Sri Lanka Institute of Information Technology

IT3070 – Information Assurance & Security

Year 3, Semester 1

Risk Management Assignment

Submitted by:

Selected Asset	Name	Registration Number
Electronic Medical Records System	Navodya P.K.C.	IT22217868 (Leader) Lab Group – Y3.S1.WD.IT.0101
Patient Prescription Database	Karunarathna K.M.N.D.	IT22099686
Inventory Management System	P.M. Kavindu Denuwan	IT22229434

2024 September

About the Organization:

“HealthFirst” Pharmacy is a true provider of local healthcare, with the objective of caring for every person who walks through the door. Patients depend on “HealthFirst” daily for their quality prescriptions, insightful and caring advice, and a warm sense of service. This personalized care is supported by a comprehensive digital infrastructure that ensures the pharmacy operates smoothly, while maintaining patient records securely. At the core of its operations are three critical systems: the **Electronic Medical Records (EMR) System**, the **Patient Prescription Database**, and the **Inventory Management System (IMS)**.

The **EMR system** is like the heart of the pharmacy, holding all the important details about each patient’s health—medical histories, prescriptions, and treatment plans—so that pharmacists and healthcare providers can work together to deliver the best care. It ensures that patients receive accurate medications, and that any health-related information is accessible in real-time. On the other hand, The **Patient Prescription Database**, while connected to the EMR, focuses specifically on tracking medications, dosages, and refills. It ensures that prescriptions are handled accurately and safely, preventing any dangerous drug interactions. Meanwhile, the **Inventory Management System** plays a behind-the-scenes role, making sure the pharmacy is always stocked with the right medications and supplies. It tracks inventory levels, sends alerts when supplies are low, and even helps with financial management by monitoring supplier transactions. Together, these systems allow HealthFirst to provide safe, efficient, and personalized care while ensuring that everything—from patient records to medication stock—is well-organized and accessible when needed.

Asset 01 - Electronic Medical Records System

IT22217868 – Navodya P.K.C.

The Electronic Medical Records (EMR) System is a critical software platform used by the pharmacy to store, manage, and access patients' medical histories, prescriptions, and treatment plans. It acts as a single database for health-related data, making it easy for pharmacists and medical professionals to accurately dispense prescription drugs, monitor patients' progress, and offer personalized attention.

In addition, this system makes it easier for the pharmacy to communicate with medical professionals, enabling real-time updates to patient records. To ensure immediate and precise medicine dispensing, it interfaces with prescription systems, lowering errors and enhancing patient safety.

The system performs an important role in safeguarding patient privacy in addition to maintaining records. To guarantee the security and confidentiality of sensitive personal and health information. The EMR system needs to be reliable and available 24/7 because it is used daily to handle patient demands. Any failure could have an adverse effect on patients' trust in the pharmacy, delay treatments, and interrupt patient care. In summary, the EMR system is necessary for both the smooth operation of pharmacies and the delivery of effective and safe patient care.

Asset Profile Document

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?*
Electronic Medical Records System (EMR)	EMR system is useful for storing and managing patient data, include medical histories, prescriptions and treatment plans. This system is essential for providing safe and accurate healthcare service	Facilitates the management of patient health records, allowing authorized healthcare providers to access, modify and securely store patient data. It helps to reduce errors and ensures proper prescription handling.
(4) Owner(s) *Who owns this information asset?*		
IT Department of the Pharmacy		
(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 pharmacists, doctors and health care administrators can view or modify patient records.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Only authorized healthcare providers and pharmacists can make updates to data, ensuring records are accurate
□ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The system must be available 24/7 to authorized personnel to ensure continuous health care services
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	System must comply with healthcare regulations as HIPPA to ensure the security of data
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		

