Sri Lanka Institute of Information Technology

Human Computer Interaction - IT3060

Risk Management Assignment

Group No – Y3.S1.WD.IT.0101

Ceylinco Life

Ceylinco Life is one of the leading providers of life insurance services in Sri Lanka; it is particularly noted for offering an extended range of insurance services to suit different individual and family requirements. It was founded with the vision to improve financial security and peace of mind by offering a broad portfolio of services that range from life insurance to retirement plans to health insurance. It follows a customer-centric approach to provide customized service and innovative protection plans that meet the emerging needs of its clientele. Backed by more than 36 years of experience, Ceylinco Life is unique in the commitment it has made to protect the aspirations and well-being of its policyholders.

Selected Asset	Student ID	Name
Policyholder Database	IT22196460	U.U.M. Hewage
Document Management System(DMS)	IT22253408	Sandaruwan K.A.D.C
Payment Gateway System	IT22245724	Jayasundara H.M.H.D

Content

1. Qualitative Analys

1.1. Probability Values

Qualitative Scale	Numeric Scale	Description
Low	25%	May occur occasionally
Medium	50%	Is as likely as no to occur
High	75%	Is likely to occur

1.2. Impact

Qualitative Scale	Numerical Scale	Description
Very Low	1	Negligible impact
Low	2	Minor impact on time, cost, or quality
Medium / Moderate	4	Notable impact on time, cost, or quality
High	8	Substantial impact on time, cost, or quality
Very High	16	Threatens the success of the company

2. U.U.M. Hewage - IT22196460

2.1. Asset Profile Document (Allegro Worksheet 8)

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?*
Policyholder Database	The policyholder database contains sensitive information about the company's clients.	This is a database of client's personal details, insurance plans, and financial records. This database is hosted in a cloud-base infrastructure, utilizing high-performance servers and storage systems. The hardware includes enterprise-grade servers and redundancy. The data is storage array to ensure scalability, reliability, and data redundancy. The data is stored in secure, geographically distributed data
(4) Owner(s) *Who owns this information asset?*		
Data Management Department		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Policyholders should only access to view their personal information, such as policy details and payment history. This access should be read-only, ensuring that they cannot modify any sensitive information.

❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Only authorized personnel from the Data Management Department are allowed to edit, modify, or add new data to the policyholder database. Specific selections, such as personal identification details and policy coverage information, can only be edited by senior managers. Other sections, like payment history, can be updated by billing staff. Policyholders and unauthorized staff members are not allowed to modify any data in the system, ensuring that only trusted personal can make changes to critical information.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The policy holder database must be accessible 24/7 to ensure uninterrupted service for both internal staff and policyholders information, process claims, and assist clients. Any down time severely impact operations, delay customer service, and result in potential loss of business.
	This asset must be available for _24_ hours, _7_ days, _52_ weeks.	100% availability is required during peak insurance periods, such as the end of the fiscal year when at their highest.
❑ **Authentication**	This asset has special regulatory compliance protection requirements, as follows:	Role-based access control (RBAC) is implemented for accessing the policyholder database. Each user is assigned roles that dictate their level of access based on their job responsibilities. This system ensures that only authorized personal can view or modify sensitive client information according to their role in the organization.

(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 worksheets (Allegro Worksheet 10– I

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Policyholder database		
	Area of Concern	An internal employee with access privilege misuses their access to steal sensitive information		
	(1) Actor *Who would exploit the area of concern or threat?*	Disgruntled current employee		
	(2) Means *How would the actor do it? What would they do?*	The employee uses their authorize access to download policyholder data for personal or financial gain.		
	(3) Motive *What is the actor's reason for doing it?*	To sell sensitive policyholder information or use it for malicious purposes.		
	(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?*	Only authorized employees with specific role and clearances should have access to modify the Policyholder Database. Access should be restricted based on the principle of least privilege, ensuring that only those with a legitimate need can view or alter the data. Additionally, all access should be logged and reviewed regularly to detect any unauthorized activity.		
	(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 insider data theft goes unnoticed, the organization could face significant financial repercussions and severe blow to its reputation. The breach of sensitive policyholder information could	Reputation & Customer Confidence	9	4.5

