reventure™

Solutions (pvt) Ltd

Annual Risk Assessment Report

2021

Risk Assessment Team

IT Number	Name
IT19029146	Eranda H. P. D
IT19029214	J. C. Hapuarachchi
IT18220902	Mandhanayaka D. D
IT19038742	J. A. T. N. Weerasooriya

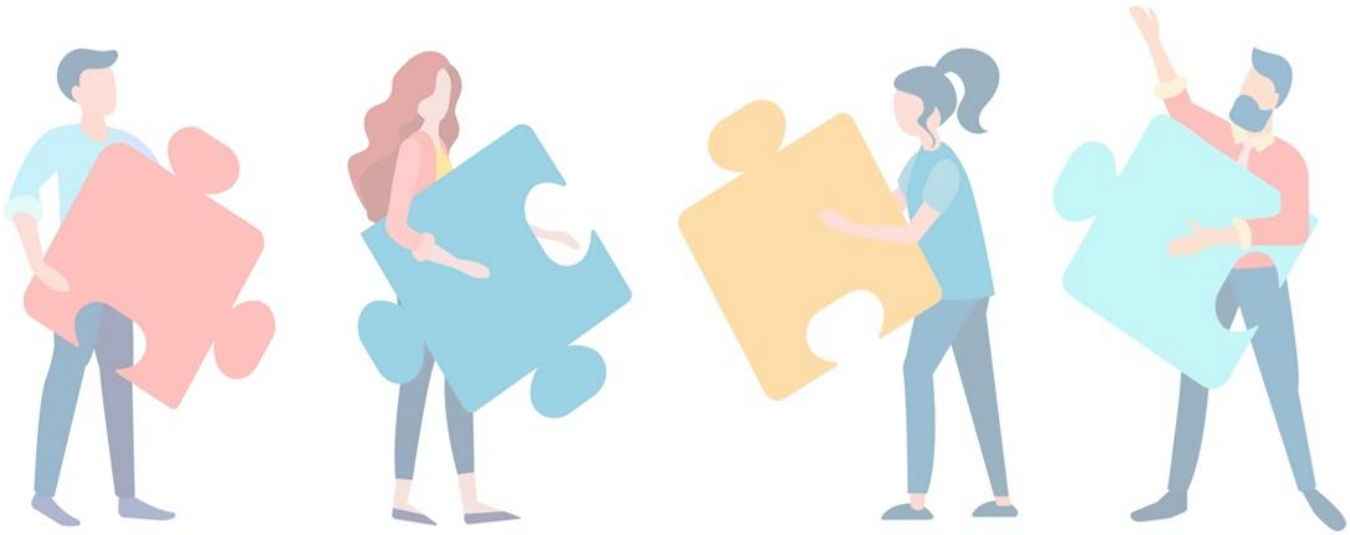


Table of Contents

1 - Executive Summary

A risk assessment was performed for the company **'Reventure Solutions'** during the period 20th of April 2021 to 5th of May 2021. To perform the risk assessment a hybrid framework was mainly used. OCTAVE allegro framework which is a Qualitative risk analysis, and a quantitative analysis approach were used. OCTAVE allegro framework was mainly used to identify the critical assets, the impact of the critical assets to various sectors of the company and for each of these identified critical asset there is a threat profile/threat analysis which contains details of each critical asset and the security requirements expected by the company for each of the critical asset. The risks associated with the critical assets, the controls for the identified risks, the monetary values of the recommended controls and whether it is worth to implement the control or not are found using quantitative risk analysis.

Below mentioned things are the identified key issues and recommendations.

1) **Lack of fire prevention mechanisms**

As identified, the company have not implemented any required controls to protect against fire. The damage cause by fire is immense. It is a must to implement the required controls to prevent against unexpected fire events. Setting fire alarms, implementing fire extinguishers, implementing fire detection devices can be used to protect the company against fire.

2) **Lack of awareness programmes and training sessions to employees to protect against cyber-attacks.**

The company have not given any awareness programmes or training session related to cyber-attacks s to the internal employees. Since this is an IT related company, most of the identified critical assets are systems. These systems contain databases. These databases are vulnerable to cyber-attacks such as SQL injections. If these kinds of attacks are addressed through these programmes or training sessions, then the developers will be very aware about these types of attacks and other related cyber-attacks.

3) **No proper regulatory-scheduled maintenance plan**

In an IT company, IT related hardware takes a very important place. As identified from the risk assessment perform to the 'Reventure Solutions', this company doesn't use a proper regulatory-scheduled maintenance plan for the hardware malfunctioning problem. Hardware related malfunctioning can happen at any time and this malfunction can affect the productivity of the entire company. As a solution for this, a regulatory-scheduled maintenance plan can be used. This simply is a regular and a very well designed and planned maintenance schedule that the technicians follow, and which will help to detect hardware problems earlier.

4) **Lack of data filtering on arrival and lack of input validation mechanisms**

Reventure Solutions does not use any mechanisms to protect against attacks like Cross Site Scripting. One of the best ways to protect against Cross Site Scripting attacks is by filtering receiving data. Simply filtering receiving data means when the data is received, the received data should be filtered thoroughly as possible to find out whether it is an expected data, valid data, or invalid data. Other than that the company does not use input validation mechanisms. If input data is validated, this will prevent from happening of SQL injection attacks.

2 - Introduction

2.1 - Purpose:

The purpose of this risk assessment was mainly to identify the critical assets of Reventure Solutions, the security requirements expected by the company, the potential threats involved with the identified critical assets, the impact that the critical assets have to different sectors of the company, the risks associated with the critical assets, the recommended controls for the identified risks and lastly to determine whether it is beneficial to implement the recommended controls or not.

2.2 - Risk Assessment Framework:

To perform the risk assessment a hybrid approach was selected. A qualitative analysis approach was used with quantitative analysis. OCTAVE Allegro framework was selected as the best way to carry out the qualitative analysis. OCTAVE Allegro was selected because this approach mainly focuses on the IT assets, helps to focus deeply on each identified critical asset and this framework provides all the required worksheets, questionnaires, etc to gather the necessary information. Quantitative risk analysis was used because quantitative risk analysis quantifies the risks associated with the assets and cost-effective decisions can be made using the monetary values calculated in the risk analysis.

2.3 - Scope of the Risk Assessment:

The Risk Assessment was performed to identify the risks associated with the assets that effect the main security principals which Confidentiality (Preventing unauthorized access), Integrity (preventing unauthorized modifications), availability (Data, resources and services should be available to the authorized users in a timely manner). The company have the head office, a branch and there are 6 departments in the head office branch. The company uses 6 systems to perform their activities. From these 6 systems 3 systems was identified as critical assets. Without these systems the company will not be able to continue. In the company there are approximately 70 employees (Including all the employees of the departments, security officers, Janitors, etc).

3 - Risk Assessment Approach

3.1 - Participants:

Role	Participant
Chairperson	Mr. Manesh Jayasinghe
Co-Chairperson	Mr. Dushmantha Perera
CEO	Mrs.Malinthi Samaranayaka
Head of IT department	Mr. Sandun Suriyabandara
Security Management Team	Mr. Senura Fernando

3.2 - Techniques Used:

- Questionnaires was used to collect the required data to perform the risk assessment. Worksheets available in OCTAVE allegro framework were used as Questionnares.

