. Higher Nationals

Internal verification of assessment decisions – BTEC (RQF)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **INTERNAL VERIFICATION – ASSESSMENT DECISIONS** | | | | | | | | |
| **Programme title** | BTEC Higher National Diploma in Computing | | | | | | | |
| **Assessor** | Mr.Isura Kulathilake | | **Internal Verifier** | | Mr.Lakindu Premachandra | | | |
| **Unit(s)** | **Unit 05:**  **Security** | | | | | | | |
| **Assignment title** | EMC Cyber | | | | | | | |
| **Student’s name** | Ranudi Gayathmie Kariyapperuma | | | | | | | |
| **List which assessment criteria the Assessor has awarded.** | **Pass** | | **Merit** | | | | **Distinction** | |
|  | |  | | | |  | |
| **INTERNAL VERIFIER CHECKLIST** | | | | | | | | |
| **Do the assessment criteria awarded match those shown in the assignment brief?** | | Y/N | |  | | | | |
| **Is the Pass/Merit/Distinction grade awarded justified by the assessor’s comments on the student work?** | | Y/N | |  | | | | |
| **Has the work been assessed accurately?** | | Y/N | |  | | | | |
| **Is the feedback to the student:**  Give details:   * Constructive? * Linked to relevant assessment criteria? * Identifying opportunities for improved performance? * Agreeing actions? | | Y/N Y/N  Y/N Y/N | |  | | | | |
| **Does the assessment decision need amending?** | | Y/N | |  | | | | |
| **Assessor signature** | | ranudigk@gmail.com | | | | **Date** | | 18/05/2023 |
| **Internal Verifier signature** | |  | | | | **Date** | |  |
| **Programme Leader signature** (if required) | |  | | | | **Date** | |  |

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

Higher Nationals - Summative Assignment Feedback Form

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name/ID** | Ranudi Gayathmie Kariyapperuma KIR/X -00104243 | | |
| **Unit Title** | **Unit 05:**  **Security** | | |
| **Assignment Number** | 5 | **Assessor** |  |
| **Submission Date** | 17/05/2023 | **Date Received 1st submission** | 17/05/2023 |
| **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.

ranudigk@gmail.com

**Student’s Signature: Date:** 17.05.2023

**(*Provide E-mail ID*) (*Provide Submission Date*)**

Assignment Brief

|  |  |
| --- | --- |
| Student Name /ID Number | Ranudi Gayathmie Kariyapperuma KIR/X -00104243 |
| **Unit Number and Title** | Unit 5- Security |
| Academic Year | 2020/2021 |
| Unit Tutor | Isura Kulathilaka |
| **Assignment Title** | EMC Cyber |
| Issue Date | 10.04.2023 |
| Submission Date | 17.05.2023 |
| IV Name & Date |  |
| **Submission Format:** | |
| The submission should be in the form of an individual written report written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using Harvard referencing system. Please provide in- text citation and an end list of references using Harvard referencing system.  Section 4.2 of the assignment required to do a 15 minutes presentation to illustrate the answers. | |

|  |
| --- |
| **Unit Learning Outcomes:** |
| **LO1** Assess risks to IT security.  **LO2** Describe IT security solutions.  **LO3** Review mechanisms to control 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.  GThe 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).** |

0

**Grading Rubric**

|  |  |  |
| --- | --- | --- |
| **Grading Criteria** | **Achieved** | **Feedback** |
| **LO1 Assess risks to IT security** |  |  |
| **P1** Identify types of security risks to organisations. | Achieved |  |
| **P2** Describe organizational security procedures. | Achieved |  |
| **M1** Propose a method to assess and treat IT security risks. | Achieved |  |
| **LO2 Describe IT security solutions** |  |  |
| **P3** Identify the potential impact to IT security of incorrect configuration of firewall policies and thirparty VPNs. | Achieved |  |
| **P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security. | Achieved |  |
| **M2** Discuss three benefits to implement network monitoring systems with supporting reasons. | Achieved |  |
| **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. | Achieved |  |
| **P6** Explain data protection processes and regulations as applicable to an organisation. | Achieved |  |
| **M3** Summarise the ISO 31000 risk management methodology and its application in IT security. | Achieved |  |
| **M4** Discuss possible impacts to organizational security resulting from an IT security audit. | Achieved |  |
| **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. | Achieved |  |
| **P8** List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion. | Achieved |  |
| **M5** Discuss the roles of stakeholders in the organisation to implement security audit recommendations. |  |  |
| **D3** Evaluate the suitability of the tools used in an organisational policy. |  |  |

G

**ACKNOWLEDGEMENT**

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

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

CONTENT

[Activity 1 21](#_Toc135960154)

[LO1 : Assess risks to IT security. 21](#_Toc135960155)

[P1 : Identify types of security risks to organizations. 21](#_Toc135960156)

[1 What Means Security in IT industry? 21](#_Toc135960157)

[1.1 Types of Security 21](#_Toc135960158)

[ Network Security 21](#_Toc135960159)

[ Cloud Security 21](#_Toc135960160)

