CLIVER MIND POB ICT

Risk Assessments Plan

Jordan University of Science and Techno

&

CLEVER MIND POP ICT

- Distribution of Tasks :

Student Name	*ID #*	*His/her Work*
Mohammd Riyad Qasaymeh (Team leader)	*152152*	*Entire section – 1 (Context Establishment) , and make an analysis on one 3 risks that related with one asset , designing the scales , mapping tables.*
Shahed Sharadgah	151511	*Entire section – 1 (Context Establishment) , and make an analysis on one 3 risks that related with one asset.*
Hamza Al-Zoubi	154202	*Entire section – 1 (Context Establishment) , and make an analysis on one 3 risks that related with one asset.*
Tala Saleh	153217	*Entire section – 1 (Context Establishment) , and make an analysis on one 3 risks that related with one asset.*
Abdulaziz Tbaishat	151652	*Entire section – 1 (Context Establishment) , and make an analysis on one 3 risks that related with one asset.*

Table of Contents

Context Establishment

1.1 Context, Goals, and Objectives

Let's to begin with internal context , define the assets that’s collected from the survey :

A- Database.
B- The Financial information and transactions.
C- Hard Drive Storage.
D- Cloud Storage.
E- Servers.

The goal after this step is to predict any risk can that may be face these assets ,
And how to mitigate the extent of the threats.

1.2 Scope, Focus, and Assumptions

1.2.1 Scope

All assets that have been collected , are related to IT Department or any asset that associate with digital information , and make an elaboration explain how to prevent the risks, threats and vulnerabilities from make any malicious activity of the sensitive information.

1.2.2 Focus

the central focus of the assessment is on protecting sensitive data and ensuring the availability of the online services. areas of attention include risks related to exposure of sensitive data, Unauthorized Access, identity theft and service outages.

1.2.3 Assumptions

identity theft and service outages , all employees have a background in IT , the org enforces policies regarding access controls , the org does not conduct regular penetration testing .

Assets, Scales, and Risk Evaluation Criteria

1.2.4 Assets

Assset	Description
Database	The database contain sensitive data , employees , clients , bank accounts information .
The Financial information and transactions	The transactions between the clients and the employees, employees and third party, and the financial information about it.
Web Server	The network service that presents an interface allowing fetching and storing of asset items
Hard Drive Storage	hard drives stores all the digital content including all the software installed on a computer, as well as all the data files created and used by the organization.
Cloud Storage	storage of data on remote servers that are hosted by a third party service provider instead of storing it on local servers or physical hardware within the organizatin's premises

1.2.5 Scales

a) Risk Sensitivity Scale

Level	Criteria
Low	A compromise would be limited and generally acceptable for the organization, resulting in minimal monetary, productivity, or reputational losses There would be only minimal impact on normal operations and/or business activity
Moderate	A compromise would be marginally acceptable for the organization, resulting in certain monetary, productivity, or reputational losses Normal operations and/or business activity would be noticeably impaired, including the potential for breaches of contractual obligations
High	A compromise would be unacceptable for the organization, resulting in significant monetary, productivity, or reputational losses The ability to continue normal operations and/or business activity would be greatly impaired, potentially resulting in noncompliance with legal or regulatory requirements and/or loss of public confidence in the organization

b) Likelihood Scale

Level	Criteria
Low	The threat source is part of a small and trusted group, or controls are in place to prevent the vulnerability from being exercised without physical access to the target.
Moderate	The threat source is part of defined community of users, and controls are in place that may impede successful exercise of the vulnerability without significant inside knowledge.
High	The weakness is accessible publicly on the Internet, and controls to prevent the vulnerability from being exercised are ineffective.

