Sri Lanka Institute of Information Technology

IT3070 – Information Assurance & Security

BSc (Hons) in Information Technology
3rd Year 1st Semester
Faculty of Computing
SLIIT – 2024

Name	Registration number	Batch number	Workload Distribution
Liyanahetti L.H.R.S. D	IT22592088	Y3. S1.03.01	Policy management system- • Critical Information Asset Profile • Information Asset Risk Worksheet 1 • Information Asset Risk Worksheet 2
Udesha S.M. S	IT22586902	Y3. S1.03.02	Customer Relationship management system- • Critical Information Asset Profile • Information Asset Risk Worksheet 1 • Information Asset Risk Worksheet 2
Gunathilaka K.R. D	IT22571120	Y3. S1.03.01	Financial management system- • Critical Information Asset Profile • Information Asset Risk Worksheet 1 • Information Asset Risk Worksheet 2

Table of Content

Introduction

This section contains worksheet examples from a multinational Insurance and Finance Cooperation (**AIA**) assessment. The goal of this example is to show how to completed OCTAVE® Allegro worksheets by considering three main IT related assets. And we have discussed about the actual risks to assets and how to mitigate the risk. This assessment focuses on the three most important factors in determining "information risk," which impacts the **confidentiality**, **integrity**, and **availability** of systems and data.

In this assessment we mainly focus on

1. Policy Management System
2. Customer Relationship Management System
3. Financial Management System

As IT related assets in AIA insurance company. We discuss about the

- What is the asset?
- Why is this information asset important to the company?
- What type of hardware and software components used in the assets?
- What are the security requirements for this information asset?
- What are the risks?
- How to mitigate the risk?

By this OCTAVE® Allegro worksheets. We use Employee Trust and Moral as our User Defined Impact Area in worksheet10.

1.Policy Management System

1.1 Critical Information Asset Profile

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?*
Policy Management System	This asset handles the entire lifecycle of insurance policies. This ensures that policies are managed and administered. This asset enables efficient customer management by automating policies. This asset reduces manual errors and increases operational efficiency. This asset helps ensure that policies comply with legal and regulatory requirements. This system keeps data about policyholders, policy, claims,	This asset automates the issuance of new policies, renewing policies, stores detailed records for all active and inactive policies. This asset used SQL Databases such as Microsoft SQL Server or Oracle DB as database and in some cases, NoSQL like MongoDB used to store unstructured data. This asset typically run on Windows Server or Linux based operating system. This asset typically runs on high-speed internet connection with strong security protocols. This asset uses secure network connections provided via VPNs and cloud infrastructure
(4) Owner(s) *Who owns this information asset?*		
Chief Information Security Officer and IT Security Team		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Customers and Chief Information Security Officer and IT Security Team are authorized to access to policy management to see policies relevant to them.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Chief Information Security Officer and IT Security Team have authorized to update, renew and remove policies. But customers are unauthorized to edit policies.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The system is operational 24/7 to allow customers to access it for processing claims and security team to policy renewals, updates, and customer service.
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	

❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	The system can handle high volumes of transactions, especially during peak periods such as renewal deadlines or claims surges.

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

1.2. Information Asset Risk Worksheet 1

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	**Threat**	Information Asset	Policyholder databases
		Area of Concern	An agent steal data and selling information to a third party.
		(1) Actor *Who would exploit the area of concern or threat?*	insider
		(2) Means *How would the actor do it? What would they do?*	Steal sensitive policyholder information in the system by misusing his access. The agent would access, download, or copy sensitive data, attempt to cancel their tracks, and then sell the stolen data to third parties
		(3) Motive *What is the actor's reason for doing it?*	Deliberate