□ Confidentiality	□ Integrity	□ Availability	□ Other

Critical Information Asset Risk Worksheet 1

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET 2**			
Information Asset Risk	Threat	Information Asset	Electronic Medical Records System (EMR)		
		Area of Concern	Phishing Attack leading to Data Breach		
		(1) Actor *Who would exploit the area of concern or threat?*	External Hacker		
		(2) Means *How would the actor do it? What would they do?*	A phishing email is sent to an employee of the pharmacy, tricking them to reveal login credentials for the EMR system, which the attacker uses to access sensitive patient data		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate: financial gain from selling data or using it for identity theft		
		(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?*	Protect data by enhancing multi – factor authentication system, improving email filtering system and ensuring security awareness training for all staff to mitigate the attacks		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High**	□ **Medium**	□ **Low**

(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**
Unauthorized access to sensitive patient data may lead to severe consequences, including exposure of privacy	Reputation & Customer Confidence	8	4.0 (50%*8)
	Financial	7	3.5
System may need to be taken offline for investigating and recovery disrupting the pharmacy's daily activities	Productivity	6	3.0
	Safety & Health	0	0
Legal actions could occur due to non-compliance with data protection regulations	Fines & Legal Penalties	8	4.0
	User Defined Impact Area	7	3.5

Relative Risk Score	18

(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	• Conduct regular employee training programs on awareness • Enforce stronger email filtering and attachment scanning policies • Ensure policies for reporting phishing emails are clear and well understood by employees
Technical Controls	• Implement multi – factor authentication for access to critical systems, like the EMR system • Regularly update anti – phishing and anti – virus software to detect and prevent known threats
Physical Controls	• Limit physical access to servers hosting the EMR system to authorized personnel only • Ensure security cameras and access control systems where sensitive data is stored

Impact Area	Value	Justification
Probability	50%	Healthcare data breaches frequently occur because of phishing attacks. The probability is somewhat high, particularly in the absence of regular staff training. Industry reports list phishing as one of the main reasons for data breaches.
Reputation and Customer confidence	8/10	A breach of data may seriously damage the pharmacy's reputation and cause people to lose trust in it. Mishandling sensitive data can have detrimental effects on one's reputation.
Financial	7/10	There may be significant costs associated with legal fees, HIPAA fines, and payments to impacted patients. Because the data is sensitive, data breaches in the healthcare industry are frequently expensive.
Productivity	6/10	While employees concentrate on damage management and system reconstruction, operations might fall off. Still, while the breach is being handled, the company can continue to operate.
Safety & Health	0/10	Patient safety and health are not directly impacted by this phishing attempt on patient data.
Fines & Legal Penalties	8/10	Serious financial penalties for violating the Health Insurance Portability and Availability Act (HIPAA) might exceed millions of dollars, depending on the severity of the violation.
User defined impact	7/10	There is a chance of legal disputes and patient lawsuits, which raises the possibility of long-term financial and reputational harm.

Critical Information Asset Risk Worksheet 2

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET 2**		
Information Asset Risk	**Threat**	Information Asset	Electronic Medical Records System (EMR)		
		Area of Concern	Ransomware Attack leading to system downtime		
		(1) Actor *Who would exploit the area of concern or threat?*	External Hacker (Cybercriminals)		
		(2) Means *How would the actor do it? What would they do?*	A malicious third-party program or an infected email attachment are the two ways that the ransomware enters the EMR system. The ransomware encrypts the whole EMR system once it is activated, preventing the pharmacy from accessing vital patient data until a ransom is paid.		
		(3) Motive *What is the actor's reason for doing it?*	Financial gain through ransom payments		
		(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?*	To stop flaws that ransomware could exploit, implement regular system backups, set up Endpoint Detection and Response (EDR) systems, and make sure that continuous patch management is maintained. Additionally, be sure that network partitioning prevents malware from spreading.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High**	□ **Medium**	□ **Low**
	(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 inability of pharmacy systems to perform transactions or access electronic medical records could result in a complete loss of responsiveness.		Reputation & Customer Confidence	7	3.5
			Financial	8	4.0
	Extended periods of inactivity might affect the pharmacy's ability to operate normally, resulting in lost profits.		Productivity	9	4.5
			Safety & Health	7	3.5
	Inability to deliver services in a timely manner can cause patients to lose faith in the pharmacy.		Fines & Legal Penalties	6	3.0