[ Application Security 22](#_Toc135960161)

[ Internet of Things Security 22](#_Toc135960162)

[1.2 Security Attacks. 23](#_Toc135960163)

[1.3 What is IT Security Risk ? 24](#_Toc135960164)

[1.4 Types of Security Risks for Companies 24](#_Toc135960165)

[ Vulnerability 24](#_Toc135960166)

[1. Program Flows 25](#_Toc135960167)

[2. Zero day 25](#_Toc135960168)

[3. Features 25](#_Toc135960169)

[4. User Errors 25](#_Toc135960170)

[ Threats 26](#_Toc135960171)

[1 .Malware Attacks 26](#_Toc135960172)

[2 .Social Engineering Attacks 26](#_Toc135960173)

[3. Supply chain Attacks 27](#_Toc135960174)

[4. Man in the middle Attack 27](#_Toc135960175)

[5 . Denial of Service Attack 27](#_Toc135960176)

[2. Organizational Risks 28](#_Toc135960177)

[3. CIA Triad Concept 29](#_Toc135960178)

[3.1 CIA Main 3 Principles 29](#_Toc135960179)

[3.2 Importance of applying CIA Triad Concept to EMC Cyber. 30](#_Toc135960180)

[P2 : Organizational security procedures. 31](#_Toc135960181)

[1.Security Procedures that should have in an organization. 31](#_Toc135960182)

[Common Security Procedures 31](#_Toc135960183)

[1.2 Technical Security Procedures 31](#_Toc135960184)

[LO2 : IT security solutions 33](#_Toc135960185)

[P3 : The potential impact to IT security of incorrect configuration of firewall policies and third party 33](#_Toc135960186)

[VPNs. 33](#_Toc135960187)

[1 . Firewalls 33](#_Toc135960188)

[1.1 History of Firewall. 33](#_Toc135960189)

[1.2. Types of Firewalls 34](#_Toc135960190)

[1.3 . Common Firewall Configuration mistakes 35](#_Toc135960191)

[P5 Discuss risk assessment procedures. 42](#_Toc135960192)

[P6 : Data protection processes and regulations as applicable to an organization. 44](#_Toc135960193)

[P7 : Design and implement a security policy for an organisation 46](#_Toc135960194)

[P8 :The main components of an organizational disaster recovery plan, justifying the reasons for inclusion. 47](#_Toc135960195)

[1 . Disaster Recovery Plan 47](#_Toc135960196)

[1.1Steps of Disaster Recovery Plan 47](#_Toc135960197)

[1.2 Importance of Disaster Recovery Plan 47](#_Toc135960198)

[1.3 Disaster Recovery Plan 48](#_Toc135960199)

[2. Disaster Recovery Plan for EMC Cyber 49](#_Toc135960200)

[M1: A method to assess and treat IT security risks 54](#_Toc135960201)

[1. Organizational security risks and Solutions to reduce it 54](#_Toc135960202)

[2 IT security Risks and Solutions to reduce it 56](#_Toc135960203)

[References 64](#_Toc135960204)

**TABLE OF FIGURES**

[Figure 1 : IT Security (https://www.exabeam.com) 22](#_Toc135960205)

[Figure 2 : Active Attacks vs Passive Attacks (https://intellipaat.com) 23](#_Toc135960206)

[Figure 3: What is a Security Risk( https://www.wealthmanagement.com/ ) 24](#_Toc135960207)

[Figure 4 : Vulnerabilities (https://www.spiceworks.com) 25](#_Toc135960208)

[Figure 5 : Organizational Risks (https://evacuteer.org) 28](#_Toc135960209)

[Figure 6 : CIA triad Concept (https://websitesecuritystore.com) 30](#_Toc135960210)

[Figure 7 : Security Procedures in organization (https://linfordco.com) 32](#_Toc135960211)

[Figure 8 : Firewalls (https://forumautomation.com) 34](#_Toc135960212)

[Figure 9 : VPN (www.kaspersky.com) 37](#_Toc135960213)

[Figure 10 : Disaster Recovery Plan slide 1 (made by author) 49](#_Toc135960214)

[Figure 11 : Disaster Recovery Plan slide 2 (made by author) 49](#_Toc135960215)

[Figure 12 : Disaster Recovery Plan slide 3 (made by author) 50](#_Toc135960216)

[Figure 13 : Disaster Recovery Plan slide 4 (made by author) 50](#_Toc135960217)

[Figure 14 : Disaster Recovery Plan slide 5 (made by author) 51](#_Toc135960218)

[Figure 15 : Disaster Recovery Plan slide 6 (made by author) 51](#_Toc135960219)

[Figure 16 : Disaster Recovery Plan slide 7 (made by author) 52](#_Toc135960220)

[Figure 17 : Disaster Recovery Plan slide 8 made by author) 52](#_Toc135960221)

[Figure 18 : Disaster Recovery Plan slide 9 (made by author) 53](#_Toc135960222)

**Table of Tables**

[Table 1 : Active attacks vs Passive Attacks 23](#_Toc135960223)