		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	In this case, the **primary security requirement breached** is **confidentiality** Confidentiality of this asset is violated by the agent when steals data and sell it to third party If an agent may also modify certain policy or claims information to gain financial advantage this would lead to an integrity breach If the agent attempts to disrupt or block access to the information by deleting or altering records, it could affect availability.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **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**
A breach of this nature would severely damage the company's reputation. Policyholders trust the company to protect their personal information, and such a breach would significantly erode that trust.	Reputation & Customer Confidence	9	4.5
	Financial	8	4
Customer complaints, investigations, and legal issues resulting from the breach will divert resources from day-to-day operations. Employees may need to focus on crisis management rather than their usual tasks, leading to reduced overall productivity.	Productivity	7	3.5
	Safety & Health	5	2.5
If the breach is the result of negligence or a lack of internal controls, the company could face significant fines and legal penalties from regulatory bodies. This could include fines under data protection regulations.	Fines & Legal Penalties	8	4
	Employee Trust & Morale	7	3.5
		Relative Risk Score	**22**

(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?*
Administrative	1. Develop and enforce strict access control policies, ensuring that employees only have access to data necessary for their job function. 2. Educates employees about the consequences of data theft and the importance of reporting suspicious behavior. 3. Provide regular training on data security and privacy practices.
Technical Controls	1. Use advanced monitoring and logging systems to detect unusual access patterns or unauthorized data exports. 2. Encrypt sensitive data both in transit and at rest to protect it from unauthorized access
Physical Controls	1. Physically secure data centers and server rooms by restricted access using key cards, biometric scanners, and security personnel. 2. Limit physical access to the system and monitor access logs
Residual Risk	1. Technical controls and monitoring systems might fail or be bypassed, leading to potential data breaches. 2. Despite strong controls, there is always a risk that a determined insider may find ways to exploit security measures.

Justification of probability of impact values

Attribute	Values	Justifications
(6) Probability	50%	As this is a large cooperation this likelihood would be appropriate if the organization has some level of internal controls and monitoring but still has areas of vulnerability, such as broad access permissions or occasional lapses in monitoring
Reputation & Customer Confidence	9	Loss of trust and long-term reputational damage is highly severe due to the sensitivity of the breach.
Financial	8	Direct financial losses, legal fees, and the cost of damage control will be substantial.
Productivity	7	Diverted resources and a loss of focus will reduce operational efficiency, though less than financial impacts.
Safety and health	5	Sensitive health data breaches can lead to potential harm to individuals but have a limited scope.
Fines & Legal Penalties	8	Regulatory fines and legal liabilities are likely to be severe, especially under data protection laws.
Employee Trust & Morale	7	Employee morale may suffer if they feel unsafe or distrustful of management's response

1.3. Information Asset Risk Worksheet 2

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Policyholder database, Claim database		
		Area of Concern	DDoS attack		
		(1) Actor *Who would exploit the area of concern or threat?*	outsider		
		(2) Means *How would the actor do it? What would they do?*	Involves flooding the system with excessive traffic, and system become inaccessible to the legitimate users.		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate		
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	In this case, the **primary security requirement breached is availability**. Attackers flood the servers with a high volume of traffic, exceeding its capacity to process legitimate requests. This causes service slowdowns or a complete outage. And leaving the system unable to perform normal operations. As a result, policyholders, agents, and employees cannot access the PMS to view or update policy information, process claims, or handle customer request During the attack, attackers might try to infiltrate the network and steal sensitive policyholder information. Attackers may attempt to modify or corrupt data in the system while the system is overloaded and weakened.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **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**
	A DDoS attack can severely damage the company's reputation, especially if it leads to prolonged downtime or service unavailability. Customers may lose trust in the organization's ability to secure its systems, which can result in a loss of business and diminished customer loyalty.	Reputation & Customer Confidence	7	5.25
		Financial	8	6
	A DDoS attack disrupts normal business operations as IT teams and other departments must focus on responding to the attack rather than performing their regular duties. In severe cases, the entire business may come to a halt if key systems are affected.	Productivity	6	2.7
		Safety & Health	9	6.75
	while a DDoS attack may not directly lead to regulatory fines unless it results in data theft or a breach of compliance, certain industries could face legal action if service disruptions result in significant damage to customers.	Fines & Legal Penalties	8	6
		Employee Trust & Morale	5	3.75
			Relative Risk Score	**30.45**

(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?*
Administrative	1. Establish a dedicated team trained to identify and mitigate DDoS attacks. 2. Ensure a well-documented and regularly updated incident response plan is in place to quickly respond to DDoS attacks.
Technical Controls	1. limit the number of requests a user can make in a specified time frame, helping prevent an overload of the system 2. se web application firewalls and intrusion prevention systems to block traffic from suspicious or malicious IP addresses.