		User Defined Impact Area	6	3.0
			Relative Risk Score	**21.5**

(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 Controls	• Give the existing Intrusion Prevention System (IPS)'s regular upgrades and patches top priority in order to keep it effective against known threats. • Create a procedure for keeping an eye on security alerts and vendor updates to find important fixes and workarounds.
Technical controls	• To enhance the capabilities of the current IPS, add further layers of security, such as traffic filtering and network segmentation. • To maximize its efficacy within its constraints, the current intrusion prevention system ought to be set up by focusing on identified attack signatures and patterns frequently linked to denial-of-service attacks.
Physical controls	• Verify that all network equipment, such as switches and routers, is kept safe in locked spaces with restricted access. • Install a UPS or other backup power supply to keep the network secure in the event of a power outage.

Impact Area	Value	Justification
Probability	50%	Because patient data is so valuable, ransomware attacks are frequent, particularly in the healthcare industry. Preventive measures, however, might significantly reduce the risk.
Reputation and Customer confidence	7/10	If patients are unable to obtain prescription drugs or medical records during the period of downtime, they might become less confident of the pharmacy. Depending on how long the system is down, the severity will vary.
Financial	8/10	The price could be expensive because of lost revenue during the downtime, recovery expenses, and ransom payments. Disruptions to business could result in serious financial losses.

Productivity	9/10	Because the pharmacy's services depend on having access to the EMR system, system failure would have a significant negative influence on production. It might momentarily stop essential operations.
Safety & Health	7/10	A failure of the EMR system could cause delays in urgent treatment or drug delivery, which could have a negative impact on some patients' health.
Fines & Legal Penalties	6/10	There may be legal consequences if patient care is postponed or stopped since healthcare laws need prompt access to services and medical records.
User defined impact	6/10	If ransomware has a major negative effect on the system, long-term operational inefficiencies might result. Recovery expenses and lasting disruptions could persist even after restoration.

Asset 02 - <u>Patient prescription database</u>

IT 22099686 – Karunarathna K.M.N.D.

The Patient Prescription Database, which securely stores and manages sensitive patient data, plays an important role in the pharmacy. Every patient's prescription history, including medications, dosages, and the medical professionals who prescribed them, is kept up to date in this database. It guarantees that we can give the best treatment possible along with the appropriate drugs at the appropriate moment.

This system shows our patients' trust in us and is more than just a means of storing data. Each prescription has important information that helps physicians and pharmacists prevent dangerous medication interactions, monitor patients while they are receiving therapy, and assure patient safety. Also, this database provides information to the Electronic Medical Records System (EMR) to ensure that prescription details are accurately reflected in a patient's overall medical records, enabling healthcare providers to monitor medication adherence and coordinate treatment plans effectively. We respect each person's privacy and well-being by protecting this data in addition to adhering to legal requirements.

We are dedicated to preserving the privacy, accuracy, and accessibility of these records as a pharmacy organization. Not only do our patients trust us with their health, but also with the appropriate handling of their most private and sensitive data.

Asset Profile Document

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?*
Patient Prescription Database	The Patient Prescription Database is essential for tracking and managing all medication-related information within the pharmacy. It ensures that medications are dispensed accurately and safely, based on each patient's prescription history. This database supports pharmacy-specific functions and does not include broader health information like diagnoses or treatment plans, which are managed by the EMR system.	In order to track medication history and guarantee safe treatments, the database safely stores patient prescription details. It gives medical professionals a thorough understanding of their patients' health and allows them to provide individualized care.
(4) Owner(s) *Who owns this information asset?*		
IT Department of the Pharmacy and The Pharmacy Manager		
(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 pharmacists and healthcare providers, can access this database.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	This data can only be modified by authorized personnel and licensed professionals.
□ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The database needs to be available to authorized staff members 24/7 because patient care never ends.
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	To protect patient privacy and data security, this asset complies fully with GDPR and HIPAA regulations.
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		