	encode customer trust, leading to a loss of confidence in the company's ability to safeguard personal data. This decline in reputation can result in decreased customer retention and difficulty attracting new clients. Financially, the company could incur high cost from legal actions, fines and compensation, alongside increase expenses for new security measures.	Financial	8	4
	If the insider data theft occurs, significant labor will be required to audit and review system access, investigate the breach, and implement corrective actions, leading to reduced productivity and increased operational costs. While there may be no direct impact on safety and health, the stress and pressure on staff involved in managing the incident could affect their	Productivity	4	2
		Safety & Health	2	1
	Exposure of sensitive policyholder data may lead to significant fines and potential lawsuits, as the organization could be held liable for violating data protection regulations. In the **User Defined Impact Area,** such as **Compliance,** the breach could trigger audits and increased scrutiny from regulatory bodies, requiring costly compliance and overhauls and further legal actions.	Fines & Legal Penalties	8	4
		User Defined Impact Area	7	3.5
			Relative Risk Score	**19**

(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?*
User Activity Monitoring	**Administrative Controls:** ▪ Create regulations that demand regular audits of user access logs. Examine high-risk users and issue alerts of any suspicious activities. **Technical Controls:** ▪ Use powerful monitoring technologies to log and evaluate user behavior in real time. A security information and Event Management (SIEM) system, for example, can be used to detect and report on unusual data access patterns or illegal efforts to extract significant volumes of sensitive information.

	Physical Controls: ▪ Limit physical access to servers and data centers to vetted workers.
Multi-Factor Authentication (MFA)	**Administrative Controls:** ▪ Regularly examine access controls and ensure that users follow stringent authentication methods. Conduct monthly checks to ensure that only the necessary persons have access. **Technical Controls:** ▪ Set up multi-factor authentication (MFA) for all workers who have access to the policyholder database. This increase security by needing more than a password to access sensitive data, such as a one-time code or biometric authentication.
Role-Based Access Control (RBAC)	**Administrative Controls:** ▪ Create a policy for periodically reviewing access rights to ensure that workers' access to sensitive data is still justified based on their job duties. **Technical Controls:** ▪ Use role-based access control (RBAC) to restrict access to the policyholder database based on employment role. Employees should only have access to the data they need to complete their tasks.
Data Encryption	**Administrative Controls:** ▪ Employes should be trained on the necessity of encryption. As well as given rules for property managing encrypted data. Also, make sure encryption keys are stored in secure locations. **Technical Controls:** ▪ Encrypt sensitive policyholder data both at rest and during transit. This assures that even if the data is accessed or stolen, it will be unintelligible without the proper decryption keys.
Incident Response Plan	**Administrative Controls:** ▪ Create an implement a through incident response plane that focuses on insider risks. This plan should describe what steps to take if suspicious conduct is noticed, as well as how to respond in the event of data theft. **Technical Controls:** ▪ Integrate automated system that can send alerts and lockdown if insider data theft is discovered, as well as launch per-configure incident response methods.
Employee Awareness and Training Programs	**Administrative Controls:** ▪ Provide regular training sessions to staff on insider threats and the necessity of data confidentiality. Emphasize the legal and economic impact of data theft on the organization and its personnel.

	Physical Controls: ▪ Create simulations or exercises for staff to practice spotting and responding to suspicious conduct involving data access.

2.2.1 Justification of severity values

Attribute	Value	justification
Probability	50%	The likelihood is medium for this threat scenario, since human error is common in such routine maintenance tasks, even if preventive controls are in place. Employees may accidentally delete or alter sensitive data despite policies and training.
Reputation & Customer Confidence	9	Failure to promptly address data integrity issues could cause serious damage to the organization's reputation. The policyholders will lose confidence in the organization to protect their information, and this could lead to loss of clients and negative publicity.
Financial	8	The cost in terms of financial expenses would increase due to elaborate recovery operations, compensation to customers, and maybe even new measures of security. This would be heavier in terms of financial consequences on the health of the organization.
Productivity	7	The recovery of altered or lost data will require huge resources, thereby reducing operational efficiency. Employees will concentrate on correcting errors, thus delaying other business activities.