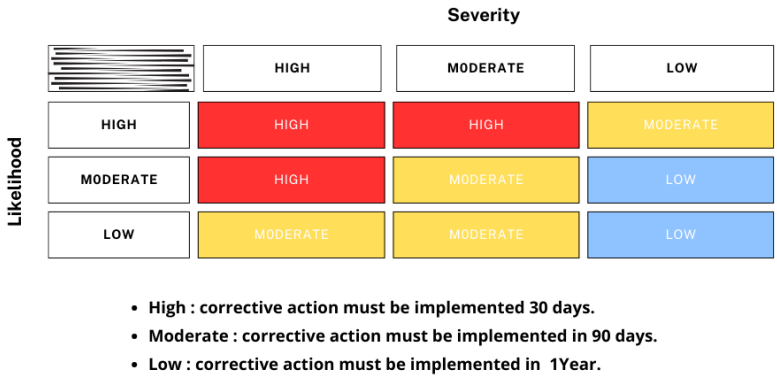
c) Severity Scale

Level	Description
Low	May indirectly contribute to unauthorized activity or just have no known attack vector. May result in a degradation of service and/or a noticeable decrease in service performance.
Moderate	May allow limited access to or control of the application, system, or communication, including only certain data and functionality. May result in a short disruption of service and/or denial of service for part of the user community
High	May allow full access to or control of the application, system, or communication, including all data and functionality. May result in a prolonged outage affecting all users of the service.

CIAA , severity Scale , and it depends on what the target of the risk, threat and vulnerability , and the aspects of CIAA that's affected .

Risk Evaluation Criteria

RISK EVALUATION CRITERIA



- **High : corrective action must be implemented 30 days.**
- **Moderate : corrective action must be implemented in 90 days.**
- **Low : corrective action must be implemented in 1Year.**

2 Risk Identification & Risk Analysis

2.1 Database Risk 1 (Unauthorized Access) :

Before go to identify and analysis lets briefly describe the risk :
It look for Unauthorized individuals gaining access to sensitive data that locate in (DB) ; like (employees , clints , bank accounts information) that may be the targeted by the attacker for malicious intent .

2.1.1 Threat Identification and Analysis

Hackers exploiting weak authentication mechanisms , weak login credentials , vulnerable authentication logic , these are examples of how the attacker can exploit weak authentication .
In this case we can assign a level to the threat analysis : (High) .

2.1.2 Vulnerability Identification and Analysis

Weak or easily guessable passwords , but the organization recommends the employees to set strong passwords for themselves accounts and it has a policies for set the passwords , so in conclusion of vulnerability analysis we can give (Moderate) level of consequences in this case , because the employee may comly to recommendations and policies or may not .

2.2 Database Risk 2 (SQL Injection) :

This attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS) .
[OWASP].

2.2.1 Threat Identification and Analysis

Manipulation of SQL queries to gain unauthorized access or damage data , and make tamper with existing data , or maybe make the data unavailable if the attacker get the admin privileges , and this type of threats limited by attacker skills , also depend on what (OWASP) say , we will give (High) level of likelihood , but we have an auditing team to make a review of access , and the organization enforce the principle of least privilege for users accounts , so likelihood will mitigated to (Moderate).

2.2.2 Vulnerability Identification and Analysis

SQL injection attack occurs when:

1. An unintended data enters a program from an untrusted source.
2. The data is used to dynamically construct a SQL query.

The main consequences are:

- Confidentiality: Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities. [High].

- Authentication: If poor SQL commands are used to check usernames and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password . [Moderate].

- Integrity: Just as it may be possible to read sensitive information, it is also possible to make modification or even delete this information with a SQL Injection attack. [High]

We will make an oral comprehensive explain of the rating of consequences , High, Moderate and low .

[OWASP].

2.3 Database Risk 3 (Lack of Encryption) :

Exposure of sensitive data during transmission or storage , so we need to keep the data secure int rest, transmission and any activity can used the data .

2.3.1 Threat Identification and Analysis

Interception of unencrypted data by eavesdroppers , in this case the data should be encrypted to keep it secure from interception , any to apply confidentiality term on the data , up to this critical point ,we give (High) level likelihood.

2.3.2 Vulnerability Identification and Analysis

Failure to implement strong encryption protocols ,but the organization had been “TowFish” : (Type of AES) encryption algorithm implemented on there system , that’s mean the company have strong encryption method , and it has a penetrating testing plan every period of time , so the consequences or severity is (Low).

2.4 The Financial information and transactions risk 1 (Identity Theft):

occurs when someone uses another's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

Unauthorized individuals gain access to personal information for fraudulent purposes.

2.4.1 Threat Identification and Analysis

Phishing attacks, social engineering, and data breaches may cause the leak of financial information of the company and lead to heavy loss. The company employees have a good background in IT so the likelihood is (low).

2.4.2 Vulnerability Identification and Analysis

Weak authentication methods and lack of multi-factor authentication can highly increase the impact of such attacks. The severity is (high).

2.5 The Financial information and transactions Risk 2 (Phishing Attacks):

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

2.5.1 Threat Identification and Analysis

Malicious emails, websites, or messages tricking users into providing information. This will lead to unauthorized access to sensitive information. it was reported that in 2021 nearly 83% of companies experienced phishing attacks. So, the likelihood is (high).