- To validate the information gathered, virtual interviews and discussions were conducted with the employees of the company.

- Not only that we also used the Quantitative Risk Analysis techniques too, in order to get a proper understanding about the company assets and identified risk scenarios.

3.3 - System Characterization:

Applications	• Visual Studio, PyCharm to develop software. • Word Processing Programs. • Payroll Software and Billing Software for financial activities. • Adobe photoshop and Adobe illustrator to develop the required graphics.
Operating Systems	Kali Linux 2020, Windows 10, Fedora 2020
Databases	MySQL
Networking devices	Firewall Hardware, Routers, Switches, Dell Personal Computers
Protocols	SSL, HTTPS, TCP/IP

3.4 - Physical Locations:

Location	Address
Head Office	No.40/B, Reventure Solutions, Janata Road, Colombo 3.
Branch	No.30/D, Reventure Solutions, Kotuwa Mawatha, Pettah.
Warm site	No.5, Sriyani Rd, Sinhapura, Wijerama.

4 - Risk Assessment Criteria

- In this risk assessment report, we are using following parameters to evaluate the risks.

Risk = Probability * Potential Impact

4.1 - Threat Probability / Likelihood:

Probability(likelihood) weight factor	Definition
High (1.0)	These are the events most certainly occur (Can be exploit the vulnerability soon/easily) because of the current countermeasures are ineffectual or the controllers are not enough to cover the vulnerabilities. High probability events need more effective countermeasures right away.
Medium (0.5)	This type of events has decent probability to occur/exploit. current controllers can be useful to discourage the exploitation. The threat is being significantly monitored.
Low (0.1)	These events most unlikely to occur (hard to exploit or hidden vulnerabilities). Controllers are very effective and can block the threat regarding asset. Doesn't consider very much.

4.2 - Potential Impact:

Impact (score)	Definition
High (10)	Loss of business reputation, trade secrets, customer services, business services and huge damage to finance and a significant consequence of failure for the organization and affect business continuity.
Medium (5)	Can leads to a considerable damage to the organization. But it can be afforded. Most critical business processes may not get damaged. Mostly damage the business productivity.
Low (1)	Low impact on financial loses reflecting fines, minor asset losses.

4.3 - Risk Calculation:

	Impact		
Threat likelihood section	**Low impact (1)**	**Medium impact (5)**	**High impact (10)**
High (1.0)	Low Risk → (1.0 x 1 = 1.0)	Medium Risk → (1.0 x 5 = 5.0)	High Risk → (1.0 x 10 = 10)
Medium (0.5)	Low Risk → (0.5 x 1 = 0.5)	Medium Risk → (0.5 x 5 = 2.5)	High Risk → (0.5 x 10 = 5)
Low (0.1)	Low Risk → (0.1 x 1 = 0.1)	Medium Risk → (0.1 x 5 = 0.5)	High Risk → (0.1 x 10 = 1)
Risk Scale: [Low (0.1 to 1)] [Medium (>1 to 5)] [High (>5 to 10)]			

5 - Critical Asset Identification & Cost Benefit Analysis

Critical Assets	Description	Container	Security Requirements	Value
Finance Information System	Financial Information System stores and analyses the financial related data which are used for financial decision-making activities.	Dell PowerEdge R720 8B LFF Server, 2x 2.60GHz E5-2670 16-Cores Total, 24x8GB (192GB) RAM, 8x 2TB 7.2K SATA 3.5"" HDD, Windows Server 2012 Evolution Edition	Confidentiality – 100% Integrity – 100% Availability – 99%	Rs. 11,000,000/=
Customer Information System	Customer Information system is a system which is used by the organization to get the information about the customers efficiently.	HP ProLiant DL380P G8 8 Bays 2.5 Server, 2x Intel Xeon E5-2620 2.0GHz 6 Core, 48GB DDR3 REG MEMORY, 600GB (2x 300GB 10K SAS HDD), Windows Server 2012 Evolution Edition	Confidentiality – 100% Integrity – 100% Availability – 99%	Rs. 12,100,000/=
Daily Project Progress system	Daily project progress system will store the activities in a daily basis.	Dell PowerEdge R710 6B LFF Server2x 2.93GHz X5670 12-Cores Total8x8GB (64GB) RAM6x 2TB 7.2K SAS 3.5" HDD, Debian 9.0 OS	Confidentiality – 100% Integrity – 100% Availability – 99%	Rs. 9,070,000/=
Organization's critical IT hardware including firewall, main server	The main asset which helps in the process of developing software.	HPE ProLiant DL360 G10 1U Rack Server -1 x Xeon Gold 6230-32 GB RAM HDD SSD -Serial ATA/600, Debian 9.0 OS	Confidentiality 0% Integrity – 100% Availability – 99%	Rs. 32,270,000/=

Finance Information System:

Risk/ Threat Scenario	ALE before Safeguard	ALE after Safeguard	Annual Cost of Safeguard	Cost / Benefit
1) Viruses	Rs. 6,600,000/=	Rs. 440,000/=	Rs. 125,000/=	**Rs. 6,035,500/=**
2) Human errors	Rs. 39,600,000/=	Rs. 10,560,000/=	Rs. 140,000/=	**Rs. 28,900,000/=**
3) Fire	Rs. 825,000/=	Rs. 5,500/=	Rs. 240,000/=	**Rs. 579,500/=**
4) Hardware malfunction	Rs. 500,000/=	Rs. 55,000/=	Rs. 90,000/=	**Rs. 355,000/=**
5) Unauthorized access	Rs. 500,000/=	Rs. 44,000/=	Rs.115,000/=	**Rs. 341,000/=**

Customer Information System:

Risk/ Threat Scenario	ALE before Safeguard	ALE after Safeguard	Annual Cost of Safeguard	Cost / Benefit
1) SQL Injection	Rs. 6,050,000/=	Rs. 1,512,500/=	Rs. 215,000/=	**Rs. 4,322,500/=**
2) Cross Site Scripting (XSS)	Rs. 2,904,000/=	Rs. 726,000/=	Rs. 115,000/=	**Rs. 2,063,000/=**
3) DDoS Attack	Rs. 907,500/=	Rs. 193,600/=	Rs. 262,000/=	**Rs. 451,900/=**
4) Fire	Rs. 290,400/=	Rs. 24,200/=	Rs. 145,000/=	**Rs. 121,200/=**
5) Hardware Malfunction	Rs. 544,500/=	Rs. 151,250/=	Rs.325,000/=	**Rs. 68,250/=**

