Sri Lanka Institute of Information Technology

B.Sc. (Hons) in Information Technology

Year 3 Semester 1 & 2

IT3070 – Information Assurance & Security

Risk Management Assignment

Student Name	Student ID	Batch
IT22285188	N.H Afaaf Hariri (Leader)	Y3.S2.WE.IT.04.01
IT22131256	Shazni M.I.A	Y3.S2.WE.IT.01.02
IT23321236	Nafy F.A	Y3.S1.WE.IT.04.01

Table of Contents

Company Overview

Elephant House, a flagship brand of Ceylon Cold Stores PLC under the John Keells Group, stands as one of Sri Lanka's most iconic names in the FMCG sector. Renowned for its wide portfolio of ice creams, soft drinks, processed foods, and beverages, the brand has established a strong presence across supermarkets, retail outlets, and restaurants nationwide. Its operations span advanced manufacturing facilities, extensive logistics networks, and a robust corporate IT backbone—making digital systems integral to supply chain efficiency, customer engagement, and manufacturing automation.

In today's competitive and digitally driven business landscape, safeguarding information assets is as critical as protecting physical production lines. Any unauthorized disclosure, alteration, or disruption of critical data can compromise brand reputation, interrupt production processes, and lead to significant financial losses. Against this backdrop, this study leverages the **OCTAVE Allegro risk evaluation framework** to examine Elephant House's information security posture, with a focus on identifying threats, assessing vulnerabilities, and recommending mitigation strategies for three key information assets.

Declaration

We hereby declare that this report has been completed as part of our group assignment and reflects the collective effort of all members. Except where proper citation is made, it does not contain any material that has been previously published, written by another person, or submitted for any academic qualification at any university or institution. All sources of information and ideas used in this report have been appropriately cited and acknowledged in the references section.

Assets Selection Summary

Assets	Student ID	Student Name
Enterprise Resource Planning (ERP) System and Corporate Network	IT22285188	N.H Afaaf Hariri (Leader)
Servers and Manufacturing Control Systems	IT22131256	Shazni M.I.A
Customer and Employee Information	IT23321236	Nafy F.A

1. Enterprise Resource Planning (ERP) System and Corporate Network

ERP System: Integrates procurement, manufacturing, HR, finance, and distribution, ensuring real-time coordination and efficient decision-making.

Corporate Network: Connects factories, warehouses, and offices, enabling access to ERP, email, and shared resources essential for supply chain and financial operations.

2. Servers and Manufacturing Control Systems

Servers: Store financial records, sales data, supplier contracts, and production schedules while hosting critical applications and backups.

Supervisory Control and Data Acquisition /Industrial Control Systems: Control refrigeration units, bottling lines, and quality checks, ensuring safe, efficient, and continuous production of perishable goods.

3. Customer and Employee Information

Customer Information: Includes loyalty program data, purchase history, and payment details, supporting marketing and engagement but requiring strict data protection.

Employee Information: Contains payroll, HR, and personal data essential for workforce management, needing confidentiality and access controls.

1. Critical Information Asset Profile – IT22285188

1.1 Assets

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?*
Enterprise Resource Planning (ERP) System and Corporate Network	They are the backbone of the company's operations, integrating finance, HR, procurement, manufacturing, and logistics. Any disruption directly impacts production, supply chain, and decision-making.	The ERP system provides centralized real-time data processing for finance, HR, procurement, and logistics. The corporate network links offices, warehouses, and factories, enabling ERP access, email, and file sharing are essential for supply chain and business operation.
(4) Owner(s) *Who owns this information asset?*		
Corporate IT Department and Business Operations Division		
(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 staff can access sensitive ERP and corporate records (finance, HR).
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	• Transactions and records must remain accurate and tamper-proof.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	• Must be online 24/7 to ensure continuous operations.
	This asset must be available for _24_ hours, __7_days/week, _52_ weeks/year.	

❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Data Protection Regulation - Compliance with **GDPR**, **Sri Lanka Personal Data Protection Act (2022)**, or equivalent local privacy laws for employee/customer data processed in the ERP. Financial Regulations - Compliance with **SOX (Sarbanes-Oxley Act)** or similar financial reporting controls, since ERP manages finance and accounting. Cybersecurity for Networks - Compliance with **NIST Cybersecurity Framework** and **CISA ERP security guidelines**. Industry Standards - Alignment with **ISO/IEC 27001 (Information Security Management System)** and **ISO/IEC 27002 (Security Controls)** for network and ERP data.

