Risk Assessment Report of the Red Devils Merch Co.

29th April 2023

1.0 Executive Summary

This risk assessment report was carried out at the Red Devils Merch Co. during the period from the 3rd of April to the 4th of March 2023 to assess the risk management of the critical assets at the Red Devils Merch Co. The risk evaluation was conducted to provide an overall understanding of the risk faced towards Confidentiality, Integrity, and availability of all aspects of the system concerned. The most severe vulnerabilities and threats to the assets in Red Devils Merch Co. have been identified and mitigation plans have been given along with the risk assessment strategy. Not only qualitative analysis but also we have used quantitative analysis of the analysis. The risk summary is also provided mainly for the technical staff.

1.1 Key Issues and Recommendations

Security requirements of the company lay a major role in this modern world. The attacks can be in various kinds of ways. These attacks lead to revenue loss, damage to the reputation, and reduce customer confidence. This is why we have to give our attention to risk assessment. The report is based on a well-known risk assessment framework developed by CERT, known as OCTAVE Allegro.

- **Payment processing system**
  To enhance security, we suggest implementing multi-factor authentication (MFA) for all users, enforcing strong password policies, and regularly reviewing and updating our authentication mechanisms. These measures will help protect against unauthorized access, ensure our system is up-to-date and effective, and maintain a strong security posture.
- **E-commerce platform**
  To enhance security, enforce strong passwords, use multi-factor authentication, and secure authentication protocols like OAuth and SAML.
- **Network Infrastructure**
  We recommend upgrading our Cisco ASA software to versions 8.7(1.8) and 8.4(7.2) for improved security and performance. This upgrade will provide essential security updates and new features to help protect against potential threats. Staying up to date with the latest software versions is crucial to maintaining a secure and efficient system.
- **Employee Devices**
  Enhance security and protect sensitive data by implementing full-disk encryption with software programs such as BitLocker for Windows or File Vault for Mac.
- **Customer Information Management System (CIMS)**
  To enhance the security of our system and protect sensitive data, we recommend implementing two key measures enforcing strong passwords to prevent unauthorized access, and, encrypting our data to ensure it remains confidential and secure.
- **Human Resource Management System (HRMS)**
  Enhance security by encrypting sensitive data at rest and in transit, enforcing strong passwords, implementing access controls, monitoring user activity, and conducting regular security audits and assessments.

These key issues and recommendations are further explained in the technical report.

2.0 Detailed Analysis.

2.1 Introduction.

Red Devils Merch Co. is a leading sports merchandise company that provides customers with a wide range of sports products and items around the Word. Ole Gunnar is the CEO of the company and has a great reputation in merchandising. There are 500 employees with a combination of modern technology striving to deliver merchandise that exceeds their expectations. They offer fast and reliable shipping, easy returns, and exceptional customer service to ensure that everyone is completely satisfied with their purchase. A Head office and network operations center in a single building (6 floors) at. Sir Matt Busby Way, Manchester M16 0RA, United Kingdom. Figure 2.1. A outlines the organization structure with regards to this report and a few keywords/names are introduced.

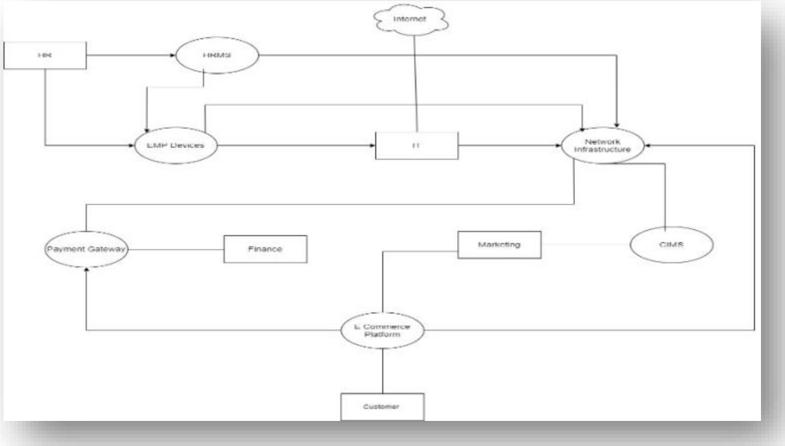


Figure 2.1.A

2.2 Purpose.

The purpose of this risk assessment was to look at and find the vulnerabilities and loopholes in the company's information technology assets and identify the existing threats to the most critical assets. This report consists of 6 critical information assets. Each Department was represented by members of the staff who were involved in a two-day workshop organized by the IT department to familiarize themselves with the OCTAVE procedure. This report can be used as the framework for the company's future references about the course of action.