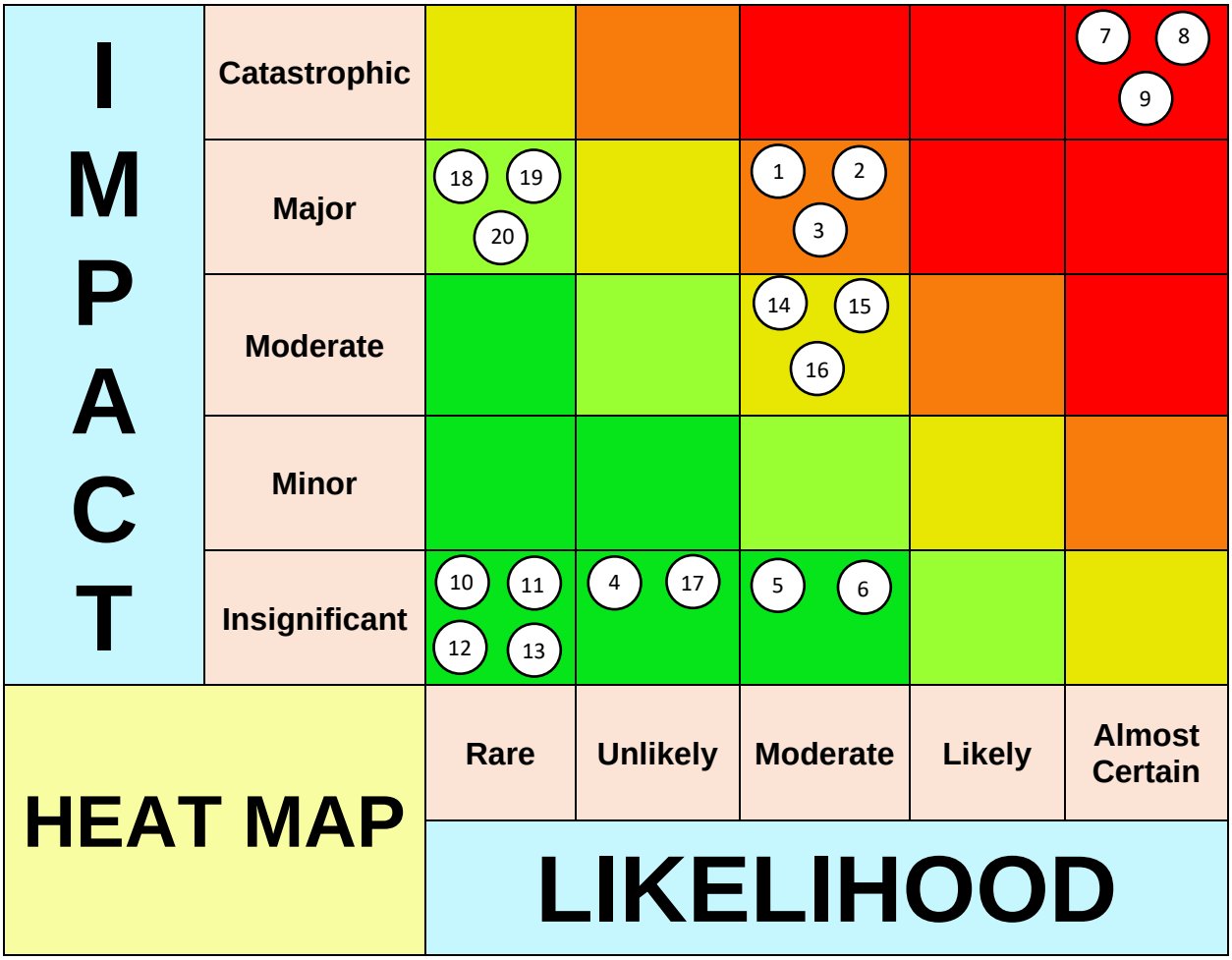
Daily Project Progress system:

Risk/ Threat Scenario	ALE before Safeguard	ALE after Safeguard	Annual cost of Safeguard	Cost / Benefit
1) Natural disaster	Rs. 907,000/=	Rs. 453,500/=	Rs. 145,000/=	**Rs. 308,500/=**
2) DDoS attack	Rs. 907,000/=	Rs. 226,750/=	Rs. 262,000/=	**Rs. 418,250/=**
3) SQL Injection	Rs. 3,628,000/=	Rs. 453,500/=	Rs. 215,000/=	**Rs. 2,959,500/=**
4) Hardware Malfunction	Rs. 1,360,500/=	Rs. 272,100/=	Rs. 325,000/=	**Rs. 763,400/=**
5) Data modification by internal member	Rs. 2,267,500/=	Rs. 181,400/=	Rs. 440,000/=	**Rs. 1,646,100/=**

Organization's critical IT hardware including firewall, main server:

Risk/ Threat Scenario	ALE before Safeguard	ALE after Safeguard	Annual cost of Safeguard	Cost / Benefit
1) Hardware Malfunctioning	Rs.2,581,600,000	Rs. 161,350,000	Rs.73,333.33	**Rs.2,420,176.667**
2) Fire	Rs. 322,700,000	Rs. 40,337,500	Rs. 30,000	**Rs.282,332,500**
3) Lightning	Rs. 322,700,000	Rs. 40,337,500	Rs.110,000	**Rs.282,252,500**
4) Power Faults	Rs. 2,904,300,000	Rs.322,700,000	Rs.36,666.66	**Rs.2,581,563,333**
5) Hardware Theft	Rs.1,936,200,000	Rs. 161,350,000	Rs.170,000	**Rs.1,774,680,000**

6 - Heat Map


IMPACT
Catastrophic
Major
Moderate
Minor
Insignificant
7
8
9
18
19
20
1
2
3
14
15
16
10
11
12
13
4
17
5
6
HEAT MAP
Rare
Unlikely
Moderate
Likely
Almost Certain
LIKELIHOOD

7 - Summary

We have identified threats that can be affected to the Confidentiality, Integrity, and Availability of Reventure Solutions. We advise that the control implementation should be done in an order derived using Annualized Loss Expectancy (ALE) and cost / benefit analysis financial parameters.

CIS (Customer Information System): - CIS is the most critical asset that we have in our company. According to the past incidents and past logs we could be able to identify some of the threats. SQL Injection, XSS, DDoS attack, Natural disaster, Hardware Malfunction. To mitigate these kinds of threats, we can implement some controls. Give proper training for the security team. Practice basic network security protocols. Install fire detection devices. Regularly do maintenance. If an attack happens mainly, it affects the company's reputation.

DPPS (Daily Project Progress System): - DPPS system holds our all the project details. We have records of threats that we have faced in past. Natural disasters, DDoS Attacks, SQL Injections, Hardware malfunction, and also, we have faced a data modification did by an internal staff member. Most of these took place because that we did not maintain a log and biometric security system to track down internal activities. Must upgrade ventilation system. And frequently give latest security training to the staff members. Mainly daily backing up company data is also mandatory. This system is an ongoing process that functions 24 hours. So due to a lack of a backup system or an attack the system will not be able to perform the tasks.

FIS (Finance Information System: - FIS directly affects our company because company all transactions and all money allocation happen through this system. There are some risks like viruses, human errors, fire, hardware malfunction, unauthorized access that took place in the past. To avoid these threats, we can have proper virus guards and daily update our systems. Conduct training sessions for employees, create granting levels for employees to avoid unauthorized access to the system.

CIH (Critical IT Hardware): - CIH directly affects company system availability. Without getting access to the company system. The Company cannot continue. Therefore, regulatory schedule maintenance plan, install fire detectors, alarm system to the server room. Must maintain a backup system, install a lightning protection system, and have to install a biometric security system also.

If there is an attack or power failure this may result in the loss of Confidentiality, Integrity, and Availability. It may cause to company's reputation, due to that customer loss will occur. Company has to monitor these critical assets thoroughly. Because these assets directly affect to our company growth.