□ Confidentiality	□ Integrity	□ Availability	□ Other

Critical Information Asset Risk Worksheet 1

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Threat	Information Asset	Patient prescription database
		Area of Concern	Unauthorized Access to Patient Prescription Database
		(1) Actor *Who would exploit the area of concern or threat?*	An External hacker
		(2) Means *How would the actor do it? What would they do?*	The actor could gain access to the database by taking advantage of security flaws in the system, such as unpatched software or weak passwords.
		(3) Motive *What is the actor's reason for doing it?*	They may be motivated to steal identities, sell private medical information on the dark web, or demand a ransom.
		(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 confidentiality of the patient data is risked by this attack since private information is accessed by unauthorized parties.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** □ **Medium** □ **Low**

(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 patient trust	Reputation & Customer Confidence	9	4.5
	Financial	8	4.0
Harm to the organization's image 9	Productivity	6	3.0
	Safety & Health	4	2.0
Potential fines in accordance with HIPAA and GDPR	Fines & Legal Penalties	9	4.5

	regulations	User Defined Impact Area	10	5.0
		Relative Risk Score		**23.0**

(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:	Phishing awareness and security procedures are often taught to staff members. To guarantee adherence to data security regulations, rigorous confidentiality agreements would need to be signed by every employee, and audits would be carried out on a regular basis.
Technical Controls:	Intrusion detection systems (IDS) are used to immediately identify any suspicious behavior, encrypted communications between the database and users, frequent system patches, and multi-factor authentication (MFA) are all recommended.
Physical Controls:	To guarantee that only authorised workers may access the actual hardware, the database servers would be kept in a safe, access-controlled building complete with security cameras and biometric entry.

Impact Area	Value	Justification (Humanized)
Probability	50%	Although there is a slight possibility of illegal access—particularly when healthcare systems are the subject of cyberattacks—our security precautions reduce this danger.
Reputation & Customer Confidence	9/10	Patient trust would be severely impacted by a data breach. People would go elsewhere for care if they trusted us to protect their health information.
Financial	8/10	In addition to losing clients, there would be substantial legal fees and HIPAA/GDPR fines, which would result in financial loss.
Productivity	6/10	While operations would continue, other duties would be slowed down while resources were redirected to fix the attack.
Safety & Health	4/10	Although there would be no immediate effect on direct patient care, worries over data integrity might cause future treatments to be postponed.
Fines & Legal Penalties	9/10	Legal costs under GDPR and HIPAA for failing to secure patient data would be highly expensive.
User Defined Impact (Patient Trust)	10/10	In the medical field, trust is essential. Patients may not come back after a breach, which can have long-term effects.

Critical Information Asset Risk Worksheet 2

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	Threat	Information Asset	Patient prescription database
		Area of Concern	Data Loss Due to System Failure
		(1) Actor *Who would exploit the area of concern or threat?*	Accidental failure due to hardware malfunction or software bugs
		(2) Means *How would the actor do it? What would they do?*	The system crashes, or a power failure occurs, causing loss of access to the **Patient Prescription Database**. This could also occur due to a lack of system updates or failure in backup processes.
		(3) Motive *What is the actor's reason for doing it?*	Not deliberate – this is caused by system malfunction rather than a malicious attack.
		(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 system is not available to authorized users, causing delays in medication dispensing.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** □ **Medium** □ **Low**

(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**
Unable to obtain prescriptions, which causes delays in patient treatment	Reputation & Customer Confidence	7	1.75
	Financial	5	1.25
Losses incurred financially as a result of paying the ransom or allocating funds for recovery operations	Productivity	7	1.75
	Safety & Health	5	1.25
Legal consequences for failing to secure data in keeping with GDPR and HIPAA	Fines & Legal Penalties	4	1
	User Defined Impact Area	7	1.75
		Relative Risk Score	**8.75**

(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:	• Create and update a plan to manage system failures, including recovery steps and staff responsibilities. • Train staff to handle operations manually if the system fails, ensuring they can keep the pharmacy running.
Technical Controls:	• Automatically back up the database and store backups securely offsite or in the cloud for quick recovery. • Use backup systems that take over automatically if the main system fails to keep data accessible.
Physical Controls:	• Install UPS or backup generators to keep the system running during power outages. • Protect physical access to servers with locks and surveillance to prevent tampering.