Physical Controls	1. Ensure that physical data centers hosting the system have high levels of security, including restricted access, 24/7 monitoring, and environmental controls. 2. Have geographically distributed backup data centers or cloud regions.
Residual Risk	1. Attackers might use more sophisticated DDoS techniques. 2. As DDoS attack methods evolve, attackers may discover new vulnerabilities or weaknesses that current controls don't fully address.

Justification of probability of impact values

Attribute	Values	Justifications
(6) Probability	75%	Given the critical nature of the PMS in an insurance company, the potential exposure to the internet, and the industry's attractiveness as a target, the likelihood of a DDoS attack is generally **High (75%)** unless strong DDoS mitigation measures are in place.
Reputation & Customer Confidence	7	Service unavailability damages trust, especially if downtime is prolonged
Financial	8	Lost revenue and the cost of mitigation make financial losses significant, particularly in online industries.
Productivity	6	Operations are disrupted, diverting resources to handle the crisis.
Safety and health	9	Service downtime can impact safety-critical systems, especially in healthcare or emergency services.
Fines & Legal Penalties	8	Legal penalties are less likely unless there is a regulatory or contractual breach.
Employee Trust & Morale	5	Prolonged attacks can cause stress and frustration, impacting morale.

2.Customer Relationship management system

2.1. Critical Information Asset Profile

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 Relationship Management System	The CRM system is a vital asset for AIA as it centralizes all customer data, including personal details, transaction history, and communication records. This asset is crucial for managing customer relationships, delivering personalized services, and ensuring operational efficiency. Protecting the CRM system is vital for maintaining customer trust, complying with legal regulations, and preventing financial and reputational damage from data breaches or loss.	The CRM system is a software platform that manages customer data, including personal details, policy history, communication logs, and transaction records. It allows AIA employees, such as customer service and sales staff, to access and manage customer information securely. Data is encrypted during transmission and at rest, and access is restricted based on role-based permissions to protect data integrity and confidentiality. This asset used SQL Databases such as Microsoft SQL Server or Oracle DB as database and in some cases, NoSQL like MongoDB used to store unstructured data. This asset typically run on Windows Server or Linux based operating system. This asset typically runs on high-speed internet connection with strong security protocols. This asset uses secure network
(4) Owner(s) *Who owns this information asset?*		
IT Department & Customer Relations Department		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Only authorized personnel, such as customer service and IT staff, can view or modify customer information to prevent unauthorized access or data breaches.

❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Data should be accurate, up-to-date, and protected against unauthorized modification or deletion.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	This asset must be available for authorized personnel to perform their duties effectively.
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	The CRM system must be available 24/7 to support global operations, ensuring that customer data is accessible at any time.
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Compliance with data protection regulations like GDPR and local privacy laws is mandatory to protect customer data.

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

☑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

2.2. Information Asset Risk Worksheet 1

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Customer Relationship Management (CRM) System		
	Area of Concern	Unauthorized Access		
	(1) Actor *Who would exploit the area of concern or threat?*	outsider		
	(2) Means *How would the actor do it? What would they do?*	Attacker could attempt phishing attacks to trick employees into revealing login credentials. Using these credentials, they could gain unauthorized access to the CRM, exposing sensitive customer information.		
	(3) Motive *What is the actor's reason for doing it?*	deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure**	❑ **Destruction**	
		❑ **Modification**	❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Confidentiality would be compromised due to unauthorized access to customer data.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **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**
Loss of customer trust and damage to reputation	Reputation & Customer Confidence	9	4.5
	Financial	9	4.5
Financial losses due to potential lawsuits and regulatory fines	Productivity	7	3.5
	Safety & Health	5	2.5
Disruption to business operations	Fines & Legal Penalties	9	4.5
	Employee Trust & Morale	6	3