8 - Reference

https://sectigostore.com/blog/what-is-sql-injection-8-tips-on-how-to-prevent-sql-injection-attacks
→ Used to find safeguards.

https://www.guru99.com/potential-security-threats-to-your-computer-systems.html → Used to find out about the risks associated with assets.

https://www.ccsinet.com/blog/common-security-risks-workplace/ → Used to find out about potential risks.

https://documentation.commvault.com/commvault/v11/article?p=1662.htm → Used to find information about servers.

http://www2.mitre.org/work/sepo/toolkits/risk/StandardProcess/definitions/occurence.html

→Risk definitions.

https://www.assetinsights.net/Glossary/G_High_Impact_High_Probability_HIHP.html → Risk definitions.

https://www.firesuppression.co.uk/fire-suppression-systems-server-rooms.aspx → About fire controls.

https://www.esecurityplanet.com/networks/how-to-prevent-ddos-attacks-tips-to-keep-your-website-safe/ → About DDoS attack controls

https://www.sciencedirect.com/topics/computer-science/single-loss-expectancy

→ Annualized loss expectancy calculations

9 - Appendix

Allegro Worksheets:

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area *(1-10 Scale)*	**Low (1)**	**Moderate (5)**	**High (9)**
Reputation	• Reputation is minimally affected. • Can be recovered using a very little or no effort or expense.	• Reputation is damaged. • Can be recovered using some effort and expense.	• Reputation is destroyed entirely. • Due to the immense damage, reputation is irrevocable.
Customer Loss	➢ **Less than 5% →** • Reduction in customers due to loss of confidence.	➢ **5% to 20% →** • Reduction in customers due to loss of confidence.	➢ **More than 20% →** • Reduction in customers due to loss of confidence.
New Customer Growth	➢ **Reduced by 10% →** • Reduction in customer growth rate due to inconsistency & lack of innovative ideas.	➢ **10% to 30% →** • Reduction in customer growth rate due to inconsistency & lack of innovative ideas.	➢ **More than 30% →** • Reduction in customer growth rate due to inconsistency & lack of innovative ideas.
Negative feedbacks	• **10** negative feedbacks per month.	• **10 to 50** negative feedbacks per month.	• More than **50** negative feedbacks per month.
Customer Satisfaction *(1-10 Scale)*	➢ **Less than 4 →** • Satisfaction Survey Score due to bad quality of service. • Very close in losing the market share.	➢ **4 to 8 →** • Satisfaction Survey Score due to bad quality of service. • Due to the lack of attention, customers may seek out for alternative solutions.	➢ **More than 8 →** • Proves that the quality of service is up to the standard.

Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of **less than 2%** in yearly operating costs.	Yearly operating costs increase by **2% to 7%**.	Yearly operating costs increase by **more than 8%**.
Revenue Loss	**Less than 5%** yearly revenue loss.	**5% to 10%** yearly revenue loss.	**Greater than 10%** yearly revenue loss.
One-Time Financial Loss	One-time financial cost of **less than $50,000**.	One-time financial cost of **$50,000 to $75,000**.	One-time financial cost **greater than $75,000**.
Other:			

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	• Staff work hours are increased by **less than 10% for 5** to **10 day(s).**	• Staff work hours are increased **between 25% and 45%** for **10 to 20 day(s).**	• Staff work hours are increased by **greater than 45%** for **20 to 30 day(s).**
Investors loss	➢ Less than **5%** • Due to loss of confidence.	➢ **5%** to **20%** • Due to loss of confidence.	➢ More than **20%** • Due to loss of confidence.
Customer Growth	➢ Reduced by **10%** • Reduction in customer growth rate due to reputation reduction.	➢ Reduced by **10%** to **35%**. • Reduction in customer growth rate due to reputation reduction.	➢ Reduced by more than **35%** • Reduction in customer growth rate due to reputation reduction.
Customer Satisfaction ***(1-10 Scale)***	➢ Less than **5** • Satisfaction survey score due to Production delay. • Due to loss of confidence	➢ Between **5** and **8** • Satisfaction survey score due to production delay. • Due to loss of confidence.	➢ More than **8** • Satisfaction survey score due to production delay. • Due to loss of confidence.

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area *(1-10 Scale)*	**Low (1)**	**Moderate (5)**	**High (9)**
Life	• No loss or any severe injuries to the employees' lives.	• Customers' or employees' lives are threatened and may be having moderate number of injuries up to some extent. • But they will recover after receiving medical treatment.	• Most probably a loss of customers' or employees' lives.
Health	• Minimal effect on customers' or staff members' health. • Can be recovered within 2-3 days.	• Considerable amount of effect on customers' or staff members' health. • Can be recovered within 5-10 days.	• Has an immense effect on customers' or staff members' health. • Effects may be permanent throughout their entire the lifetime.
Safety	• Safety of either assets or employees are affected.	• Safety of both assets and employees are affected.	• Safety of all assets, employees and customers are affected permanently.
Workplace	• Minimal effect on both the organization's hardware & software equipment' quality. • In a case of emergency, the standard survival procedure might be slightly affected.	• A moderate level of impact on both the organization's hardware & software equipment' quality. • In a case of emergency, the standard survival procedure might completely be failed.	• Both the organization's hardware & software may fail in a catastrophic manner. • In a case of emergency, there might not be any kind of survival mechanism.

Allegro Worksheet 5	RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES		
Impact Area	**Low**	**Moderate**	**High**
Fines	• Fines **less than $100** are levied.	• Fines **between $100 to $250** are levied.	• Fines **greater than $250** are levied.
Lawsuits	• Non-frivolous lawsuit or lawsuits **less than $200** are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	• Non-frivolous lawsuit or lawsuits **between $200 to $500** are filed against the organization.	• Non-frivolous lawsuit or lawsuits **greater than $500** are filed against the organization.
Investigations	• No queries from government or other investigative organizations	• Government or other investigative organization requests information or records ***(low profile)***.	• Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.
Other:			

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
5	**Reputation and Customer Confidence**
4	**Financial**
3	**Productivity**
2	**Safety and Health**
1	**Fines and Legal Penalties**
N/A	**User Defined**

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
`Finance Information System`	This asset holds the financial data and other related data to the financial activities. If by chance Confidentiality, Integrity or Availability of this system is violated, it will cause severe damage to the organization.	Financial Information System stores and analyzes the financial related data which are used for financial decision-making activities.

(4) Owner(s) *Who owns this information asset?*
`Head of the Department`

(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows: High level Management. Senior Software Engineers. HR managers.	**100%**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: High level Management. HR managers.	**100%**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows: High level Management. Senior Software Engineers. HR managers.	**99%**
	This asset must be available for **20 hours**, **7 days/week**, **50 weeks/year**.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows: Authentication, Non – Repudiation.	**100%**

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ **Confidentiality**	❑ Integrity	❑ Availability	❑ Other

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
`Customer Information System`	This asset holds every data related to customers of the organization. If by chance Confidentiality, Integrity or Availability of this system is violated, it will cause severe damage (Such as reputation problems) to the organization.	Customer Information system is a system which is used by the organization to get the information about the customers efficiently.