(6) Most Important Security Requirement

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

❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

1.2 Risk - 1

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Enterprise Resource Planning (ERP) System and Corporate Network		
		Area of Concern	Unauthorized access or ransomware disrupting ERP.		
		(1) Actor *Who would exploit the area of concern or threat?*	**External hackers** (cybercriminal groups, ransomware gangs) **Insider threats** (disgruntled employees, contractors with excessive privileges)		
		(2) Means *How would the actor do it? What would they do?*	Launch **phishing campaigns** to steal ERP admin credentials Exploit **unpatched VPN/firewall vulnerabilities** to gain remote access Deploy **brute-force / credential stuffing attacks** on ERP logins Inject **malware/ransomware payloads** to encrypt ERP data and halt operations		
		(3) Motive *What is the actor's reason for doing it?*	Financial gain via ransom demand and data 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?*	**Confidentiality:** breached if ERP financial/payroll records are exfiltrated **Integrity:** breached if malicious actors modify supplier, HR, or accounting records **Availability:** breached if ransomware encrypts ERP databases or network downtime occurs		
		(6) Probability *What is the likelihood that this 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**
	Severe reputational damage: loss of customer and supplier trust **Financial loss**: ransom payments, downtime, loss of contracts, recovery costs	Reputation & Customer Confidence	9	4.5
		Financial	9	4.5
	Operational disruption: halted manufacturing, delayed logistics, stalled decision-making **Safety risk**: if ERP is tied to production environments, downtime may create safety incidents	Productivity	9	4.5
		Disruption of Services	8	4
	Legal penalties: regulatory fines (GDPR, data protection laws) for breach of employee/customer data	Fines & Legal Penalties	7	3.4
		Data Loss	9	4.5
			Relative Risk Score	**25.5**

(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?*
Network Perimeter & Infrastructure	**Administrative:** - Implement a strict Patch Management Policy requiring all network devices (VPNs, firewalls) to be updated within a defined SLA. - Establish a Change Management process to review and approve all firewall rule changes. **Technical:** - Deploy a Next-Generation Firewall (NGFW) with an Intrusion Prevention System (IPS) to detect and block exploit attempts. - Conduct regular external and internal vulnerability scans and penetration tests. - Enforce network segmentation to isolate the ERP environment from the general corporate network, limiting lateral movement for attackers.

	Physical: - Ensure all network hardware is located in a secure, access-controlled data centre or server room. - Residual Risk: - The organization accepts the risk that a sophisticated, zero-day vulnerability in a network device could be exploited before a patch is available.
Endpoints & Servers	**Administrative:** - Enforce a policy for Principle of Least Privilege, ensuring users and systems only have the access necessary. - Create and test an Incident Response Plan (IRP) specifically for ransomware attacks. **Technical:** - Deploy Endpoint Detection and Response (EDR) or advanced antivirus on all servers and user workstations. - Implement a robust backup and recovery strategy (e.g., the 3-2-1 rule) with immutable, offline, and regularly tested backups. - Use application whitelisting on critical servers to prevent unauthorized executables (like ransomware) from running. **Physical:** - Secure physical access to servers to prevent unauthorized direct access or hardware tampering.
ERP Application & Data	**Administrative:** - Mandate a strong password policy (complexity, rotation). - Conduct regular access reviews (quarterly) for all ERP accounts, especially for privileged users. **Technical:** - Enforce Multi-Factor Authentication (MFA) for all ERP access, especially for administrative and remote logins. This is the single most effective control against credential theft. - Configure account lockout policies to thwart brute-force attacks (e.g., lock account after 5 failed attempts). - Enable comprehensive logging of all ERP activities and forward logs to a central SIEM (Security Information and Event Management) system for monitoring and alerting on suspicious behaviour. **Physical:** - Not directly applicable to the application itself but covered by server/data center security.