Relative Risk Score	**22.5**

(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?*
Administrative	• Conduct regular cybersecurity training for employees on phishing and secure access practices. • Develop and enforce an incident response plan for CRM breaches to ensure a quick, coordinated response to unauthorized access incidents.
Technical	• Implement multi-factor authentication (MFA) and deploy intrusion detection systems. • Apply **data masking** for sensitive customer information, so that even if unauthorized access occurs, sensitive data remains obfuscated.
Physical	• Restrict access to the data center where the CRM servers are housed. • Ensure that any devices accessing the CRM (e.g., employee laptops) are physically secured and require authentication to use (e.g., **lock screens**, **secure workstations**).
Residual Risk	• A small risk remains due to advanced phishing techniques that may bypass existing controls. • Even with robust access controls, there remains a risk of employees or contractors with legitimate access abusing their privileges (malicious insiders)

Justification of probability of impact values

Attribute	Values	Justifications
(6) Probability	50%	If this organization has moderate security in place (such as password protection, role-based access control, and regular monitoring), but lacks more advanced security measures like multi-factor authentication or encryption of sensitive data, the probability of unauthorized access could be medium
Reputation & Customer Confidence	9	Loss of trust due to customer data exposure can severely damage the company's reputation.
Financial	8	Regulatory fines, legal fees, and customer compensation will result in substantial financial losses.
Productivity	7	Diverting resources to handle the breach will affect operational efficiency.
Safety and health	5	CRM systems generally don't involve safety-critical data, but in some industries, the impact could be higher.
Fines & Legal Penalties	8	Significant fines and penalties may arise from violations of data protection laws.
Employee Trust & Morale	7	Internal morale may suffer due to a lack of confidence in security measures.

2.3. Information Asset Risk Worksheet 2

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Customer database		
	Area of Concern	Data Corruption		
	(1) Actor *Who would exploit the area of concern or threat?*	insider		
	(2) Means *How would the actor do it? What would they do?*	An employee may accidentally input incorrect customer data, delete records, or modify key information due to inadequate training. Alternatively, a disgruntled employee could intentionally manipulate or delete customer data.		
	(3) Motive *What is the actor's reason for doing it?*	accidental		
	(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?*	The integrity of the data would be breached if data is altered or deleted without authorization, leading to inaccurate or unreliable customer information.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **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**
Operational disruptions due to inaccurate data	Reputation & Customer Confidence	8	4
	Financial	9	4.5
Loss of data integrity, leading to customer dissatisfaction	Productivity	7	3.5
	Safety & Health	4	2
Potential financial losses from corrective actions	Fines & Legal Penalties	8	4

		Employee Trust & Morale	6	3
			Relative Risk Score	**21**

(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?*
Administrative	• Provide continuous training to staff on proper data management and implement clear data handling guidelines. • Implement data access controls that define who can create, edit, or delete records within the CRM. This should be role-based to minimize exposure to those who don't need certain permissions.
Technical	• Set up regular backups, version control, and automated data validation checks to detect errors. • Apply input validation mechanisms in the CRM system to prevent accidental or malicious data corruption
Physical	• Restrict physical access to server rooms and apply environmental controls to prevent damage. • Ensure that all devices accessing the CRM, such as workstations and laptops, are physically secured and that access to these devices is restricted when unattended.
Residual Risk	• A minor risk of accidental data changes remains due to human error, despite controls. • Bugs or vulnerabilities within the CRM software itself that go unnoticed during testing may cause data corruption over time, especially during updates or maintenance.

Justification of probability of impact values

Attribute	Values	Justifications
(6) Probability	50%	The organization has moderate protections in place, such as regular backups, but these backups are not always verified for integrity.
Reputation & Customer Confidence	8	Customer trust will erode if data corruption leads to poor service or incorrect information.
Financial	9	Lost sales, recovery costs, and compensation can lead to substantial financial losses.
Productivity	7	Employees will need to spend significant time recovering data or addressing issues caused by corrupted data.
Safety and health	4	Minimal impact unless the CRM contains safety-critical information, in which case the consequences could be higher.
Fines & Legal Penalties	8	Potential legal liabilities if data corruption leads to compliance violations or mishandling of sensitive data.
Employee Trust & Morale	6	Repeated data issues will cause frustration and negatively impact employee morale.