[Table 2 : Risk Assessment (Made by Author ) 43](#_Toc135960224)

[Table 3 : Policy table ( Made by Author) 46](#_Toc135960225)

[Table 4 : Disaster Recovery Plan (Made by Author) 48](#_Toc135960226)

# Activity 1

# LO1 : Assess risks to IT security.

## P1 : Identify types of security risks to organizations.

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

### What Means Security in IT industry?

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

### Types of Security

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

#### Network Security

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

So, in every Company should monitor their network usually, refresh the passwords and also should maintain and monitor the internet access. Companies should always implement firewalls and antivirus protections for their network to prevent threats. (lint, 2023)

#### Cloud Security

Clouds is a platform that can store data safely. So, when choosing a cloud user should choose a trust worthy platform that has a minimum of risk. In cloud-based platforms there has a usually safe instructions that need to be applied when user get into clouds. So, when a user need to protect the cloud system it is good that Acorn’s cloud protect. (lint, 2023)

#### Application Security

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

For an example when people play games sometimes when the game is over it will pop up an advertisement to click when user click the advertisement it can be a virus so then it can spread all over your device and get your important details through your device. So, people should be aware when using applications and also need to apply safe guard for every application in the device. (lint, 2023)

#### Internet of Things Security

Internet of things means that devices that connected to the Internet. In internet there should always protect the devices that connected because it can easily get threats. It is important to have a security risk assessment to find vulnerabilities in users’ device and network. (lint, 2023)

A picture containing diagram

Description automatically generated

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

### 1.2 Security Attacks.

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

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

Table 1 : Active attacks vs Passive Attacks

Graphical user interface

Description automatically generated

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

### 1.3 What is IT Security Risk ?

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

(Anon., n.d.)

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

Graphical user interface, application

Description automatically generated

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

### Types of Security Risks for Companies

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

#### Vulnerability

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

##### Program Flows

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

##### Zero day

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

##### Features

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

##### User Errors

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

A picture containing text, parking, meter, screenshot

Description automatically generated

Figure 4 : Vulnerabilities (https://www.spiceworks.com)

### Threats

In RFC 4949 explain what threat is ,

A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm. (Hell, 2021)

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

* + **Natural Threats** - Natural threats are that happens naturally like floods, tsunamis, tornados.

etc...

* **Intentional Threats** - This threat means that someone purposely harms a computer or

organization. Information. Examples like computer crimes and credit

card theft.

* **Unintentional Threats** – This threat happens accidently like deleting some important

information on the computer by mistake.

In computer threats there are many types of it . Like,

#### 1 .Malware Attacks

In malware attacks their main types :

* Viruses -Viruses means that spreads between computers and damage the data and

software.

* Worms - Spreads all over the network immediately
* Trojan – This malware threat is coming like a game , apps, email attachments if user click

it will spread in the computer.

* Adware – It means that the treat is coming as an advertisement.
* Spyware – Collect user activity data without user knowing.

#### 2 .Social Engineering Attacks

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

* Baiting – this type of threats are coming as a gift cards or something that valuable

for victim and victim give them sensitive information to the attacker.

* Phishing – Phishing threat is coming as an email to attack victim.
* Vishing
* Smishing
* Tailgating

#### 3. Supply chain Attacks

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

#### 4. Man in the middle Attack

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

#### 5 . Denial of Service Attack

* Denial of Service Attack is target in a large volume of a system .
* HTTP flood DDOS
* SYN flood DOOS
* UDP flood DDOS
* ICMP flood
* NTP amplification

**6. Injection Attacks**

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

Main types of Injection Attacks are ,

* SQL injection
* Code injection
* OS Command injection
* LDAP injection

### 2. Organizational Risks

* Even EMC Cyber company may have organizational risks. It is better to know organizational risks to prevent from them .the risks are,
* Business Risk
* Economic Risk
* Financial Risk
* Health & Safety
* Risk Identification
* Human Error
* Credit Risk
* Country Risk

Diagram

Description automatically generated

Figure 5 : Organizational Risks (https://evacuteer.org)

### 3. CIA Triad Concept

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

* Confidentially
* Availability
* Integrity

For an example for begin a fire there should be main three elements that are oxygen , Fuel , heat if one of those were

missing then it will not begin a fire so this example equal to CIA concept if the one of the principles were missing

then it can’t be a successful Defense mechanism.

#### 3.1 CIA Main 3 Principles

1 . Confidentially

In CIA Concept the C letter is known as Confidentially . Protect information and for look the protect.

information can get access only to the authorized ones. In Companies identify sensitive data as

employee data , accounts etc... To secure data it is better to implement security mechanisms like

passwords , encryptions etc...

1. Integrity

In CIA concept I stand for Integrity. So, in this principle authorized person can change the data under this concept. For an example In a Company when a data that should be change then as a authorized

The person supervisor will change it but if the person that is under the supervisor cant change data. If that person changes it will not be accepted. Also the data can be changed when transmitting data , when storing data and when use data .

