maintaining data integrity. An audit trail will provide ingredients to the organization, highlighting the source of the problem so that it can be resolved on time.

7. Performing Penetration Testing and Security Audits

Penetration testing is another effective method for ensuring data integrity. That entails having an ethical hacker attempt to break into our company's database and identify vulnerabilities. It will assist us in determining where we are lacking and resolving issues in a timely manner. We can also conduct security audits because they only require the participation of internal sources.

8. Establishing Collaboration in the Organization

Another way to ensure data integrity in our company is to keep all of our employees on the same page. They should be aware of who is creating, changing, and transfer data and when they are doing so. That is why we must foster collaboration within our organization. Everyone should be able to collaborate and work well together. For collaboration and communication, use email, business phone systems, conference calling services, or tools like Microsoft Teams. Everyone should be aware of the situation by the end.

9. Running Volume and Stress Tests on the Database Actively

Data integrity breaches can also occur when the hardware is unable to handle the amount of information that must be processed. These conditions frequently result in technical attacks and server failures. Another reason could be bad code and poor configuration, which attackers can use to brute strength login screens and steal user passwords. That is why it is critical to run volume and stress tests on the database on a regular basis so that all of these issues can be tracked and resolved on time while maintaining data integrity.

10. Encrypting our Data

In our organization, encryption can also be a useful safeguard for maintaining data integrity. It makes sure that even if someone has access to our data, they cannot decrypt it and read it. It works well in situations where attackers have easy access to the files kept in our database through means like stealing the server or downloading files through database hacking.

11. Enabling SSL Encryption on our company Websites

Websites are one of the most popular ways for cyber criminals to gain access to our data and compromise its integrity. They are vulnerable to man-in-the-middle and downgrade attacks. That is why SSL encryption should be enabled on our website. All of these threats will be eliminated by encrypting our communication.

12. Developing Process Maps for Critical Data

We also need control over how and where the data is used, as well as who is using it, to ensure data integrity. It will keep an eye on our company's data and prevent it from being misused. That is why it is critical to create process maps for critical data so that our organization can have more control over how it is used. It will also assist us in implementing appropriate security measures and regulatory requirements.

13. Promoting a Culture of Integrity

In my opinion, data integrity is more than just taking precautions; it is also about fostering a culture of transparency, honesty, and integrity. Our team members must be truthful about their work and take responsibility for their data. They must also report instances where other members violate the rules or fail to fulfill their duties.

These are the small steps that will ensure our entire organization stays on track and our data integrity remains intact.

14. Paying Attention to Cybersecurity

In order to maintain the integrity of our organization's data, cybersecurity will be essential. It will ensure that no one can access critical data without our authorization, and it will reduce the likelihood of a security breach. As a result, ensuring cybersecurity in our company should be our number one priority. We must establish strict policies, employ advanced security tools, and implement necessary security measures.

2.7.3 Data Integrity Evaluation

In my opinion data integrity cannot directly define as data security. Data security aims to shield information from intrusions from the outside world, whereas data integrity is concerned with maintaining information's accuracy and consistency throughout its entire existence. Data security is only one aspect of data integrity. Data security is not broad enough to encompass the numerous processes required to maintain data consistency over time.

And also, data integrity cannot directly define as data quality. Data quality, like data security, is only a component of data integrity, but it is an important one. Data integrity encompasses all aspects of data quality and goes above and beyond by implementing plenty of rules and processes that govern how data is entered, stored, transferred, and so on.

With data integrity I was able to remove excess storage used for outdated, incorrect, or redundant data, which eventually allowed me to better manage data access. This improved performance by reducing or eliminating incomplete records and removing duplicate records. Data integrity is essential because data is the basis of everything. It is an essential component of any organization's infrastructure and must be treated as such. Well-executed data integrity initiatives guarantee that information is findable, traceable, reliable, and up to the highest standards of usability. Maintaining data integrity throughout our organization resulted in improved insights, lower costs, and increased efficiency.

Activity 3

3.1 Risk Assessment Procedure

Introduction

This risk management procedure's goal is to instruct employees on how to perform consistent and comprehensive risk management. This procedure explains how to identify, analyze, evaluate, and treat risks. It also lists additional critical actions that are required for a successful risk management plan. Risk is the possibility of anything happening that will have an impact on objectives.

Objectives

The risk management plan's objective is to support the identification and recording of potential risks. The strategy also allows for the development and tracking of prevention measures. The Risk Management Plan should be updated on a monthly basis or as needed.

Risk management is a shared responsibility, with specific risk duties assigned to various departments and levels within the company. It's critical to have accurate and up-to-date risk information on hand since it helps us make better judgments about our strategic vision and operational goals. Risk management is a shared responsibility, with specific risk duties assigned to various departments and levels within the company. It's critical to have accurate and up-to-date risk information on hand since it helps you make better judgments about your strategic vision and operational goals. In order to provide us with the best benefits, risk management must be integrated with existing company processes such as business planning and Internal Audit.

The following are the goals of a risk management framework.

- Support in the early detection and management of risks using a systematic manner.
- Provide continues risk assessment standards.

- Make accurate and simple risk information available to support decision-making, including business strategy.
- Employ risk-reduction measures that are both cost-effective and successful in minimizing risk to a tolerable level.
- Risk levels should be monitored and reviewed on a regular basis to ensure that risk exposure remains within tolerable limits.

Benefits

Risk management will assist us in being able to live up to our principles and achieve our goals. These advantages will be achieved if a continuous and thorough risk management procedure is implemented.

- Increase our chances of achieving our business and strategic goals.
- Encourage a high level of accountability within the organization.
- Improved understanding of risk exposures will assist in effective decision-making.
- Build an environment that allows us to provide consistent service while also meeting performance goals in a cost-effective and efficient manner.
- Protect our most valuable assets, our people, our property, and our reputation.
- Meet with regulatory and policy standards.

Risk Assessment and relationships with other processes

Risk management is not an isolated subject. It must be connected with existing corporate processes in order to maximize risk management benefits and opportunities. The following are some of the important business processes of EMC Cyber's that require risk alignment:

Internal Audit →

The efficiency of controls is examined through internal audit. The role of the Risk & Compliance Manager is to ensure that the Internal Audit function and the controls within the Risk Management process are matched.

Business Planning (including budget) →

Identifying risk during the planning process allows to set continuous delivery timeframes for strategies or to eliminate a strategy if the associated risks are too large or uncontrolled.

Performance Management →

All risk responsibilities, whether basic tasks like using the risk management process or specific responsibilities as risk ownership or risk treatment implementation, should be contained in the performance plans of the relevant personnel.

Target Audience

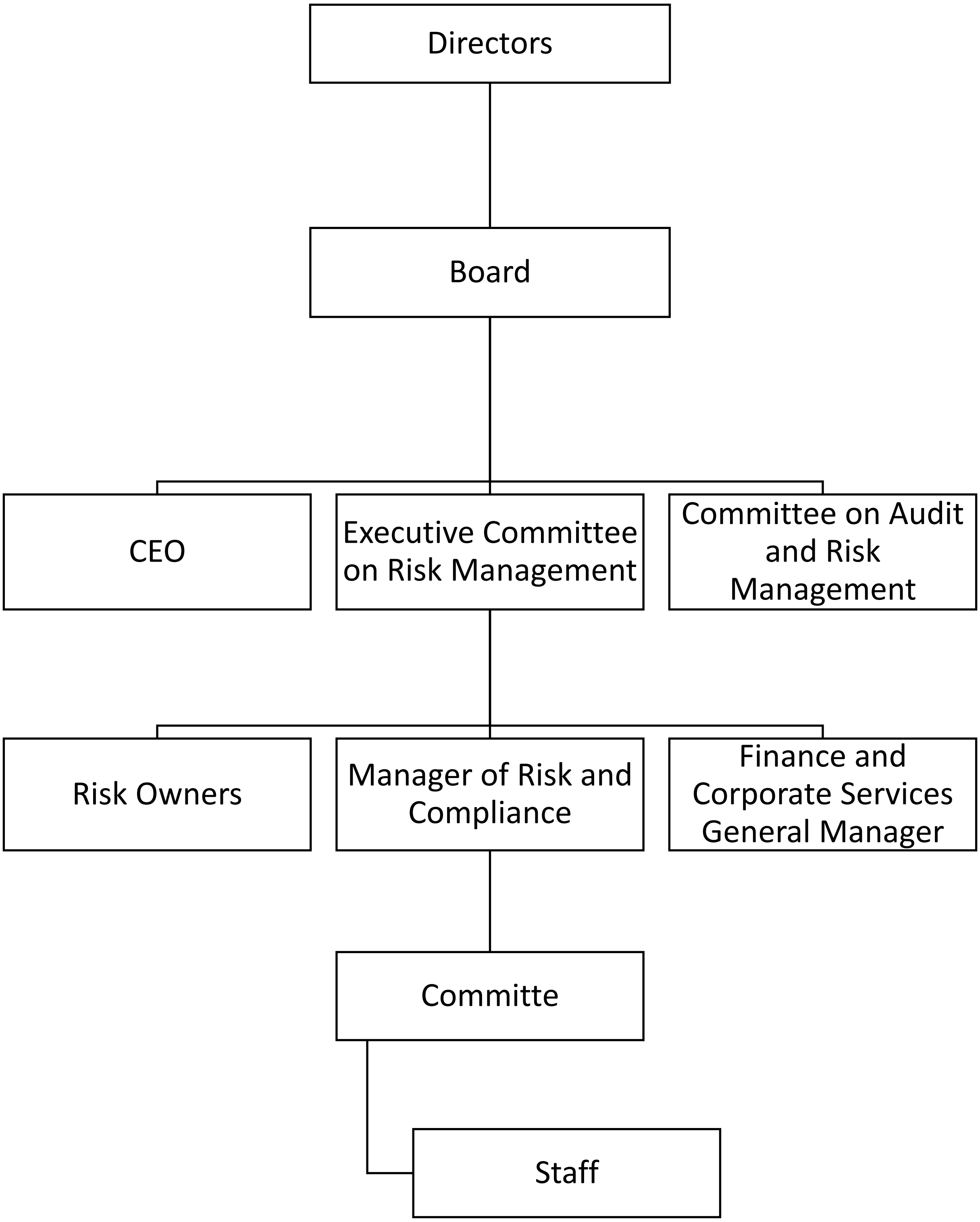
The following groups are targeted by this risk management plan.

Table 3. 1 Target audience for risk management plan.

Group	Responsibilities
Directors	• Responsibility for governance.
Board	• Taking decisions by considering the information they have. • Analyze the reports. • Return to the organization with risk information issues. • Recognize new and emerging risks.
Committee on Audit and Risk Management	• Return to the organization with risk information issues. • Identify new and existing risks and communicate them to the board.
CEO	• Keep an eye on high-risk situations. • Recognize new and developing risks.
Executive Committee on Risk Management	• Inform the Audit and Risk Committee about critical risk issues. • Recognize new and developing risks.
Risk Owners	• They should keep an eye on and analyze the risks they are responsible for. • Prepare reports for the risks that they are responsible for. • Provide information on the risks that they are responsible for to the Risk and Compliance Manager. • Recognize new and developing risks.

Group	Responsibilities
Finance and Corporate Services General Manager	• The Risk and Compliance Manager prepares review reports. • Providing executive support to the Risk and Compliance Manager, such as directing the organization to provide risk information to the Risk and Compliance Manager on a timely basis.
Manager of Risk and Compliance	• Make reports. • Obtain risk information from relevant organizational personnel, such as Risk Owners. • Analyze and evaluate internal and external risks.
Committee	• Gather information and inform the board of upcoming risks that they have predicted.
Staff	• Responsibility for the operation.

Control Structure for Risk Management


Directors
Board
CEO
Executive Committee on Risk Management
Committee on Audit and Risk Management
Risk Owners
Manager of Risk and Compliance
Finance and Corporate Services General Manager
Committe
Staff

Build and implement a risk management plan

Risk Management Procedure Key Process Steps

Risk management is a continuous process that includes the key steps below:

- Communicate and consult.
- Establish the context.
- Identify risks.
- Analyze risks.
- Evaluate risks.
- Treat risks.
- Monitor and review.

When doing risk management, it is critical to follow this procedure since it guarantees that the risk management approach is both comprehensive and consistent. On an annual basis, this process is formally carried out across the entire organization. This is done in combination with the corporate and business planning processes, and it include reviewing and updating risk profiles for the entire company, as well as an evaluation of each individual division. This highlights the difference between a "top-down" and a "bottom-up" risk management approach.

Risk management is not only an annual procedure, even though it is carried out across the entire organization. It should take place at all times and in connection with all company activities. As a result, everyone has a responsibility to use this process consistently when making company choices and managing day-to-day operations. Each process stage is detailed in greater detail to assist in the completion of the risk management process.

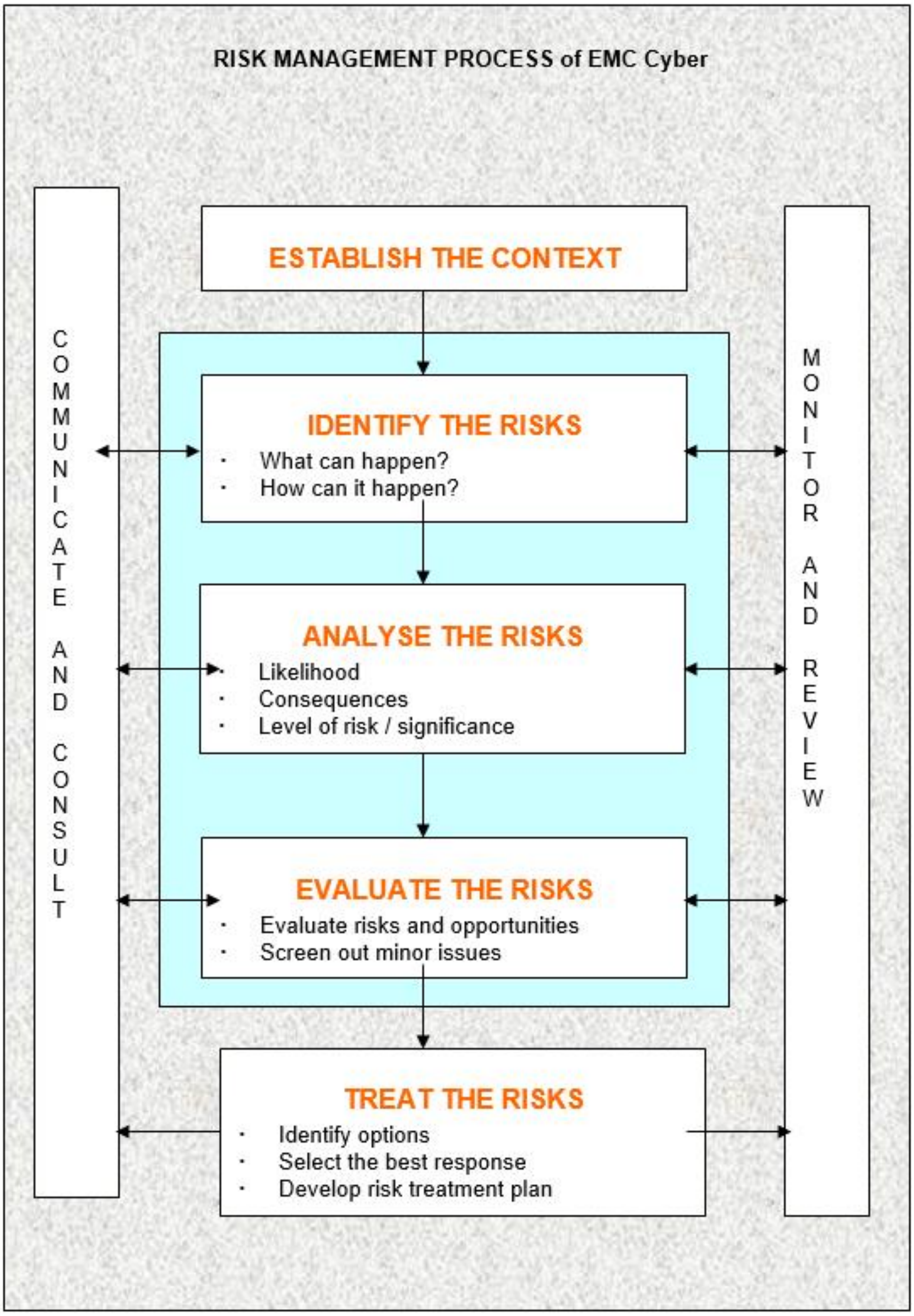


Figure 3. 1 Risk diagram

Step 1: Communicate and Consult

Throughout the risk management process, communication and consultation with internal and external stakeholders is critical to ensure that the organization has a complete view of the risks it faces.