Personnel (The Human Layer)	**Administrative:** - Conduct mandatory, ongoing Security Awareness Training for all employees, with a focus on identifying phishing and social engineering attempts. - Implement formal onboarding and offboarding procedures to ensure access is granted appropriately and revoked immediately upon termination. - Perform background checks for employees with access to sensitive systems like the ERP. **Technical:** - Deploy an advanced email filtering gateway to block phishing, spam, and malicious attachments before they reach user inboxes. - Use email banners to clearly mark messages originating from outside the organization. Physical: - Promote a "clean desk" policy and the use of privacy screens to prevent shoulder surfing of credentials in the office.

1.3 Risk - 2

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Threat	Information Asset	Enterprise Resource Planning (ERP) System and Corporate Network
		Area of Concern	Unauthorized disclosure of ERP data due to weak access controls or insider misuse.
		(1) Actor *Who would exploit the area of concern or threat?*	**Malicious insider** (employee with elevated ERP access) **Third-party contractor/vendor** misusing integration accounts **External hacker** exploiting stolen credentials
		(2) Means *How would the actor do it? What would they do?*	**Privilege misuse**: downloading payroll, supplier, or financial data **Credential theft**: phishing ERP users to obtain admin rights **Exploiting weak role-based access controls**: using excessive permissions to exfiltrate sensitive records
		(3) Motive *What is the actor's reason for doing it?*	**Financial gain**: selling payroll/financial info on black markets **Revenge**: disgruntled insider exposing company data **Espionage**: competitors seeking pricing, contracts, and supply chain info
		(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**: breached if employee, supplier, or financial records are disclosed **Integrity**: potentially compromised if insiders manipulate records before leaking **Availability**: not directly impacted in this scenario

		(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**
Severe **reputational damage** from public disclosure of sensitive data	Reputation & Customer Confidence	9	4.5
	Financial	7	3.5
Financial penalties due to regulatory non-compliance (e.g., GDPR, local privacy laws)	Productivity	4	2
	Safety & Health	1	0.5
Loss of **customer/supplier trust** and future contracts Possible **legal action** from impacted stakeholders	Fines & Legal Penalties	8	4
	User Defined Impact Area	6	3
		Relative Risk Score	**17.5**

(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?*
Personnel & Access Governance	**Administrative:** - Strictly enforce the Principle of Least Privilege (PoLP): Users must only have the absolute minimum permissions required for their job function. Review all privileges quarterly. - Implement Separation of Duties: Ensure no single individual can control a critical process end-to-end. - Mandatory background checks for all staff and contractors with access to the control systems. - Formal offboarding process: Ensure all physical and logical access is immediately and completely revoked upon termination or role change.

	Technical: - Utilize a Role-Based Access Control (RBAC) model within the Identity and Access Management (IAM) system to standardize permissions for different job roles (e.g., operator, engineer). - **Physical:** - N/A (Handled in the Physical Environment container)
SCADA/ICS Network & Systems	**Administrative:** - Develop and enforce a strict Change Management policy. All changes to control system logic or configurations must be documented, reviewed, and approved. **Technical:** - Deploy a Privileged Access Management (PAM) solution. This vaults admin credentials, forces users to "check out" access, and records all privileged sessions to detect malicious use of valid credentials. - Enforce Multi-Factor Authentication (MFA) for all remote access and for privileged accounts, where supported by the ICS technology. - Implement continuous monitoring and logging. Forward all system, network, and application logs to a SIEM. Create specific alerts for after-hours activity, unauthorized configuration changes, or multiple failed login attempts. This directly counters the "lack of monitoring" weakness. - Isolate the ICS network from the corporate IT network using a properly configured firewall/DMZ (per the Purdue Model). **Physical:** - Not directly applicable to the network .
Physical Environment & Hardware	**Administrative:** - Maintain a log of all physical entries into the control center and other sensitive areas. - Develop an incident response plan for physical security breaches. **Technical:** - Use CCTV cameras to monitor access to critical areas like the data center and operator control rooms. **Physical:** - Implement strict physical access control using card readers or biometrics for all sensitive locations (e.g., server rooms, control centers). - Disable unused USB and network ports on Human-Machine Interfaces (HMIs) and servers to prevent unauthorized device connections. - Place critical controllers and network equipment in locked cabinets or enclosures on the plant floor.