1. Availability

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

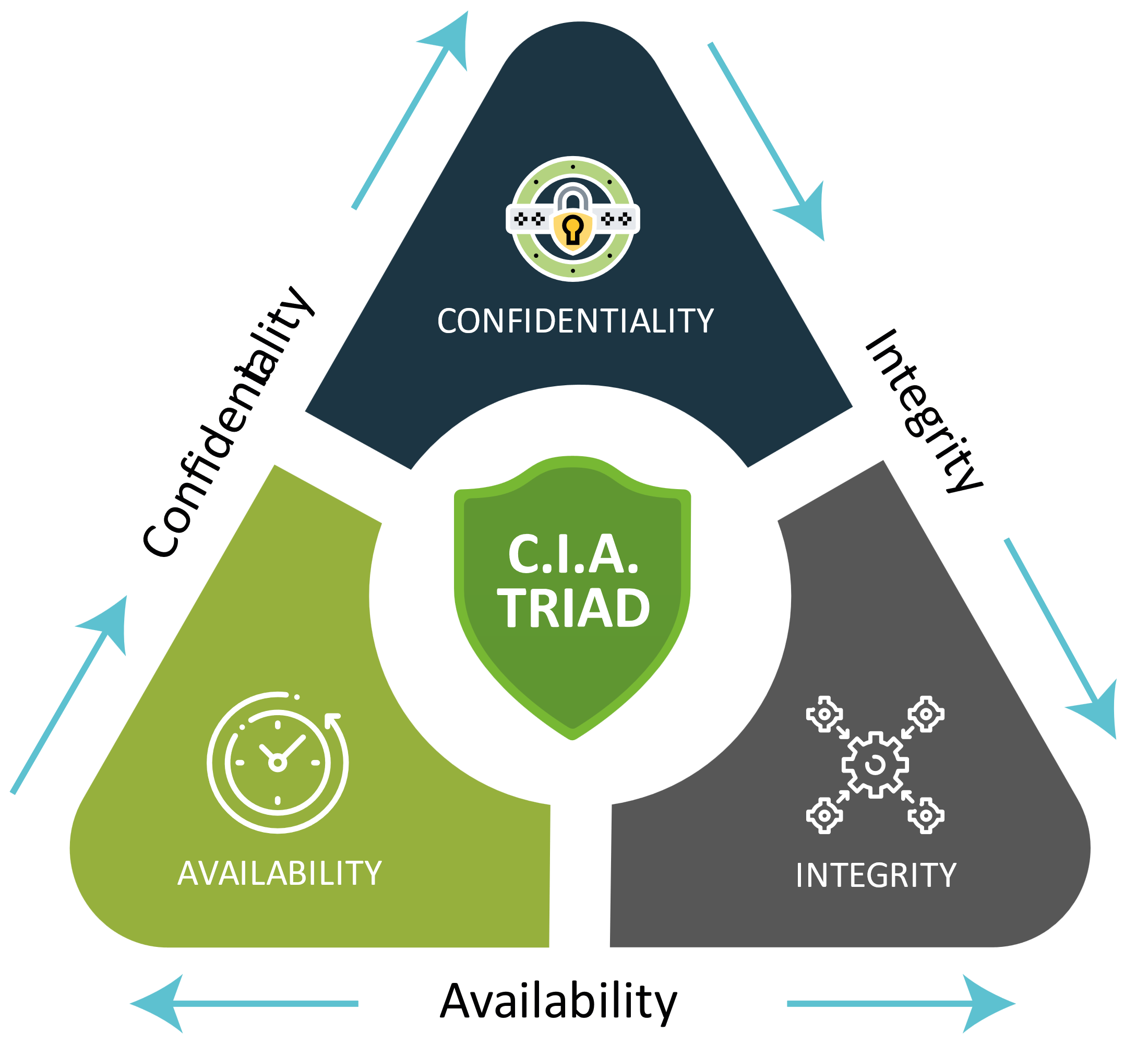
****

Figure 6 : CIA triad Concept (https://websitesecuritystore.com)

#### 3.2 Importance of applying CIA Triad Concept to EMC Cyber.

Using CIA concept is very important because EMC Cyber also can secure data more efficiently using this

Method. Mainly 3 elements that are confidentiality , integrity and availability have power to secure very

Important data. Also, EMC can introduce the CIA concept to EMC clients that other companies also can save

the data Secure in this concept. In confidentiality can protect data an allows to look authorized users

unauthorized users can’t get any information in confidentiality part , in integrity part only authorized person

can change data and in availability information should always available when needed them.

## P2 : Organizational security procedures.

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

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

### 1.Security Procedures that should have in an organization.

#### Common Security Procedures

* Emergency Procedures

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

* Security Training

In security Training helps individually understand about the security procedures correctly. Security training is

provided through classes and online resources .This is great starting points to improve their business security in

work place.

#### 1.2 Technical Security Procedures

* Access Control

Access control is a security measure that restricts or manages people's access to particular places. Physical

barriers like locks, gates, fences, and security personnel can be used to implement these, as well as electronic

systems like key cards or biometric scanners. Access control is frequently used in conjunction with other

security measures including alarm systems and CCTV surveillance.