The purpose of external communication and consultation is to inform external stakeholders about the following topics.

- The company's risk management strategy.
- The risk management strategy's effectiveness.
- Requesting feedback when appropriate.

Risk management is an important management and governance function to which external stakeholders, such as the government and business, are increasingly paying attention. The image of the organization will be affected if we can convince these stakeholders that we apply suitable risk management strategies.

Internal communication and consultation aim to keep internal stakeholders informed about the following topics.

- The procedure for risk management.
- Inquiring about the procedure and getting feedback.
- Risks that need to be managed and who is responsible for them.

Step 2: Establish the Context

1. The external context

Developing an awareness of our external stakeholders and, as a result, the amount to which this external environment will affect our ability to fulfill corporate goals like the ones listed below.

- Economic, social, legal, cultural, competitive, financial, and political environments.
- It also involves taking into account our assets, liabilities, opportunities, and threats.

2. The internal context

This is focused on comprehending organizational elements and how they interact, such as the following.

- Culture, internal stakeholders, structure, abilities (in terms of human, system, process, and capital resources), goals and objectives, and the approaches and strategies to achieve these are all factors to consider.

3. The risk management context

The risk management process's goals, objectives, strategies, scope, and parameters must also be evaluated.

Step 3: Identify Risks

Risk identification is an important phase in the risk management process since it ensures that all issues are identified.

Risks can be discovered using a variety of methods and procedures, such as the ones listed below.

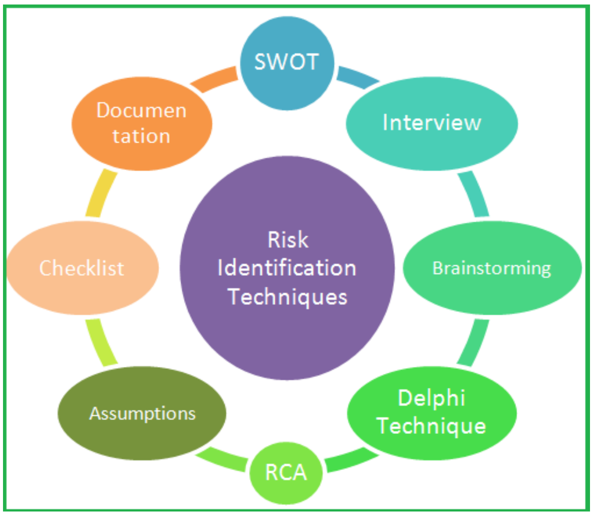


Figure 3. 2 Risk Identification Techniques

Identifying risks that may develop "beyond the horizon" is also a part of risk identification. The following are some instances of possible concerns.

- Events from around the world.
- The public's expectations of government bodies are rising.
- People's opinion of government is changing.

Identifying all risk variables improves understanding of the risk and helps in the evaluation of current controls and the identification of additional possible treatments. It also lowers risk duplication and minimizes risk-related damage.

Step 4: Analyze Risks

It's important to fully describe a risk once it's been detected. The following are the elements of a comprehensive risk description. As an example, event such as high staff turnover, causes such as job dissatisfaction among employees and impacts such as failure to meet strategic goals.

Followings are a part of risk analysis.

- Identifying the present controls in place to manage the risk by lowering the risk's impact or possibility.
- Examining the effectiveness of present controls.
- Identifying the risk's likelihood of occurrence.
- Identifying the potential impact or consequence of the risk if it were to occur.

The goal of controls is to keep the risk at a manageable level. Current controls can be evaluated using a variety of methods, including the ones listed below.

- Control self-assessment.
- The effectiveness of controls is being examined by Internal Audit.
- The effectiveness of controls is being examined by an external audit.

After considering current controls, the consequence and likelihood ratings are combined to produce the total risk level.

Step 5: Evaluate Risks

When evaluating a risk, it's important to examine the risk's total degree of danger. This enables for the decision of whether more risk treatment measures are required to reduce the risk to an acceptable level. The risk evaluation process produces a prioritized list of risks.

Step 6: Treat Risks

Risk treatment is examining various treatment alternatives in order to find the best course of action for managing a risk. When present controls fail to keep the risk under set levels of tolerance, treatment is required. Treatment methods may include strengthening existing controls and adding new ones.

The following are some examples of risk treatment options.

- To avoid the risk, modify the business process or the goal.
- Change the likelihood by taking measures aimed at minimizing the risk's origin.
- Change the outcome by taking steps to reduce the risk's impact.
- Transfer ownership and liabilities to a third party to share/transfer risk.
- Retain the risk as long as we accept the risk's consequences.

Step 7: Monitor and Review

To ensure that risk information is up to date, it must be monitored and reviewed on a regular basis. The environment in which we operate is always changing, and our risks are evolving as well. We may make terrible actions that may have been prevented if risk information is inaccurate. As a result, Risk Owners and Risk Treatment Owners have important risk and control review and update procedures to make sure that information about their specific risks remains current. In addition, the complete risk registry will be evaluated on an annual basis, with review participation extending beyond Risk Owners and Risk Treatment Owners.

The effectiveness of the risk management system must also be assessed and reviewed. This framework determines how well risks are managed across the organization. One such monitoring mechanism is to monitor the Risk Management Strategy's implementation. The risk management framework will also be evaluated on a yearly basis, with the results being reported to the ARC and the Board. Since risk management evolves at a rapid pace, this review method will give us with current risk management information, allowing us to make continual risk management changes.

Risk Capture and Logging

Risks will be documented on a risk form and presented to the risk review board by the Risk Manager, who will document the risk on the Risk Register. The risk review board will evaluate the threat and decide whether to accept, reject, or request additional information. If the risk is accepted, the board will approve the recommended mitigation and backup actions, as well as a budget for risk management.

Throughout the lifecycle of EMC Cyber, the amount of risk will be recorded, managed, and reported. The project team will keep a "Top 10 Risk List," which will be reported as part of this company's project status reporting process. All project change requests will be evaluated for their potential impact on EMC Cyber security concerns. As part of the Executive Project Status Report, management will be advised of significant changes in risk status.

Risk Report Form

Risks can be reported on a risk form and forwarded to the Risk Manager for evaluation.

Table 3. 2 Sample Risk Report Form

RISK REPORT FORM		
Person reporting	Job title	Date
Risk description		
Is the risk date driven? i.e. if the risk was to occur would be on or related to a date or event?		
Deliverables impacted		
Initial assessment	Impact	Likelihood
Suggested risk response		

Color coded Heat Map

The concept of a risk heat map is widely utilized in operational risk management. It's a graphical representation of risk data in which the individual values in a matrix are represented as colors based on risk scores The risk map offers a visualized comprehensive view of the likelihood and impact of an organization's risks. It is a technique that is used to convey the results obtained during the risk assessment process in an understandable manner in 2-dimensional presentations. The heat map indicates to management which risks are more critical to handle.

Operational risks are often evaluated and quantified depending on their likelihood and significance. Each risk's likelihood and significance are graded on a 1–5 scale as follows.

Likelihood:

1. Rare
2. Unlikely
3. Possible
4. Likely
5. Certain

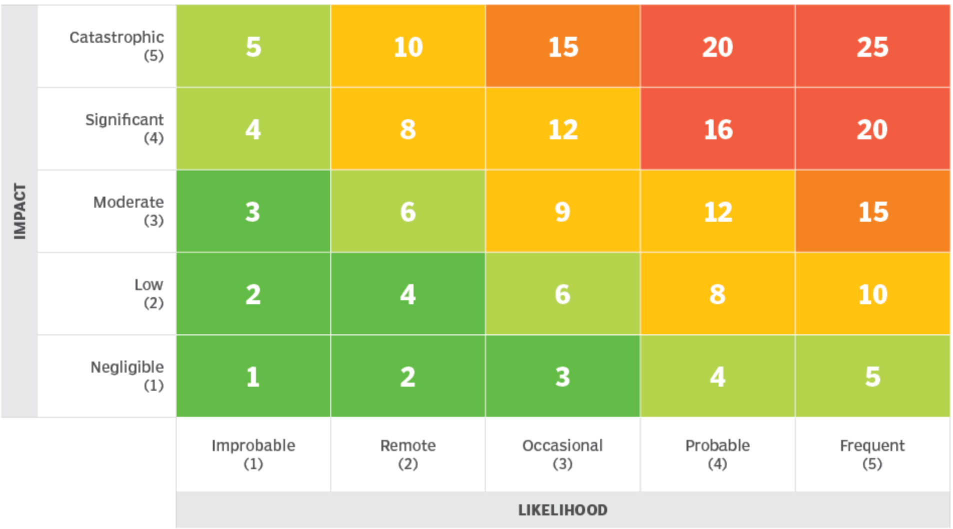
Significance:

1. Insignificant
2. Minor
3. Significant
4. Major
5. Catastrophic

The following formula can be used to calculate the overall risk score.

Risk Score = Likelihood Score x Significance Score

- ➢ That fall into green areas of the map require no action or monitoring.
- ➢ yellow and orange risks require action.
- ➢ Risks that fall into red portions of the map need urgent action.



IMPACT					
Catastrophic (5)	5	10	15	20	25
Significant (4)	4	8	12	16	20
Moderate (3)	3	6	9	12	15
Low (2)	2	4	6	8	10
Negligible (1)	1	2	3	4	5
	Improbable (1)	Remote (2)	Occasional (3)	Probable (4)	Frequent (5)
	LIKELIHOOD				

Figure 3. 3 Example of Colour coded Heat Map

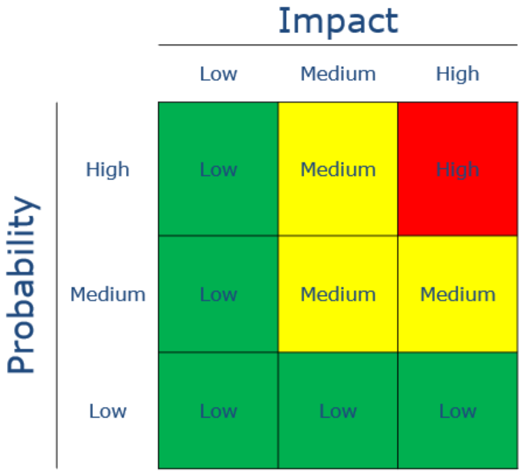
Table 3. 3 Risk Assessment

Identified Risk	Risk Rating	Consequences	Risk Controls
Spread of biological diseases	15	• Illness. • Disability. • Death.	• Set an emergency medical team. • Updating first aid equipment. • Providing health insurance.
Fire damage	20	• Loosing vital data. • Loss of lives. • Building damage.	• Backup data regular basis. • Install smoke alarms and testing. • Fire escape plan practice.
Natural disaster damage	10	• Loosing vital data. • Loss of lives. • Building damage.	• Backup data regular basis. • Repair the building damages.
Power Failure	25	• Loosing vital data. • Loss of business economy.	• Purchase in a cloud backup and recovery service. • Make sure computers has a backup battery. • Surge protectors should be used.
Cyber attack	25	• Loosing vital data. • Loss of business economy.	• Educate staff. • Keep software and systems fully up to date. • Installing a firewall. • Backup data. • Controlling the access to the systems. • Enabling strong Wi-Fi security.

Risk Assessment Matrix

3 x 3 Risk Matrix :

This simple 3 by 3 risk assessment matrix is frequently used for assessing project risks where there are no immediate health and safety concerns. For instance, projects involving organizational change, software implementation, or system upgrades. The low, medium, and high scales are flexible and can be used in a variety of scenarios. A high impact risk for a software project, for example, could be something that causes a delay in going live or a +10 % overspend. A high impact risk for a conference could be something that causes the event to be canceled.



		Impact		
		Low	Medium	High
Probability	High	Low	Medium	High
	Medium	Low	Medium	Medium
	Low	Low	Low	Low

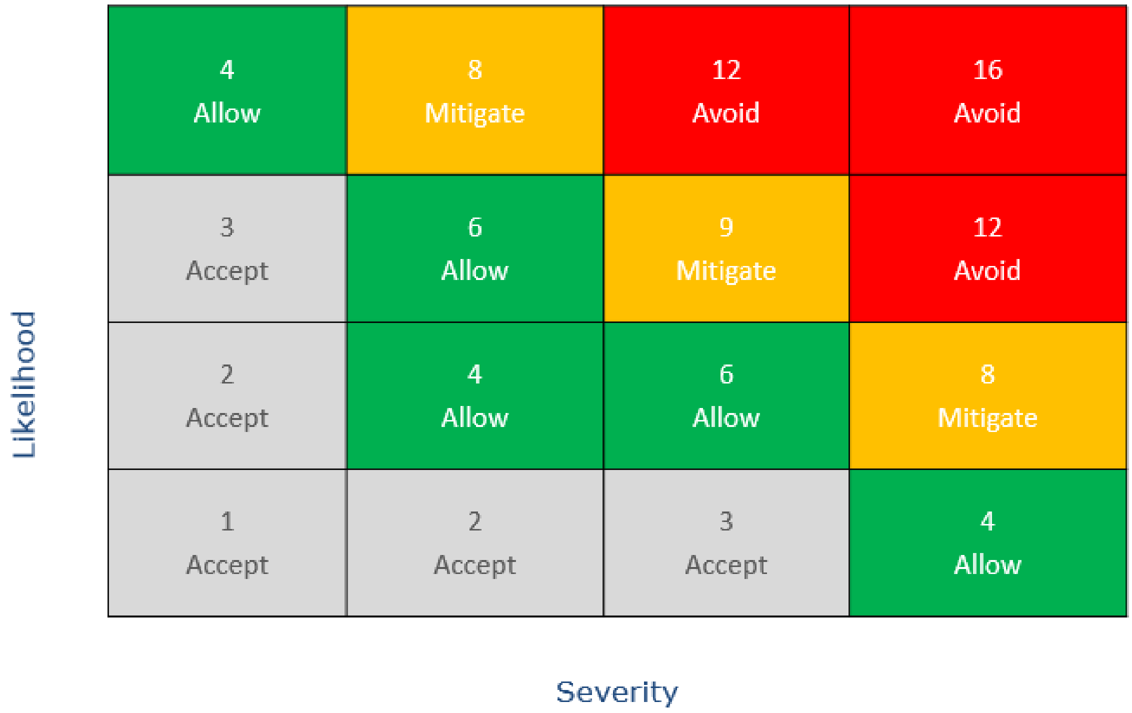
Figure 3. 4 3x3 Risk Matrix

4 x 4 Risk Matrix :

A scale of 1 to 4 is used to measure the chance of a risk occurring vs the intensity of the risk in 4 by 4 risk matrices. A high severity risk rated 4 may appear to be something that needs to be controlled, but if the likelihood of it happening is minimal, say 1, taking action may not be cost effective, and the risk may be ignored.

On a scale of 1 to 4, this risk matrix provides a numerical rating that combines risk likelihood and risk severity. A risk with the lowest probability and severity is given a score of one. A risk with the highest rating receives a score of 16. (likelihood rating 4 multiplied by severity rating 4).