2. Critical Information Asset Profile – IT22131256

2.1 Assets

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?*
Servers and Manufacturing Control Systems	Manage real-time operations, automation, and data storage, ensuring continuous production, quality, safety, and coordination. A compromise could cause downtime, safety risks, reputational harm, and financial loss.	**Servers:** Host financial records, sales data, supply chain applications, and backups. Provide centralized business data storage. **SCADA/ICS:** Automate and monitor refrigeration, bottling, and QA processes in plants. Support operational continuity and safety.
(4) Owner(s) *Who owns this information asset?*		
Head of IT Infrastructure (Servers) and Operation Manger (Manufacturing Control System)		
(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 IT and engineering staff may access system configurations, production data, and financial records.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	• Only designated administrators may update configurations, apply patches, or alter production schedules.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	• Must be accessible 24 hours/day, 7 days/week, 365 days/year, as downtime directly halts production.

	This asset must be available for __24__ hours, _7_ days/week, __52__ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	IEC 62443 - International standard for Industrial Automation and Control Systems (IACS) security. Defines roles, responsibilities, and controls for protecting SCADA/ICS. ISO/IEC 27001 - Information Security Management System (ISMS) framework ensuring secure handling of information assets. NIST SP 800-82 (Guide to ICS Security) - U.S. National Institute of Standards and Technology guidelines specifically for securing ICS/SCADA. NERC CIP (Critical Infrastructure Protection) - North American Electric Reliability Corporation's regulations for power/energy companies running SCADA/ICS. Local Data Protection Laws - If servers handle employee or operational data, they must comply with data protection regulations.

(6) Most Important Security Requirement

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

❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

2.2 Risk - 1

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Servers and Manufacturing Control Systems		
	Area of Concern	Privileged employees or contractors could misuse their access rights, intentionally or accidentally, to access or alter sensitive data and system operations.		
	(1) Actor *Who would exploit the area of concern or threat?*	Disgruntled employee, insider with excessive privileges, or careless staff member**.**		
	(2) Means *How would the actor do it? What would they do?*	Using valid but misused credentials. Exploiting weak authentication mechanisms. Bypassing security controls due to lack of monitoring.		
	(3) Motive *What is the actor's reason for doing it?*	Revenge against employer Negligence or human error. Gaining unauthorized advantage (e.g., altering schedules).		
	(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:** Unauthorized access to critical SCADA/ICS system information. **Integrity:** Unauthorized alteration of configurations or records. **Availability:** Potential downtime of control systems.		
	(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 customer trust due to system outages	Reputation & Customer Confidence	4	4

	Financial impact from production downtime and recovery costs	Financial	5	5
	Productivity losses from halted operations	Productivity	4	4
		Safety & Health	3	3
	Potential safety risks if machinery is misconfigured Possible regulatory non-compliance penalties	Fines & Legal Penalties	4	4
			Relative Risk Score	**20**

(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?*
Identity & Access Governance	**Administrative:** - Enforce the Principle of Least Privilege (PoLP): Review and re-architect ERP roles to ensure users only have access to the data essential for their job. This is the primary defence against "exploiting weak role-based access controls." - Conduct mandatory semi-annual access reviews where data owners must re-certify user permissions. - Establish a strict Third-Party Access Policy that grants temporary, purpose-based access to contractors and vendors. **Technical:** - Mandate Multi-Factor Authentication (MFA) for all ERP logins. This is the most effective control against credential theft from phishing.
Data Protection & Endpoints	**Administrative:** - Develop a Data Classification Policy to identify and tag sensitive information within the ERP (e.g., financial, payroll). - Update the Acceptable Use Policy (AUP) to explicitly prohibit unauthorized data transfer. **Technical:** - Deploy a Data Loss Prevention (DLP) solution. This is a critical control that can detect and block sensitive data from being copied to USB drives, sent via email, or uploaded to the cloud.

	- Implement a Database Activity Monitoring (DAM) tool to alert on anomalous queries, such as a single user downloading thousands of employee records. - Enforce full-disk encryption on all company laptops and workstations. **Physical:** - Physically or electronically disable USB ports on machines for users who do not have a business need for them.
Network Monitoring & Egress Control	Administrative: - Create and test an Incident Response Plan specifically for data breach scenarios. Technical: - Configure web filtering / proxy servers to block access to unauthorized personal cloud storage, file-sharing websites, and personal webmail. - Forward all relevant logs (ERP, DLP, firewall, DAM) to a SIEM solution to correlate events and detect indicators of a data breach in progress. - Monitor for unusual outbound network traffic, especially encrypted traffic to unknown destinations. .