Impact Area	**Value**	**Justification**
Probability	25%	While rare, system failures can occur due to aging hardware, unpatched software, or insufficient disaster recovery plans.
Reputation & Customer Confidence	7/10	The trust of the patient would be damaged, but a quick recovery would lessen the long-term effects on our reputation.
Financial	5/10	The financial impact would be moderate, as the pharmacy could lose business if patients turn to competitors, and there may be costs associated with fixing or replacing hardware or software.
Productivity	7/10	Operations at the pharmacy would be significantly slowed down as manual procedures, so keeping paper records, would have to be used until the system was repaired, leading to inefficiencies.
Safety and Health	5/10	Patients may not receive prescriptions or treatments on time as a result of delays in obtaining patient records, which could be dangerous for their health.
Fines and Legal Penalties	4/10	Legal penalties are less likely but could occur if the system failure results in prolonged delays in service or breaches of regulatory standards like HIPAA.
User Defined Impact (Operational Continuity)	7/10	Longer system failure would cause operational continuity to be interrupted, requiring the pharmacy to convert to less effective manual operations. This would have an effect on patient satisfaction and overall service performance.

Asset 03 – Inventory Management System

IT22229434 – P.M. Kavindu Denuwan

The Inventory Management System (IMS) is a full-featured software program created to manage and enhance the inventory procedures of the pharmacy. It ensures the smooth transfer of drugs and supplies from suppliers to final customers while upholding operational transparency and financial accuracy. Because it oversees essential operations, this system is essential to the pharmacy's functioning. They are as follows:

1. **Inventory Tracking:**
   - Oversees inventory from multiple vendors.
   - Records the dissemination of documents to distributors, clients, and medical experts.
   - Prevents shortages by automatically notifying when inventories are low.

2. **Financial Oversight:**
   - Produces daily, monthly, and annual financial statements.
   - Reports contain information on payments, loans, inventory distributions, and supplier activities.
   - Guarantees precise monitoring of cash and credit transactions.

3. **Error Detection:**
   - Verifies entries by Reps and IT Operators.
   - Preserves data integrity by alerting management to any irregularities.

4. **Restricted Access:**
   - Representatives who enter delivery information and IT Operators who deal with inventory problems and receipts are the only two groups with access.

5. **Decision Support:**
   - Updates financial status in a timely manner.
   - Encourages sensible decision-making and effective management of the supply chain.

Asset Profile Document

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?*
Inventory Management System (IMS)	Tracking inventory from suppliers and controlling the transfer of products to patients, physicians, and distributors require the IMS. Ensuring real-time stock level monitoring, it lowers the possibility of stockouts. The system also automates financial reporting, which is essential for the long-term and daily financial management of the pharmacy.	All inventory movement within the pharmacy is tracked by the IMS, from receiving stock from many suppliers to send products to different customers. At the end of the day, month, and year, it automatically compiles financial reports and sends out notifications when stock levels are low. The system keeps track of cash and credit transactions, guaranteeing accuracy in financial and inventory management. Only two jobs have access to the system: IT Operators, who deal with inventory receipts and inconsistencies, and Representatives, who oversee deliveries.
(4) Owner(s) *Who owns this information asset?*		
Pharmacy Manager IT 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 Reps and IT Operators can access the system. The system’s financial and inventory data must remain confidential to prevent misuse or manipulation.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Accurate inventory levels and financial records are ensured by limiting access to the IMS to authorized personnel only. When inconsistencies are discovered, the system generates alarms and cross-verifies the data provided by representatives and IT operators.

❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The IMS must be available 24/7 to ensure continuous pharmacy operations, enabling timely stock reordering, accurate financial reporting, and preventing delays in delivery.
	This asset must be available for __24___ hours, __7_ days/week, __56___ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Financial reporting guidelines and inventory management laws must be followed by the IMS. The system's correctness is vital for financial audits and maintaining proper records of transactions and inventory levels.