2.3 Scope.

Functional	Personal	Factorial
Six information systems and sub-systems were identified as critical systems. We have found some new functional requirements.	The process of evaluating risk involved a comprehensive team that includes the IT sector and the company employees at various levels (Management, Staff). All the employees of the company's boundaries are included.	Confidentiality, integrity, and availability and three as are the essential information security factors that have a direct effect on company currency flows and organizational structure.

2.4 Risk Assessment Framework.

We utilized the OCTAVE Allegro risk management framework to evaluate and analyze the potential risk and impacts resulting from the above-mentioned factors.

- OCTAVE ALLEGRO is a well-defined system that allows us to thoroughly assess the potential risks and develop effective strategies to mitigate or manage them.
- The OCTAVE Allegro methodology is a streamlined and efficient top-down approach to risk management that provides satisfactory results with minimal time and resources.

2.5 Assets profile

The essential assets identified throughout the risk assessment process are included in the following section along with vital details such as their definition, availability of resources, and projected worth.

Critical Asset	Description	Systems	Security Requirement				Asset value ($)
			Property	High	Medium	Low	
Payment processing System (PPS)	Our payment system manages all transactions, including credit card payments, refunds, and security. It is crucial and requires strict controls to prevent fraud and maintain customer trust.	Payment Gateway	Confidentiality			🟩	22,440
			Integrity		🟧		
			Availability	🟥			
E-commerce Platform	The cloud-based E-commerce platform facilitates online shopping, purchases, and order	Cloud Server	Confidentiality			🟩	6,350
			Integrity		🟧		

	tracking with features such as product listing, shopping cart, payment processing, order management, and customer service.		Availability	🟥			
Network Infrastructure	Our company's network infrastructure consists of hardware devices like routers, switches, servers, etc. It facilitates connectivity, resource sharing, and data transfer, supporting essential business operations.	Interconnected Hardware and software devices.	Confidentiality		🟧		12,900
			Integrity		🟧		
			Availability	🟥			
Employee Devices	Employee devices like laptops, smartphones, and tablets are vital for remote work and accessing critical data.	Hardware components (Interconnected/not)	Confidentiality	🟥			420,000
			Integrity		🟧		
			Availability			🟩	
Customer Information Management System (CIMS)	The system will handle customer information from registration to delivery and store it for future marketing. It	Software with backend database	Confidentiality		🟧		180,000
			Integrity	🟥			

	will include details like name, address, payment, shipment, credit/debit card info, etc. The data will be updated daily from the payment processing system and E-commerce platform.		Availability		🟧		
Human Resource Management System (HRMS)	The HRMS manages and secures staff personal and biometric data like name, address, age, bank details, fingerprints, and facial recognition. It also handles data consumption, generation, modification, and exchange.	Software-based backend database.	Confidentiality		🟧		150,000
			Integrity	🟥			
			Availability			🟩	

2.6 Threat Profile and Mitigation Analysis

Critical Asset	**Vulnerability**	**Threat Profile**	**Impact Assessment**	**Mitigation plan**	**Cost for a mitigation plan.**	**Cost/Benefit**
The payment processing system (PPS) (Amazon Web Services (AWS) EC2: AWS EC2)	Using weak authentication methods to authenticate the user.	Unauthorized access to payment data due to weak authentication mechanisms	The risk was identified as 8.0/10 since it has a higher impact on Availability and confidentiality.	Implement multi-factor authentication (MFA) for all users, enforce strong password policies, and regularly review and	$1,8000	+$6,684