(4) Owner(s) *Who owns this information asset?*
`Head of the Department`

(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows: High level Management, Employees.	**100%**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: High level Management, Employees.	**100%**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows: High level Management, Employees.	
	This asset must be available for **20 hours**, **7 days/week**, **50 weeks/year**.	**99%**
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ **Confidentiality**	❑ Integrity	❑ Availability	❑ Other

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
`Daily Project Progress system.`	This system is used to store the daily activities done by the organization (stored in a daily basis). If by chance Confidentiality, Integrity or Availability of this system is violated, it will cause severe damage to the organization.	Daily project progress system will store the activities in a daily basis.

(4) Owner(s) *Who owns this information asset?*
`Head of the Department`

(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows: High level Management, Authorized employees (Senior software engineers, Junior software engineers, Assistant software engineers, Interns)	**100%**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: High level Management, Authorized employees (Senior software engineers, Junior software engineers, Assistant software engineers, Interns)	**100%**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows: High level Management, Authorized employees (Senior software engineers, Junior software engineers, Assistant software engineers, Interns) High level Management, Authorized employees (Senior software engineers, Junior software engineers, Assistant software engineers, Interns)	**99%**
	This asset must be available for **20 hours**, **7 days/week**, **50 weeks/year**.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ Confidentiality	❑ **Integrity**	❑ Availability	❑ Other

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Organization's critical IT hardware including firewall, main servers	This asset is important as it supports in the process of developing software (Which is the main purpose of our organization). If availability or integrity is violated it will provide a huge damage to the organization.	The main asset which helps in the process of developing software.
(4) Owner(s) *Who owns this information asset?*		
Head of the Department		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: High level management, authorized employees in the IT department.	**100%**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows: High level management, authorized employees in the IT department.	**99%**
	This asset must be available for **20 hours**, **7 days/week**, **50 weeks/year**.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	❑ **Availability** ❑ Other

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Threat	Information Asset	Customer Information system, Finance information system, daily project progress system.	
		Area of Concern	SQL Injection	
		(1) Actor *Who would exploit the area of concern or threat?*	Hacker	
		(2) Means *How would the actor do it? What would they do?*	The attacker get access to the network by the mobile application, because of the weakness of the application attack did a SQL injection and got access to the data base.	
		(3) Motive *What is the actor's reason for doing it?*	Financial gain or make damage to the reputation.	
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	This attack will result in interruption and will violate the confidentiality requirement define in the asset sheet. 100% requirement will be violated by 30minuets.	
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **90%**	❑ **Medium** **50%** ❑ **Low** **25%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
From SQL injection attacker can get access to the customer sensitive data. because of that customer's confidence about this company will loss. Then the reputation also will decrease. the impact value is high.	Reputation & Customer Confidence	8	4
The matter of customer loss financially also will impact.	Financial	5	2.5
Because of the attack security department should work hard and do over time to overcome this.	Productivity	9	4.5
	Safety & Health	0	0
The chances of attacker get caught is very low.	Fines & Legal Penalties	3	1.5
	User Defined Impact Area	-	-

Relative Risk Score	12.5

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	❑ Defer	❑ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Mobile application	Instead of saving credit card credentials in the sever side, we can save them in customer side.
Application	Update and patch
Data base	Reduce your attack surface. Get rid of any database functionality that you don't need to prevent a hacker taking advantage of it

Quantitative Risk Analysis:

Critical Asset ⟶ Customer Information System

1) Risk factors :-

i. SQL Injection
ii. Cross Site Scripting (XSS)
iii. DDoS Attack
iv. Fire
v. Hardware Malfunction

2) Historical Attitude :-

- Our company has faced DDoS attacks in the past. Actually, this has happened to our company twice in a row. At the very 1st time this happened, we didn't even know that the system was down due to a DDoS attack. Although the systems alerts were enabled, they did not work properly. It took about half an hour to identify that the system was down due to a DDoS attack. But soon after the identification of it, our team was able to successfully fix the system back to the normal within an hour.

- Our company also faced a SQL Injection attack once. Although the necessary security solutions were pre-implemented, they failed to protect the system against the attack. However, our team was able to successfully identify the attack with several minutes due to the automatic system alert triggering system. With the assistance of the tech lead, we were able to overcome this issue within an hour.

- In last year, our company faced a sudden hardware malfunction. This included the malfunction of system servers and firewalls. At the moment our company did not have enough amount of backup hardware. Although the issue was identified within several minutes, it took about 2 full days to fix this issue entirely. On this occasion, our company had to spend lot of money on purchasing new & reliable backup hardware.

3) Determining the Value of Asset :-

Tangible :-

1) Market Value of Customer Information Server = Rs. 350,000/=
2) Senior Database Administrator (Team Leader) = Rs. 250,000/=
3) Backup tools ***(Contingency)*** = **- Rs. 900,000/=**
4) Installation cost = Rs. 150,000/=
5) Troubleshooting cost = Rs. 250,000/=
6) Depreciation = **- Rs. 500,000/=**
7) Loss of business services to outside customers = Rs. 3,000,000/=
8) Loss of business services to internal employees = Rs. 5,000,000/=

Intangible :-

1) Data & information in Customer Information Server = Rs. 1,000,000/=
2) Research & Development = Rs. 500,000/=
3) Marketing = Rs. 700,000/=
4) Middleware Platform (Software) with licensed OS = Rs. 800,000/=
5) License & software Update Rs. 1,500,000/=

Total Value of the Asset = Rs. 12,100,000/=

4) Exposure Factor :- *(On Average)*

✓ **Initial Exposure Factor = 100%**

i. Does the system under attack have any redundancies/ backups/ copies?

- Yes
- Exposure Factor = 100% - 30% = 70%

ii. Is the system under attack behind a firewall?

- Yes
- Exposure Factor = 70% - 10% = 60%

iii. Is the attack from outside?

- Yes
- Exposure Factor = 60% - 20% = 40%

iv. What is the potential rate of attack?

- 10% damage/hr.
- Exposure Factor = 40% - 10% = 30%

v. What is the likelihood that the attack will go undetected in time for a full recovery?

- Less than 20%
- Exposure Factor = 30% - 10% = 20%

vi. How soon can a countermeasure be implemented in time if at all?