* CCTV Monitoring

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

* Alarm Systems

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



Figure 7 : Security Procedures in organization (https://linfordco.com)

# LO2 : IT security solutions

## P3 : The potential impact to IT security of incorrect configuration of firewall policies and third party

## VPNs.

### 1 . Firewalls

Firewalls are a defense like a wall. This is a network security model . On a set of rules firewalls monitor

network traffic that incoming and outgoing through the network system and give the permission to enter the

data or block the data. The important of firewall is that viruses or malware can’t go through a firewall to

attack a computer .

#### 1.1 History of Firewall.

* Gen 1 Virus - The beginning of Firewall is in the late 1980s . It was built on virus focused. In the

Time period was the internet was found after building these firewalls then

businesses focused on developing anti- virus software.

* Gen 2 Network - This was built in the 1990s. This was built to prevent the internet from attack. In

This generation had the advanced firewall.

* Gen 3 Application – In this generation hidden security flaws can also capture and also because of

this IPS was started build that time period .

* Gen 4 Payload - This generation was found for highly invasive and to trace hard attacks . This

Specific attacks were happening in the 2019 – 2010 time.

* Gen 5 Mega - In 2017 this was launched, and this was the threat prevent measures that globally

recognized.

#### 1.2. Types of Firewalls

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

1. Packet filtering firewalls
2. Application-level firewalls
3. Circuit Level Gateway

**Packet Filtering Firewalls**

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

* + - 1. **Application -level Firewalls**

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

* + - 1. **Circuit Level Gateways**

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

A diagram of a firewall and earth

Description automatically generated with medium confidence

Figure 8 : Firewalls (<https://forumautomation.com>)

#### 1.3 . Common Firewall Configuration mistakes

Gartner said that 99% of firewall breaches are caused by configuration errors. A wrong configuration can

affect. the whole organization system. If a firewall was damaged attackers can easily

get into their network and can easily access it. The mostly common mistakes are known as,

* Relaying on Import/Export

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

* Using Broad Policies

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

* Forgetting outbound rules

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

* Neglecting Security Features

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

1. **. VPN**

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

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

* **Site-to-Site VPN**

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

* **Intranet VPN**

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

* **Extranet VPNs**

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

* 1. **The Benefits of VPN**
* dependable encryption
* covering up your whereabouts
* Availability of regional connections
* Transferring data securely

A person holding a virtual screen

Description automatically generated with low confidence

Figure 9 : VPN (www.kaspersky.com)

**P4 : How implementing a DMZ, static IP and NAT in a network can improve Network Security**

1. **DMZ**

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

* 1. **Benefits of DMZ**

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

* **Improved Network Security**

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

* **Controlled Access**

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

* **Network segmentation:**

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

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

* **Scalability and Flexibility**

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

1. **Static IP**

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

**2.1 Benefits Of Static IP**

* **Fixed Address**

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

* **Reliable Remote Access**

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

* **Services that require hosting**

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

* **DNS Management**

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

1. **NTP**

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

* 1. **Benefits of NTP**
* **Time Synchronization**

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

* **Client-Server Architecture**

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

* **Stratum Levels**

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

* **Redundancy and fault tolerance**

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

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

* **Applications and Importance**

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

## P5 Discuss risk assessment procedures.

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

Table 2 : Risk Assessment (Made by Author )

4

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

The risk assessment ,

1 Recognized the danger

2 Evaluate the danger

3 Control the risk

## P6 : Data protection processes and regulations as applicable to an organization.

Data Protection process and regulations play a key role in the security of an organization. It takes actions to stop

the Threats and protects confidential information from damaging or destroying Data. ‘

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

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

* **General Data Protection policy (GDPR):**

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

* **Data Security Measures**

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

* **Consent and Privacy Notices**

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

## P7 : Design and implement a security policy for an organisation

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

Table 3 : Policy table ( Made by Author)

## P8 :The main components of an organizational disaster recovery plan, justifying the reasons for inclusion.

### 1 . Disaster Recovery Plan

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

#### 1.1Steps of Disaster Recovery Plan

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

#### 1.2 Importance of Disaster Recovery Plan

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

#### 1.3 Disaster Recovery Plan

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

Table 4 : Disaster Recovery Plan (Made by Author)

#### 2. Disaster Recovery Plan for EMC Cyber



Figure 10 : Disaster Recovery Plan slide 1 (made by author)