				update authentication mechanisms		
E-commerce platform (Apache Web Server)	Weak authentication mechanism (e.g., default passwords, no multi-factor authentication)	Vulnerable to brute force attacks , attackers can gain access to the system.	Unauthorized access to sensitive information, data breaches, and system compromise	Use strong passwords and enforce password complexity policies, implement multi-factor authentication, and use secure protocols for authentication (e.g., OAuth, SAML)	$8,000	+ $3,450
Network Infrastructure (Cisco routers (e.g., ASR 1000 Series, ISR 4000 Series), switches (e.g., Catalyst 9000 Series), and firewalls (Cisco ASA 5585-X)	Outdated or unpatched firmware/software	Vulnerable to denial-of-service (DoS) attacks	A successful DoS attack can result in system downtime, making the affected resources unavailable to legitimate users. This can lead to lost productivity, revenue, and customer dissatisfaction.	Upgrade Cisco ASA Software versions to 8.7(1.8) and 8.4(7.2).	$10,000	+ $ 5,480
Employee Devices (Desktops, laptops, smartphones, tablets)	Lack of encryption, weak passwords, unpatched software	Vulnerable to social engineering and, phishing attacks, and unauthorized access	Data breaches, theft of sensitive information, and system compromise	Implement full-disk encryption, by software program that encrypts all the data on the hard drive, such as BitLocker for Windows or File Vault for Mac.	$127,000	+ $1,002,800
Customer information management system	Weak password policies, unencrypted communication	Threat actors could intercept sensitive data transmitted	threat actors can potentially gain access to sensitive	Implementing strong passwords, encrypting	$30,000	+ $4,000

(CIMS) (ORACLE database server)	channels, and lack of access controls	over unencrypted channels (e.g., HTTP instead of HTTPS)	information such as login credentials, financial information, personal identification information, and data. This can result in a range of negative impacts, including financial loss, and legal and regulatory consequences.	communication channels, enforcing access controls, regularly backing up data, conducting vulnerability scans, updating software, and using DLP and SIEM solutions for data leakage prevention and monitoring.		
Human Resource management system (HRMS) (Microsoft SQL Server)	Lack of Encryption	Unauthorized Access, Data Theft	Financial Loss, Reputational Damage	Encrypt sensitive data at rest and in transit, monitor user activity with security information and event management (SIEM) solutions and conduct regular security audits and vulnerability assessments.	$8,000	+ $3,250

3.0 Risk Assessment Summary

The Red Devils Merch Co. possesses critical assets that require immediate attention to reduce the risk of potential threats that could negatively impact the company. There are low-level and serious vulnerabilities that must be addressed urgently to prevent system failure. The risk assessment management team established control mechanisms for identified threats by calculating estimations for successful prevention, avoidance, transference, and acceptance plans. They utilized a risk assessment model called OCTAVE Allegro.

The payment processing system, Amazon Web Services (AWS) EC2, uses weak password authentication methods to verify users, which could lead to unauthorized access to the system. To prevent this vulnerability, the company can use multifactor authentication and enforce strong password policies. Asset availability is of utmost priority. The e-commerce platform, Apache web server, has weak authentication mechanisms that could result in brute force attacks. To prevent this vulnerability, the company can use security protocols like OAuth and SAML for authentication, which can improve asset availability. The network infrastructure contains Cisco routers (e.g., ASR 1000 Series, ISR 4000 Series), switches (e.g., Catalyst 9000 Series), and firewalls (Cisco ASA 5585-X), which have outdated or unpatched firmware/software, making them vulnerable to DoS attacks. To enhance availability and integrity, the company can upgrade Cisco ASA Software versions to 8.7(1.8) and 8.4(7.2).

Employee devices are susceptible to phishing attacks and unauthorized access due to a lack of encryption, weak passwords, and unpatched software. To ensure confidentiality and reduce risk, the company can implement full-disk encryption by using software such as BitLocker for Windows or File Vault for Mac.The Customer Information Management System (CIMS), which is an ORACLE database server, has unencrypted communication channels and lack of access controls, making it vulnerable to risks. To mitigate these risks and improve integrity as a high priority, the company can update the software and use Data Loss Prevention (DLP) and Security Information and Event Management (SIEM) solutions.

The Human Resource Management System (HRMS), which is a Microsoft SQL Server, requires more focus on integrity, and it is vulnerable to lack of encryption mechanisms. To reduce the risk and improve integrity, the company can use technologies like encrypting sensitive data at rest and in transit, monitoring user activity with SIEM solutions, and conducting regular security audits and vulnerability assessments.