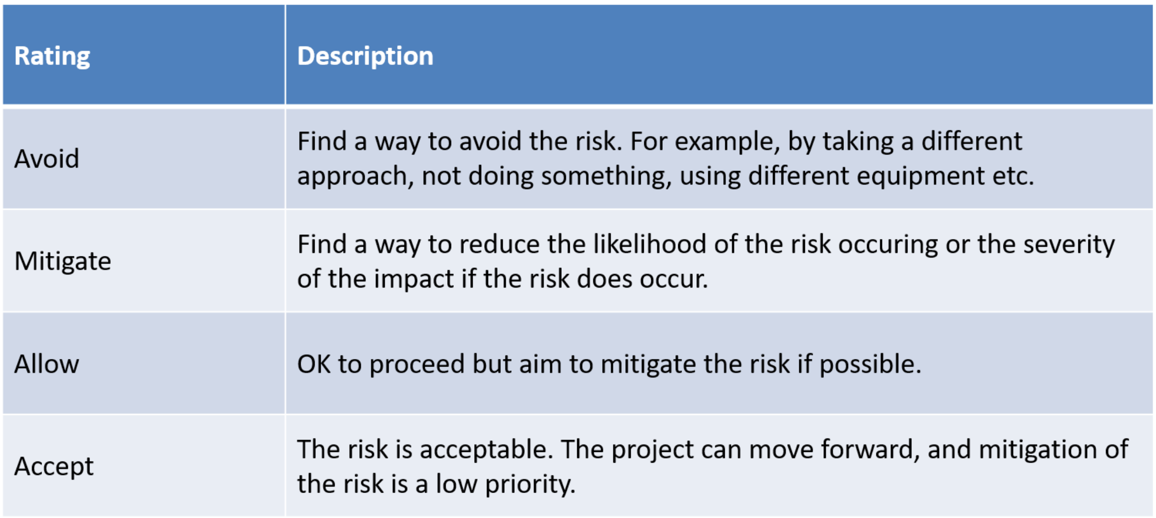
This matrix, unlike a 3 x 3 matrix, provides for a more sophisticated risk assessment and specifies which hazards should be minimized or avoided entirely. Risks with a grade of 1 to 3 are minor and do not require action. Risks with a rating of 8 or 9 require mitigation, while those with a value of 12 or 16 should be avoided.



4 Allow	8 Mitigate	12 Avoid	16 Avoid
3 Accept	6 Allow	9 Mitigate	12 Avoid
2 Accept	4 Allow	6 Allow	8 Mitigate
1 Accept	2 Accept	3 Accept	4 Allow

Likelihood
Severity

Figure 3. 5 4 x 4 Risk Matrix



Rating	Description
Avoid	Find a way to avoid the risk. For example, by taking a different approach, not doing something, using different equipment etc.
Mitigate	Find a way to reduce the likelihood of the risk occuring or the severity of the impact if the risk does occur.
Allow	OK to proceed but aim to mitigate the risk if possible.
Accept	The risk is acceptable. The project can move forward, and mitigation of the risk is a low priority.

Figure 3. 6 Risk Rating

Each significant risk (those in the Red and Yellow zones) will be allocated to a member of the project team for monitoring to ensure that it does not "slip between the cracks." The project team will find ways to prevent or minimize the risk's impact or probability of occurring for each risk that will be mitigated. Prototyping, adding tasks to the project plan, increasing resources, and so on are examples of this.

Risk Escalation

Risk escalation is a risk management and control approach that is necessary to recognize the higher level of authorization's continuing and increasing degrees of risk. A risk is escalated to the relevant organization to ensure that it is recognized, understood, and handled properly.

Risks should be managed by line management as much as feasible, according to the EMC Cyber Policy, and treated by the Risk Owner or the person appointed by the Risk Owner. However, in rare cases, circumstances relating to the treatment itself may exceed the Risk Owner's authorization. If the Head of Office/Risk Owner believes the risk fulfills one or more of the following criteria, the risk should be escalated.

1. Risk treatment demands decisions/actions, such as expenses, that are outside the risk owner's authority.
2. The risk impacts or could affect several offices, such as a number of Offices Across the country or the entire company.
3. Addressing risk demands organizational changes, such as policy modifications.
4. Stakeholder complaints have been received, to which the risk owner is unable to respond impartially and/or efficiently.

Table 3. 4 Risk Escalation

Risk Level	Escalation Recipient	Timing
High	Board	As soon as possible.
Significant	Executive Committee of Risk Management.	Within 1 week.
Medium	Manager of Risk and Compliance.	Within 1 month.
Low	Committee.	Any period of time.

3.2 ISO 31000 Risk Management

3.2.1 Introduction

The ISO 31000 Risk Management framework is an international standard developed by the International Organization for Standardization that provides businesses with risk management guidelines and principles. Regulatory compliance initiatives are typically country-specific and apply to specific sized businesses or businesses in specific industries. ISO 31000, on the other hand, is intended for use in organizations of any size. Its concepts are applicable in both the public and private sectors, as well as in large and small businesses and nonprofit organizations.

3.2.2 ISO 31000's risk management principles

ISO 31000 aims to assist organizations in taking a methodical approach to risk management by focusing on three key areas as follows:

- Identify potential hazards.
- Evaluate the possibility of an event associated with an identified risk happening
- Determine the magnitude of the problems caused by the occurrence of the event

As a result, ISO 31000 doesn't really attempt to remove risks because total risk elimination is impossible. Instead, it is intended to assist organizations in identifying their risks and developing a strategy for mitigating or reducing risks as appropriate.

The decision to implement an ISO 31000-based risk management framework is frequently a simple one because the benefits are well documented. A structured and effective methodology ensures that an organization covers all of the minimum procedures required for the implementation of a risk management program. There is no single road map for implementing ISO 31000 that will work for all businesses. However, there are some common steps that will enable us to balance the frequently conflicting requirements and prepare for an effective certification audit.

3.2.3 ISO 31000 framework and guidelines

This risk management framework is divided into six key sections:

1. Leadership : Organizational leaders must take the initiative to ensure that ISO 31000 is embraced and applied in a way that is consistent with the organization's culture and business targets.
2. Integration : While it is critical to incorporate mitigating risk into as many organizational processes as possible, it is also critical to avoid creating operational slowdowns or impeding the performance of core business processes.
3. Design : Organizations must develop a risk management strategy that is designed for specific needs.
4. Implementation : The process of implementation incorporates the organization's risk management design into operational procedures. Implementation is typically a formal process with clearly defined objectives, deadlines, and reporting requirements.
5. Evaluation : The design is evaluated to determine what is working and what needs to be improved.
6. Improvement : Organizations should look for ways to improve their ISO 31000 implementation on a regular basis.

3.2.4 Benefits of ISO 31000 Standard

Effectiveness has been proved : Numerous organizations use ISO 31000 because it is an internationally recognized standard. This means that ISO 31000 has been thoroughly tested and proven to work.

Legal risk is reduced : Companies will be able to decrease their legal exposure and litigation risks by identifying key drivers.

Increase the organization's profitability : When an organization reduces unnecessary risks, it also reduces the possibility of financial damage from events related to those risks.

3.2.5 Implementing ISO 31000 Standard to IT security

1. Consultation and communication : This step intend to boost stakeholders' knowledge and understanding while also obtaining feedback and data to support decision-making. It should occur at all stages of the implementation process.
2. Scope, context and criteria : The goal of these three steps is to personalize ISO 31000 to the needs of the company's risk management. Organizations should be aware of the scope of risk management implementation. They should also be aware of the company's internal and external environments.
3. Risk assessment : This step is made up of the three separate processes. They are as follows: risk identification, risk analysis, and risk evaluation.
4. Treatment for risk : The goal of this step is to select and implement risk management options.
5. Monitoring and evaluation : This should be done at all stages of the implementation process. The goal is to evaluate the effectiveness of process implementation and identify any areas for improvement.
6. Monitoring and reporting : This step aim to communicate activities and results to the organization while documenting the implementation process.

(Posey, 2021)

3.3 Security Audit

3.3.1 Introduction

An IT security audit can be stressful for a company, but it doesn't have to be. Security audits are technical examinations of an IT system's configurations, technologies, infrastructure, and other elements in order to decrease the probability of a cybersecurity breach. These data details can be challenging to those who are not IT knowledgeable but understanding the resources and strategies available to protect against modern attacks makes IT security less challenging.

An IT security audit includes both manual and automated assessments. An external or internal IT security auditor conducts manual assessments by interviewing employees, reviewing access controls, analyzing physical access to hardware, and performing vulnerability scans. These reviews should take place at least once a year, though some organizations do it more frequently. Additionally, organizations should review automated, system-generated assessment reports. In addition to incorporating that information, automated assessments also react to software monitoring reports and modifications to server and file settings.

(RECIPROCITY, 2021)

3.3.2 Importance of a security audit to maintain the organizational security

To begin with, a comprehensive IT security audit allows us to validate the security of our entire company's infrastructure: software, hardware, services, networks, and data centers. An audit can assist us in answering the following crucial questions:

- Is there any flaws or vulnerabilities in our current security?
- Are there any unnecessary extra tools or processes that serve no purpose in terms of security?
- Are we prepared to defend against security threats and reestablish business capabilities in the event of a system outage or security breach?
- What concrete steps can we take to address security flaws if they are discovered?

We can continue to comply with data security laws with the assistance of a thorough audit. Many national and international regulations, such as GDPR and HIPAA, necessitate an IT security audit to ensure that our data systems meet their requirements for the collection, use, preservation, and destruction of sensitive or personal data.

Typically, an independent third-party vendor or a certified security auditor from the relevant regulatory agency conducts a compliance audit. However, in some cases, our company's personnel may conduct an internal audit to ensure regulatory compliance or overall security posture.

3.3.3 The systems covered by an IT security audit

Each system used by an organization may be examined for vulnerabilities in the following areas during a security audit.

- Vulnerabilities in the network :- Auditors look for flaws in any network device that an intruder could use to gain access to systems or information or cause harm. Information is especially vulnerable as it travels between two points. Regular network monitoring and security audits keep track of network traffic, including email messages, instant messages, files, and other communications. This section of the audit also covers network availability and access points.
- Controls for security :- The auditor examines the effectiveness of a company's security controls in this section of the audit. This includes assessing how effectively a company has followed the policies and procedures put in place to protect its information and systems. An auditor, for example, may examine whether the company holds administrative control over its portable devices. The auditor examines the company's controls to ensure their effectiveness and that the company adheres to its own policies and procedures.
- System software :- Software systems are examined here to ensure that they are functioning properly and providing accurate information. They are also examined to ensure that safeguards are in place to prevent unauthorized users from accessing private data. Data processing, software development, and computer systems are some of the areas that are looked at.
- Encryption :- This section of the audit confirms that a company has established controls to manage data encryption procedures.
- Capabilities for architecture management :-Auditors confirm that IT management has established organizational structures and procedures to establish a productive and controlled environment for information processing.

As a result, security audits are one component of a comprehensive strategy for protecting IT systems and data.

3.4 IT Security Policies

3.4.1 Introduction of IT Security Policy

IT security policies are critical to any organization's success. They are the foundation of all procedures and must be consistent with the company's primary mission and commitment to security. They specify who is in charge of what information within the company. IT security policies influence how organizations prepare for and respond to security incidents. Information security is based on well-documented policies that are recognized and adhered to by all members of an organization.

3.4.2 The importance of aligning IT security policies with organizational policies

Organizational policies and procedures provide guidelines for decision-making processes and how work should be done in an organization. There is a broad area which need to cover up in whole company when making policies. Some of them are equal opportunity policies, workplace health and safety policies, employee code of conduct policies, employee disciplinary action policies, and so on.

However, according to the SANS Institute, a company's security policy establishes the guidelines for how vital business data and systems will be safeguarded against both internal and external threats. These policies and procedures must be updated in conjunction with their annual Security Risk Assessment.

Having comprehensive security policies has a number of advantages for the company. Policies can aid in the improvement of an organization's overall security posture. There are numerous security incidents involving the company, and employees can refer to policies for dealing with them. Having a comprehensive IT security policy in place also helps companies prepare for an audit, which ensures proper regulatory compliance. Additionally, it increases stakeholder and user accountability within an organization, which can be advantageous for the business from a legal and commercial standpoint.

(adserosecurity, 2022)

3.4.3 Consequences of not having an security policy

Despite a rise in the frequency of data breaches, most small and medium-sized businesses lack well-established information security policies. The absence of a data security program exposes organizations to a wide range of security risks, including data theft, information leakage, and unauthorized access to sensitive information. A single data breach can be far more catastrophic and result in massive financial loss. It can also have the following serious consequences.

- Brand Reputation Damage :- A security breach can harm the company's reputation and drive away potential clients. The customers' trust and confidence in one's company will continue to decrease.
- Interfere with business operations :- Downtime from the time a security incident occurs until it is resolved has a significant impact on business operations, resulting in low productivity, revenue loss, and dissatisfied customers.
- Legal Consequences :- Organizations that are victims of data breaches face serious consequences such as fines, legal action, and customer compensation.
- Intellectual property loss :- A data breach not only compromises the company's and customers' information, but we also risk losing patent protection, blueprints, and other certifications.

(sossupport, 2022)

3.5 Data protection laws and regulations in the world

3.5.1 Data protection laws and regulations around the world

Information privacy regulations differ significantly from region to region and even country to country. Some regions, such as Europe, have implemented strict controls that enforce heavy fines on those who violate the rules, whereas countries, such as the United States, are still struggles with formal and centralized laws that provide cohesive protection. Organizations all over the world are concerned about privacy and protecting personal information. In recent years, new, more comprehensive data privacy laws have been enacted or proposed, and it has become absolutely essential for businesses of all sizes and across all businesses to prioritize the protection of personal data.

Here is a list of Data Protection Laws, Acts, and Regulations from around the world:

- General Data Protection Regulation (GDPR)
- ePrivacy Regulation on Privacy and Electronic Communications (PECR).
- Irish Data Protection Act 2018 (which replaced the Data Protection Act 1988)
- UK GDPR (replaced the Data Protection Act 1998)
- Sector-specific data protection laws
- California Privacy Act, 2020 (CPRA)
- California Consumer Privacy Act (CCPA)
- The EU-US Privacy Shield
- Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA)
- Australian Privacy Act
- New Zealand Privacy Act
- Indian Personal Data Protection Bill 2018
- The APEC Privacy Framework and the OECD Privacy Framework

(michalsons, n.d.)

3.5.2 Data protection laws and regulations around the world that EMC Cyber should aware

Here are some data protection laws and regulations around the world that EMC Cyber should be aware of.

1. GDPR (EU) :-

Since the EMC Cyber works with European countries, EMC Cyber should be aware of this law. On May 25, 2018, the EU's General Data Protection Regulation (GDPR) went into effect. Data protection has now become a global issue and is on the legislative agendas of all countries thanks to the broad massive impact it has produced. The GDPR represents the most significant change in data privacy regulation in the last two decades, offering unprecedented protection and individual empowerment.

The European Union's new data protection framework introduces significant commitments on businesses and organizations. They ensure the privacy and safeguarding of personal data, offer data subjects certain rights, and empower regulators to demand accountability demonstrations or even issue fines in cases of failure to comply.

2. PIPEDA (Canada) :-

Since the EMC Cyber works with Canada, EMC Cyber should be aware of this law. The Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal data protection law, was enacted in early 2000. PIPEDA applies to private-sector organizations and governs, among other things, how businesses collect, use, and disclose sensitive and personal data. The law is divided into ten core principles that businesses must adhere to.

3. NDB (Australia) :-

The Notifiable Data Breach (NDB) Scheme went into effect on February 22, 2018, and is piece of Australia's Privacy Act, which includes 13 principles governing entities' obligations for personal data management. Companies that handle personal data, such as bank account information or medical records, are required by the NDB Scheme to report data breaches to the Office of the Australian Information Commissioner (OAIC). They must also notify those whose information has been compromised.

The NDB Scheme, like the GDPR, aims to allow affected individuals to take the necessary steps to protect their personal information, and it imposes significant penalties on organizations that fail to comply.

4. CCPA (California) :-

The California Consumer Privacy Act (CCPA), which goes into effect on January 1, 2020, responds to the increased role of personal data in modern business practices as well as the security implications surrounding the collection, utilize, and safeguarding of personally identifiable information. The Golden State's new data privacy law, signed into law on June 28, 2018, gives consumers access to and control over their personal information gathered online.It requires companies doing business in California to make structural changes to their privacy programs. The CCPA, like the GDPR, is expected to have a global impact, given California's position as the world's fifth largest economy.