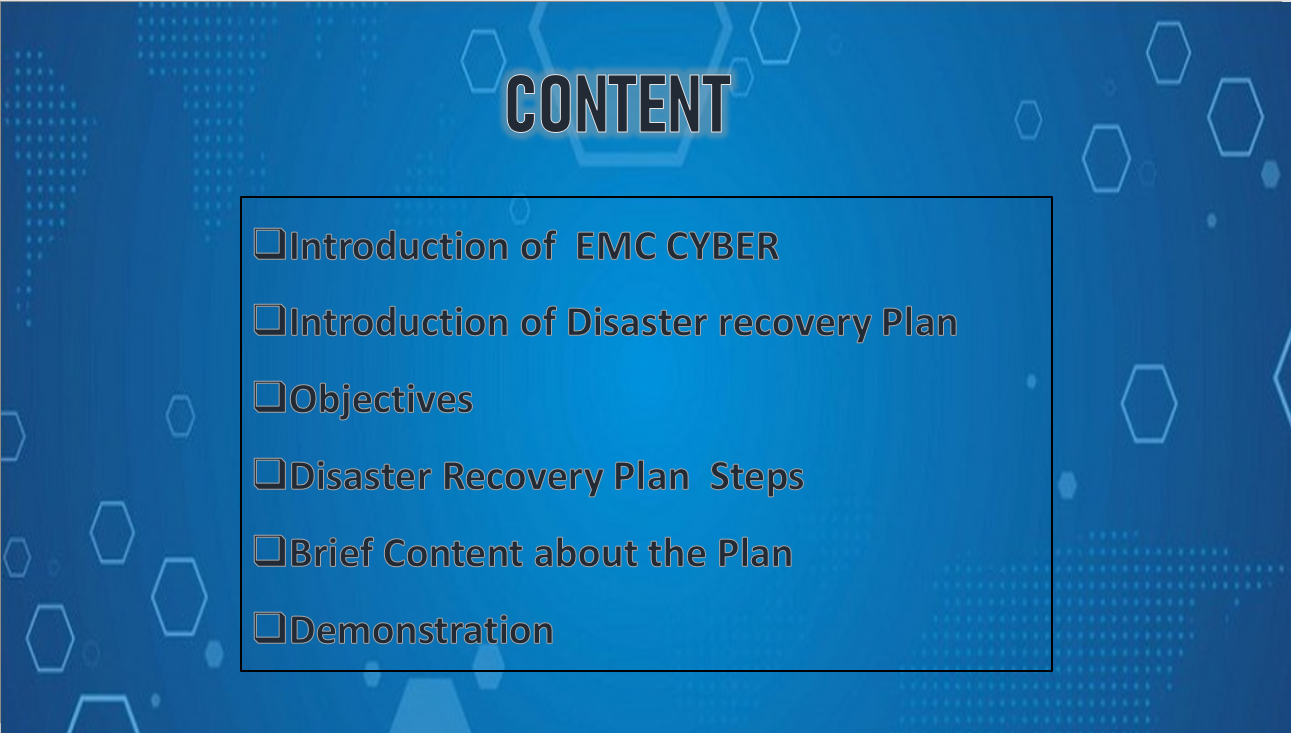


Figure 11 : Disaster Recovery Plan slide 2 (made by author)

A blue and black text on a blue background

Description automatically generated with low confidence

Figure 12 : Disaster Recovery Plan slide 3 (made by author)

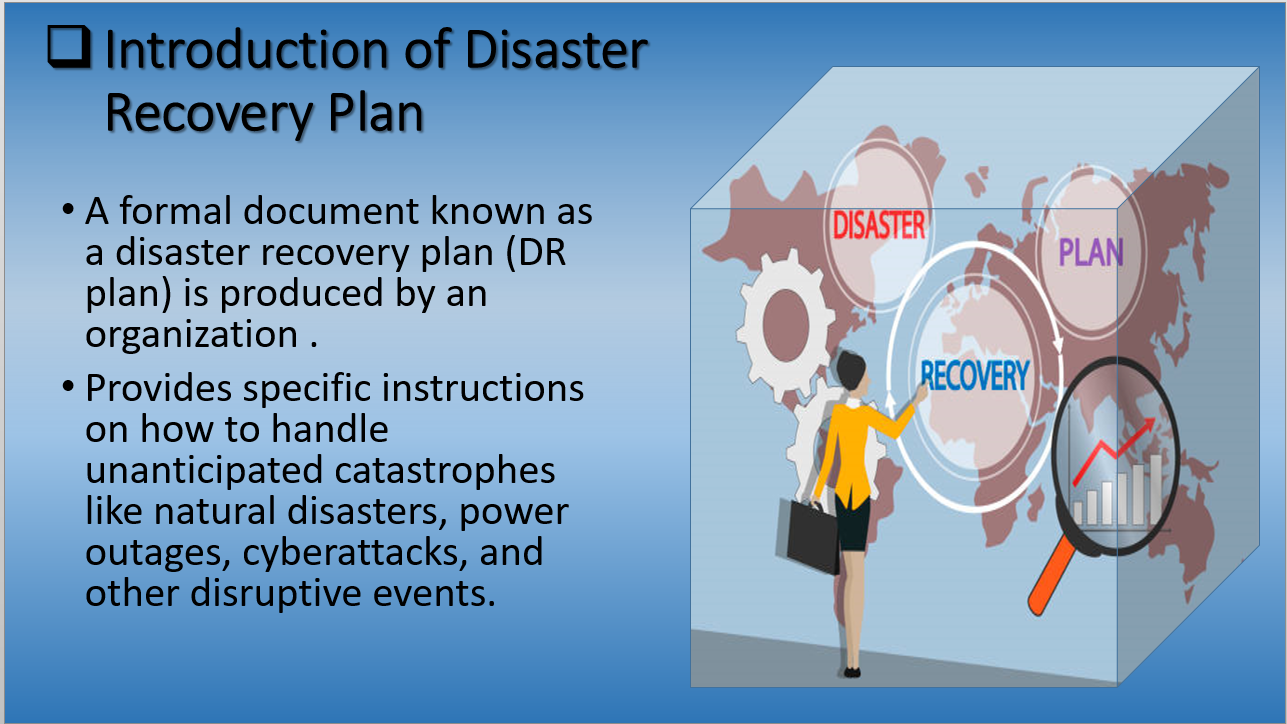


Figure 13 : Disaster Recovery Plan slide 4 (made by author)