2.3 Risk – 2

Allegro - Worksheet 10			INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Threat	Information Asset	Servers and Manufacturing Control Systems		
		Area of Concern	ICS endpoints (Programmable Logic Controller, Human Machine Interface), outdated OS/firmware, unpatched servers, removable media, vendor supply chain		
		(1) Actor *Who would exploit the area of concern or threat?*	External attackers (cybercriminals, hacktivists, nation-state attackers), or infected vendor supply chain		
		(2) Means *How would the actor do it? What would they do?*	Spear phishing targeting employees. Malware via infected USB or removable devices. Exploiting unpatched vulnerabilities in ICS software.		
		(3) Motive *What is the actor's reason for doing it?*	Financial gain (ransomware). Spying to steal secrets or competitive advantage. Disrupt or damage systems to push a political or ideological goal.		
		(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:** Operational details are stolen or leaked. **Integrity:** Compromised process controls and system reliability. **Availability:** Service outages or plant shutdowns.		
		(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**
Financial losses from downtime, ransom demands, and recovery.	Reputation & Customer Confidence	5	5

		Financial	5	5
	Severe safety hazards if industrial equipment malfunctions Safety hazards in manufacturing environment	Productivity	5	5
		Safety & Health	4	4
	Regulatory penalties for lack of safeguards.	Fines & Legal Penalties	5	5
			Relative Risk Score	**24**

(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?*
Network Perimeter & IT/OT Boundary	**Administrative:** - Policy of strict network segregation: Formally prohibit any direct network traffic between the corporate (IT) network and the control (OT) network. All connections must be brokered through a secure Demilitarized Zone (DMZ). **Technical:** - Implement a properly configured firewall at the IT/OT boundary, using a "deny all, permit by exception" rule set. Only allow specific, necessary protocols and sources/destinations. - Use a unidirectional gateway for data that only needs to flow from the OT to the IT network (e.g., for reporting), as this physically prevents any inbound connections. - Deploy an Intrusion Detection System (IDS) with ICS-specific protocol awareness to monitor for malicious traffic attempting to cross the boundary. -
ICS Endpoints & Internal Network	**Administrative:** - Establish a formal ICS patch management program. This must include testing all patches in a non-production environment before deployment to avoid causing operational disruptions. - Maintain a comprehensive asset inventory of all hardware and software within the ICS environment. **Technical:** - Deploy Application Whitelisting on HMIs and servers. This is a critical control that prevents any unauthorized software (including malware) from running. - Harden all endpoints: Change all default passwords, disable unused ports and services, and apply secure configuration settings.

	- Utilize network segmentation within the ICS network to isolate critical control processes from each other, preventing malware from spreading laterally
Personnel & Removable Media Controls	**Administrative:** - Conduct mandatory security awareness training for all staff with access to the ICS environment, focusing on spear phishing and the dangers of removable media. - Create and strictly enforce a policy for all removable media (USBs, laptops, etc.). This policy should either ban their use entirely or require that all media be scanned for malware at a dedicated, isolated kiosk before being connected to any ICS asset. **Technical:** - Technically disable USB ports and CD/DVD drives on all ICS endpoints where they are not essential for operation. - Deploy advanced email filtering on the corporate IT network to block spear-phishing attempts before they reach employee inboxes. **Physical:** - Enforce strict physical access control to the plant floor and control rooms to prevent unauthorized personnel from connecting any devices.

3. Critical Information Asset Profile – IT23321236

3.1 Asset

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Customer and Employee Information	This asset is essential because it supports customer engagement, marketing, payment transactions, and workforce management. A breach can cause legal, financial, and reputational damages.	Customer Information: Loyalty program details, purchase history, and payment data. Employee Information: Payroll records, HR data, personal details, and performance history. Both are stored in secured databases, processed in HR/CRM applications, and accessed by authorized personnel.
(4) Owner(s) *Who owns this information asset?*		
HR Department (Employee Information) & Marketing Division. (Customer)		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	• Only HR staff, payroll managers, and authorized IT administrators may access employee data; only marketing officers with approval can access customer data.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	• Only HR managers and payroll admins can modify employee records; only marketing division admins can modify customer data.

❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	• The information must be available **24/7**, 365 days/year for transactions, HR processing, and compliance reporting
	This asset must be available for __24___ hours, __7_ days/week, __365___ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	**Data Protection and Privacy** Comply with PDPA – Personal Data Protection Act/ GDPR – General Data Protection Regulation for lawful collection. **Data Security** Implement INIST National Institute of Standards and Technology.frameworks and protect against unauthorized access and breaches. **Audit and Reporting** \Maintain logs and audit trails to monitor data access and changes

(6) Most Important Security Requirement

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

❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

3,2 Risk - 1

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	Access Customer and Employee Information		
		Area of Concern	SQL Injection		
		(1) Actor *Who would exploit the area of concern or threat?*	External attackers (cybercriminals, hacktivists). Malicious insiders (disgruntled employees with access)		
		(2) Means *How would the actor do it? What would they do?*	Phishing employees for credentials. SQL Injection / exploiting unpatched CRM-HR systems. Misusing authorized access (insider copying data).		
		(3) Motive *What is the actor's reason for doing it?*	Financial gain (sell data on dark web, commit fraud, identity theft). Revenge by insiders (disgruntled employee leaking payroll). Hacktivism (public exposure of sensitive data to damage reputation).		
		(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 breached by: credential theft (phishing, credential-stuffing), compromised admin accounts, or stolen backups/cloud misconfigurations. Integrity breached by: SQL injection, unauthorized privileged changes (compromised admin/insider), or malware that alters records. Availability breached by: targeted DoS on application endpoints or account lockouts from repeated credential abuse (secondary to intrusion).		
		(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**
	Reputation & Customer Confidence: Loss of trust, customer churn, negative press, longer-term brand damage.	Reputation & Customer Confidence	5	4
	Financial: Incident response costs, breach remediation, fraud losses, potential compensation and remediation costs	Financial	3	4
	Productivity: Business disruption while forensic/containment actions occur; diverted staff time to IR and recovery.	Productivity	4	3
		Safety & Health	2	1
	Safety & Health: Low direct physical-safety impact for typical CRM/HR systems, but potential employee stress and operational disruption	Fines & Legal Penalties	3	4
			Relative Risk Score	**16**

(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?*
Access Control & Authentication	**Administrative:** - Enforce a **Role-Based Access Control (RBAC) policy** ensuring least privilege. - Conduct **mandatory employee training** on password hygiene, phishing resistance, and data handling procedures. **Technical:** - Implement **Multi-Factor Authentication (MFA)** across CRM/HR systems. - Apply **encryption at rest** - Enable **centralized logging and monitoring** of authentication attempts with alerts for anomalies. **Physical:** - Restrict physical server room access with **biometric/ID badge entry**. - CCTV monitoring of data center access points.
Data Protection & Monitoring	**Administrative:** • Implement a Data Classification Policy (Public / Internal / Confidential / Restricted). • Mandate secure data disposal (shredding, wiping drives).

	Technical: - Encrypt all databases and backups - Deploy Data Loss Prevention (DLP) to prevent unauthorized sharing via email/cloud. **Physical:** - Lock and audit access to tape/disk backup storage**.**
Continuous Monitoring & Response	**Administrative:** - Develop and regularly test an Incident Response Plan specifically for data breach events. - Conduct quarterly tabletop exercises simulating insider and external attacks. **Technical:** - Deploy Security Information and Event Management (SIEM) for real-time log analysis and threat hunting. - Enable automated alerting and containment (e.g., isolate compromised accounts). - Regular penetration testing and red team exercises to validate defenses.
Endpoint & Network Security	**Administrative:** - Define and enforce a Bring Your Own Device (BYOD) policy. - Provide staff with secure baseline configurations. **Technical:** - Deploy Endpoint Detection & Response (EDR) agents across all devices. - Use network segmentation (separating HR/finance servers from general IT). - Enforce email filtering and sandboxing for phishing prevention**.** **Physical:** - Secure laptops with cable locks and screen privacy filters for HR staff. - Track devices with asset tagging.