4.0 References

[1] J. Beeskow, "Reducing security risk using data loss prevention technology", Healthcare Financial Management: Journal Of The Healthcare Financial Management Association, vol. 69, no. 11, pp. 108-112, 2015.

[2] Suroso, Jarot S., and Muhammad A. Fakhrozi. "Assessment of information system risk management with octave allegro at education institution." *Procedia Computer Science* 135 (2018): 202-213.

[3] K. Abdullah, I. N. Isnainiyah and M. I. Faried, "Risk Management Analysis on Organizational Website Using Octave Allegro Method," 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia, 2020, pp. 201-206, doi: 10.1109/ICIMCIS51567.2020.9354298.

[4] A. D. Prajanti and K. Ramli, "A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods," 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), JeJu, Korea (South), 2019, pp. 1-4, doi: 10.1109/ITC-CSCC.2019.8793421.

[5] J. S. Suroso, A. Januanto and A. Retnowardhani, "Risk Management of Debtor Information System At Bank XYZ Using OCTAVE Allegro Method," 2019 International Conference on Electrical Engineering and Informatics (ICEEI), Bandung, Indonesia, 2019, pp. 261-265, doi: 10.1109/ICEEI47359.2019.8988890.

[6]M. T. Jufri, M. Hendayun and T. Suharto, "Risk-assessment based academic information System security policy using octave Allegro and ISO 27002," 2017 Second International Conference on Informatics and Computing (ICIC), Jayapura, Indonesia, 2017, pp. 1-6, doi: 10.1109/IAC.2017.8280541.

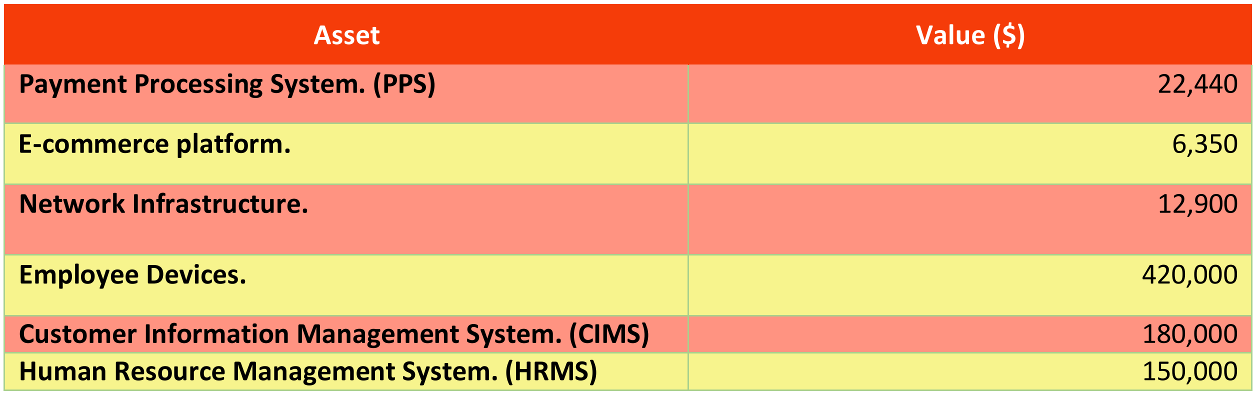
5. Appendix.

5.1 Calculations and Assumptions

Qualitative Analysis

Impact Level	Value Out of 10	Description
High	7-10	a serious incident that could cause significant reputational and financial harm and result in significant client and business losses.
Medium	4-6	An incident that may cause some damage but is unlikely to cause major harm.
Low	1-3	An incident with minimal impact.

Probability	Value (%)	Description
High	75	A situation with a high probability of occurring.
Medium	50	An event with a medium possibility of occurring.
Low	25	something unusual happens.