Safe and health	2	There may be increased stress associated with this incident since some employees might be stressed recovering data, but no risk to physical safety would occur.
Fines & Legal Penalties	7	If the breach in security involves some regulatory standards, such as data protection laws, significant fines could be levied against an organization, or other legal penalties impeding operations. The greater the impact on customer data, the higher the risk of serious financial consequences.
User Define Impact Area	7	There may be an increased tendency toward compliance reviews and audits, resulting in higher operational costs. The organization can fall deeper into scrutiny, needing to put in place even stronger measures than usual, affecting other areas of business.

2.3. Information asset risk worksheets (Allegro Worksheet 10) – II

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Policyholder database		
		Area of Concern	Accidental deletion or modification of data by an employee during routine updates or maintenance.		
		(1) Actor *Who would exploit the area of concern or threat?*	IT staff		
		(2) Means *How would the actor do it? What would they do?*	During system changes, an employee inadvertently alters or removes important customer data.		
		(3) Motive *What is the actor's reason for doing it?*	An error made during standard database maintenance.		
		(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?*	Only authorized IT staff with specific roles and permissions should be allowed to perform updates or modifications to Policyholder Database. Access should be restricted to minimize the risk of accidental data changes, and all changes must be logged and reviewed to maintain data integrity.		
		(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 accidental data deletion or modification goes unnoticed, it could result in serious financial losses for the company. Inaccurate policyholder data may result in mistakes throughout the claims processing procedure, which could cause financial losses or involve paying clients compensation. Furthermore, policyholders' confidence in the organization may be momentarily damaged if they are unable to obtain accurate data, which could have an effect on customer retention.	Reputation & Customer Confidence	8	2
		Financial	6	1.5
	If accidental data deletion or modification occurs, a significant amount of work will be needed to audit and restore the policyholder information that is impacted. This will cause a temporary decrease in production as IT professionals and other staff members concentrate on data recovery operations. Employee well-being and morale may be impacted by the increased effort and stress from fixing the problem, even while there are no direct effects on safety and health	Productivity	7	1.75
		Safety & Health	2	0.5
	Accidental deletion or change of policyholder data may result in fines or legal penalties if it violates data protection standards, particularly if it causes considerable data loss. In the User Defined Impact Area, the organization may face heightened scrutiny from regulatory agencies, requiring audits and maybe tougher compliance measures to avoid future errors.	Fines & Legal Penalties	4	1
		User Defined Impact Area	6	1.5
			Relative Risk Score	**8.25**

(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?*
Automated Backups	**Administrative Controls:** ▪ Create a policy that requires frequent testing of backup restorations to ensure data integrity and recovery processes. **Technical Controls:** Implement daily or weekly automated backups of the Policyholder Database. Backups should be saved in a secure, off-site place so that data may be restored in the event of corruption.

	Physical Controls: ▪ Backup media is securely stored at a disaster-resilient facility, ensuring both on-site and off-site backups.
Data Integrity checks	**Administrative Controls:** ▪ Implement Standard Operating procedures (SOPs) for employee performing updates, emphasizing on integrity-checking processes before finalizing changes. **Technical Controls:** ▪ Implement regular data validation tools that can detect irregularities in the database. This allows for early detection of unauthorized alterations or corruption.
User Training Programs	**Administrative Controls:** ▪ Providing ongoing training for IT employees, emphasizing best practices during database updates and maintenance operations to reduce human error. **Physical Controls:** ▪ Include hands-on training or simulations to assist employee practice error recovery.
Access Control and Auditing	**Administrative Controls:** ▪ Conduct routine audits on all database activity to ensure transparency and accountability. Keep audit logins secure and review them often to detect any unauthorized changes. **Technical Controls:** ▪ Strengthen access controls by implementing role-based access to limit who can make crucial database changes.
Changes Management Procedures	**Administrative Controls:** ▪ Implement tight change management procedures. To reduce error during updates, all policyholder database revisions should be explicitly reviewed and approved by a supervisor prior to implementation. **Technical Controls:** ▪ Use version control software to log any database changes and allow for rollbacks when needed.