5. PDPB (India) :-

On July 27, 2018, the national government's 'Srikrishna Committee' released its long-awaited draft legislation for a new Personal Data Protection Bill (PDPB). The proposed framework would govern the processing of personal information about individuals (data principals) by government and private companies (data financial advisors) incorporated in India and elsewhere. It also specifies how personal data should be collected, processed, and stored.

(Berecki, 2019)

Activity 4

4.1 Security Policy Document for EMC Cyber

1. Scope

This policy applies to all users of EMC Cyber information assets as defined in the EMC Cyber system. All employees are responsible for protecting the company's resources.

This policy applies to all EMC Cyber Information Systems that are operated or contracted with a third party. The term Information Systems refers to the entire environment, including, but not limited to, all documentation, logical and physical controls, personnel, hardware (e.g., desktop, network, and wireless devices), software and details.

Although this policy expressly addresses user responsibilities, it does not do so completely. Additional responsibilities are defined by EMC Cyber Company's Information Security policies, standards, and procedures. Other Information Security policies, standards, and procedures must be read, understood, and followed by all users. If a user does not fully understand anything in these documents, he or she should contact the HR Team at EMC Cyber Company. Any conflicts arising from this policy will be resolved collaboratively by Information Security (IS) and the relevant department/division units.

2. Policy Statement

A risk-based approach will be used by EMC Cyber Company to safeguard its sensitive client data and critical information assets from likely and high-impact threats. Information security principles will also be embedded in the organizational culture, making it everyone's duty to maintain a strong information security structure.

3. Purpose

This policy outlines the organization's intention to identify and safeguard its critical information assets. The following are the company's security principles:

1. Confidentiality: Only authorized personnel should have access to information.
2. Integrity: Only authorized personnel should be able to change information.
3. Availability: Personnel who require information should have access to it.

Users, vendors, hackers, and ex-employees are all potential threats to information and infrastructure. The threat of viruses and worms remains constant. Furthermore, Business Continuity and Disaster Recovery (BCP/DRP) plans must be put in place in the event of a disaster so that the critical business operations continue to operate, and the entire operations are recovered within an acceptable time frame.

In such a case, it is the responsibility of each and every employee to safeguard the company's and its customers' information. All internal processes and procedures are also critical and must adhere to the adopted information security principles.

4. Policy Selection Clauses

4.1 Document Description :

All employees and vendors are responsible for adhering to this policy and other related security standards. The information security team is in charge of reviewing and modifying this policy as needed and/or at least once a year.

4.2 Objective :

The ultimate objective of is to secure sensitive data and systems that support the company's activities and assets.

4.4 Security Awareness Program :

Security awareness programs must be implemented at all levels of the business, including top management, middle management, team leaders, department heads, support workers, and any third parties.

The information security awareness training will be a continuing endeavor to ensure that all employees and contractors are informed of the essential information security policies. Furthermore, all policies, rules, and information security best practices as implemented by the organization, in combination with other laws, regulations, and management best practices.

Online annual information security awareness will be conducted in addition to onboarding and induction sessions for new employees by different HR departments.

4.5 Competence :

The company shall ensure that the workers and contractors in the scope have the necessary skills and competence and shall keep records of the same.

4.6 Monitoring, Measurement, Analysis and Evaluation :

It is critical to monitor and measure the ongoing efforts and results of the information security management system in addition to maintaining it. There will be a thorough defined process for identifying metrics for particular controls used in the company, as well as for implementing and analyzing measures of the selected metrics. The measurements' inputs and outputs will be examined on a regular basis.

4.7Continual improvement :

The following are EMC Cyber's continuous improvement policies -

- Continuously improve the effectiveness of the company's security.

- Improve existing operations to fully comply to good practice as defined by ISO/IEC 27001 and related standards.
- Obtain and maintain ISO/IEC 27001 certification on an ongoing basis.
- Become more proactive about information security.
- Increase the measurable nature of information security processes and controls to provide a solid foundation for informed decisions.
- On the basis of gathered historical data, review relevant metrics on a regular basis to determine whether it is time to change them.
- At routine management meetings, prioritized improvement ideas are discussed along with the benefits and time frames.

4.8 Review :

The Corporate Information Security Policy, along with the other security policies, must be reviewed on a regular basis. This review will take place under the following conditions -

- 12 months a year.
- If the company's technologies undergo significant change.
- If the external threat environment undergoes a significant change that necessitates a review of the risk profile.
- If the client's information security requirements or guidelines significantly change.

4.9 Communication :

- The Information Policy will be distributed via email to all employees and contractors.
- All communication with stakeholders in the media and financial markets will be handled by the executive team only on an as-needed basis via press events, conferences, and emails. No employees of the organization may communicate with the media or financial markets unless authorized by the department manager.

- All employees should act as company representatives and ambassadors in their daily work and are authorized to speak with clients about their project and KRA. Inside information must be kept private.
- In accordance with the executive committee agreement, information on the EMC Cyber website will be uploaded following the approval of the IT Department Manager.
- Communication with both internal and external stakeholders has to be consistent with the organization's position and strategy and will be done on a case-by-case basis. Marketing Officers are permitted to communicate with external stakeholders in accordance with contractual obligations.
- When speaking at conferences, the presentations should be reviewed by HR officers.

5. Policy Details

This policy, as well as the policies listed below, must be followed by all mobile and computing devices that connect to the internal network.

- Account management.
- Anti-Virus.
- Possession of a Mobile Device Security and Acceptable Use
- E-mail.
- Internet.
- Safeguarding Information for Members
- Password.
- Computing in the Cloud.
- Connectivity via wireless (Wi-Fi).
- Telecommuting.

- Passwords at the system and user levels must adhere to the Password Policy. Authorized personnel should not share their EMC Cyber Company user account ID(s), account(s), password authentication, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or other identification and authentication information or devices.
- It is prohibited to provide access to another individual, either intentionally or by failing to secure its access.
- Access to, use of, and sharing of proprietary information by authorized users are only permitted to the extent necessary to carry out their assigned tasks for the EMC Cyber Company.
- All PCs, laptops, and workstations should have a password-protected screensaver installed, with the automatic activation function set to 10 minutes or less.
- When the host will be unattended for any length of time, all users must lock down their PCs, laptops, and workstations by locking (control-alt-delete). Employees must log off or restart (but not shut down) their computers at the end of their shift.
- EMC Cyber Company retains sole ownership of all proprietary information stored on electronic and computing devices, whether they are owned or leased by EMC Cyber, the employee, or a third party. All proprietary information must be safeguarded legally or technically.
- All users are responsible for notifying their immediate supervisor and/or the IT Department of any theft, loss, or unauthorized disclosure of EMC Cyber proprietary information.
- All users must notify their immediate supervisor and/or the IT Department of any weaknesses in EMC Cyber computer security, as well as any incidents of possible misuse or violation of this agreement.
- Users must not give out dial-up or dial-back modem phone numbers to others without first obtaining permission from the EMC Cyber IT Department.
- When opening e-mail attachments from unknown senders, authorized users must exercise extreme caution because they may contain viruses, e-mail bombs, or Trojan Horse codes.

6. Prohibited activities for the user

- Violations of any person's or company's rights protected by copyright, trade secret, patent, or other intellectual property laws or regulations, which include, but not limited to, the installation or distribution of "pirated" or other software applications not appropriately licensed for use by EMC Cyber.
- Unauthorized reproduction of copyrighted material is prohibited, including, but not limited to, digitization and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which EMC Cyber or the end user does not have an active license. Unlicensed copies of installed software must be reported to IT.
- Malicious software is introduced into a network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Uncovering your login information to others or permitting others to use your account when doing work at home, this includes family and other household members.
- Using a computing asset owned by an EMC Cyber Company to actively acquire or transmit material that violates sexual harassment or hostile workplace laws.
- Trying to access any data, electronic material, or programs on EMC Cyber Company's systems for which they lack permission, explicit consent, or implicit need for their job responsibilities.
- Installing any software, updates, patches, or upgrades without first obtaining the IT department's approval from EMC Cyber Company.
- Installing or using non-standard shareware or freeware software without the IT approval of EMC Cyber Company.
- Trying to install, unplugging, or relocating any EMC Cyber Company-owned hardware and software or external devices without the prior approval of COMPANY-IT NAME's Department.
- Buying software or hardware for EMC Cyber Company without first ensuring IT compatibility.
- Personal use of EMC Cyber information systems is prohibited.

7. Enforcement

Any employee who fails to comply with the company's policies and procedures will face disciplinary action. Similarly, employees who encourage/observe such behavior and do not report it to the appropriate authorities will face disciplinary action. Any employee who is found to have violated this policy may face disciplinary action.

4.2 Evaluation on suitability of the tools used in an organizational policy

4.2.1 Introduction

It takes planning, research, and revision to create effective policy and training content. EMC Cyber should always strive to update and enhance policy and tools that have been used to create it. Of course, the content must be comprehensive, covering all necessary procedures. However, policy writing is more likely to be recognized if the content is well-written and engaging. This part is about tools used for writing policy and procedures that assisted in covering some of the fundamental steps of creating policy, such as following a template, and distributing content.

4.2.2 Tools used in an organizational policy

Coggle :-

Coggle is a free mind-mapping tool which enabled me to easily list down all of my policy proposals. I was able to keep track of related ideas by making clutter-free notes and diagrams. Within a document, Coggle allows multiple users to collaborate, comment, and chat. Collaborators can use simple drag-and-drop tools to add text, links, images, and more, as well as rearrange information.

Since I am a visual thinker, doing a brain dump within a mind-mapping software assisted me in beginning to make relationships between complex ideas. After I finished connecting everything, I simply copied my "nodes" and pasted them into text editor. My ideas were automatically organized by Coggle into an outline for simple editing.

Hemingway App :-

A well-written policy and training materials keep things simple. Writing procedures with endless run-on sentences or complex language is the simplest way to confuse the staff. The Hemingway App assisted me in shortening sentences and simplifying language in order to make policy and training content more understandable. I could copy and paste my content into the website or desktop app.

Very long sentences, unclear words, passive voice, as well as other popular errors were highlighted by the app. My policy was made easier to read and understand by addressing the highlighted portions.

Grammarly :-

Grammar was the last thing on my mind as I focused on creating solid content for policy writing. Grammarly assisted me in finding and correcting hundreds of complex spelling, grammar, and punctuation mistakes. This allowed me to stay focused on the content rather than getting sidetracked in the details. Grammarly has a free browser extension that did help me catch errors while writing online. It highlighted errors and allowed me to fix them with a click of the mouse.

Power DMS :-

With guidance, the PowerDMS application assisted me with policy writing. I used the PowerDMS workflows tools, and it was simple to integrate with Microsoft Office 365 and Google Drive, as well as uploading content and policies from third-party sources such as online tools and templates.

4.3 Disaster Recovery Plan to EMC Cyber with the roles of stakeholders to implement security audit recommendations

Introduction About the Company

EMC Cyber is a well-known cyber security firm headquartered in Colombo, Sri Lanka. EMC Cyber provides security products and services. They have a lot of customers both in Sri Lanka and internationally. They create cyber security software such as firewalls, anti-virus, intrusion prevention, and endpoint security. EMC Cyber is in charge of safeguarding the company's networks, clouds, web applications, and emails. They also provide enhanced threat prevention, secure unified access, and endpoint security. They also advise clients on security threats and how to minimize them.

A Disaster Recovery Plan (DRP) is a formal document developed by a company that gives precise instructions on how to respond to unexpected crises such as natural disasters, power outages, cyber-attacks, and other disruptive events. The plan includes measures for reducing the consequences of a disaster, allowing an organization to continue operations as if there had been no disruption. A good DRP facilitates fast recovery from disruption, regardless of their cause.

This Disaster Recovery Plan (DRP) gathers all information describing EMC Cyber's ability to withstand a disaster as well as the steps that must be followed to achieve disaster recovery into a central repository.

Definition of a Disaster

Disasters are severe disturbances to a community's functioning that surpass its ability to cope using its own resources. Natural, man-made, and technical risks, as well as a variety of other elements, can all contribute to disasters. A disaster, whether caused by man or nature, prevents EMC Cyber's IT department from performing all or portion of their regular functions and responsibilities for an extended length of time. Disasters are defined by EMC Cyber as the following:

- One or more critical systems have disabled.
- Although the building will be unavailable for an extended period of time, all of its systems are operational.
- The structure is available, but all systems are disabled.
- The structure and all of its systems are disabled.

The following events can cause a disaster, requiring the activation of this Disaster Recovery document:

- Fire.
- A flash flood occurs.
- Pandemic.
- Power failure.
- War.
- Theft.
- Terrorist Attacks
- Ransomware/Virus.

Risk Assessment

There are numerous possible disruptive threats that might strike at any time and disrupt normal corporate operations. This section contains the outcomes of our considerations after considering a wide range of potential dangers. Every possible natural disaster or emergency circumstance has been investigated. The emphasis here is on the extent of commercial interruption that each calamity could cause.

Table 4. 1 Types of risks and with risk assessment

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance			
Potential Disaster	**Probability Rating**	**Impact Rating**	**Brief Description Of Potential Consequences & Remedial Actions**
Flood	1	4	The last floor contains all critical equipment.
Fire	1	2	In the main computer centers, an FM200 suppression system has been installed. All floors include smoke and fire detectors.
Tornado	5	1	Most of the critical data is handled through cloud servers.
Electrical storms	2	5	Installed lighting conductors.
Act of terrorism	3	2	Security personnel with extensive training were hired.
Act of sabotage	2	3	A thorough recruitment process when hiring an employee. Background checks of hired employees.

Electrical power Failure	1	5	Redundant UPS system with auto standby generator that is tested regularly and remotely monitored 24 hours a day, 7 days a week. UPSs are also monitored remotely.
Loss of communications network services	1	4	Two T1 trunks are routed differently into the building. Voice network resilience and WAN redundancy.

Purpose of this DRP

If any secondary actions are undertaken, we shall ensure the safety and security of all employees and visitors to the organization's premises. After all individuals have been declared safe, the next priority will be to follow the measures outlined in this DRP to quickly restore services to normal. The following are examples:

- Keeping the company's resources, including as hardware, data, and physical IT assets, safe.
- Keeping IT downtime to a minimum.
- In the event of a disaster, keep the business going.

This DRP document also will explain how this document will be maintained and tested.

Scope

The EMC Cyber DRP takes into account all of the following factors:

- Infrastructure of networks.
- Infrastructure of servers
- System of communication.
- Data backup and storage systems
- Devices for data output.
- Computers for end-users.
- Software Systems for Organizations.
- Database Management Systems.
- Information Technology Documentation

Updates and Version Information

Any revisions, modifications, or updates to the DRP will be documented here. The Disaster Recovery Lead is responsible for ensuring that all existing copies of the DRP are updated. When the DRP is updated, EMC Cyber demands that the version number be updated to reflect this.

Table 4. 2 EMC Cyber DRP Updates and Version Information

Person Making the Change	Person in Charge of Change	Date of Change	Version Number	Notes
Sumith Fernando	DR Lead	01/01/2020	1.0	Initial version of Disaster Recovery Plan
Mahinda Rajakaruna	Infrastructure Lead	01/02/2021	2.0	New standby facilities have been added.
Suresh Fernando	CEO	01/03/2022	2.1	Replaced John Sugath Pallewatta as DR Lead

Disaster Recovery Teams and Responsibilities

Different organizations will be necessary to help the IT department restore regular operation to EMC Cyber personnel in the case of a disaster. The following are the different groups and their roles:

- Team for Disaster Recovery
- Team in charge of the network
- Team for Servers
- Team for Applications.
- Senior Management Team
- Teams specific to other organizations

Team for Disaster Recovery

The Disaster Management Team will be in charge of overseeing the entire recovery process. In the case of a disaster, they will be the first to respond. This group will assess the disaster and identify what steps must be taken to return the organization to normal operations.

During a disaster, this team will be in charge of all communication. They will specifically communicate with EMC Cyber employees, customers, vendors and suppliers, banks, and, if necessary, the media.