3.2 Risk - 2

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Threat	Information Asset	Customer and Employee Information Systems
		Area of Concern	Ransomware through phishing, unpatched software, and insider misuse, risking downtime and data leakage
		(1) Actor *Who would exploit the area of concern or threat?*	External attackers (cybercriminal gangs deploying ransomware). Malicious insiders introducing malware via USB/removable media.
		(2) Means *How would the actor do it? What would they do?*	Phishing with ransomware-laden attachments. Exploiting unpatched software vulnerabilities Insider introducing infected removable drives. Lateral movement across network to encrypt HR databases.
		(3) Motive *What is the actor's reason for doing it?*	Financial gain via ransom payment (demanding cryptocurrency). Double extortion – encrypting + threatening to leak employee/customer data. Insider sabotage to disrupt operations.
		(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?*	**Availability** – primary breach (databases unavailable until ransom is paid or recovery is complete). **Confidentiality** – secondary breach if data is exfiltrated. **Integrity** – possible if encrypted/altered files cannot be restored cleanly

		(6) Probability *What is the likelihood that this 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**
Reputation & Customer Confidence: Customers lose trust if loyalty/financial data is leaked.	Reputation & Customer	5	4
Financial: Heavy incident response, ransom demands, lost sales.	Financial	4	4
Productivity: Major disruption while systems are encrypted; payroll delays; HR operations halted	Productivity	5	4
	Safety & Health	2	1
Fines & Legal Penalties: Non-compliance with PDPA/GDPR for leaked data.	Fines & Legal Penalties	4	3
		Relative Risk Score	**16**

(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?*
Patch & Vulnerability Management	**Administrative:** • Establish a **formal patch management policy** with defined SLAs. • Maintain an **asset inventory** to track patch status. **Technical:** • Automate **patch deployment** across endpoints and servers. • Conduct **regular vulnerability scans** and penetration testing. **Physical:** • Ensure secure handling of legacy servers awaiting decommissioning.
Data Protection & Backup	**Administrative:** • Create a **Backup & Recovery Policy** with defined RPO/RTO. • Train staff on **secure backup handling procedures**.

	Technical: - Maintain **immutable, encrypted backups** stored offline/offsite. - Test **disaster recovery drills** quarterly to ensure ransomware-resilient recovery. - Use **backup anomaly detection** (alerts for mass encryption in progress). **Physical:** - Store offline media in **locked, fireproof vaults**. - Secure secondary data center with restricted access.
Legal, Compliance & Vendor Risk Management	**Administrative:** - Ensure compliance with **PDPA/GDPR** for breach reporting. - Include **cybersecurity clauses in vendor contracts** (incident notification, data protection). **Technical:** - Require vendors to use **secure APIs, MFA, and patching practices**. - Restrict third-party access to time-bound, monitored accounts. **Physical:** - Vendors accessing facilities require **escorted entry** and logging.

4 Justification

4.1 Asset 1 – Risk 1

Attribute	Value	Justification
Probability	High	External hackers and insider threats can exploit phishing, unpatched VPN/firewall vulnerabilities, or brute-force attacks, making this risk very likely.
Reputation & Customer Confidence	Very High	A breach or ransomware incident would damage customer and supplier trust, causing severe reputational harm.
Financial	Very High	Ransom payments, downtime costs, contract losses, and recovery expenses create major financial impact.
Productivity	Very High	Disruption of ERP halts finance, HR, manufacturing, and logistics operations, leading to stalled decision-making and supply chain delays.
Safety & Health	Medium	ERP downtime in production environments may create safety risks (e.g., halted manufacturing processes or unsafe work conditions).
Fines & Legal Penalties	High	Non-compliance with GDPR, Sri Lanka Data Protection Act, or SOX regulations results in regulatory fines and potential lawsuits.

4.2Asset 1 – Risk 2

Attribute	Value	Justification
Probability	Medium	Insider misuse or weak access control exploitation is moderately likely, especially through privilege misuse or phishing-based credential theft.
Reputation & Customer Confidence	Very High	Public disclosure of sensitive ERP/financial data would severely damage trust with customers, suppliers, and partners.
Financial	High	Losses may occur from stolen data, black-market sales, and regulatory fines, directly impacting revenue and operations.
Productivity	Moderate	While operations may not completely stop, disclosure incidents cause internal disruptions, investigations, and delays.
Safety & Health	Low	No direct health/safety impact, though insider stress or pressure may indirectly affect workforce wellbeing.
Fines & Legal Penalties	High	Regulatory non-compliance with GDPR, Sri Lanka Personal Data Protection Act, or privacy laws may result in heavy fines and lawsuits.