2.3.1 Justification of severity values

Attribute	Value	justification
Probability	25%	This is less likely to happen because there are strong access controls and role-based permissions, with periodic audits taking place. This will reduce the likelihood of accidental data modification or deletion by employees performing routine maintenance.
Reputation & Customer Confidence	8	Temporary damage to the organization's reputation due to accidental modification or deletion of data is possible. The confidence in maintaining accurate records by the organization from the policyholder may be lost, and that will affect customer retention.
Financial	6	The financial impact involves costs related to recovery operations and possible compensation for the errors in policyholder data. However, since this is an accident, the overall financial impact remains moderate.
Productivity	7	The process of recovery from backup or readjustment will involve immense efforts, which will divert IT staff and productivity for the time being. This would be noticed but still manageable
Safe and health	2	The situation could increase tensions on employees dealing with data recovery and restoration. No direct impact on physical safety
Fines & Legal Penalties	4	Data loss as a result of negligence might cause compliance issues resulting in fines. However, these

		fines are not that severe compared to those imposed as a result of an actual breach in a deliberate manner. The organization might be under inquiry upon the interest of regulators.
User Define Impact Area	6	Compliance requirements can increase in the form of more regulatory audits. Resources would thereby be consumed more, and efficiency in operation would be at least partially affected.

3. Sandaruwan K.A.D.C - IT22253408

3.1. Asset Profile Document (Allegro Worksheet 8)

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?*
Document Management System(DMS)	The DMS is essential for managing and safeguarding the organization's vital documents. It handles contracts, employee records, financial documents, and other sensitive information crucial to business operations. The DMS ensures compliance with legal standards and provides secure, efficient document storage and retrieval.	The DMS serves as a centralized, cloud-based repository for document management. It ensures version control, role-based access, data encryption, and comprehensive access logging. The system is designed to be scalable and resilient, with redundancy features that minimize downtime.
(4) Owner(s) *Who owns this information asset?*		
IT and Document Control 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 can access documents within the system based on their roles. Document Owners and Administrators may have full access to view, edit, and manage the documents. Other users, such as Collaborators or Viewers, may only have restricted access based on permissions, ensuring that sensitive documents can only be viewed or modified by those with appropriate authorization**.**

❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Only authorized personnel can modify documents stored in the DMS. This ensures that the content of critical documents remains accurate and trustworthy. Document Owners or designated Administrators are the only individuals permitted to edit, update, or delete documents within the system. Specific document categories (e.g., contracts, legal documents) can only be modified by senior management or individuals with high-level clearance, ensuring that key information is handled by those with the required expertise.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The Document Management System (DMS) must be accessible 24/7 to ensure that authorized personnel can access critical documents whenever needed. This is essential for smooth business operations, enabling employees to retrieve, share, and collaborate on documents without interruption. Internal staff such as managers, administrators, and collaborators rely on uninterrupted access to perform tasks, make decisions, and manage projects efficiently.
	This asset must be available for __24___ hours, __7___ days/week, __52___ weeks/year.	The system should guarantee 100% availability during critical business periods, such as major project deadlines, financial audits, or legal reviews, to ensure that document access is never compromised.

❑ **Authentication**	This asset has special regulatory compliance protection requirements, as follows:	Role-based access control (RBAC) is implemented to govern access to the DMS. Each user is assigned specific roles based on their job functions, ensuring that only authorized personnel can access, view, or modify documents. Users are classified into roles such as Administrator, Editor, Viewer, or External Collaborator, and their permissions are restricted to only what is necessary for their responsibilities. For example, administrators can manage all documents, while viewers may only have read-only access to certain files.