Roles and Responsibilities :

- After the Disaster Recovery Lead has declared a disaster, activate the DRP.
- Determine the disaster's scale and category.
- Determine how the disaster has impacted systems and processes.
- Notify the other disaster recovery teams of the disaster.
- Decide what the disaster recovery teams should do first.
- Keep the disaster recovery teams on track by setting expectations and goals ahead of time.
- Keep track of how much money they spent on catastrophe recovery.
- Ensure that all choices are made in accordance with EMC Cyber's DRP and policies.
- Prepare the alternative site for business operations to resume.
- Make that the backup site is completely operational and secure.
- Make a complete report detailing all of the steps followed during the catastrophe recovery process.
- Once the disaster has passed and normal business operations have been restored, notify the appropriate parties.
- This team will be responsible to summarize all costs and produce a report to the Disaster Recovery Lead detailing their operations throughout the disaster once EMC Cyber is back to normal.

Contact Details :

Table 4. 3 Contact details of Disaster Recovery Team

Name	Role/Title	Contact Option	Contact Number
Sugath Pallewatta	Primary Disaster Lead	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Email	sugath@emc.com
Shenal Smith	Secondary Disaster Lead	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Email	shenal@emc.com
Sandun Mahesh	Operation Coordinator	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Email	sandun@emc.com

Team in charge of the Network

The Network Team will be in charge of assessing network infrastructure damage and establishing data and voice network connectivity, including WAN, LAN, and any internal telephone connections, as well as telephony and data links with the outside world. They will be in charge of providing basic network operation and may be called upon to support other IT DR Teams as needed.

Roles and Responsibilities :

- In the event of disaster that does not need a move to a backup location, the company will evaluate which network services are not operational at the primary site.
- If multiple network services are affected, the team will prioritize service recovery in the order that will have the least impact on business.
- If third-party network services are used, the team will communicate and coordinate with them to ensure that connectivity is restored.
- In the case of a disaster that necessitates a move to backup facilities, the team will ensure that all network services are restored at the backup location.
- Employees will be given with connectivity in the following order when essential systems have been connected:
  - Everyone on the DR Teams.
  - Executive and C-level personnel.
  - All IT personnel.
  - All remaining workers
- In the backup facility, install and implement any tools, hardware, software, and systems that are required.
- In the primary facility, install and implement any equipment, hardware, software, and systems that are required.
- After EMC Cyber returns to normal operations, this team will review all costs and provide a report to the Disaster Recovery Lead detailing their work throughout the disaster.

Contact Details :

Table 4. 4 Contact details of Network Team

Name	Role/Title	Contact Option	Contact Number
Abishek Alwis	Network Manager	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Email	abishek@emc.com
Ashen Sigera	Network Administrator	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Email	ashen@emc.com
Ashini Koshila	Operation Coordinator	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Email	ashini@emc.com
Gayan Fernando	LAN Team Lead	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Email	gayan @emc.com
Ash Mahen	LAN Team Support	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Email	ash@emc.com
Yupun Abeykoon	LAN Team Lead	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Email	yupun@emc.com

Jayani Perera	LAN Team Support	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Email	jayani@emc.com

Team for Servers

In the case of a disaster, the Server Team will be responsible for supplying the physical server infrastructure required for the organization to run its IT operations and applications. They will be in charge of providing basic server operation and may be called upon to support other IT DR Teams as needed.

Roles and Responsibilities :

- In the event of a disaster that does not necessitate a move to a backup location, the team will determine which servers at the primary facility are unavailable.
- If numerous servers are affected, the team will prioritize server recovery in the order that will have the least impact on the business. The following tasks will be performed during recovery:
    - Examine any servers that have been damaged.
    - If necessary, restart and reload the servers.
- Ensure that system patches are kept up to date on secondary servers in standby facilities.
- Ensure that application patches are kept up to date on backup servers in standby facilities.
- Ensure that data copies are kept up to date on backup servers in standby facilities.
- Ensure that the secondary servers in the standby facility are properly backed up.
- Ensure that the standby facility's servers all follow the server policy.

Contact Details :

Table 4. 5 Contact details of Server Team

Name	Role/Title	Contact Option	Contact Number
Raveen Dissanayake	Server Operations Manager	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Email	raveen @emc.com
Sherini Fernando	Server Administrator	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Email	sherini @emc.com
Malika Perera	Server Admin Associate	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Email	malika @emc.com

Team for Applications

In the case of a disaster, the Applications Team will be in charge of ensuring that all business applications function as needed to accomplish business objectives. They will be in charge of guaranteeing and certifying proper application performance, as well as assisting other IT DR Teams as needed.

Roles and Responsibilities :

- The team will determine which applications are not operating at the primary site in the case of a disaster that does not necessitate migration to standby facilities.
- If many apps are affected, the team will prioritize application recovery in the order that will have the least impact on the business. The following tasks will be completed during recovery:
  - Examine the effect on the application procedure.
  - As needed, restart programs.
  - As necessary, patch, recode, or rebuild apps.
- Ensure that application patches are kept up to date on backup servers in standby facilities.
- Ensure that data copies are kept up to date on backup servers in standby facilities.
- Install and configure any necessary tools, software, and fixes in the standby facility.
- Install and configure any necessary tools, software, and fixes in the primary facility.
- After EMC Cyber returns to normal operations, this team will review all costs and provide a report to the Disaster Recovery Lead detailing their work throughout the disaster.

Contact Details :

Table 4. 6 Contact details of Application Team

Name	Role/Title	Contact Option	Contact Number
Sharah Ashika	Program Manager	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Email	sharah @emc.com
Hashan Fernando	Systems Administrator	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Email	hashan @emc.com
Malika Perera	App Coordinator	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Email	malika @emc.com

Senior Management Team

Any business decisions that are outside the scope of the Disaster Recovery Lead shall be made by the Senior Management Team. The Senior Management Team should make decisions such as building a new data center or relocating the primary site. This team will eventually report to the Disaster Recovery Lead.

Roles and Responsibilities :

- Ensure that the Disaster Recovery Team Lead is held accountable for his or her responsibilities.
- As needed, assist the Disaster Recovery Team Lead in his/her duties.
- Make decisions that will have an influence on the business. This can include decisions on the following topics:
    - Reconstruction of primary facilities.
    - Reconstruction of data centers.
    - Significant upgrades and investments in hardware and software.
    - Other business and financial decisions.

Contact Details :

Table 4. 7 Contact details of Management Team

Name	Role/Title	Contact Option	Contact Number
Suresh Fernando	CEO	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Email	suresh @emc.com
Nadun Fernando	COO	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Email	nadun @emc.com
Marlon Perera	Management Team Lead	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Email	marlon @emc.com

Disaster Recovery Call Tree (Hierarchy of stakeholders' roles)

Timing is important in a disaster recovery or business continuity issue, so EMC Cyber will employ a Call Tree to ensure that the necessary people are contacted as soon as possible.

- All Level 1 Members are contacted by the Disaster Recovery Team Lead (Blue cells).
- All Level 2 team members are contacted by Level 1 members (Green cells).
- All Level 3 team members are contacted by Level 1 members (Beige cells).
- All Level 3 team members are contacted by Level 2 members (Beige cells).
- If a team member is unavailable, the first caller takes up responsibility for all following calls (If a member of the Level 2 team is unavailable, the Level 1 team member contacts members of the Level 3 team directly.).

Table 4. 8 Disaster Recovery Call Tree

Contact	Office	Mobile	Home
DR Lead *Sugath Pallewatta*	011-3424356	077-5354932	031-7324355
Secondary Disaster Lead *Shenal Smith*	011-5324357	077-3424356	031-9842457
Operation Coordinator *Sandun Mahesh*	011-6524353	077-7854358	031-3624353
Facilities Team Lead *Abishek Alwis*	011-7324356	077-5354932	031-1624357
Facilities Team 1 *Sandun*	011-7854358	077-1624357	031-9324355
Network Manager *Abishek Alwis*	011-1324359	077-9324355	031-2254341
Network Administrator *Ashen Sigera*	011-7524351	077-5354932	031-8424353
Operation Coordinator *Ashini Koshila*	011-7424352	077-5354932	031-7424352
LAN Team Lead *Gayan Fernando*	011-8424353	077-3424356	031-2254341
LAN Team Supporter *Ash Mahen*	011-9324355	077-7324356	031-1324359
WAN Team Lead *Yupun Abeykoon*	011-1624357	077-5354932	031-7324356
WAN Team Supporter *Jayani Perera*	011-3624353	077-3424356	031-1624357

Server Operations Manager *Raveen Dissanayake*	011-9842457	077-7854358	031-7324355
Server Administrator *Sherini Fernando*	011-7324355	077-5354932	031-9842457
Server Admin Associate *Malika Perera*	011-3424356	077-1624357	031-3624353
Program Manager *Sarah Ashika*	011-1324359	077-9324355	031-1624357
System Administrator *Hashan Fernando*	011-7524351	077-5354932	031-9324355
App Coordinator *Malika Perera*	011-7424352	077-5354932	031-2254341
CEO *Suresh Fernando*	011-8424353	077-3424356	031-8424353
CCO *Nadun Fernando*	011-9324355	077-7324356	031-7424352
Management Team Lead *Marlon Perera*	011-1324359	077-5354932	031-2254341
Communications Team Lead *Janani Perera*	011-3624353	077-3424356	031-1324359
Call Center *Shalindra Teshan*	011-9842457	077-7854358	031-7324356
Finance Team Lead *Oshada Basnayake*	011-3624353	077-5354932	031-1624357
Accountant *Judith Michelle*	011-9842457	077-1624357	031-7324355

In the event of an emergency, a flow diagram might help clarify the call procedure.

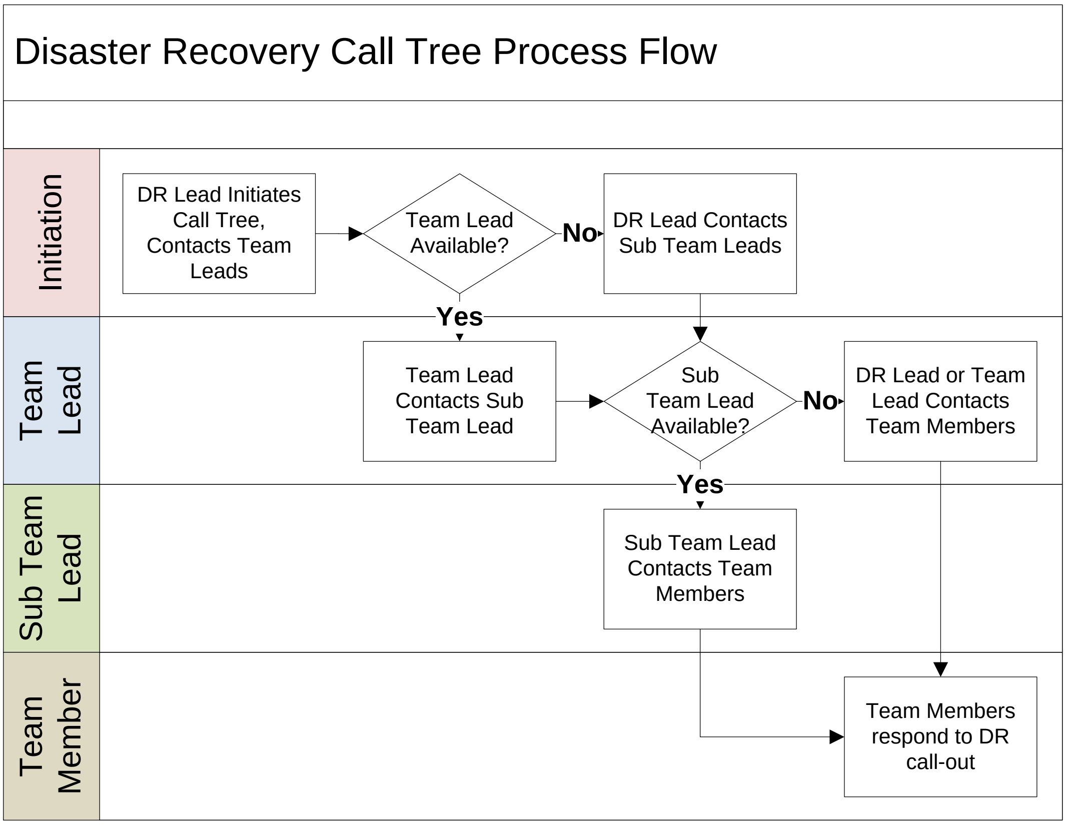

Disaster Recovery Call Tree Process Flow
Initiation
Team Lead
Sub Team Lead
Team Member
DR Lead Initiates Call Tree, Contacts Team Leads
Team Lead Available?
No
DR Lead Contacts Sub Team Leads
Yes
Team Lead Contacts Sub Team Lead
Sub Team Lead Available?
No
DR Lead or Team Lead Contacts Team Members
Yes
Sub Team Lead Contacts Team Members
Team Members respond to DR call-out

Figure 4. 1 Disaster Recovery Call Tree Process Flow

Recovery Facilities

Recovery Facilities Description

EMC Cyber has provided separate dedicated standby facilities to ensure that it can withstand a severe outage caused by a disaster. After the Disaster Recovery Lead has declared a disaster, the Disaster Command and Control Center or Standby facility will be used. This facility is separate from the primary facility. The current facility, located in Ragama (1054 Lankamatha Rd, Ragama), is 16 kilometers from the primary site.

The IT department and the Disaster Recovery teams will utilize the standby facility. It will serve as a central place where all disaster-related decisions will be taken. It will also serve as an EMC Cyber communications hub.

The following resources must always be available at the standby facility:

- Copies of the DRP.
- Server room with full redundancy.
- Server and storage infrastructure that is sufficient to support enterprise business activities.
- In the case of a disaster, DR teams and IT will need office space.
- Data and voice connectivity from the outside.
- Employees who work various shifts may require sleeping quarters.
- Facilities for cooking (including food, kitchen supplies and appliances).
- Bathrooms (Including toilets, showers, sinks and appropriate supplies).
- Employee parking spaces.

Facility Maintenance on Standby

Table 4. 9 Facility Maintenance on Standby

Maintenance Company	SPI Facility Services (Pvt) Ltd
Address	20 - 2/2 Lauries Rd, Colombo 00400
Phone Number	077-277022

Location of the Standby Facility

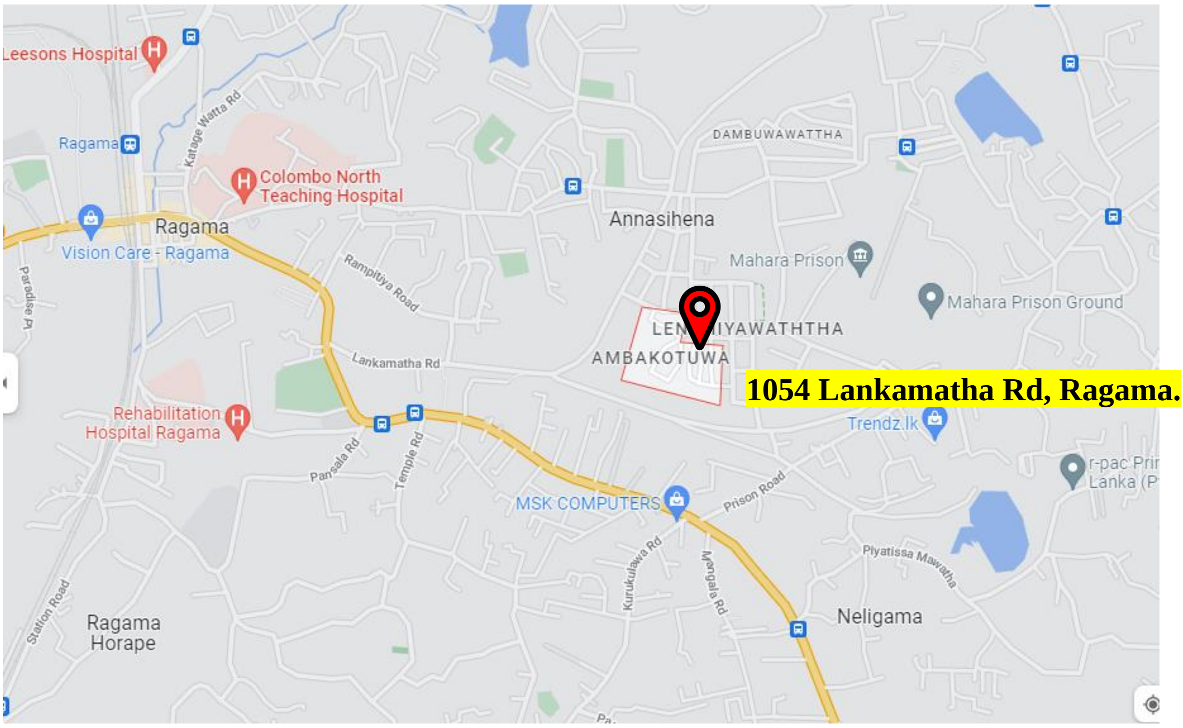


Figure 4. 2 Location of the Standby Facility

Directions to Recovery Facility

If the internet connection is unavailable, there are several ways of getting to the Standby Facility.