(6) Most Important Security Requirement

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

Confidentiality	[✓ Integrity]	Availability	❑ Other

Critical Information Asset Risk Worksheet 1

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET 1**
Information Asset Risk	Threat	Information Asset	Inventory Management System (IMS)
		Area of Concern	An IT operator's intentional manipulation of financial records and inventory for their own financial benefit.
		(1) Actor *Who would exploit the area of concern or threat?*	IT Operator - Internal
		(2) Means *How would the actor do it? What would they do?*	When stock is still available, the IT Operator intentionally enters false information into the IMS by claiming that it has been issued. The IMS is manipulated in such a way that the supplier places needless reorders. The supplier may be paying the IT operator bribes for reordering unnecessary material. The IT operator falsifies debt payments that are still owed to the supplier for undelivered or excess stock in order to distort financial records.
		(3) Motive *What is the actor's reason for doing it?*	Gaining a personal financial advantage by manipulating supplier debt and fraudulently reordering products, possibly in exchange for kickbacks from the supplier.
		(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: The financial and inventory data are no longer confidential as a result of the fraudulent acts. • Integrity: False inputs about debt and stock levels jeopardize the accuracy of the financial records and inventory. • Availability: Although the system is still accessible, the information it offers is extremely deceptive, which might result in bad business decisions.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	**High** **[✓ Medium]** **Low**

(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 o owner by impact area?*		
	Impact Area	**Value**	**Score**
If fraudulent activity is discovered, it can damage the pharmacy's reputation, eroding customer and supplier trust.	Reputation & Customer Confidence	8	4.0 (50%*8)

	Reordering from a supplier repeatedly on the basis of fraudulent information can cause serious financial losses and even bankruptcies.	Financial	9	4.5
	Operational delays will result from the fraud's investigation and handling, which will take a lot of time and money.	Productivity	7	3.5
	Essential pharmaceuticals may run out of stock, which could have an impact on patient care if inventory levels are not appropriately reported.	Safety & Health	5	2.5
	Legal action could be taken against the pharmacy for possible fraud and for failing to keep correct financial records.	Fines & Legal Penalties	8	4.0
	This fraud may lead to a decline in internal trust between staff members and management, creating a difficult work atmosphere and necessitating future increases in oversight.	User Defined Impact	7	3.5

Relative Risk Score **22.0**

(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 mandatory internal audits and regular stock reconciliations to detect discrepancies between physical inventory and system data. • To lessen the possibility of fraud, separate the duties of authorizing new stock orders and entering inventory data. • Strictly enforce whistleblower laws to encourage reporting of suspicious activities.
Technical Controls	• Automate the processes for validating inventory by comparing system records with actual stock levels. (Can be used Scanners to connect with inventories)
Physical Controls	• Limit who has access to financial and inventory information to avoid unapproved manipulation. • Rotate responsibilities among IT operators regularly to reduce the possibility of persistent fraud.

Impact Area	Value	Justification
Probability	50%	Internal fraud is likely due to lax auditing procedures, insufficient controls, and a lack of oversight over financial and inventory data. Employees with substantial control can easily falsify data in the absence of frequent reviews, which raises the likelihood of such fraud.
Reputation and Customer confidence	8/10	If fraudulent activity is found, the pharmacy's reputation will be badly harmed, and suppliers and consumers will stop trusting it. The drugstore can sustain serious damage to its reputation.
Financial	9/10	Financial records and inventory manipulation can result in overstocking, false reporting of stock levels, significant financial losses, and even bankruptcy.
Productivity	7/10	Investigating fraud will disrupt regular operations and redirect staff resources, causing significant downtime and inefficiencies in operations.
Safety & Health	5/10	Patient safety may be compromised if fraudulent manipulation causes a scarcity of essential medications, leading to potentially hazardous treatment delays.
Fines & Legal Penalties	8/10	The pharmacy may be subject to severe fines and other penalties if it is found to have engaged in inventory fraud or false financial reporting.
User-defined impact	7/10	Long-term repercussions can include higher operating expenses as a result of tighter controls being put in place as well as a substantial effort being made to restore confidence and lessen reputational harm.