(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 worksheets (Allegro Worksheet 10) – I

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	Document management system		
	Area of Concern	Data Leakage via Unauthorized File Sharing		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	Unauthorize employee or external hacker		
	(2) Means *How would the actor do it? What would they do?*	The actor gains access to sensitive documents and shares them externally without permission		
	(3) Motive *What is the actor's reason for doing it?*	Financial gain or revenge		
	(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?*	Security requirements for a document management system would be breached through unauthorized file sharing, leading to data leakage, bypassing access controls, and compromising confidentiality of sensitive 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**
• Sensitive information leaks can severely damage reputation and customer confidence, leading to lost trust, legal consequences and financial loss. • Exposure of sensitive document can lead to legal liabilities, fines and compensation claims, increasing financial risk and regulatory scrutiny.	Reputation & Customer Confidence	7	3,5
	Financial	8	4

	• Investigating and responding to a breach disrupts normal operations, diverts resources, delays projects, and impacts overall business productivity. • Data leakage via unauthorized sharing generally has minimal safety and health impact unless it involves health data or safety protocols.	Productivity	6	3
		Safety & Health	2	1
	• Sensitive information leaks can result in significant fines and penalties under data protection laws like GDPR, HIPAA, or industry-specific regulations. • Impacts vary by organization, including operational continuity, IP protection, or compliance; relevance depends on specific business model and regulations.	Fines & Legal Penalties	4	2
		User Defined Impact Area	6	3
		Relative Risk Score	**16.5**	

(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?*		
Data Access Controls	**Administrative Control** • Regularly review and update the access control lists (ACLs) to ensure that only the necessary personnel have access. Implement procedures to immediately revoke access for employees who leave the organization or change roles. **Technical Control** • Implement role-based access controls (RBAC) to ensure that employees can only access documents that are relevant to their roles. This restricts unauthorized employees from viewing or sharing sensitive documents. **Physical Control** • Limit access to physical servers or systems that house the DMS to authorized personnel only, ensuring that sensitive documents cannot be accessed through physical means		

File Encryption	**Administrative Control** • Establish encryption policies and require that all documents classified as sensitive or confidential are encrypted**.** **Technical Control** • Encrypt sensitive documents both in storage and during transmission to prevent unauthorized individuals from intercepting or reading the data. Use strong encryption standards
Employee Training and Awareness	**Administrative Control** • Conduct regular training sessions for employees on the risks of unauthorized file sharing and the importance of maintaining document confidentiality. Provide education on how to recognize and avoid social engineering attacks, such as phishing, which may lead to accidental document sharing. **Physical Control** • Incorporate simulations or practical workshops to help employees practice handling sensitive documents securely.

3.2.1 Justification of severity values

Attribute	Value	justification
Probability	50%	A 50% probability indicates a moderate risk, where existing security measures reduce but don't eliminate threats. Vulnerabilities may still be exploited due to moderate exposure, past incidents, or system complexity
Reputation & Customer Confidence	7	Sensitive information leaks can severely damage the company's reputation, leading to a loss of customer trust, negative media coverage, and legal consequences.
Financial	8	Financial losses may arise from breach response costs, including investigation, recovery, legal fees, and compensation for affected individuals.
Productivity	6	Breach incidents disrupt business operations, divert resources to mitigation efforts, and lead to delays in normal tasks or projects.
Safe and health	2	While most breaches don’t directly affect safety and health, data leaks involving personal, or health information could pose moderate safety risks.
Fines & Legal Penalties	4	Legal penalties, fines, and lawsuits can follow if regulatory standards like GDPR are violated due to mishandling of sensitive data.
User Define Impact Area	6	Additional impacts such as operational continuity, protection of intellectual property (IP), or industry-specific regulatory compliance. Varies based on business model.

3.3. Information asset risk worksheets (Allegro Worksheet 10) – II

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Information Asset	Document Management System		
	Area of Concern	Accidental Deletion of Important Documents		
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Internal employee	
		(2) Means *How would the actor do it? What would they do?*	The employee mistakenly deletes critical documents from the system.	
		(3) Motive *What is the actor's reason for doing it?*	No malicious intent, purely accidental	
		(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?*	The accidental deletion compromises the integrity of the document management system because it causes the unintended loss or alteration of data. The system no longer contains the complete set of critical documents as intended, leading to gaps or inaccuracies in the information it holds.	
		(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**