3.Financial Management System

3.1Critical Information Asset Profile

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?*
Financial Management System	This system is the backbone in handling AIA's financial activities, such as billing, accounting, and financial reporting. It provides the necessary regulatory compliance, an accurate track of finances, and flow of cash. Without it, some of the major business functions dependent on it include severely disrupted processes like bill payments, revenues, and conduction of financial audits.	The AIA insurance handles all the financial transactions over the Financial Management System. It controls the billing, accounts payable/receivable, claims processing, and financial reports which are required internally or by statute. It further integrates with the other systems in such a way that there is smooth movement of financial data within the departments.
(4) Owner(s) *Who owns this information asset?*		
The Finance Department		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Authorized persons such as financial analysts, accountants, and auditors should access this system. Strict access controls must be enforced to prevent unauthorized access to sensitive financial data.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Authorized financial and IT persons can modify data within the system. Modifications should be logged and tracked to ensure data accuracy and auditability.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	System must be available to authorized persons during business hours, 5 days a week, for 52 weeks a year. Extended availability is needed during financial reporting periods.

	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	The system should be compatible with the industry standard-for example, the Sri Lanka Accounting and Auditing Standards Act-when it generates financial reports, and all other relevant local and international financial laws, regulations, and directives of the Central Bank of Sri Lanka and the Sri Lanka Accounting Standards-SLFRS.

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

3.2. Information Asset Risk Worksheet 1

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Financial Reporting System		
		Area of Concern	Incorrect Generation or Manipulation of Financial Reports		
		(1) Actor *Who would exploit the area of concern or threat?*	insider		
		(2) Means *How would the actor do it? What would they do?*	accidental		
		(3) Motive *What is the actor's reason for doing it?*	Internal actors could alter financial reports to present enhanced performance, mislead regulators, or conceal financial irregularities that they could highlight.		
		(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?*	In the Payment Processing System, Confidentiality, Integrity, and Availability are highly important components of the process, which must be strictly followed in their implementation. The prevention of unauthorized changes and the maintenance of the payment record's integrity are the main goals of this system. Therefore, the access to it should be heavily restricted to only those who are authorized, and authentication methods such as multi-factor authentication (MFA) should be used. Encryption of sensitive information, whether it is stored or transmitted, is the most important measure of confidentiality. Availability is secured by having regular system backups and disaster recovery plans in place, so that the availability of payments is not hampered. Monitoring tools should be in place to identify any abnormal transaction activities or unauthorized access attempts, and regular auditing should be done to keep the system well-protected.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **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**
	If the financial reports of our system are faulty, there is a high probability of stakeholder trust being lost.	Reputation & Customer Confidence	9	4.5
		Financial	10	5
	The operations may be delay due to the correction or regeneration of the financial records.	Productivity	7	3.5
		Safety & Health	4	2
	Fines for misrepresenting financial statements or financial losses that occur due to incorrect reporting or if errors result in financials being misstated are a possibility.	Fines & Legal Penalties	10	5
		User Defined Impact Area	6	3
			Relative Risk Score	**23**

(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?*
Administrative	1. Establish multiple layers of approval for all financial reports, ensuring that no report is finalized without thorough review by authorized personnel. 2. Conduct frequent audits of financial reporting processes and reports to identify discrepancies and enforce compliance with internal policies and regulatory requirements.
Technical	1. Use software to automate the generation of financial reports, reducing human error and adding validation checks to flag inconsistencies or anomalies. 2. Implement regular, encrypted backups of financial data to ensure integrity and availability in case of data loss or corruption.
Physical	1. Limit access to locations where financial reports are generated and stored to authorized personnel only, using ID badges, biometric authentication, or security locks. 2. Install cameras and maintain access logs in areas where financial reporting takes place, to track any unauthorized physical access attempts.

Residual Risk	1. Despite automation and controls, there remains a risk of human errors during report creation or approval. 2. Unidentified software bugs or system failures could still affect the accuracy of financial data, even with automated processes in place.