A picture containing text, screenshot, graphic design, graphics

Description automatically generated

Figure 14 : Disaster Recovery Plan slide 5 (made by author)

A picture containing text, screenshot, font

Description automatically generated

Figure 15 : Disaster Recovery Plan slide 6 (made by author)

A picture containing text, screenshot, diagram, font

Description automatically generated

Figure 16 : Disaster Recovery Plan slide 7 (made by author)

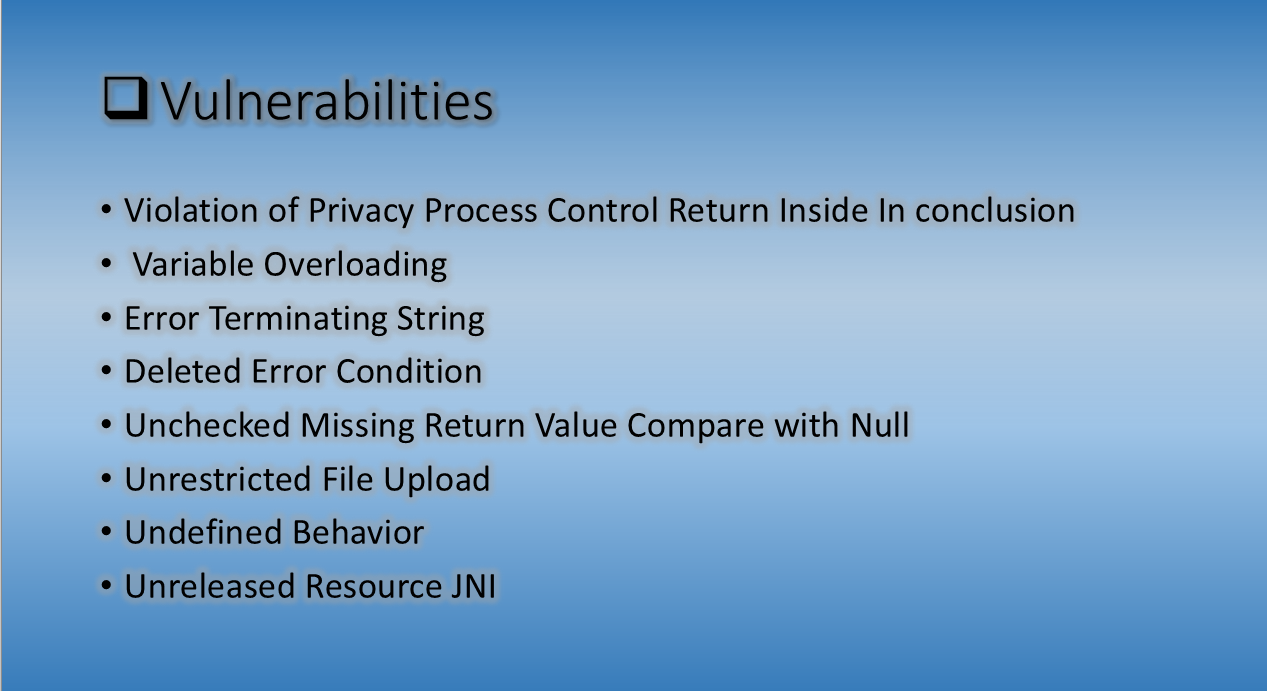


Figure 17 : Disaster Recovery Plan slide 8 made by author)



Figure 18 : Disaster Recovery Plan slide 9 (made by author)