	The accidental loss of critical documents could affect trust between the organization and its customers or partners, especially if key documents (contracts, agreements, reports) are lost. This could lead to a moderate impact on the organization's reputation, particularly if clients rely on those documents for ongoing projects.	Reputation & Customer Confidence	9	2.25
	The accidental loss of critical documents could affect trust between the organization and its customers or partners, especially if key documents (contracts, agreements, reports) are lost. This could lead to a moderate impact on the organization's reputation, particularly if clients rely on those documents for ongoing projects.	Financial	8	2
	There will likely be a significant productivity hit as employees spend time recovering deleted documents, restoring backups, or recreating lost work. This diverts resources away from other important tasks.	Productivity	7	1.75
	This may not apply unless the documents directly impact safety-related operations or health records. In most cases, this impact will be minimal or not applicable.	Safety & Health	5	1.25
	If the documents are required for regulatory compliance or are legally mandated to be stored, the loss could result in fines or legal penalties. This can have severe financial and reputational consequences, depending on the jurisdiction and the type of documents.	Fines & Legal Penalties	7	1.75
		User Defined Impact Area	8	2
			Relative Risk Score	**11**

(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?*
Automated Document Backups	**Administrative Control** • Establish a policy that requires periodic testing of backup recovery processes to ensure that they function correctly, and data integrity is maintained

	Technical Control • Set up automated, regular backups for all documents within the DMS. Ensure that backup copies are stored in a secure, off-site or cloud-based location. Implement versioning systems that maintain multiple versions of a document, allowing easy recovery of previous versions in case of accidental deletion. **Physical Control** • Secure backup servers or storage locations to prevent unauthorized access or tampering with backups**.**
Document Archiving	**Administrative Control** • Establish a retention policy that defines how long documents should be archived before deletion is permitted. **Technical Control** • Set up a document archiving system that prevents the permanent deletion of important files for a specified retention period. Instead of direct deletion, documents should be moved to an archive where they can be reviewed before being permanently deleted.
Monitoring and Auditing	**Administrative Control** • Conduct regular audits of document deletion logs to ensure compliance with organizational policies and spot any unauthorized or accidental deletions early **Technical Control** • Enable detailed logging and monitoring of all deletion activities within the DMS. Use these logs to track which documents are deleted, by whom, and when. Implement automated alerts for abnormal deletion patterns that may indicate an issue

3.3.1 Justification of severity values

Attribute	Value	justification
Probability	25%	Due to strong cybersecurity measures and the rarity of external attacks, the likelihood of this threat scenario occurring is low. Most organizations follow best practices
Reputation & Customer Confidence	9	Significant reputation damage could occur if sensitive information is leaked. Customers may lose trust, leading to a decline in business and negative media coverage.
Financial	8	Financial losses could include investigation, mitigation, and legal fees. Lost business from affected clients may also lead to a substantial revenue drop.
Productivity	7	Incident response could severely disrupt daily operations, causing a drop in productivity as staff focus on recovering from the breach and restoring normal operations.
Safe and health	5	Although this primarily affects information security, breaches in sectors like healthcare or insurance could indirectly harm the safety and health of clients.
Fines & Legal Penalties	7	Legal penalties could arise from failing to secure sensitive data, especially under regulations like PDPA. This could lead to lawsuits, fines, or regulatory sanctions.
User Define Impact Area	9	Additional business-specific impacts, such as loss of competitive advantage or disruption of supply chains, could be significant, causing further harm to the organization.

4. Jayasundara H.M.H.D - IT22245724

4.1. Asset Profile Document (Allegro Worksheet 8)

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?*
Payment Gateway System	The Payment Gateway System is premium and efficiently. It is critical for maintaining cash flow, customer satisfaction, and trust.	The Payment Gateway System is an online platform used by the insurance company to process payments from clients, including credit card transactions, bank transfers, and other digital payment methods.
(4) Owner(s) *Who owns this information asset?*		
IT Department & 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:	Only authorized personnel can view this information asset. This includes IT staff, finance team members, and other designated individuals involved in transaction processing and security
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Only authorized personnel can modify this information asset. Any changes must be made by authorized IT and finance staff.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	This asset must be available for these personnel to do their jobs. IT support and finance staff.
	This asset must be available for __24___ hours, ____7_ days/week, ___52__ weeks/year.	Payment Gateway System should always be accessible without interruption, ensuring seamless transaction handling and customer satisfaction

❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	This asset has special regulatory compliance protection requirements, including adherence to Payment Card Industry Data Security Standards and other relevant financial and data protection regulations

(6) Most Important Security Requirement

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

❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

4.2. Information asset risk worksheets (Allegro Worksheet 10) – I

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Payment Gateway System		
		Area of Concern	Phishing attack (Unauthorized users into disclosing sensitive payment information)		
		(1) Actor *Who would exploit the area of concern or threat?*	Unauthorized user or group		
		(2) Means *How would the actor do it? What would they do?*	The unauthorized user creates a fake payment portal or phishing email and take the sensitive payment information.		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate-The phishing attacks can steal payment credentials (credit card numbers, CVVs, Bank details). Attackers can be used to commit fraud. Such as hacking or stealing money directly from insured accounts. And also, they can sell data		
		(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?*	Use strong encryption to protect sensitive payment data during transmission and storage and can implement secure protocols for communication. And also, can train users to recognize phishing attempts and understand the importance of not disclosing sensitive 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**
	A Phishing attack on payment gateway system could damage the company's reputation due to exposure of		Reputation & Customer	5	3.75

	sensitive payment information, customer trust and unavailability could lead to user frustration. Financial losses from fraudulent transactions, potential compensations to affected clients, and costs associated with rectifying the breach.	Financial	8	6
	Increased workload for investigating and resolving the phishing attack.	Productivity	3	2.25
		Safety & Health	4	3
	Potential legal consequences and fines due to non-compliance with data protection regulations and failure to secure sensitive information.	Fines & Legal Penalties	7	5.25
		User Defined Impact Area	0	0
			Relative Risk Score	**20.25**

(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 Controls	• Regular training programs to educate users on recognizing phishing attempts and safeguarding sensitive information. • Develop and maintain an incident response plan for handling phishing attacks. • Implement strict access control policies to limit access to sensitive payment information.
Technical Controls	• Deploy advanced email filtering solutions to detect and block phishing emails. • Use strong encryption protocols to secure data in transit and at rest • Implement tools to detect and block phishing websites and fraudulent communications.
Residual Risk	• Sophisticated phishing attacks that bypass detection tools. • Users might still fall victim to phishing attempts despite training. • New and emerging phishing methods that could exploit unforeseen vulnerabilities.

4.2.1 Justification of severity values

Attribute	Value	justification
Probability	75%	Phishing attacks on payment systems are highly likely due to the valuable nature of sensitive payment data, and the increasing sophistication of phishing techniques.
Reputation & Customer Confidence	5	A successful attack could severely damage the company's reputation by compromising sensitive customer information, which could erode customer trust and loyalty.
Financial	8	Phishing attacks can result in fraudulent transactions, compensations, and recovery costs, leading to significant financial losses.
Productivity	3	Addressing the attack would consume significant internal resources, slowing down operations and affecting day-to-day productivity due to investigations and recovery efforts.
Safe and health	4	Although less direct, the stress and pressure from handling such attacks could potentially impact employee well-being.
Fines & Legal Penalties	7	There is a high risk of legal repercussions, including regulatory fines, due to non-compliance with data protection laws and the mishandling of sensitive customer information.
User Define Impact Area	0	No additional impact area has been identified for this scenario, indicating that the primary focus is on financial and reputational damage.