- Within 2 hours
- Exposure Factor = 20% - 10% = 10%

Final Exposure Factor = 10% ***(On Average)***

5) Single Loss Expectancy :- *(Based on each threat scenario)*

Risk/ Threat Scenario	Asset Value	Exposure Factor	SLE
1) SQL Injection	Rs. 12,100,000/=	10%	**Rs. 1,210,000/=**
2) Cross Site Scripting (XSS)	Rs. 12,100,000/=	12%	**Rs. 1,452,000/=**
3) DDoS Attack	Rs. 12,100,000/=	15%	**Rs. 1,815,000/=**
4) Fire	Rs. 12,100,000/=	8%	**Rs. 968,000/=**
5) Hardware Malfunction	Rs. 12,100,000/=	9%	**Rs. 1,089,000/=**

6) Annualized Rate of Occurrence :- *(Based on each threat scenario)*

Risk/ Threat Scenario	Source	ARO
1) SQL Injection	CSI	5
2) Cross Site Scripting (XSS)	Symantec	2
3) DDoS Attack	Stephens	0.5
4) Fire	Kensington	0.1
5) Hardware Malfunction	Symantec	0.5

7) Annualized Loss Expectancy :- *(Based on each threat scenario)*

Risk/ Threat Scenario	SLE	ARO	ALE
1) SQL Injection	Rs. 1,210,000/=	5	**Rs. 6,050,000/=**
2) Cross Site Scripting (XSS)	Rs. 1,452,000/=	2	**Rs. 2,904,000/=**
3) DDoS Attack	Rs. 1,815,000/=	0.5	**Rs. 907,500/=**
4) Fire	Rs. 968,000/=	0.3	**Rs. 290,400/=**
5) Hardware Malfunction	Rs. 1,089,000/=	0.5	**Rs. 544,500/=**

8) Safeguards :- *(Based on each threat scenario)*

Risk/ Threat Scenario	Controls
1) SQL Injection	• Input validation & use of parameterized queries. • Give a mandatory training for the security team.
2) Cross Site Scripting (XSS)	• Use appropriate response headers. • Filter input on arrival. • Encode data on output.
3) DDoS Attack	• Develop a Denial-of-Service Response Plan. • Secure Your Network Infrastructure. • Practice Basic Network Security.
4) Fire	• Reduce the likelihood of ignition. • Establish fire detection devices such as heat sensors. • Design fire evacuation plans.
5) Hardware Malfunction	• Create a regulatory-scheduled maintenance plan.

9) Cost of the Safeguards :- *(Based on each threat scenario)*

Risk/ Threat Scenario	One-Time Cost	Annual (Continual) Cost	Total Cost
1) SQL Injection	Provide mandatory training for the security team. → **Rs.200000/=**	License cost → **Rs.10000/=** Service cost → **Rs. 5000/=**	**Rs. 215,000/=**
2) Cross Site Scripting (XSS)	Implement a proper Data Filtering Mechanism. → **Rs.100000/=**	License cost → **Rs.10000/=** Service cost → **Rs. 5000/=**	**Rs. 115,000/=**
3) DDoS Attack	Secure the Network Infrastructure. → **Rs.250000/=**	Maintenance cost → **Rs.7000/=** Service cost → **Rs.5000/=**	**Rs. 262,000/=**
4) Fire	Purchasing necessary hardware & tools. → **Rs.100000/=**	Maintenance cost → **Rs.30000 /=** License cost → **Rs.10000/=** Service cost → **Rs. 5000/=**	**Rs. 145,000/=**
5) Hardware Malfunction	Purchase industry-standard hardware. → **Rs.300000/=**	Maintenance cost → **Rs.20000/=** Service cost → **Rs.5000/=**	**Rs.325,000/=**

10) **New Annualized Loss Expectancy** :- ***(After the safeguards)***

Risk/ Threat Scenario	Asset Value	New EF	New SLE	New ARO	New ALE
1) SQL Injection	Rs. 12,100,000/=	5%	Rs. 605,000/=	2.5	**Rs. 1,512,500/=**
2) Cross Site Scripting (XSS)	Rs. 12,100,000/=	6%	Rs. 726,000/=	1	**Rs. 726,000/=**
3) DDoS Attack	Rs. 12,100,000/=	8%	Rs. 968,000/=	0.2	**Rs. 193,600/=**
4) Fire	Rs. 12,100,000/=	4%	Rs. 484,000/=	0.05	**Rs. 24,200/=**
5) Hardware Malfunction	Rs. 12,100,000/=	5%	Rs. 605,000/=	0.25	**Rs. 151,250/=**

Critical Asset ⟶ Organization's critical IT hardware including firewalls, servers.

1) Risk factors :-

i. Hardware malfunctioning
ii. Fire
iii. Lightning
iv. Power Faults
v. Hardware Theft

2) Historical Attitude :-

- A fire happened in the company in 2015. The fire happened just after 1 month our company started. Our company is a two storied building and the fire happened on the first floor. Most of our IT hardware was installed on the 2nd floor. Luckily, nothing happened to the critical hardware because we were able to control the fire before the fire spreads to the second floor. But our first floor was severely damaged, and we had to close the company for 4 months continuously to repair the building.

- In 2019, a customer tried to enter to the server room, However the customer was caught red handed because the security saw the man trying to enter to the server room from the CCTV cameras and when we asked from the person the reason why he tried to enter the server room he was speechless. Then the responsible people took him to the required authorities and took the actions required.

- About two months ago, A hardware malfunction happened in firewall hardware. The firewall got shutdown for 1 hour. Luckily, any sort of unauthorized attack did not happen at this time. After about one hour, our team was able to fix the problem and firewall came back to normal.

3) Determining the Value of Asset :-

Tangible:

Market value of critical IT hardware = Rs.32,670,000

Installation cost = Rs.100,000

Troubleshooting cost = Rs.200,000

Technician = Rs.30,000

Intangible:

License & software Updates= Rs.100,000

Total Asset Value = Rs.32,270,000

4) Exposure Factor :-

- Hardware malfunctioning = 20%
- Fire = 40%
- Lightning = 40%
- Power Faults = 30%
- Hardware Theft = 20%

5) **Single Loss Expectancy** :- ***(Based on each threat scenario)***

Risk/ Threat Scenario	Asset Value	Exposure Factor	SLE
1) **Hardware malfunctioning**	Rs. 32,270,000/=	20%	**Rs.645,400,000**
2) **Fire**	Rs. 32,270,000/=	40%	**Rs.1,290,800,000**
3) **Lightning**	Rs. 32,270,000/=	40%	**Rs.1,290,800,000**
4) **Power Faults**	Rs. 32,270,000/=	30%	**Rs.968,100,000**
5) **Hardware Theft**	Rs. 32,270,000/=	20%	**Rs.645,400,000**

6) **Annualized Rate of Occurrence** :- ***(Based on each threat scenario)***

Risk/ Threat Scenario	ARO
1) **Hardware malfunctioning**	4
2) **Fire**	0.25
3) **Lightning**	0.25
4) **Power Faults**	3
5) **Hardware Theft**	3

7) Annualized Loss Expectancy :- *(Based on each threat scenario)*

Risk/ Threat Scenario	SLE	ARO	ALE
1) **Hardware malfunctioning**	Rs.645,400,000	4	**Rs.2,581,600,000**
2) **Fire**	Rs.1,290,800,000	0.25	**Rs. 322,700,000**
3) **Lightning**	Rs.1,290,800,000	0.25	**Rs. 322,700,000**
4) **Power Faults**	Rs.968,100,000	3	**Rs. 2,904,300,000**
5) **Hardware Theft**	Rs.645,400,000	3	**Rs.1,936,200,000**

8) Safeguards

i. **Hardware malfunctioning** –use a regulatory-scheduled maintenance plan.
ii. **Fire** – Automatic Fire detectors and fire extinguishers
iii. **Lightning**- Lighting protection system
iv. **Power Faults** – Surge protector
v. **Hardware Theft**- Biometric door locks

9) Cost of Safeguards

//Assume the safeguards are 3 years

Cost of safeguards:

For Hardware malfunctioning:

One time cost = Rs.100,000

For one year = 100,000 / 3 = 33,333.33

Annual cost

- Maintenance cost = Rs.20,000
- Service cost = Rs.20,000

Total cost of safeguard = Rs.73,333.33

For Fire:

One time cost = Rs.30,000

For one year = Rs.10,000

Annual cost

- Maintenance cost = Rs.10,000
- Service cost = Rs.10,000

Total cost of safeguard = Rs.30,000

For Lightning:

One time cost = Rs.150,000

For one year = Rs50,000

Annual cost

- Maintenance cost = Rs.40,000
- Service cost = Rs.20,000

Total cost of safeguard = Rs.110,000

For Power Faults:

One time cost = Rs.50,000

For one year = 50,000/3 = 16,666.66

Annual cost

- Maintenance cost = Rs.10,000
- Service cost = Rs.10,000

Total cost of safeguard = Rs.36,666.66

For hardware Theft:

One time cost = Rs.300,000

For one year = 300,000/3 = 100,000

Annual cost

- Maintenance cost = Rs.40,000
- Service cost = Rs.30,000

Total cost of safeguard = Rs.170,000

10) **New Annualized Loss Expectancy** :- ***(After the safeguards)***

Risk/ Threat Scenario	Asset Value	New EF	New SLE	New ARO	New ALE
1) Hardware Malfunctioning	Rs. 32,270,000/=	5%	Rs. 161,350,000	1	Rs. 161,350,000
2) Fire	Rs. 32,270,000/=	10%	Rs.322,700,000	0.125	Rs. 40,337,500
3) Lightning	Rs. 32,270,000/=	10%	Rs.322,700,000	0.125	Rs. 40,337,500
4) Power Faults	Rs. 32,270,000/=	10%	Rs.322,700,000	1	Rs.322,700,000
5) Hardware Theft	Rs. 32,270,000/=	5%	Rs. 161,350,000	1	Rs. 161,350,000

Critical Asset ⟶ Daily Project Progress System

1) Risk factors :-

i. DDoS Attack
ii. SQL Injection
iii. Natural Disaster
iv. Hardware Malfunction
v. Data modification by internal member

2) Historical Attitude :-

- Our company has faced a natural disaster in April of 2020. This was the first time that we faced this kind of disaster. Suddenly our server room gets fire. And all the servers went down due to the fire. However, our smoke detectors alert us about the fire. we called to fire brigade and until they come, we try to stop it from getting spread to other servers. It took 1 hour to stop the fire. Because of this, our servers went down for 6 hours and our all systems were stopped.

- Data Modification by an internal staff member has caused us a huge reputation loss and customer loss. We could not identify this issue until our customer asks their project. When a customer asks about his project and we show them our agreement which is saved in our system. It said that we had another year to finish it. Then the customer showed his copy of the agreement it said that we should give it in last week. We arranged a meeting with staff members and discussed. At that time, we could be able to identify there was a data modification.

3) Determining the Value of Asset :-

Tangible :-

1) Market Value of Project Progress System Server = Rs. 600,000/=
2) Installation cost = Rs. 150,000/=
3) Troubleshooting cost = Rs. 100,000/=
4) Backup server system = **- Rs. 700,000/=**
5) Depreciation = **- Rs. 300,000/=**
6) Loss of business services to outside customers = Rs. 3,000,000/=
7) Loss of business services to internal employees = Rs. 5,000,000/=

Intangible :-

1) Computer software = Rs. 200,000/=
2) Project data = Rs. 1,020,000/=

Total Value of the Asset = Rs. 9,070,000/=

4) Exposure Factor :- *(Based on each threat scenario)*

i. Natural disaster = **20%**
ii. DDoS attack = **10%**
iii. SQL Injection = **20%**
iv. Hardware Malfunction = **5%**
v. Data modification by internal member = **50%**

5) Single Loss Expectancy :- *(Based on each threat scenario)*

Risk/ Threat Scenario	Asset Value	Exposure Factor	SLE
1) Natural disaster	Rs. 9,070,000/=	20%	**Rs. 1,814,000/=**
2) DDoS attack	Rs. 9,070,000/=	10%	**Rs. 907,000/=**
3) SQL Injection	Rs. 9,070,000/=	20%	**Rs. 1,814,000/=**
4) Hardware Malfunction	Rs. 9,070,000/=	5%	**Rs. 453,500/=**
5) Data modification by internal member	Rs. 9,070,000/=	50%	**Rs. 4,535,000/=**

6) Annualized Rate of Occurrence :- *(Based on each threat scenario)*

Risk/ Threat Scenario	Source	ARO
1) Natural disaster	CSI	0.5
2) DDoS attack	Symantec	1
3) SQL Injection	Stephens	2
4) Hardware Malfunction	Kensington	3
5) Data modification by internal member	Symantec	0.5

7) Annualized Loss Expectancy :- *(Based on each threat scenario)*

Risk/ Threat Scenario	SLE	ARO	ALE
1) Natural disaster	Rs. 1,814,000/=	0.5	**Rs. 907,000/=**
2) DDoS attack	Rs. 907,000/=	1	**Rs. 907,000/=**
3) SQL Injection	Rs. 1,814,000/=	2	**Rs. 3,628,000/=**
4) Hardware Malfunction	Rs. 453,500/=	3	**Rs. 1,360,500/=**
5) Data modification by internal member	Rs. 4,535,000/=	0.5	**Rs. 2,267,500/=**

8) Safeguards :- *(Based on each threat scenario)*

Risk/ Threat Scenario	Controls
1) Natural disaster	• Set fire alarms. • Reduce the likelihood of ignition. • Design fire evacuation plans.
2) DDoS attack	• Develop a Denial-of-Service Response Plan. • Secure Your Network Infrastructure. • Practice Basic Network Security.
3) SQL Injection	• Input validation & use of parameterized queries. • Give a mandatory training for the security team.
4) Hardware Malfunction	• Create a regulatory-scheduled maintenance plan.
5) Data modification by internal member	• Install biometric security system.

9) Cost of the Safeguards :- *(Based on each threat scenario)*

Risk/ Threat Scenario	One-Time Cost	Annual (Continual) Cost	Total Cost
1) Natural disaster	Purchasing necessary hardware & tools. → **Rs.100000/=**	Maintenance cost → **Rs.30000 /=** License cost → **Rs.10000/=** Service cost → **Rs. 5000/=**	**Rs. 145,000/=**
2) DDoS attack	Secure the Network Infrastructure. → **Rs.250000/=**	Maintenance cost → **Rs.7000/=** Service cost → **Rs.5000/=**	**Rs. 262,000/=**
3) SQL Injection	Provide mandatory training for the security team. → **Rs.200000/=**	License cost → **Rs.10000/=** Service cost → **Rs. 5000/=**	**Rs. 215,000/=**
4) Hardware Malfunction	Purchase industry-standard hardware. → **Rs.300000/=**	Maintenance cost → **Rs.20000/=** Service cost → **Rs.5000/=**	**Rs. 325,000/=**
5) Data modification by internal member	Install biometric security system. → **Rs.400000/=**	Maintenance cost → **Rs. 25000/=** License cost → **Rs.10000/=** Service cost → **Rs. 5000/=**	**Rs. 440,000/=**