Asset	Value ($)
Payment Processing System. (PPS)	22,440
E-commerce platform.	6,350
Network Infrastructure.	12,900
Employee Devices.	420,000
Customer Information Management System. (CIMS)	180,000
Human Resource Management System. (HRMS)	150,000

Quantitative Analysis

Assets	Before Mitigation Applied		After Mitigation Applied	
Payment Processing System	EF	75%	EF	20%
	SLE	$22440 x 75% = $16,830	SLE	$22,440 x 20%= $4,488
	ARO	2	ARO	2
	ALE	$16,830 x 2= $33,660	ALE	$4,488 x2= $8,976
	Cost/Benefit: $33,660 - $8,976- $18,000 = + $6,684			
E-commerce platform	EF	80%	EF	35%
	SLE	$6,350x 80% = $5,080	SLE	$6,350 x 35%= $2222.50
	ARO	4	ARO	4
	ALE	$5,080 x 4= $20,320	ALE	$2222.50 x 4= $8,890
	Cost/Benefit: $20,320 - $8,890 - $8,000 = + $3,450			
Network Infrastructure.	EF	70%	EF	10%
	SLE	$12,900 x 70% = $9,030	SLE	$12,900 x 10%= $1,290
	ARO	2	ARO	2
	ALE	$9,030 x 2= $18,060	ALE	$1,290 x 2= $2,580
	Cost/Benefit: $18,060- $2,580- $10,000 = + $ 5,480			
Employee Devices.	EF	70%	EF	15%
	SLE	$420,000 x 70% = $294,000	SLE	$420,000 x 15%= $63,000
	ARO	5	ARO	5

	ALE	$$294,000 x 5= $1,470,000	ALE	$63,000 x 5= $315,000
	Cost/Benefit: $1,470,000- $315,000 - $127,000 = + $1,002,800			
Customer Information Management System. (CIMS)	EF	80%	EF	40%
	SLE	$180,000 x 80% = $144,000	SLE	$180,000x 40%= $72,000
	ARO	0.5	ARO	0.5
	ALE	$144,000 x 0.5= $72,000	ALE	$72,000 x 0.5= $36,000
	Cost/Benefit: $72,000-$36,000-$30,000- = + $4,000			
Human Resource Management System. (HRMS)	EF	50%	EF	20%
	SLE	$150,000 x 50% = $75,000	SLE	$150,000 x 20%= $30,000
	ARO	0.25	ARO	0.25
	ALE	$75,000 x 0.25= $18,750	ALE	$30,000 x 0.25= $7,500
	Cost/Benefit: $18,750 - $7,500 - $ 8,000= + $3,250			

5.2 OCTAVE Allegro

Asset 01

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 processing system (PPS)	The Payment Processing System is a critical asset because it is the backbone of the financial dealings of the company. Any system malfunction or compromise could lead to sizable monetary losses, reputational harm, and legal liabilities.	The Payment Processing System oversees handling all financial transactions, including chargebacks, refunds, and customer payments. The system transmits payment data to financial institutions after validating payment information and confirming the legitimacy of payment methods.
(4) Owner(s) *Who owns this information asset?*		
Finance Manager		
(5) Security Requirements *What are the security requirements for this information asset?*		
□ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	The system must guarantee that payment information is kept private and shielded from unauthorized access.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	During transmission and processing, the system must make sure that payment data is accurate, complete, and unaltered.
□ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The system must be functional. 24/7 to process payments, and downtime must be kept to a minimum.
	This asset must be available for _24____ hours, _7____ days/week, _____ weeks/year.	

□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	The system has to abide by all applicable laws and professional standards, like PCI-DSS.	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
□ Confidentiality	□ Integrity	□ Availability	□ Other

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**		
Information Asset Risk	**Threat**	Information Asset	Payment processing system		
		Area of Concern	Unauthorized access		
		(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?*	To gain unauthorized access to the payment processing system, the hacker may try many numbers of techniques, including phishing, malware, or social engineering.		
		(3) Motive *What is the actor's reason for doing it?*	Financial gain, the theft of payment information, or the disruption of services for payment processing could be the hacker's motivations.		
		(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?*	Weak passwords, unsecured network connections, or unpatched software vulnerabilities could all be used by the hacker to get past security measures.		
		(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**
		Reputation & Customer Confidence	8	6
		Financial	9	6.75
		Productivity	7	5.25
		Safety & Health	1	0.75
		Fines & Legal Penalties	9	6.75
		User Defined Impact Area		
			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?*
Payment Gateway	Implement multi-factor authentication for all payment transactions. The residual risk of unauthorized access to the payment gateway may still be accepted by the organization. For all payment transactions, use multi-factor authentication. The business may still accept the risk of unauthorized access to the payment gateway.
Payment Database	Encrypt both the transit and storage of all payment data. The organization may continue to accept a residual risk of data breaches due to weaknesses in the implementation of encryption.