2.5.2 Vulnerability Identification and Analysis

Lack of user awareness and education on phishing threats. This is not dominant in the company as they are aware and have a good background in phishing emails. The severity is (moderate).

2.6 The Financial information and transactions Risk 3 (Insider Trading):

An individual who has information as an insider is guilty of insider dealing if they disclose this information, otherwise than in the proper performance of the functions of their employment, office, or profession, to another person. unauthorized use of confidential financial information for trading purposes.

2.6.1 Threat Identification and Analysis

Employees or insiders exploiting their access to privileged information. The company is small, so the likelihood of this happening is (low).

2.6.2 Vulnerability Identification and Analysis

Inadequate monitoring of employee activities and transactions. This will make it very hard to recover from it happening. The severity is (moderate).

2.7 Web Server Risk 1(Downtime):

When a web service is not available online or doesn't function well enough for end users to complete a task, the site is considered to be experiencing **downtime.**

What causes downtime?
1.Human error.
2. Equipment failure.
3. Malicious Attack(DDOS).

2.7.1 Threat Identification and Analysis

Overloading servers with traffic to render them unavailable. Server overload is an issue that occurs when a web or application server receives a larger volume of requests than it is able to efficiently handle. When this happens, it can result in performance issues such as latency and bottlenecks.

The likelihood of a web server overload depends on various factors, and it can be influenced by aspects such as the server's capacity, the amount of traffic it receives, the efficiency of its configuration, and the nature of the applications it hosts.

so, the likelihood of this happening is (moderate).

2.7.2 Vulnerability Identification and Analysis

Failure to apply timely updates and patches to server software.

There are some challenges for patch management:

1. **Time-consuming patching processes**
2. **Lack of endpoint visibility**
3. **Different systems & software**

Technology is always changing, and that means the challenges that come with technological advances are changing as well. The severity is (High).

2.8 Web Server Risk 2(Denial of Service Attacks):

A Denial of Service (DoS) attack is a type of cyberattack that aims to make a computer or network resource unavailable to its intended users. It is usually caused by flooding the target with requests or data packets until it is overwhelmed and unable to respond.

2.8.1 Threat Identification and Analysis

Attackers flooding the system with traffic to exhaust resources and oversaturate the capacity of a targeted machines, so the likelihood of this happening is (low).

2.8.2 Vulnerability Identification and Analysis

Inadequate capacity planning and lack of effective traffic filtering. The severity is(high) Resource capacity planning is the process of determining and managing the availability and allocation of resources required to execute web server successfully.

2.9 Web Server risk 3(data loss):

Data loss is an incident where data is destroyed, deleted, corrupted, or made unreadable by users and software applications. A data loss incident can be intentional or accidental.

Common Causes of Data Loss:

1. **Human error**
   a. **Accidental deletion of data files**
   b. **Spillage of liquids**
2. **Theft**
3. **Computer viruses**

2.9.1 Threat Identification and Analysis

Encryption of critical data by malicious actors who demand a ransom for its release. Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access. So, the likelihood is (moderate).

2.9.2 Vulnerability Identification and Analysis

Cross-site scripting (XSS) is a type of computer security vulnerability that can allow an attacker to inject malicious code into a web page, resulting in the execution of the code by unsuspecting users who visit the page. The malicious code can take the form of a

script that is executed in the context of the vulnerable web page. The code can be used to exploit the trust that a user has in the site to steal cookies, login credentials, or other sensitive information.

XSS vulnerabilities can be difficult to detect because the code is usually invisible to the user and is executed in the context of the site. However, there are a number of measures that can be taken to help prevent XSS vulnerabilities, including proper input validation and output encoding, so the severity is(high)

2.10 Hard drive storage Risk1 (Physical Damage):

Hard drives are delicate devices, and even minor physical damage can cause them to fail. This can be a devastating experience, especially if you have important data stored on the drive.
A loss of data may happen due to physical damage to the hard drive.

2.10.1 Threat Identification and Analysis:

Accidental drops, power surges, or exposure to environmental hazards may happen.
The organization has no indicator to such threats, so the likelihood is (low).

2.10.2 Vulnerability Identification and Analysis:

Lack of proper backup and physical protection measures can increase the chance of hard drive damage. The severity is (moderate).