10) New Annualized Loss Expectancy :- *(After the safeguards)*

Risk/ Threat Scenario	Asset Value	New EF	New SLE	New ARO	New ALE
1) Natural disaster	Rs. 9,070,000/=	10%	Rs. 907,000/=	0.5	**Rs. 453,500/=**
2) DDoS attack	Rs. 9,070,000/=	5%	Rs. 453,500/=	0.5	**Rs. 226,750/=**
3) SQL Injection	Rs. 9,070,000/=	5%	Rs. 453,500/=	1	**Rs. 453,500/=**
4) Hardware Malfunction	Rs. 9,070,000/=	3%	Rs. 272,100/=	1	**Rs. 272,100/=**
5) Data modification by internal member	Rs. 9,070,000/=	20%	Rs. 1,814,000/=	0.1	**Rs. 181,400/=**

Critical Asset → Finance information system

1) Risk factors :-

i. Viruses
ii. Human errors
iii. Fire
iv. Hardware malfunction
v. Unauthorized access

2) Historical Attitude :-

- Once, an employee who was working in our company accidently deleted some important finance data regarding our company. unfortunately, our employees did not know that modification till the month end. At that moment our company did not have any backup mechanism regarding Finance system. But we maintained a manual written log files to maintain our finance accounts. Because of that we were able to correct those errors but after spend two days. After that incident our company had to bought new backup drives for Finance system.

- Also, our finance system had to face a virus attack. That virus changed the file extensions. Because of that virus, our important log files were corrupted. However luckily, due to our backup mechanisms our technical team were able to recover our finance system.

- Last month, an employee who worked in another department were accidently logged into our finance system. Luckily it was an accident, and he was reported that immediately to the admin. The reason for that incident is our poor authorization policy. After that incident company was immediately re-create new policies for authorizations.

3) Determining the Value of Asset :-

- **Tangible**

1) Market value of finance information system server = Rs. 1,000,000/=
2) Installation cost = Rs. 300,000/=
3) Troubleshooting cost = Rs. 200,000/=
4) Backup sever system = Rs 1,000,000/=
5) Depreciation = Rs. 100,000/=
6) Loss of business services to outside customers = Rs. 3,000,000/=
7) Loss of business services to internal employees = 5,000,000/=

- **Intangible**

1) Computer software = Rs. 500,000/=
2) Finance data = Rs. 1,600,000
3) Sales data = Rs. 500,000/=

- **Total value of the asset = Rs. 11,000,000/=**

4) Exposure Factor :- *(On Average)*

Initial exposure factor = 100%

1. Does the system under attack have any redundancies/ backups/ copies?
   Yes, Exposure factor = 100% - 30% = 70%

2. Is the system under attack behind a firewall?
   Yes, Exposure Factor = 70% -10% = 60%

3. Is the attack from outside?
   Yes, Exposure Factor = 60% -20% = 40%

4. What is the potential rate of attack?
   10% damage/hr, Exposure Factor = 40% -10% = 30%

5. What is the likelihood that the attack will go undetected in time for a full recovery?
   Less than 20%, Exposure Factor = 30% -10% = 20%

6. How soon can a countermeasure be implemented in time if at all?
   Within 2 hours, Exposure Factor = 20% -10% = 10%

   Final exposure factor = 10% (on average)

5) Single Loss Expectancy :- *(Based on each threat scenario)*

Risk/ Threat Scenario	Asset Value	Exposure Factor	SLE
1) Viruses	Rs. 11,000,000/=	5%	**Rs. 1,100,000/=**
2) Human errors	Rs. 11,000,000/=	15%	**Rs. 1,650,000/=**
3) Fire	Rs. 11,000,000/=	15%	**Rs. 1,650,000/=**
4) Hardware malfunction	Rs. 11,000,000/=	10%	**Rs. 1,000,000/=**
5) Unauthorized access	Rs. 11,000,000/=	10%	**Rs. 1,000,000/=**

6) Annualized Rate of Occurrence :- *(Based on each threat scenario)*

Risk/ Threat Scenario	Source	ARO
1) Viruses	CSI	6
2) Human errors	Symantec	24
3) Fire	Stephens	0.1
4) Hardware malfunction	Kensington	0.5
5) Unauthorized access	Symantec	0.5

7) Annualized Loss Expectancy :- *(Based on each threat scenario)*

Risk/ Threat Scenario	SLE	ARO	ALE
1) Viruses	**Rs. 1,100,000/=**	6	**Rs. 6,600,000/=**
2) Human errors	**Rs. 1,650,000/=**	24	**Rs. 39,600,000/=**
3) Fire	**Rs. 1,650,000/=**	0.5	**Rs. 825,000/=**
4) Hardware malfunction	**Rs. 1,000,000/=**	0.5	**Rs. 500,000/=**
5) Unauthorized access	**Rs. 1,000,000/=**	0.5	**Rs. 500,000/=**

8) Safeguards :- *(Based on each threat scenario)*

Risk/ Threat Scenario	Controls
1) Viruses	• Use a proper virus guard. • Apply security policies when using third party devices.
2) Human errors	• Conduct training sessions for employees. • Implement proper accountability mechanisms.
3) Fire	• Conduct training sessions for employees. • Implement fire control mechanisms. • Design fire evacuation plans.
4) Hardware malfunction	• Implement proper service and maintain routines. • Create backup plans.
5) Unauthorized access	• implement a heavy password policy. • Create granting levels to employees.

9) Cost of the Safeguards :- *(Based on each threat scenario)*

Risk/ Threat Scenario	One-Time Cost	Annual (Continual) Cost	Total Cost
1) Viruses	Implement virus guards → **Rs.100000/=**	License cost → **Rs.20000/=** Service cost → **Rs. 5000/=**	**Rs. 125,000/=**
2) Human errors	Training sessions for employees → **Rs.100000/=**	License cost → **Rs.30000/=** Service cost → **Rs. 10000/=**	**Rs. 140,000/=**
3) Fire	Implement fire control mechanisms → **Rs.200000/=**	Maintenance cost → **Rs.25000/=** Service cost → **Rs.15000/=**	**Rs. 240,000/=**
4) Hardware malfunction	Create a service routine → **Rs.10000/=**	Maintenance cost → **Rs.60000 /=** Service cost → **Rs. 20000/=**	**Rs. 90,000/=**
5) Unauthorized access	Create and implement password policies and granting levels. → **Rs.100000/=**	Maintenance cost → **Rs.10000/=** Service cost → **Rs.5000/=**	**Rs.115,000/=**

10) New Annualized Loss Expectancy :- *(After the safeguards)*

Risk/ Threat Scenario	Asset Value	New EF	New SLE	New ARO	New ALE
1) Viruses	Rs. 11,000,000/=	2%	Rs. 220,000/=	2	**Rs. 440,000/=**
2) Human errors	Rs. 11,000,000/=	8%	Rs. 880,000/=	12	**Rs. 10,560,000/=**
3) Fire	Rs. 11,000,000/=	5%	Rs. 550,000/=	0.01	**Rs. 5,500/=**
4) Hardware malfunction	Rs. 11,000,000/=	5%	Rs. 550,000/=	0.1	**Rs. 55,000/=**
5) Unauthorized access	Rs. 11,000,000/=	4%	Rs. 440,000/=	0.1	**Rs. 44,000/=**