1) Fastest route due to traffic conditions.

- Via Colombo - Kandy Rd/Kandy Rd/A1
- 32min (15.8km)

* Continue to Baseline Rd/Dr Danister De Silva Mawatha/A1 [1 min (140 m)].

* Take Colombo - Katunayake Expy and Colombo - Kandy Rd/Kandy Rd/A1 to Dalupitiya Rd/B460 [22 min (10.8 km)].

* Continue on Dalupitiya Rd/B460 to your destination in Ragama [13 min (4.9 km)].

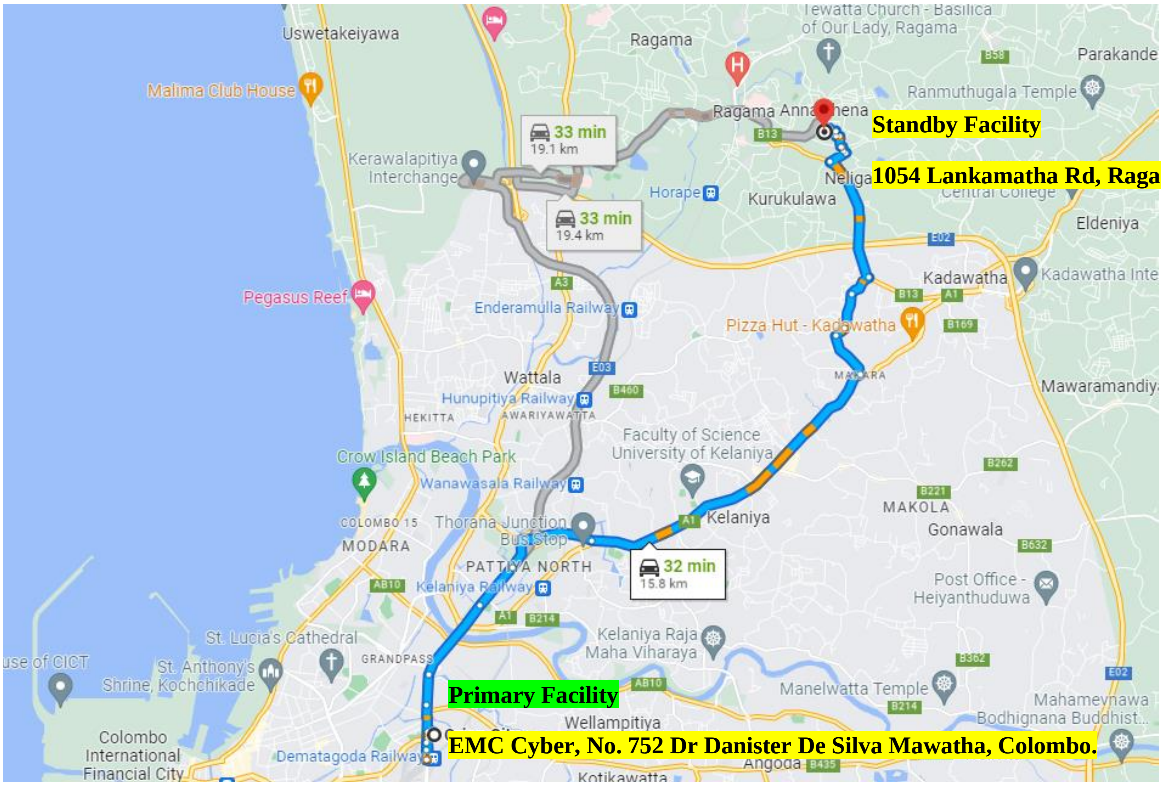


Figure 4. 3 Directions to Recovery Facility Fastest route

1) This route has tolls.

- Via Colombo - Katunayake Expy/E03
- 33min (19.4km)

* Continue to Baseline Rd/Dr Danister De Silva Mawatha/A1 [1 min (140 m)].

* Take Colombo - Katunayake Expy to CPSTL Muthurajawela Terminal Rd. Exit from Colombo - Katunayake Expy/E03 [16 min (11.8 km)].

* Continue on CPSTL Muthurajawela Terminal Rd. Take Dion Amarasekera Mawatha to Chilaw - Colombo Main Rd/Negombo Rd/Negombo-Colombo Main Rd/Puttalam - Colombo Rd/A3 in Magammana [4 min (2.1 km)].

* Continue on Ragama Rd/B13 to your destination in Ragama [12 min (4.7 km)].

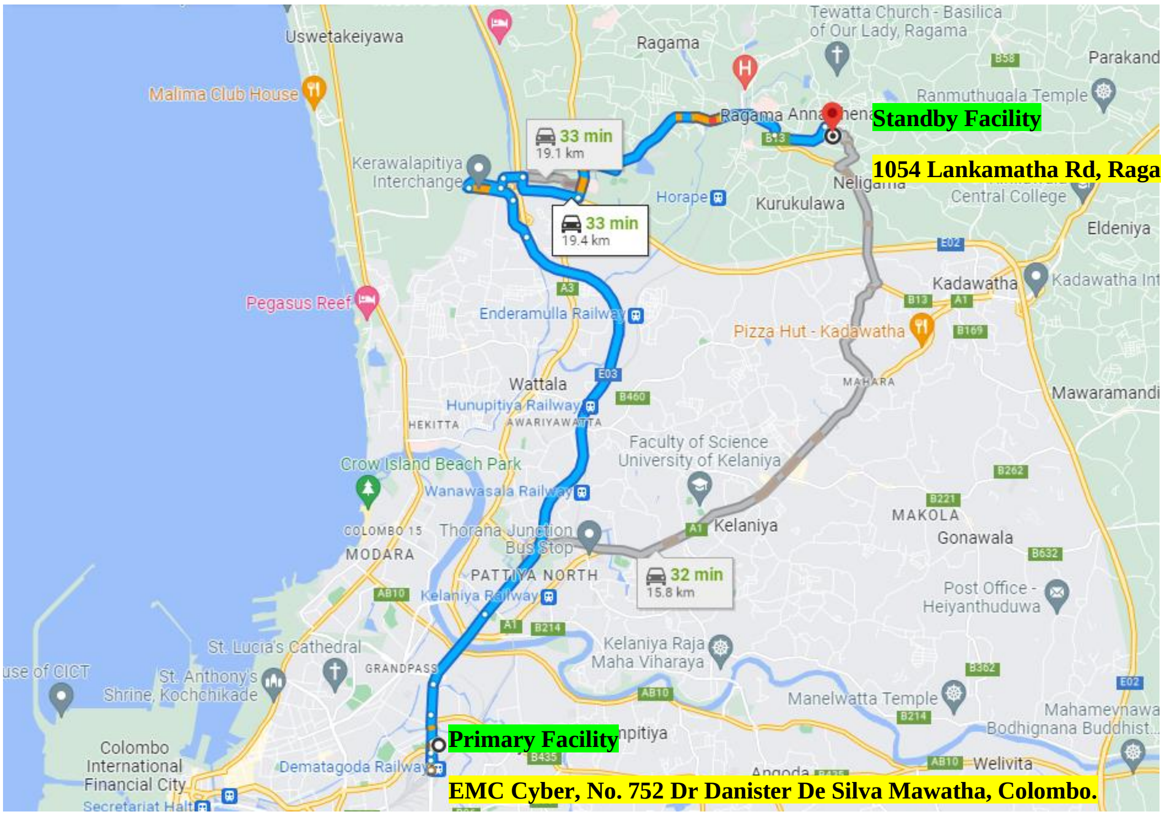

Standby Facility
1054 Lankamatha Rd, Ragama.
Primary Facility
EMC Cyber, No. 752 Dr Danister De Silva Mawatha, Colombo.
33 min
19.1 km
33 min
19.4 km
32 min
15.8 km
Ragama
Uswetakeiyawa
Kerawalapitiya Interchange
Wattala
Kelaniya
Kadawatha
Colombo International Financial City

Figure 4. 4 Directions to Recovery Facility alternative route

Transportation to the Standby Facility

Only the Disaster Recovery Teams and chosen staff of the IT department will work out of the standby facility in the case of a disaster. Since the standby site is 16 kilometers distant from the primary facility, employees will need to be provided with transportation and overnight accommodations if they do not own or are unable to use their own vehicles.

Taxi Providers :

Taxi Company 1	Shayaan Cab Service
Address	446/B Mullawatta, 10620
Phone Number	077 822 8985

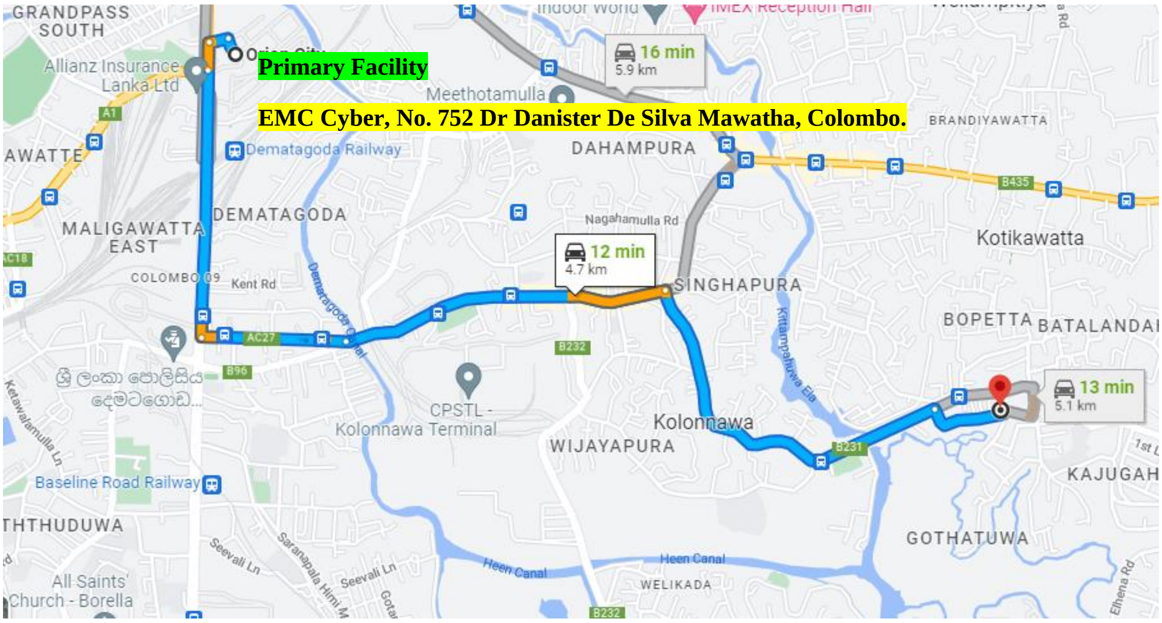


Figure 4. 5 Directions to Shayaan Cab Service

1) Fastest route due to traffic conditions.

- Via Kolonnawa Rd
- 32min (15.8km)

* Continue to Baseline Rd/Dr Danister De Silva Mawatha/A1 [1 min (140 m)].

* Continue on Baseline Rd/Dr Danister De Silva Mawatha. Take Kolonnawa Rd and to Mullawaththa Rd [11 min (4.3 km)].

* Turn right onto Mullawaththa Rd and Destination will be on the left [1 min (290 m)].

Taxi Company 2	TaxiGo Cab Service
Address	469E, Colombo 3 00400
Phone Number	077 083 3772

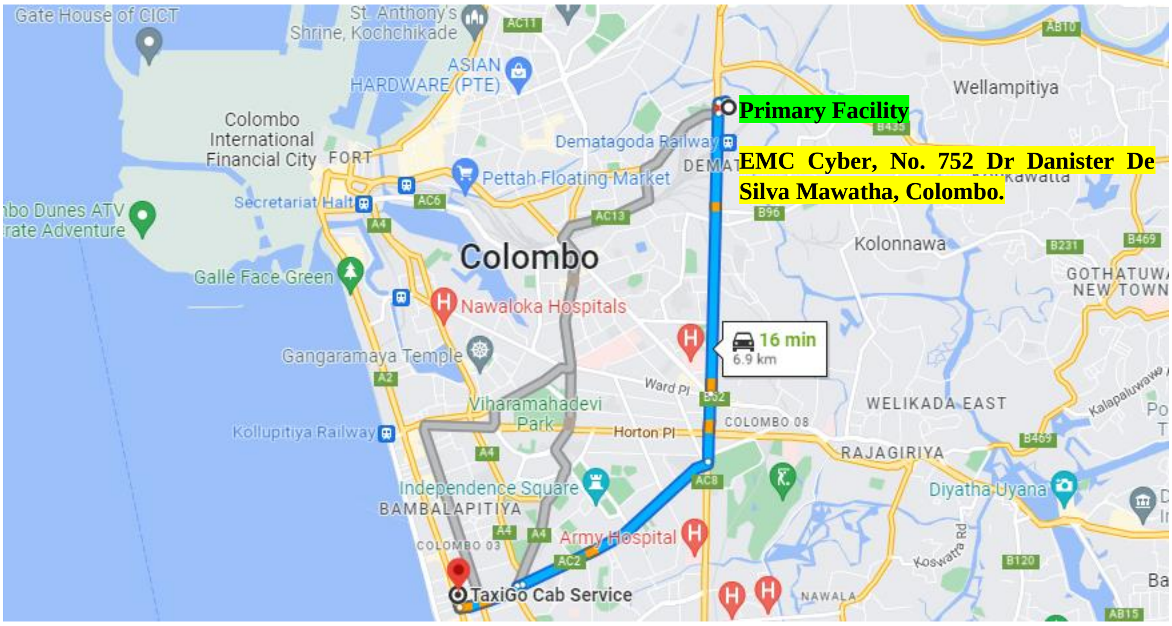


Figure 4. 6 Directions to TaxiGo Cab Service

1) Fastest route due to traffic conditions.

- Via Baseline Rd/Dr Danister De Silva Mawatha and Bauddhaloka Mawatha.
- 36 min (6.9 km)

* Continue to Baseline Rd/Dr Danister De Silva Mawatha/A1 [1 min (140 m)].

* Continue on Baseline Rd/Dr Danister De Silva Mawatha. Take Bauddhaloka Mawatha to Temple Ln [19 min (6.7 km)].

* Turn right onto Temple Ln and the Destination will be on the left [1 min (290 m)].

Data and Backups

Data backup is the process of copying data from one location to another in the event of a disaster, accident, or malicious attack. Data is the lifeblood of modern businesses and losing it can have devastating results and interrupt operations.

Table 4. 10 Data backup process

Rank	Data	Data Type	Back-up Frequency	Backup Location(s)
1	Internal data	Confidential information	Weekly	Cloud Backup Services
3	Personal Data	Personal information	Monthly	Servers
4	Engagement Data	Customer information	Monthly	Servers
5	Behavioral Data	Transactional information	Daily	Cloud Backup Services
6	Big data	Public information	Monthly	Servers
7	Time-stamped data	Public, Personally identifying information	Monthly	Cloud Backup Services

Communication during disaster

EMC Cyber may need to communicate with numerous parties in the event of a disaster to alert them of the consequences on the business, nearby locations, and timescales. EMC Cyber's Communications Team will be in charge of contacting all of the company's stakeholders.