## M1: A method to assess and treat IT security risks

### Organizational security risks and Solutions to reduce it

|  |  |  |
| --- | --- | --- |
| **Risk** | **Definition** | **Solutions** |
| * Operational Risk | A risk of system mistake, Human instruction and also technical issues in organization called as a operational risk . | * Need to have s strong relationship between business to business . * Implement a plan of risk management . * Need to have backup plans . * Obey the rules and regulations of the organization correctly. * Train the employees about the risks and how to reduce it . |
| * Natural risk | * Natural risk is a risk of natural events like Tornado , Tsunami , Landscaping etc. In this risk it is happening unexpected times. | * Identify the natural risk. * Inform about the risk to the people. * Provide financial protection to the people and for the business. * Have to have a Disaster risk Management plan. |
| * Security Risk | * Security risk means an organization that could have a risk of financial. Also for the can have security risks. | * Identify the risk in the organization. (network , Servers, Data centers etc.) * Create risk profiles. * Measure risks in the organization. * Apply mitigating controls for each risk in the organization. |
| * Environmental Risk | * Environmental risk known as the environmental issues like pollution , noises , climate changes etc.. | * Identify the Environmental risk and the sources that harm. * Research the harm that costs. |
| * Business Risk | * Business risk means when forcedly business reaching downwards in business. | * Identify the risk that negatively effect in an organization. * Then identify if there had a risk who or what could be harmed . * Develop risk Document. * Then evaluate controls for risk . |
| * Liquidity Risk | * The risk of being unable to buy or sell assets in each size over a given period without adversely affecting the price of the asset.   (Anon., n.d.) | * Identify the cash flow of the organization and improve it. * Improve risk reporting abilities. * Identify the balance sheet and improve it . |

### 2 IT security Risks and Solutions to reduce it

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

## M2: Three benefits to implementing network monitoring systems.

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

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

* + - 1. **Allocate resources most effectively.**

In a company the workloads and projects are very heavy, and it is very complex . So It teams cant do the work without any work managed also It teams cant spent time for any other works. So by implementing the network monitoring system then can understand what’s the problem and can place protective measures and fix it .

* + - 1. **Issues can Fix Quickly**

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

* + - 1. **Enhance Customer Satisfaction**

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

A picture containing text, screenshot, diagram, electric blue

Description automatically generated

Figure 19 : Network monitoring system (www.wallarm.com)

## M3 : The ISO 31000 risk management methodology and its application in IT security

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

A risk management framework

A risk management process

### The components of ISO 31000

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

* + 1. The framework
    2. The Process

#### The Framework

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

The major components of frameworks are,

* + - 1. Government policy
* It means that begin the mission and then it will appear about the organization commitment
  + - 1. Program design
* Design a program framework for continuous improvement.
  + - 1. Implementation
* Implement the risk management framework and program it correctly.
  + - 1. Monitoring and Evaluation
* monitoring the management system's effectiveness and organizational structure
  + - 1. Continuous Enhancement
* Check overall management system performance.

#### The Process

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

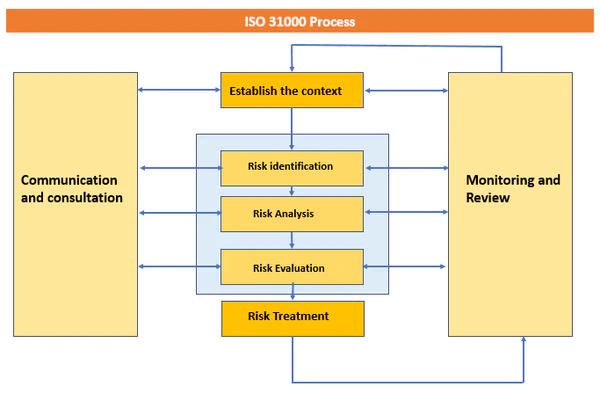


Figure 20 : ISO 31000 Risk Management System (https://iso-docs.com/)

## M4 : Possible impacts to organizational security resulting from an IT security audit

**What is an IT security audit ?**

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

**Types of IT security Audits**

It security audit types can be divided into two categories. That are know as,

**Approached Based**

In approached based category there are 3 types of Audits .

* Black box audit – In this category auditor only knows the publicly available information

regarding the organization.

* White box audit – In this audit the auditor will provide the details of the organization that

to be audited.

* Grey box audit – This audit gathered the information and saved in that time also its provide

the beginning of the audit and proceed it.

**Methodology Based**

* Penetration Test – In this method auditor tries to interrupt the organization Framework.
* Compliance Audits - Only certain can check if the organization observe security standards
* Risk Assessment – Analysis of various types of resources that can be threaten to the

organization

**Importance of an It security audit for an organization**

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

## M5: The roles of stakeholders in the organisation to implement security audit recommendations.

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

(Team, 2023)

### Roles and responsibilities

**Owners**

A company's assets and business may be subject to the owner's sole control. A business may have a single owner or numerous owners, depending on the corporate structure and incorporation. Major company decisions are made by these owners, and they also negotiate contract conditions with other parties. They also decide on the manufacturing method and the available goods and services. Owners may also collaborate on the development of the company's growth and sales plans with other stakeholders including the board, consultants, and staff. Owners of the firm are personally accountable for its success and design the objectives to do so. (Team, 2023)

**Managers**

For the purpose of coordinating staff operations, managers interact closely with senior management. They supervise teams and departments to make ensuring that their operations follow the mission and rules of the business. These individuals manage teams and assign work while ensuring that staff members have access to the tools they need to complete their assignments. Additionally, they determine project deadlines, assess employee performance, and deliver crucial reports to top management. Managers may work alongside senior executives and participate in the decision-making process, depending on the firm structure. (Team, 2023)

There are 3 levels of managers in a Company.

* Senior Manager
* Middle-tier managers
* Lower managers

**Employees**

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

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

**Labour Unions**

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

# References

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

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

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

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