4.3 Asset 2 – Risk 1

Attribute	Value	Justification
Probability	Medium	Insider misuse or negligence is moderately likely, especially with weak authentication and monitoring gaps.
Reputation & Customer Confidence	High	System outages caused by insider misuse or misconfiguration can damage supplier and customer trust.
Financial	High	Downtime leads to production losses, recovery costs, and potential contract penalties.
Productivity	High	Unauthorized access or system misconfiguration can halt operations, reducing overall output.
Safety & Health	Medium	Misconfigured ICS/SCADA controls may create unsafe conditions in automated machinery, posing risks to workers.
Fines & Legal Penalties	Medium	Regulatory non-compliance penalties may apply under IEC 62443, NIST SP 800-82, or local data protection rules.

4.4 Asset 2 – Risk 2

Attribute	Value	Justification
Probability	High	ICS systems often run outdated firmware, rely on removable media, and face phishing/supply chain threats, making malware injection highly likely.
Reputation & Customer Confidence	High	Public knowledge of malware in manufacturing environments undermines trust in the company's reliability and product safety.
Financial	Very High	Losses occur from ransom payments, downtime, production delays, and expensive recovery operations.
Productivity	Very High	Malware disrupting PLCs/HMIs can halt automation, bottling, and QA processes, leading to complete production shutdowns.
Safety & Health	High	Malfunctioning industrial equipment due to malware creates severe safety hazards for workers and factory environments.
Fines & Legal Penalties	High	Non-compliance with IEC 62443, NIST SP 800-82, and local regulations results in regulatory fines and penalties.

4.5Asset 3 – Risk 1

Attribute	Value	Justification
Probability	Medium	Phishing, SQL injection, and insider misuse are common, but can be reduced with proper security measures, so likelihood is moderate.
Reputation & Customer Confidence	Very High	Breach of customer or employee information causes severe trust loss, customer churn, and long-term brand damage.
Financial	High	Incident response, fraud losses, breach remediation, and compensation costs result in heavy financial burdens.
Productivity	Medium	Breach investigations, forensic actions, and recovery efforts slow down business operations and divert resources.
Safety & Health	Low	Minimal direct physical impact, but affected employees may suffer stress, lowering workplace morale.
Fines & Legal Penalties	High	Non-compliance with GDPR/PDPA leads to regulatory fines, lawsuits, and mandatory notifications.

4.6 Asset 3 – Risk 2

Attribute	Value	Justification
Probability	Medium	Ransomware via phishing, unpatched systems, or insider actions is moderately likely given common exploitation trends.
Reputation & Customer Confidence	Very High	Customers lose trust if loyalty program or payroll/financial data is leaked, causing long-term reputational harm.
Financial	High	Ransom demands, incident response, downtime, and potential loss of sales create significant financial damage.
Productivity	Very High	HR operations and payroll processing may be halted during encryption, causing major disruption to business activities.
Safety & Health	Low	Direct safety impact is minimal, though employees may experience stress from payroll and HR delays.
Fines & Legal Penalties	High	Non-compliance with GDPR/PDPA due to data leakage results in fines, penalties, and possible lawsuits.

References

[1] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Pearson, 2012.

[2] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[3] National Institute of Standards and Technology (NIST), *Glossary of Key Information Security Terms*. Gaithersburg, MD, USA: NIST, 2011.

[4] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL, USA: ISACA, 2012.

[5] C. Alberts and A. Dorofee, *OCTAVE Method Implementation Guide*, CMU/SEI-2001-HB-006. Pittsburgh, PA, USA: Software Engineering Institute, Carnegie Mellon Univ., 2001.

[6] C. Alberts and A. Dorofee, *OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, CMU/SEI-2007-TR-012. Pittsburgh, PA, USA: Software Engineering Institute, Carnegie Mellon Univ., 2007.

[7] NIST, *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82, Rev. 2. Gaithersburg, MD, USA: NIST, May 2015.

[8] International Organization for Standardization, *ISO/IEC 27001: Information Security Management Systems – Requirements*. Geneva, Switzerland: ISO, 2013.

[9] International Organization for Standardization, *ISO/IEC 27002: Information Security Controls*. Geneva, Switzerland: ISO, 2013.

[10] International Electrotechnical Commission, *IEC 62443: Security for Industrial Automation and Control Systems*. Geneva, Switzerland: IEC, 2018.

The End.