Communication with employees

The second priority for the Communications Team will be to guarantee that the disaster has been communicated to the entire firm. The best and/or most practical means of contacting all employees will be employed, with priority given to the following techniques (in order of preference):

- E-mail (via corporate e-mail where that system still functions)
- E-mail (via non-corporate or personal e-mail)
- Call the employee's home phone number
- Call the employee's cell phone number

The following must be communicated to the employees:

- Is it okay for them to come into the office?
- If they are unable to enter the office, where should they head to?
- What services do they have access to now?
- What are their work responsibilities throughout the disaster?

Employee Contacts

Table 4. 11 Key Personal Contact Information

Name	Role/Title	Contact Option	Contact Number
Disaster Recovery Team			
Sugath Pallewatta	Primary Disaster Lead	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	sugath@emc.com
		Personal Email	sugath@gmail.com
Shenal Smith	Secondary Disaster Lead	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	shenal@emc.com
		Personal Email	shenal @gmail.com
Sandun Mahesh	Operation Coordinator	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	sandun@emc.com
		Personal Email	sandun @gmail.com
Network Team			

Abishek Alwis	Network Manager	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	abishek@emc.com
		Personal Email	abishek @gmail.com
Ashen Sigera	Network Administrator	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	ashen@emc.com
		Personal Email	ashen @gmail.com
Ashini Koshila	Operation Coordinator	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	ashini@emc.com
		Personal Email	ashini @gmail.com
Gayan Fernando	LAN Team Lead	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	gayan @emc.com
		Personal Email	gayan @gmail.com
Ash Mahen	LAN Team Support	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	ash@emc.com
		Personal Email	ash @gmail.com
Yupun Abeykoon	LAN Team Lead	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341

		Cooperate Email	yupun@emc.com
		Personal Email	yupun @gmail.com
Jayani Perera	LAN Team Support	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	jayani@emc.com
		Personal Email	jayani @gmail.com
Server Team			
Raveen Dissanayake	Server Operations Manager	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	raveen @emc.com
		Personal Email	raveen @gmail.com
Sherini Fernando	Server Administrator	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	sherini @emc.com
		Personal Email	sherini @gmail.com
Malika Perera	Server Admin Associate	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	malika @emc.com
		Personal Email	malika @gmail.com
Applications Team			

Sharah Ashika	Program Manager	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	sharah @emc.com
		Personal Email	sharah @gmail.com
Hashan Fernando	Systems Administrator	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	hashan @emc.com
		Personal Email	hashan @gmail.com
Malika Perera	App Coordinator	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	malika @emc.com
		Personal Email	malika @gmail.com
Senior Management Team			
Suresh Fernando	CEO	Work	011-3424356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	suresh @emc.com
		Personal Email	suresh @gmail.com
Nadun Fernando	COO	Work	011-6534356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	nadun @emc.com
		Personal Email	nadun @gmail.com

Marlon Perera	Management Team Lead	Work	011-8644356
		Mobile	077-5354932
		Home	031-2254341
		Cooperate Email	marlon @emc.com
		Personal Email	marlon @gmail.com

Communication with Clients

After all of the organization's employees have been informed of the event, the Communications Team will be responsible for alerting clients of the emergency and the impact it will have on the following:

- Impact on service offerings expected
- Impact on delivery timetables expected
- Impact on client information security that is expected
- Expected timelines

Communication with Vendors

After all of the organization's employees have been informed of the incident, the Communications Team will be responsible for informing vendors of the tragic incident and the impact it will have on the following:

- Changes in service needs
- Changes in delivery areas
- Adjustments to contacting information
- Expected timelines

The disaster situation will be communicated to critical vendors first. Vendors who are critical will be emailed first, then called to check that the message was delivered. After all critical vendors have been contacted, all other vendors will be contacted.

Vendors include both those that provide day-to-day services to the company and those who supply the IT department with hardware and software. Should additional IT infrastructure be necessary, the Communications Team will operate as a bridge between the DR Team leads and vendor contacts.

Critical Vendors :

Table 4. 12 Critical Vendors list

Company Name	Point of Contact	Phone Number	E-mail
S.P Electronics	Sanath Nishantha	076 135 5500	sanath@gmail.com
Coolbit Software Solutions	Teshan Fernando	031 456 7890	teshan@gmail.com
Networkstore.lk	Kiralu Fernando	011-3424356	kiralu@gmail.com
Colombo Net Solutions (Pvt) Ltd	Jasmine Perera	077-5354932	jasmine@gmail.com
CeylonIT.lk	Yasas Wickramaratne	031-2254341	yasas@gmail.com
Hikvision Authorized Dealer	Suresh Narayan	077-5354932	suresh@gmail.com

External Contacts :

Table 4. 13 External Contacts list

Company	Point of Contact	Phone Number
Electricity Board	Hashan Fernando	076 135 5500
Water Board	Marlon Perera	031 456 7890
Property Manager	Sahan Fernando	011-3424356
Site Security	Rosmine Perera	077-5354932
Media	Sandaru Wickramaratne	031-2254341
Insurance Company	Manush Narayan	077-5354932
Telecom	Sumudu Perera	076 135 5500
Workstation	Ilham Fernando	031 456 7890

Activation of the Disaster Recovery Plan

The first responsibility in the event of a disaster at EMC Cyber is to guarantee that all personnel are safe and accounted for. Following that, efforts must be made to prevent future damage to the facility and to minimize the disaster's impact on the company. Dealing with a disaster can be broken down into the following steps, regardless of whatever category it fits into:

1) Identifying and declaring disasters
2) Activation of DRP
3) Disaster communication
4) Evaluation of current damage and prevention of further harm
5) Activation of the standby facility
6) Set up IT operations
7) Primary facility repair and reconstruction

Activation of DRP

The Disaster Recovery Lead will begin the activation of the DRP by triggering the Disaster Recovery Call Tree once a disaster has been publicly declared. In the calls that the Disaster Recovery Lead makes, the following information will be delivered and should be passed on to subsequent calls:

- There has been a disaster.
- The disaster's nature (if known).
- The initial estimate of the disaster's magnitude (if known).
- The initial estimate of the disaster's consequences (if known).
- The initial estimate of the disaster's expected duration (if known).
- So far, the actions have been taken.
- Actions to be taken before to the Disaster Recovery Team Leads meeting.
- The location for the Disaster Recovery Team Leads' meeting has been set.
- The meeting of the Disaster Recovery Team Leads has been scheduled.

- Any more important information

Evaluation of current damage and prevention of further harm

Before any EMC Cyber personnel can access the primary facility after a disaster, the appropriate authorities must first make sure the facilities are safe to enter.

The Facilities Team will be the first to examine the primary facilities once it has been determined that it is safe to do so. The Disaster Management, Networks, Servers, and Operations Teams will be allowed to inspect the building when the Facilities Team has concluded their examination and filed its report to the Disaster Recovery Lead. Within one week following the first disaster, all teams must generate an initial report on the damage and submit it to the Disaster Recovery Lead.

Each team must identify potential places where further damage might be avoided and take the appropriate steps to secure EMC Cyber's assets throughout their examination of their relevant regions. To secure the facilities, any essential repairs or preventative measures must be implemented; these expenses must first be approved by the Disaster Recovery Team Lead.

Activation of Standby Facility

When the Disaster Recovery Lead concludes that the primary facility is no longer functional or operational to sustain normal business activities, the Standby Facility will be formally activated.

The Facilities Team will be responsible with restoring the Standby Facility to operational status once this determination has been made. After the Disaster Recovery Lead convenes a meeting of the various Disaster Recovery Team Leads at the Standby Facility to assess next measures, this should be done. The following are the next steps:

- Identifying the systems that are impacted
- Ranking of impacted systems' importance
- Recovery measures for high critical systems
- Assign responsibilities for high critical systems
- Recovery schedule for systems with high criticality
- Recovery measures for medium critical systems
- Assign responsibilities for medium critical systems
- Recovery schedule for systems with medium criticality
- Recovery measures for low critical systems
- Assign responsibilities for low critical systems
- Recovery schedule for systems with low criticality
- Tasks to be completed at the Standby Facility
- Identifying the communications activities that must be completed at the Standby Facility
- Identifying the tasks that must be completed at the Primary Facility
- Determination of additional tasks necessary at the Primary Facility
- Determination of the next steps to take

The Facilities, Networks, Servers, Applications, and Operations teams must ensure that their duties, as outlined in the "Disaster Recovery Teams and Responsibilities" part of this document, are carried out quickly and efficiently so that the other teams are not negatively affected.

Insurance

A number of insurance policies have been implemented as part of the company's disaster recovery and business continuity plans. Types of errors, directors’ and officers’ liability, general liability, and business interruption insurance are just a few examples.

Table 4. 14 Insurance policies

Policy Name	Period	Amount	Responsible	Next Renewal Date
Building	5	10 Lakhs	Finance	07/05/2023
Life	5	2 Lakhs	Finance	23/03/2023
Inventory	5	1.5 Lakhs	Finance	13/12/2023

Plan Testing & Maintenance

While efforts will be made to develop this DRP in the most full and accurate manner feasible at first, it is essentially impossible to address all potential concerns at once. Furthermore, the enterprise's Disaster Recovery requirements will evolve over time. Because of these two considerations, this plan will need to be tested on a regular basis to detect faults and errors, and it will need to be updated to resolve them.

Maintenance

The DRP will be updated on a monthly basis or if there is a major system update or upgrade, whichever comes first. In order to perform this assignment, the Disaster Recovery Lead will be responsible for updating the entire document and will be allowed to request information and changes from other employees and departments within the firm. Maintenance of the plan will involve (but is not limited to) the following:

- Making certain that call trees are up to date
- Ensure that all team lineups are updated.
- Evaluating the plan to check that all of the directions are still applicable to the company.
- Making sure that the plan meets with any new legal criteria
- Other special organizational maintenance objectives

If a member of a Disaster Recovery Team leaves the organization, it is the Disaster Recovery Lead's responsibility to designate a new team member.

Testing

EMC Cyber is committed to making this DRP operational. Every month, the DRP should be tested to ensure that it is still working. The plan will be put to the test as follows:

Simulation Test :- Normal operations are not interrupted by a disaster simulation. A simulation test should cover hardware, software, staff, communication systems, protocols, supplies and forms, documentation, transportation, utilities, and alternate sites processing. Validated checklists, on the other hand, can provide a decent level of assurance in many of these situations. Before beginning the proposed simulation, thoroughly examine the results of the previous tests to ensure that the lessons learnt from the previous parts of the cycle have been applied.

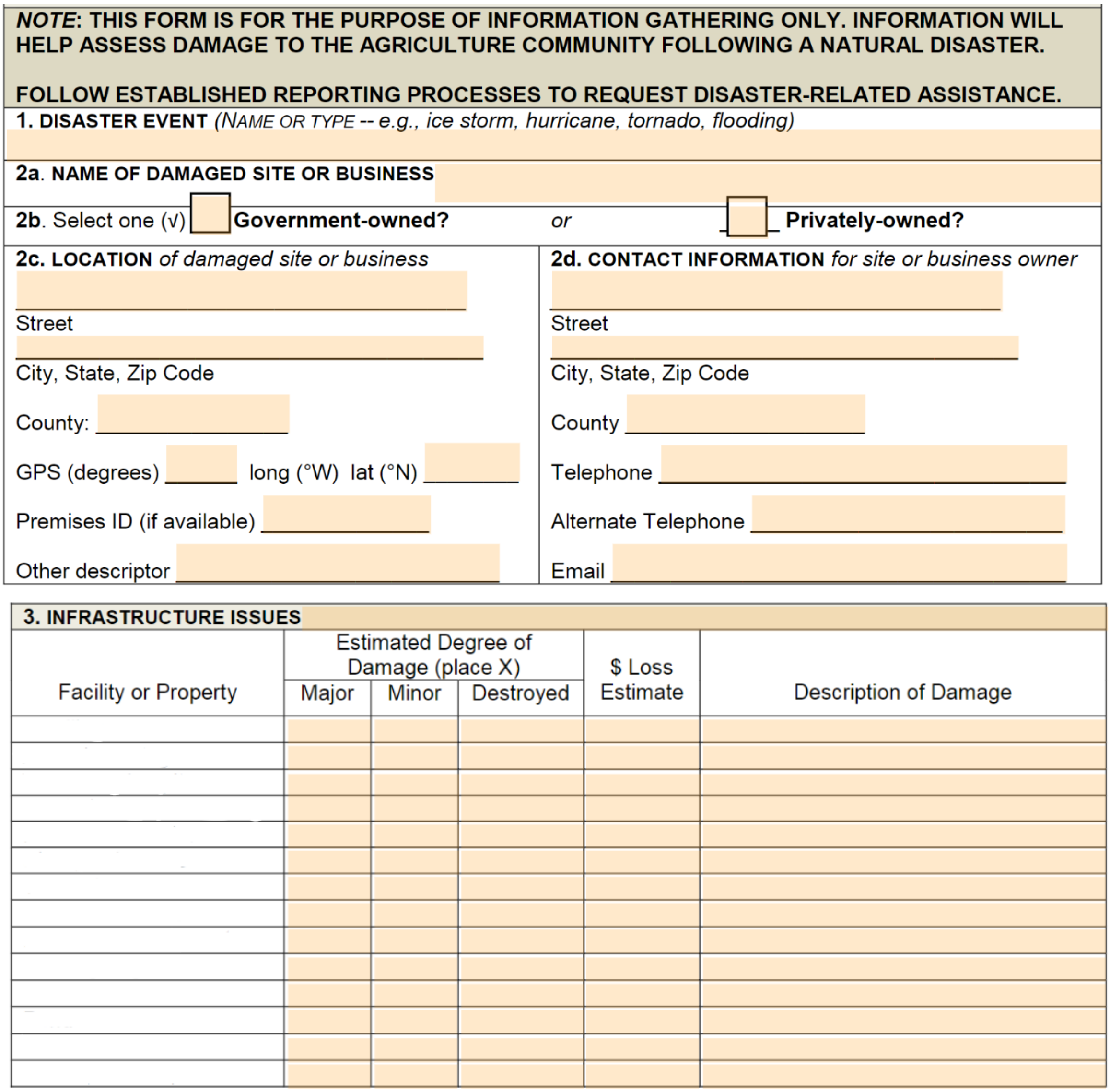
Call tree Testing

Call Trees are an important aspect of the DRP, and EMC Cyber demands that they be checked every month to ensure that they are working properly. The following tests will be carried out:

- The Disaster Recovery Lead starts the call tree and assigns a code word to the first set of employees.
- The code word is transferred from one caller to the next.
- All members of the Disaster Recovery Team are asked for the code word the next day at work.
- Any problems with the call tree or contact information will be addressed as soon as possible.

Suggested Forms

Damage Assessment Form



NOTE: THIS FORM IS FOR THE PURPOSE OF INFORMATION GATHERING ONLY. INFORMATION WILL HELP ASSESS DAMAGE TO THE AGRICULTURE COMMUNITY FOLLOWING A NATURAL DISASTER.

FOLLOW ESTABLISHED REPORTING PROCESSES TO REQUEST DISASTER-RELATED ASSISTANCE.