2.11 Hard drive storage Risk2 (Theft or Loss):

Most users place much more value on their data. Hardware is normally insured, and you can get replacements easily. However, you simply cannot replace your data and files if your hard drive is stolen.
When an unauthorized person gets access to sensitive data through theft or loss of the hard drive.

2.11.1 Threat Identification and Analysis:

Physical theft, misplacement, or loss during transportation are problems facing the physical hard drive and the inner data.
It is a small organization and not a lot of people go inside their workstations, so the likelihood is (low).

2.11.2 Vulnerability Identification and Analysis:

Inadequate physical security measures and lack of encryption.
It is not something that is implied in the company, so the severity is (high).

2.12 Hard drive storage Risk3 (Data Corruption):

It is a state under which code of a file or data inside a file alters from the original state, the hard drive may become corrupted, unreadable, or unavailable.
Intentional or unintentional alteration of data stored on the hard drive.

2.12.1 Threat Identification and Analysis:

Malware, software bugs, or hardware issues causing data corruption by deleting, or encrypting the data, incorrect processing or storage of information and causing errors in data storage or transmission.
Since the company does not have firewall or any kind of protection method applied on, so the likelihood is (high)

2.12.2 Vulnerability Identification and Analysis:

Absence of regular data integrity checks and backup procedures.
Since the company does not perform a penetration test, so the severity is (high).

2.13 Cloud Storage Risk1 (Data Transfer Insecurity):

The risk that may happen of data during the process of uploading or downloading between the user's device and the cloud server. This risk arises when data is transmitted over the internet , and if not properly secured , it may be susceptible to interception or unauthorized access by malicious entities.

2.13.1 Threat Identification and Analysis:

Man-in-the-middle , attacks ,interception, or data eavesdropping , all these are unauthorized access or capture of data during transmission between a user and a cloud storage server. Sensitive information, such as files or credentials, may be accessed by unauthorized parties because of lack of encryption or some of Network Vulnerabilities

2.13.2 Vulnerability Identification and Analysis:

Insufficient encryption during data transfer and poor network security.
Using weak encryption systems or not encrypting some data poses a great risk.

2.14 Cloud Storage Risk2 (Data Breach):

Unauthorized access or disclosure of sensitive information stored in cloud storage. Data breach may happens if there weak security measures or unauthorized access happening .

2.14.1 Threat Identification and Analysis:

Cyberattacks and hacking in cloud storage are malicious activities and manipulation of cloud systems or data but vulnerabilities is weaknesses in cloud infrastructure that could be exploited for illegal actions. The risk factors here: data compromise, service disruption, unauthorized control.

2.14.2 Vulnerability Identification and Analysis:

Inadequate encryption, misconfigured security settings, or unpatched systems.
It is not something that is implied in the company, so the severity is (high).

2.15 Cloud Storage Risk3 (Service Outages):

Disruption or unavailability of cloud storage services, impacting access to stored data because of some technical failures or cyberattacks or maintenance and upgrades, all of these possibly of business and financial operational disruption, this maybe temporary or prolonged.

2.15.1 Threat Identification and Analysis:

DDoS attacks, technical glitches, or infrastructure failures. DDoS attacks is abnormally high traffic and unusual patterns in network traffic to cloud storage services. the technical glitches are unintended service interruptions, slowdowns, or erratic behavior due to system errors, software errors, or interoperability issues. infrastructure failures due to hardware malfunctions, server crashes, or network failures, power outages or data center disruptions.