4.3. Information asset risk worksheets (Allegro Worksheet 10) – II

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	Payment Gateway System			
	Area of Concern	Doing network failure in the system by an internal attacker			
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Network service provider		
		(2) Means *How would the actor do it? What would they do?*	An authorized user with malicious intent or negligence can exploit their access rights to compromise network security. They might manipulate system settings, install malicious software, or neglect necessary security measures, leading to vulnerabilities and potential data breaches.		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate or Accidental		
		(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?*	If an authorized user needs to access the system but encounters a network failure, it can violate Availability. To prevent this, implement strong access controls ensuring users have the least privilege, use multi-factor authentication to secure access, and continuously monitor network activity to quickly detect and respond to issues. This ensures that authorized users can always access the system reliably		
		(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 network failure caused by an insider can moderately impact the organization's reputation and customer confidence, as it prevents transaction processing and a loss of trust. Financially, the company may face potential losses from missed transactions.	Reputation & Customer	8	4
		Financial	8	4
	Customers dissatisfied with network failures may switch to competitors, causing a loss of income and market share. Additionally, significant time and effort will be required to diagnose and resolve the network issue, impacting productivity. The organization might incur additional costs for security safeguards and incident response tools.	Productivity	9	4.50
		Safety & Health	7	3.50
	Network failures may lead to fines and legal penalties if customers seek compensation for losses or if regulatory compliance is breached.	Fines & Legal Penalties	7	3.50
		User Defined Impact Area	0	0
			Relative Risk Score	**19.50**

(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 Controls	• Implement strict access control policies and procedures to limit who can access critical network systems. Ensure only authorized personnel have access. • Provide ongoing security training to employees about the importance of network security and the potential risks of insider threats. • Conduct regular audits of access logs and network activity
Technical Controls	• Ensure that all network devices and systems are up-to date with the latest security patches. • Use network segmentation to isolate critical systems and limit the potential impact of a network failure. • Require Multi-Factor Authentication (MFA) for accessing sensitive systems to ensure only authorized users can log in.
Physical Risk	• Restrict physical access to data centers and server rooms to authorized personnel only.

4.3.1 Justification of severity values

Attribute	Value	justification
Probability	50%	The probability is considered medium (50%) because while internal network threats from authorized users are a recognized risk, security measures and controls can reduce the likelihood of exploitation.
Reputation & Customer Confidence	8	A network failure can harm the organization's reputation and erode customer trust, especially since it disrupts payment transactions, which are vital for customer satisfaction.
Financial	8	Financially, a network failure would result in revenue loss from disrupted transactions, potential compensation payouts, and additional costs for rectifying the issue and enhancing security.
Productivity	9	A prolonged network failure would severely impact productivity due to diagnosing and resolving issues, leading to wasted time and reduced efficiency across the organization.
Safe and health	7	Although no direct physical harm is involved, the stress from addressing a critical network failure could impact employee well-being, resulting in heightened pressure and possible burnout.
Fines & Legal Penalties	7	Legal penalties may arise from contractual breaches, non-compliance with regulatory requirements, or customer compensation claims due to service failures.
User Define Impact Area	0	No specific additional impact areas have been defined for this particular scenario, indicating that the primary focus remains on the identified standard risks

5. Reference

[1] C. 3. s. platform, "Cynet," [Online]. Available: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/ . [Accessed 12 10 2022].

[2] Cynet, "Cynet 360 security platform," [Online]. Available: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/ . [Accessed 12 10 2022].

[3] CISA, "Cyber Security & infrastructure Security Agency," United States government, [Online]. Available: https://www.cisa.gov/uscert/ncas/tips/ST04-015. [Accessed 11 10 2022].

[4] J. Wu, "Nettitude Blog," [Online]. Available: https://blog.nettitude.com/malware-costs-business-impact. [Accessed 12 10 2022].

[5] S. Weerasekara, "Impact of natural disasters on the efficiency," Taylor & Francis Online, vol. https://www.tandfonline.com/doi/abs/10.1080/17565529.2021.1893635, p. 1.

[6] AIHA, "American Industrial Hygiene Association," [Online]. Available: https://www.aiha.org/public-resources/consumer-resources/disaster-response-resource-center/health-and-safety-issues-in-natural-disasters . [Accessed 12 10 2022].

[7] "Phishing.org," [Online]. Available: https://www.phishing.org/10-ways-to-avoid-phishing-scams. [Accessed 13 10 2022].

[8] E. Kost, "UpGuard," [Online]. Available: https://www.upguard.com/blog/data-leak-prevention-tips. [Accessed 13 10 2022].