Justification of probability of impact values

Attribute	Values	Justifications
(6) Probability	50%	The organization has moderate access controls and financial reports go through some level of review, but gaps still exist that could allow errors or manipulation. That's why I choose this percentage.
Reputation & Customer Confidence	9	Manipulated or incorrect financial reports can severely damage trust among investors and customers.
Financial	10	Significant financial loss could occur due to incorrect decision-making, fines, and loss of investor confidence.
Productivity	7	Productivity will decrease due to the need to investigate and correct errors, diverting resources.
Safety and health	4	Indirect impact on safety or health in industries where financial health directly affects operations.
Fines & Legal Penalties	10	Severe legal consequences due to violations of financial regulations and accounting standards.
Employee Trust & Morale	6	Employee morale can be impacted if financial integrity is compromised, affecting trust within the organization.

3.3. Information Asset Risk Worksheet 2

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Payment Processing System		
		Area of Concern	Unauthorized Transactions and Data Manipulation		
		(1) Actor *Who would exploit the area of concern or threat?*	insider		
		(2) Means *How would the actor do it? What would they do?*	deliberate		
		(3) Motive *What is the actor's reason for doing it?*	Financial gain by stealing funds or manipulating transactions for personal benefit.		
		(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?*	Security must be maintained by regulating access to the system through user controls, identity and access management, and encrypting payments information while stored and while in transit to guard against alteration or unauthorized intrusion. Payment transactions must be safeguarded to prevent their modification by unauthorized individuals, meaning that data should be accurate and valid from time to time by conducting some validations. Availability should be maintained through physical security of servers, having backup, and having contingency to ensure that the system is up and running without interruption.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	✓ **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**
	Customers may lose confidence if payments are delayed or manipulated.	Reputation & Customer Confidence	9	4.5
		Financial	10	5
	Direct financial losses through theft or fraud, potential compensation may affect to the customers.	Productivity	7	3.5
		Safety & Health	4	2.0
	Payment processing delays cause workflow interruptions.	Fines & Legal Penalties	9	4.5
		Employee Trust & Morale	6	3
		Relative Risk Score		**22.5**

(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?*		
Administrative	1. It is recommended to check the list of payment transactions on a regular basis to identify any unauthorized or suspicious activities. 2. Implement a least-privilege policy where users only have the access necessary for their role, and regularly review access rights to ensure they are up-to-date.		
Technical	1. Make users to use more than one method of identification such as passwords and/or an app on their mobile devices before they can get access to the payment processing system. 2. Make sure that payment details are protected at the time of storage and when they are in transit so as to avoid any form of tampering.		
Physical	1. Minimize the physical contact with the data centers or the places where the payment servers are located to only those with the necessary privileges. 2. Have cameras in the payment processing areas and keep records of people that gain physical access to the area.		

Residual Risk	1. Still, there can be other less well-known vulnerabilities that have not been patched, or vulnerabilities in other software. 2. Though security controls are implemented, there is always a chance that an authorized person will misuse the privileges granted to him or her.

Justification of probability of impact values

Attribute	Values	Justifications
(6) Probability	50%	Moderate access controls are in place, but there may still be gaps, such as weak user authentication or insufficient segregation of duties.
Reputation & Customer Confidence	9	Unauthorized access to financial data damages customer trust and the company's reputation.
Financial	1	Direct financial losses, compensations, legal fees, and penalties result in significant costs.
Productivity	7	Resources are diverted to manage the breach, disrupting normal business operations.
Safety and health	4	Little to no direct impact on physical safety or health, except in cases of disrupted services in critical sectors.

Fines & Legal Penalties	9	Non-compliance with financial regulations results in steep fines and potential legal action.
Employee Trust & Morale	6	Internal morale suffers due to stress, fear, and frustration caused by the incident

References

[1] "AIA Group Limited," [Online]. Available: https://www.aia.com/en. [Accessed 19 September 2024].

[2] "Cloudflare, Inc.," 19 September 2024. [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/.

[3] "Wikimedia Foundation, Inc.," 19 September 2024. [Online]. Available: https://en.wikipedia.org/wiki/Denial-of-service_attack.

[4] Hacker Noon via Medium, 11 September 2018. [Online]. Available: https://medium.com/bugbountywriteup/risk-assessment-vs-vulnerability-assessment-which-assessment-should-you-conduct-hacker-noon-a926a6fde9e6. [Accessed 19 September 2024].