1. DISASTER EVENT *(NAME OR TYPE -- e.g., ice storm, hurricane, tornado, flooding)*

2a. NAME OF DAMAGED SITE OR BUSINESS

2b. Select one (√) □ **Government-owned?** *or* □ **Privately-owned?**

2c. LOCATION *of damaged site or business*

Street

City, State, Zip Code

County: __________

GPS (degrees) _____ long (°W) lat (°N) _____

Premises ID (if available) __________

Other descriptor __________

2d. CONTACT INFORMATION *for site or business owner*

Street

City, State, Zip Code

County __________

Telephone __________

Alternate Telephone __________

Email __________

3. INFRASTRUCTURE ISSUES

Facility or Property	Estimated Degree of Damage (place X)			$ Loss Estimate	Description of Damage
	Major	Minor	Destroyed		

Figure 4. 7 Damage Assessment Form

Disaster Recovery Event Recording Form

Table 4. 15 Disaster Recovery Event Recording Form

Activities Undertaken by DR Team	Date and Time	Outcome	Follow-On Action Required

Mobilizing the Disaster Recovery Team Form

Table 4. 16 Mobilizing the Disaster Recovery Team Form

Description of Emergency:					
Date Occurred:					
Date Work of Disaster Recovery Team Completed:					
Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

Mobilizing the Business Recovery Team Form

Table 4. 17 Mobilizing the Business Recovery Team Form

Description of Emergency:					
Date Occurred:					
Date Work of Business Recovery Team Completed:					
Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

Monitoring Business Recovery Task Progress Form

Table 4. 18 Monitoring Business Recovery Task Progress Form

Recovery Tasks *(Order of Priority)*	Person(s) Responsible	Completion Date		Milestones Identified	Other Relevant Information
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Communication Form

Table 4. 19 Communication Form

Groups of Persons or Organizations Affected by Disruption	Persons Selected To Coordinate Communications to Affected Persons / Organizations		
	Name	Position	Contact Details
Customers			
Management & Staff			
Suppliers			
Media			
Stakeholders			
Others			

Business Process/Function Recovery Completion Form

Table 4. 20 Business Process/Function Recovery Completion Form

Name Of Business Process	
Completion Date of Work Provided by Business Recovery Team	
Date of Transition Back to Business Unit Management *(If different than completion date)*	

I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.

Business Recovery Team Leader Name: ______________________________________

Signature: ____

Date: ___________________________

(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)

I confirm that above business process is now acceptable for normal working conditions.

Name: ____

Title: ____

Signature: ____

Date: ___________________________

4.4 Roles of stakeholders in the company to implement security audit recommendations

4.4.1 Stakeholders in EMC Cyber

A stakeholder in a business organization is an individual or a group who has a strong interest in the organization's potential outcome. These stakeholders are divided into two groups: internal and external stakeholders, each of whom has a strong interest in the organizational process and outcome.

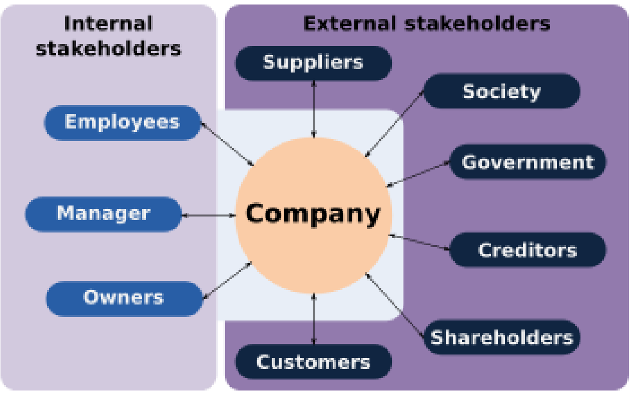


Figure 4. 8 Stakeholders in EMC Cyber

Internal Stakeholders :

Individuals and groups within an organization who are directly involved in the operations of the organization. Employees, CEOs, directors, and managers are examples of internal stakeholders in our company.

- Employees - These are the ones who create an organization's operational workforce.
- Managers - Managers are the people in charge of organizing, planning, controlling, and leading the operations of the entire organization.
- Directors - This is the group of people who decide, create, and implement the organization's policies.
- Owners - They own the company and serve on the board of directors. Eventually, they can also retain company shares.

External Stakeholders :

External stakeholders are defined as a group outside of an organization that is not directly involved with its operations but has a direct impact on the organization's actions and decisions.

- Customers - Customers, also known as clients, are potential beneficiaries of an organization's services.
- Suppliers - They can supply physical needs as well as third-party services to an organization to help it function.
- Government - This is the regulatory body that regulate and guides both businesses and consumers through its rules and policies.
- Creditors - a creditor is a person or an institution that extends its services by allowing a business to borrow money in order to run the business and is intended to be repaid in the future.
- Shareholders - Shareholders are the legal owners of the stock shares of the company. They can be individuals, businesses, or institutions.

4.4.2 Security audit recommendations for EMC Cyber

A security audit is an essential component of any business in order to keep strong security protection. It is carried out by recognizing, examining, and improving the existing information technology infrastructure through organization and identification of potential vulnerabilities.

By implementing a strict IT security audit, the organization can ensure that its cybersecurity protections are up to date and meet current standards, allowing it to effectively defend against the security risk posed by cyber-attacks, which can cripple the systems.

Before we can monitor growth and identify suspicious activity, we need to know where we are and what "normal" operating system behavior looks like. As previously stated, this is where establishing a security baseline comes into play. If we haven't already determined our security baseline, I recommend collaborating with at least one external auditor to do so. We can also create our own baseline using monitoring and reporting operating systems.

The information we need for a security risk assessment is frequently dispersed across multiple security management consoles. Finding all of these details is a tedious and time-consuming task. Using a third-party management tool, we strive to centralize our user account permissions, event logs, and so on in one easy-to-access platform. This helps to ensure that we are ready when compliance auditors arrive. If we are hiring an external auditor, we must also practice readiness by outlining all of our security objectives in detail. As a result, our auditor has a complete picture of exactly what they're auditing.

4.4.3 The advantages of performing routine security audits on an information system.

- By conducting security audits, we can determine whether the current security strategies and policies are adequate or should be improved.
- The organization could determine whether or not the security training module is operational.
- Immaterial software and hardware from the organization could be identified.
- To maximize security and reduce costs, the organization could cancel unnecessary service providers and resources.
- To make sure the organization complies with the most recent regulatory standards.

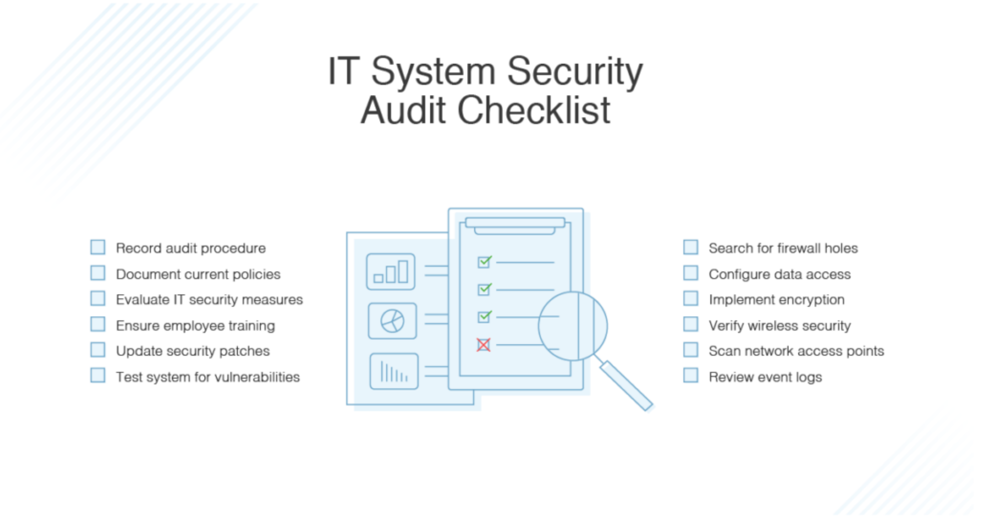

IT System Security Audit Checklist
□ Record audit procedure
□ Document current policies
□ Evaluate IT security measures
□ Ensure employee training
□ Update security patches
□ Test system for vulnerabilities
□ Search for firewall holes
□ Configure data access
□ Implement encryption
□ Verify wireless security
□ Scan network access points
□ Review event logs

Figure 4. 9 IT Security Audit Checklist

Conclusion

This entire assignment is based on assuming the role of External Security Analyst investigate and report on potential cyber security threats to LockHead web site, applications and infrastructure. After the investigation I needed to plan a solution and how to implement it according to standard software engineering principles. The purpose of this assignment is to improve knowledge and skills in Security in Computing.

Assess IT security risks in an organization by identifying types of security risks and proposing a method for assessing and treating IT security risks. Then, describing IT security solutions, including identifying the potential impact on IT security of incorrectly configured firewall policies and third-party VPNs, implementing a DMZ, static IP, and NAT in a network, and implementing network monitoring systems, with supporting reasons.

Following that, Examining control mechanisms for organizational IT security with Managing organizational security through security policies, disaster recovery plans, and IT security audits.

References

Lucidchart. 2022. Entity-Relationship Diagram Symbols and Notation | Lucidchart.

[ONLINE] Available at: https://www.lucidchart.com/pages/ER-diagram-symbols-and-meaning#:~:text=Cardinality%20and%20ordinality,instance%20in%20the%20related%20entity..

[Accessed 2 15 July 2022].

Security, S. 2020. Decoded: Examples of How Hashing Algorithms Work.

Available at: https://cheapsslsecurity.com/blog/decoded-examples-of-how-hashing-algorithms-work/#:~:text=A%20hash%20function%20is%20a,fixed%20length%20%E2%80%93%20the%20hash%20value.

[Accessed: 15 July 2022].

What is the CIA Triad? Definition and Examples | SecurityScorecard. [no date].

Available at: https://securityscorecard.com/blog/what-is-the-cia-triad#:~:text=Confidentiality%2C%20Integrity%2C%20and%20Availability.,organization’s%20security%20procedures%20and%20policies.

[Accessed: 15 July 2022].

What is the CIA Triad? Definition, Explanation, Examples - TechTarget. 2022.

Available at: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[Accessed: 15 July 2022].

The CIA triad in Cryptography - GeeksforGeeks. 2018.

Available at: https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/#:~:text=When%20talking%20about%20network%20security,Confidentiality

[Accessed: 15 July 2022].

University, G. [no date]. Confidentiality, Integrity, and Availability (CIA) triad | CCNA Security#.

Available at: https://geek-university.com/ccna-security/confidentiality-integrity-and-availability-cia-triad/

[Accessed: 15 July 2022].

Principles of Information System Security. [no date].

Available at: https://www.tutorialspoint.com/principles-of-information-system-security#:~:text=Confidentiality%2C%20integrity%2C%20and%20availability%20are,Triad%20is%20their%20collective%20name.

[Accessed: 15 July 2022].

Fruhlinger, J. [no date]. The CIA triad: Definition, components and examples | CSO Online.

Available at: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

[Accessed: 15 July 2022].

Unitrends 2021. The CIA Triad and Its Importance in Data Security | Unitrends.

Available at: https://www.unitrends.com/blog/cia-triad-confidentiality-integrity-availability

[Accessed: 20 July 2022].

What is Role-Based Access Control | RBAC vs ACL & ABAC | Imperva. 2019.

Available at: https://www.imperva.com/learn/data-security/role-based-access-control-rbac/#:~:text=Role%2Dbased%20access%20control%20(RBAC)%2C%20also%20known%20as,enable%20access%20to%20authorized%20users.&text=Using%20this%20table%2C%20you%20can%20assign%20permissions%20to%20each%20user.

[Accessed: 20 July 2022].

What is Data Encryption | From DES to Modern Algorithms | Imperva. 2021.

Available at: https://www.imperva.com/learn/data-security/data-encryption/

[Accessed: 20 July 2022].

Passwords | Information Security. [no date].

Available at: https://security.tcnj.edu/security-guidelines/passwords/

[Accessed: 20 July 2022].

A Simple Guide to Two-Factor Authentication. 2016.

Available at: https://www.imperva.com/blog/guide-to-two-factor-authentication/#:~:text=Two%2Dfactor%20authentication%20can%20secure,of%20web%20applications%20and%20sites.&text=Two%2Dfactor%20authentication%20assists%20in%20reducing%20vulnerability%20after%20a%20breach.

[Accessed: 20 July 2022].

Glossary of Application Security, Electronic Design Automation and Semiconductor IP Terms | Synopsys. [no date].

Available at: https://www.whitehatsec.com/glossary/content/data-validation

[Accessed: 20 July 2022].

Data backup: Why it’s important + strategies to protect your information. [no date].

Available at: https://us.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html

[Accessed: 1 August 2022].

What is Access Control? - Citrix. [no date].

Available at: https://www.citrix.com/solutions/secure-access/what-is-access-control.html#:~:text=Access%20control%20is%20a%20fundamental,appropriate%20access%20to%20company%20data.

[Accessed: 1 August 2022].

Zhao, J. 2021. Use an Audit Trail to Improve Security, Maintain Compliance, and Streamline Processes - Security Boulevard.

Available at: https://securityboulevard.com/2021/10/use-an-audit-trail-to-improve-security-maintain-compliance-and-streamline-processes/

[Accessed: 1 August 2022].

What is Data Integrity and How Can You Maintain it? 2021.

Available at: https://www.varonis.com/blog/data-integrity

[Accessed: 1 August 2022].

What is Failover? | Barracuda Networks. [no date].

Available at: https://www.barracuda.com/glossary/failover

[Accessed: 1 August 2022].

Tozzi, C. 2020. Best Practices for Increasing Data Availability - Precisely.

Available at: https://www.precisely.com/blog/data-availability/best-practices-increasing-data-availability

[Accessed: 1 August 2022].

What Is a DMZ and Why Would You Use It? | Fortinet. [no date].

Available at: https://www.fortinet.com/resources/cyberglossary/what-is-dmz

[Accessed: 1 August 2022].

NAT Explained - Network Address Translation. 2018.

Available at:
https://www.youtube.com/watch?v=FTUV0t6JaDA&ab_channel=PowerCertAnimatedVideos

[Accessed: 1 August 2022].

What is Network Address Translation? | Avi Networks. 2022.

Available at: https://avinetworks.com/glossary/network-address-translation/#:~:text=Network%20Address%20Translation%20(NAT)%20conserves,into%20legal%2C%20globally%20unique%20addresses.

[Accessed: 10 August 2022].

Network Address Translation Definition | How NAT Works | Computer Networks | CompTIA. [no date].

Available at: https://www.comptia.org/content/guides/what-is-network-address-translation

[Accessed: 10 August 2022].

Network Address Translation Definition | How NAT Works | Computer Networks | CompTIA. [no date].

Available at: https://www.comptia.org/content/guides/what-is-network-address-translation

[Accessed: 10 August 2022].

Private IP Address vs Public IP Address - IP With Ease. 2020.

Available at: https://ipwithease.com/public-ip-vs-private-ip/

[Accessed: 10 August 2022].

Risk Assessment Matrix 4 by 4 example with FREE Download. 2019.

Available at: https://www.stakeholdermap.com/risk/risk-assessment-matrix-4x4.html

[Accessed: 10 August 2022].

Risk Management Plan Template | FREE Download. [no date].

Available at: https://www.stakeholdermap.com/project-templates/risk-management-plan.html

[Accessed: 16 August 2022].

ldmahat 2019. Risk Heat Map - LDM | Risk Management.

Available at: https://lumbmahat.com/risk-heat-map/

[Accessed: 16 August 2022].

What is Risk Management and Why is it Important? 2021.

Available at: https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important

[Accessed: 16 August 2022].

What is the ISO 31000 Risk Management Standard? 2021.

Available at: https://www.techtarget.com/searchsecurity/definition/ISO-31000-Risk-Management

[Accessed: 16 August 2022].

What is a security audit? - Definition from TechTarget. 2022.

Available at: https://www.techtarget.com/searchcio/definition/security-audit

[Accessed: 16 August 2022].

Security, A. 2022. 10 Must Have IT Security Policies for Every Organization.

Available at: https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/

[Accessed: 16 August 2022].

40 Data Protection Regulations You Need to Know About | Endpoint Protector. 2019.

Available at: https://www.endpointprotector.com/blog/10-data-protection-regulations-you-need-to-know-about/

[Accessed: 16 August 2022].

Michalsons 2022. Data Protection Laws, Acts or Regulations - Michalsons.

Available at: https://www.michalsons.com/focus-areas/privacy-and-data-protection/data-protection-laws-acts-regulations-around-the-globe

[Accessed: 16 August 2022].