Asset 02.

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?*
E-commerce platform running on a cloud server	Due to its importance as the company's main channel for generating revenue and engaging with customers, the e-commerce platform is critical. Significant financial losses as well as reputational damage could result from any platform compromise or outage.	Online shopping, purchases, and order tracking are all made possible by the e-commerce platform, which is a cloud-based platform. It has features like a product listing, shopping cart, checkout, processing payments, order management, and customer service.
(4) Owner(s) *Who owns this information asset?*		
IT divisional head		
(5) Security Requirements *What are the security requirements for this information asset?*		
□ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Customer and transactional data must be securely encrypted and kept. Only authorized personnel should have access to sensitive information.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Every order, transaction, and piece of customer data needs to be accurate and protected from unauthorized change.
□ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The e-commerce platform ought to be accessible. 24/7 with a minimum amount of downtime for maintenance and upgrades.

	This asset must be available for ___24__ hours, __7___ days/week, _____ weeks/year.	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Relevant legal requirements, such as PCI DSS and GDPR, should be complied with by the e-commerce platform.

(6) Most Important Security Requirement

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

□ Confidentiality	□ Integrity	□ Availability	□ Other

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	**Threat**	Information Asset	E-commerce platform running on a cloud server
		Area of Concern	Unauthorized access
		(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?*	gaining unauthorized access by taking advantage of a flaw in the e-commerce platform
		(3) Motive *What is the actor's reason for doing it?*	to steal confidential financial or customer 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?*	Failure to implement sufficient access controls or properly secure the cloud server.

(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**
	Reputation & Customer Confidence	8	6
	Financial	9	6.75
	Productivity	7	5.25
	Safety & Health	5	3.75
	Fines & Legal Penalties	8	6
	User Defined Impact Area		
		Relative Risk Score	**27.75**

(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?*
Cloud infrastructure	Put access control measures in place, such as multi-factor authentication, strong passwords, and regular user account monitoring. To stop vulnerabilities, regularly apply security patches and updates. Due to flaws in cloud providers or supply chain assaults, there may still be some residual risks.
Web application	Using firewalls and intrusion detection/prevention systems, configuring access controls and authentication mechanisms, encrypting sensitive data, implementing secure coding practices, applying security patches and updates on a regular basis, performing regular security audits and assessments are a few important measures.

Asset 03.

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?*
Network infrastructure (routers, switches, firewalls)	Network infrastructure is a critical asset for our company because it serves as the foundation of our whole IT system. It contains the physical and virtual components that enable communication and data exchange across our organization's devices, systems, and users. Our organization depends on network infrastructure since it allows for smooth communication, data transmission, and collaboration while also maintaining the security and integrity of our company's information. It acts as the basis for our organization's IT system, allowing for efficient and effective operations while also supporting our business's growth and success.	The physical and virtual components, including hardware, software, and protocols, that are used to support communication and data exchange within our organization's IT environment are often referred to as an asset in our company. It includes networking hardware including routers, switches, firewalls, servers, cabling, and other networking devices, as well as the software, configurations, and protocols that enable communication and data transmission.
(4) Owner(s) *Who owns this information asset?*		
Network operations 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 have access to network infrastructure components. Use authentication mechanisms such as strong passwords, multi-factor authentication, and role-based access controls (RBAC) to restrict access to authorized personnel only.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	only authorized personnel to have access to network infrastructure components so only they can modify, update and delete data.
□ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	To provide high availability and reduce single points of failure, use separate network components, such as separate power supplies, switches, and routers. Implement technologies such as load balancing and failover techniques to ensure network availability in the case of hardware or software failure.
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement

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

□ Confidentiality	□ Integrity	□ Availability	□ Other

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	**Threat**	Information Asset	Network Infrastructure
		Area of Concern	An attacker does a DOS attack and access to the network and down all servers of the company and change sensitive data.
		(1) Actor *Who would exploit the area of concern or threat?*	An outside attacker
		(2) Means *How would the actor do it? What would they do?*	An attacker can access to the network and get all the payment details such as credit card details and other information and modify data.
		(3) Motive *What is the actor's reason for doing it?*	To harm the company reputation and gain financial benefits.
		(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?*	
		(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**
	Reputation & Customer Confidence	9	6.75
	Financial	10	7.5
	Productivity	7	5.25

		Safety & Health	2	1.5
		Fines & Legal Penalties	8	6
		User Defined Impact Area		
			Relative Risk Score	**27.00**

(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?*
Firewall	Use a latest versions of firewall.
Software updates	Regularly update the firmware/software to the latest version, use secure configurations, and implement access control policies and network segmentation. Latest versions of Cisco IOS software include IOS XE 17.x and IOS XR 7.x for routers, while the latest version of Cisco NX-OS is 9.3(7) for switches
Authentication mechanisms	Only authentication people can enter the server rooms.

Asset 4.

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?*

Employee devices	This asset enables remote work, increase efficiency, reduce costs, and provide a competitive advantage. By allowing employees to work from home or anywhere, employee devices can increase productivity and provide a more flexible working environment. This, in turn, can lead to cost savings for organizations, as employees can use their personal devices for work purposes. Additionally, organizations that embrace employee devices can gain a competitive advantage by attracting and retaining top talent.	The data or applications stored on these devices that are related to the organization's business operations. This description may be further defined through policies and agreements, such as an acceptable use policy or a bring-your-own-device (BYOD) policy, to outline specific requirements and responsibilities related to the use, management, and security of these devices.

(4) Owner(s)

Who owns this information asset?

IT Department manager

(5) Security Requirements

What are the security requirements for this information asset?

□ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Data in those devices can only view by the authorized person.
□ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Those devices contain company data, that data cannot be changed.
□ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Employees need those data available whenever they need.
	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:		
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
□ Confidentiality	□ Integrity	□ Availability	□ Other

Allegro - Worksheet 10		**Information Asset Risk Worksheet**	
Information Asset Risk	Threat	Information Asset	Employee Devices
		Area of Concern	As the devices may contain sensitive and confidential data, and the risk of data breaches or unauthorized access.
		(1) Actor *Who would exploit the area of concern or threat?*	An Outside Attacker
		(2) Means *How would the actor do it? What would they do?*	Phishing or social engineering attacks can do to gain the access to the devices.
		(3) Motive *What is the actor's reason for doing it?*	This data may include confidential business plans, intellectual property, financial information, or other sensitive information that, if obtained by an unauthorized third party, could cause significant harm to the company's reputation, finances, and 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?*	This asset needs to have confidentially, integrity and availability.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** **75%** □ **Medium** **50%** □ **Low** **25%**
	(7) Consequences *What are the consequences to the organization or the information asset owner*		(8) Severity *How severe are these consequences to the*

	as a result of the outcome and breach of security requirements?	*organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
		Reputation & Customer Confidence	9	6.75
		Financial	5	3.75
		Productivity	9	6.75
		Safety & Health	2	1.50
		Fines & Legal Penalties	5	3.75
		User Defined Impact Area	-	-
			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?*
Central Server	Administrative Controls: Security policies, access controls, security training. Technical Controls: Firewalls, intrusion detection systems, antivirus software, encryption. Physical Controls: Access control systems, security cameras, alarm systems.
Employee Workstations	Administrative Controls: Security policies, access controls, security training. Technical Controls: Antivirus software, firewalls, intrusion detection systems. Physical Controls: None.
Mobile Devices (Smartphones, tablets)	Administrative Controls: Security policies, access controls, security training. Technical Controls: Mobile device management software, encryption, remote wipe capabilities. Physical Controls: None.

Asset 5.