2.15.2 Vulnerability Identification and Analysis:

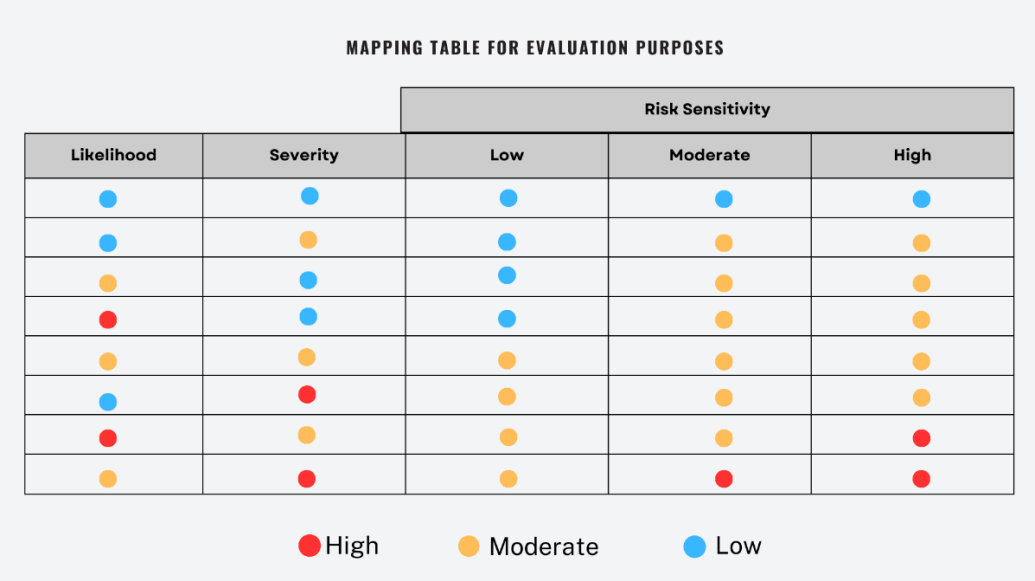
Lack of redundancy and failover mechanisms in cloud storage.
There are no backup systems or duplicate resources in the company, so if data damage occurs it will lead to the destruction of some assets such as the company database.

20 Risk Evaluation

2.16 Risk Analysis Results

Let's to begin with the equation to measure 'Risk Level' :

Depend on the following mapping table the 'Risk-Level' will determined:



Risk = Likelihood x Impact

2.17 Evaluation of Risk Level

Risk	Likelihood	Impact	Final Level
Unauthorized Access	High	Moderate	High
SQL Injection	Moderate	High	High
Lack of Encryption	High	Low	Moderate
Identity Theft	Low	High	Moderate
Phishing Attacks	High	Moderate	High
Insider Trading	Low	Moderate	Moderate
Downtime	moderate	High	High
DOS Attacks	low	High	Moderate
Data loss	Moderate	High	High
Physical Damage	Low	Moderate	Moderate
Theft or Loss	Low	High	Moderate
Data Corruption	High	High	High
Data Transfer Insecurity	Moderate	High	High
Data Breach	Moderate	High	High
Service Outages	Moderate	Moderate	Moderate

This table will make a priorities for the risk in descending way , from (High ➔ low) respectively .

3 Risk Treatment

Risk	Treatment (Avoid ,Share ,Reduction ,Retention)
Unauthorized Access	Reduce the risk by conducting access reviews and auditing on the log file .
SQL Injection	Avoid the risk by make patching and input validation after penTest for the queries , or cancel the service that make the risk rise , (website) , and keep use only the application until We find a solution .
Lack of Encryption	By Share with Third-Party , to keep the data storage and transfer secure , and the Third Party will use a encryption methods that's satisfy the company and be accountable how to store, share the data on cloud or local devices .
Identity Theft	Avoid the risk by dispose of personal information, use strict privacy settings on devices, and adding MFA.
Phishing Attacks	Reduce the risk by awareness training, simulation, and email filtering.
Insider Trading	Avoid by monitoring of employee activities, privileged access management, alerts and incident response, and auditing and reporting.
Downtime	Avoid the risk by Replacing old equipment, Maintaining software updates, Checking third-party services for guarantees and practice redundancy where possible.
DOS Attacks	Reduce the risk by Network segmentation, Load balancing, IP blocking, Rate limiting, Content Delivery Networks (CDNs).
Data loss	Avoid the risk by Safeguarding assets with a zero-trust approach, Using multifactor authentication and strong passwords to strengthen the protection of data, Maintaining offline data backups to prevent data loss and recover quickly in case of emergencies
Physical Damage	Avoid dropping or bumping the drive, treat your hard drive with extreme care to avoid physical damage.
Theft or Loss	Avoid the risk by using a two-meter cable and place it at the back of a draw or somewhere well out of site, this is one of the best ways to protect your external hard drive.

Data Corruption	Reduce the risk by performing a penetration test, updating antivirus software, using firewalls and monitoring system temperatures
Data Transfer Insecurity	By implementing security measures to protect data during transmission and save, like using encrypt data, SSL/TLS protocols, Enable Multi-Factor Authentication ,user training .
Data Breach	Reduce the risk by using robust encryption, resetting passwords promptly, notifying parties, performing forensic analysis, monitoring in real-time
Service Outages	Avoid inadequate redundancy and failover mechanisms and neglecting regular maintenance especially during peak usage hours

END OF THE PROJECT