Critical Information Asset Risk Worksheet 2

		Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET 2**
Information Asset Risk		Information Asset	Inventory Management System (IMS)
		Area of Concern	An external attacker steals the IT Operator's credentials, accesses the IMS, issues false inventory records, and coordinates with a compromised Rep to physically acquire the inventory.
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	External Cybercriminal (with cooperation from a compromised Rep)
		(2) Means *How would the actor do it? What would they do?*	By using phishing to obtain the IT Operator's credentials, the attacker is able to access the IMS. Once inside, the assailant creates fictitious orders and issues inventory using fraudulent documents. In order to obtain the stolen merchandise physically without notifying the system (when customer returns inventory), the attacker works with a representative.
		(3) Motive *What is the actor's reason for doing it?*	Financial gain through the theft of valuable medical supplies or pharmaceuticals, which the attacker can sell to other competitors. The compromised Rep acts as the conduit for physically removing the stolen items from the pharmacy.
		(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:** The attack compromises sensitive data, such as inventory levels, orders, and supplier details. • **Integrity:** The integrity of the inventory is violated as the attacker manipulates records to issue false orders. • **Availability:** The system remains available, but the data integrity is severely compromised, leading to operational risks.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	**High** **[✓ Medium]** **Low**

(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 fraud is uncovered, the pharmacy’s reputation will be severely damaged. Trust with suppliers and customers will be eroded, especially if high-value products are involved.	**Reputation & Customer Confidence**	**8**	**4.0**
The theft of large quantities of inventory, especially high-value items, will result in significant financial losses. The pharmacy will also incur costs for investigating the breach and replenishing stock.	**Financial**	**9**	**4.5**
The necessity for a thorough investigation will require the pharmacy to shift resources from ongoing business activities, which will cause a delay in the fulfillment of valid orders.	**Productivity Impact**	**7**	**3.5**
Patients may experience shortages due to medicine theft, which could hurt their health if necessary therapies are not available.	**Safety & Health Impact**	**6**	**3**
If the breach exposes sensitive data or causes significant losses, the pharmacy may face legal action and penalties for failing to secure inventory and financial records.	**Fines & Legal Penalties**	**7**	**3.5**
Suppliers may come to doubt the pharmacy's capacity to maintain inventory, which can cause tension in the relationship or cause suppliers to withhold expensive goods.	**User Defined Impact Area**	**8**	**4**

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 Controls	• Regularly teach employees about security awareness, with a focus on phishing and credential theft. • Separate jobs and use role-based access controls to make sure no one person has undue influence over inventory procedures.
Technical controls	• Implement multi-factor authentication (MFA) for privileged accounts, such as the IT Operator, to restrict access to the IMS. • Make use of cutting-edge monitoring tools to spot suspect login trends, like logins from strange devices or locations.
Physical controls	• To guarantee that all issued inventory is physically inspected by impartial workers before departing the premises, implement enhanced inventory tracking. • Limit trustworthy employees' access to high-value goods, and audit representatives' inventory-handling actions regularly.

Impact Area	Value	Justification
Probability	50%	Weak password policies and a lack of multi-factor authentication make credential theft more probable.
Reputation and Customer confidence	8/10	Customers and suppliers may lose faith in the pharmacy's capacity to protect its operations if the theft is made public, harming the business's brand.
Financial	9/10	There will be large financial losses from the theft of priceless inventory in addition to the expense of looking into the breach and restocking.
Productivity	7/10	The pharmacy will have to devote time and money to looking into the breach, which will interfere with regular business and cause delays for valid orders.
Safety & Health	6/10	Patients might not be able to obtain necessary prescriptions if vital medications are taken, which could hurt their health.
Fines & Legal Penalties	7/10	Legal action and penalties may arise if the breach exposes sensitive data or results in severe financial losses.
User defined impact	8/10	There will be a decline in trust between the management of the pharmacy and its internal workers, especially representatives and IT personnel, leading to operational issues and the requirement for more stringent supervision.