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Customer Information Management System. (CIMS)	This system manages the all-customer data. There is confidential data of customers. If the customer details lost the company cannot use the customer data for future trend forecasting and shipping addresses.	This system will manage the customer information from customer registration until the end of the delivery and store the details for future marketing strategies. His system will contain customer name, address, payment details, shipment address, credit/debit card details, shipment status and ordered date. This system will update daily basis with the data that provide by the payment processing system and E-commerce platform.
(4) Owner(s) *Who owns this information asset?*		
Marketing and sales Admin.		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Sensitive and confidential data of the customer and payment credentials cannot be visible for any unauthorized persons.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Previous stored customer data should not be erased or modified by anyone.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Payment details and shipping addresses should be available for anytime.

	This asset must be available for ___24__ hours, ___7__ days/week, _____ weeks/year.	
□ **Other**	This asset has special regulatory compliance protection requirements, as follows:	The stored data should be encrypted.

(6) Most Important Security Requirement

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

□ Confidentiality	□ Integrity	□ Availability	□ Other

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**		
Information Asset Risk	**Threat**	Information Asset	CIMS		
		Area of Concern	Attacker gain access to the CIMS and steal or modify sensitive and confidential data of the customers and sell that data to the third party.		
		(1) Actor *Who would exploit the area of concern or threat?*	Outsider attacker.		
		(2) Means *How would the actor do it? What would they do?*	Attacker can get the access to the CIMS remotely by exploiting a vulnerability and steal payment details credit/debit card details and credentials of the customers and sell it to a third party or use this information for future attacks.		
		(3) Motive *What is the actor's reason for doing it?*	Gain the financial benefit or information gathering.		
		(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?*	CIMS have some sensitive data of customers and data should be view or change by the unauthorized people.		
		(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**
		Reputation & Customer Confidence	9	6.75
		Financial	7	5.25
		Productivity	8	6.00
		Safety & Health	2	1.5
		Fines & Legal Penalties	8	6
		User Defined Impact Area	-	-
			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?*
Encrypted mechanisms for stored data.	Implement strong encryption techniques to store customer data.
Authentication mechanisms.	Implement strong authentication mechanism to authenticate the user before view or edit the data.
Backups.	Use a backup server to store the data for gain availability.

Password policies.	Implement password policies to prevent employees setting a weak password.

Asset 6.

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?*
Human Resource Management system. (HRMS)	Our HRM system is an asset to our company since it helps to optimize HR processes, centralize employee data, give self-service choices for employees, ensure compliance and reporting, assist talent management, and protect data security and confidentiality. It can help to improve HR efficiency, optimize HR operations, and contribute to overall company performance and success.	Human Resource Management (HRM) system in our company is a software or technology platform that has been implemented to efficiently manage your organization's human resources. It is a system that includes features and functionalities specific to our company's HR processes, policies, and requirements. It serves as a centralized tool for managing employee data, automating HR operations, facilitating talent acquisition and management, ensuring compliance with applicable labor laws and regulations, and maintaining data security and confidentiality.
(4) Owner(s) *Who owns this information asset?*		
HR Department Head		

(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Only the users have privileges to the system can access the system.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Any other users can not change or modify the data in the HRMS without access from the admins.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	This should be available for the ongoing process like payment processes, registration etc.
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	This should not be down for more time.
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

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

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	Threat	Information Asset	Human Resource Management system. (HRMS)
		Area of Concern	An attacker gets all personal details about employees and can change the details.
		(1) Actor *Who would exploit the area of concern or threat?*	An outside attacker
		(2) Means *How would the actor do it? What would they*	An attacker can access to the system and get all the payment details such as credit card

do?	details and other information.		
(3) Motive *What is the actor's reason for doing it?*	To harm the company reputation and gain financial benefits.		
(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?*			
(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**
	Reputation & Customer Confidence	9	6.75
	Financial	8	6.00
	Productivity	5	3.75
	Safety & Health	3	2.25
	Fines & Legal Penalties	6	4.5
	User Defined Impact Area		
		Relative Risk Score	**23.25**

(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?*

Authentication mechanisms.	Before editing the HRMS data, authenticate the person.
Maintain logs.	Use a SIEM system to monitor events on the HRMS system.

Group Details.

IT21110184	Peiris B.L.H.D
IT21051548	A.R.W.M.V. Hasaranga
IT21049354	Athauda A.M.I.R.B.
IT21085376	J.P.A.S. Pathmandre