RISK ASSESMENT REPORT

-2025-

SKYREK

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

INFORMATION SECURITY RISK MANAGEMENT - IE3052

YEAR 3 SEMESTER 2

	Registration Number	Full Name
1	IT22353184	R.M.C.A.Rathnayaka
2	IT22921512	S.I.B.Jayawardhana
3	IT22307880	Ellawala E.L.M
4	IT22904232	M.M.M.Ukasha

Contents

Abstract

This risk assessment aims to identify and mitigate weaknesses, vulnerabilities, and failures in SKYREK's digital infrastructure, with a focus on its web solutions and business-critical systems. The assessment leverages the OCTAVE Allegro risk management framework to systematically evaluate potential threats, particularly those that could impact the company's reputation, client trust, and financial stability. The report will analyze current vulnerabilities, highlight key risk areas, and provide actionable recommendations to enhance SKYREK's information security posture and safeguard its operations in the digital services industry.

1. Executive Summary

This report presents a comprehensive information security risk assessment for SKYREK, a digital solutions provider based in Kalutara, Sri Lanka. The evaluation was conducted between April 1, 2025, and April 25, 2025, with the primary objective of identifying and addressing critical risks to the organization's web-based assets and supporting infrastructure.

Using the OCTAVE Allegro methodology, the assessment focused on the following key areas:

- Evaluating threats specific to the web development and IT services sector.
- Assessing the effectiveness of existing cybersecurity controls and practices.
- Developing a roadmap for an IT security program tailored to SKYREK's current processes, personnel, and technologies.

2.1 Key Issues Identified:

- Vulnerabilities in web applications (e.g., protocol downgrade, XSS, IDOR).
- Business email compromise (e.g., No SPF, DKIM and DMARC)
- Gaps in employee security awareness and secure development practices.
- Unauthorized access to cloud platforms.
- BYOD employees use unverified applications.
- Access or steal employee records or salary information.
- Unauthorized access to WhatsApp business communications

2.2 Recommendations:

- Enforce secure protocols (HTTPS, HSTS) and remediate web vulnerabilities. [1]
- Establish a formal incident response and disaster recovery plan.
- Implement regular vulnerability assessments and security awareness training.
- Apply strong access controls and multi-factor authentication for critical systems.
- Secure and monitor all data storage solutions (cloud and on-premises).
- Require up-to-date security software on all BYOD devices.
- Apply strict access controls and role-based permissions for Employee data.
- Monitor and log all access to sensitive employee information.
- Mandate use of WhatsApp Business with approved devices only.

2.DETAILED ANALYSIS

2.1.Introduction

Skyrek is a dynamic startup specializing in providing innovative digital solutions that cater to the evolving needs of businesses in Sri Lanka. As a digital services company, Skyrek focuses on delivering customized software solutions aimed at enhancing business efficiency and driving operational success. Despite being a relatively young company, founded with a vision to leverage cutting-edge technology, Skyrek has quickly positioned itself as a trusted partner for businesses seeking to streamline their operations and improve their digital presence.

Skyrek operates primarily remotely, with a small yet highly skilled team of 20-25 employees, enabling flexibility and scalability. The company's core operations revolve around providing web development, IT infrastructure management, and cybersecurity services. By focusing on tailored, customer-centric solutions, Skyrek helps organizations optimize their workflows, secure their digital assets, and unlock their full potential through technology. With a mission to drive business growth through innovation, Skyrek is committed to delivering value-driven solutions and transforming the way businesses operate in a digital-first world.

2.2.PURPOSE

This analysis aims to conduct a thorough information security risk assessment for SKYREK, a digital solutions provider in Kaluthara, Sri Lanka, to identify and mitigate potential threats and their financial impact, thereby safeguarding the organization's operations and reputation.

2.3. Why use Octave Allegro

Octave Allegro is chosen for risk management due to its systematic, customizable, and comprehensive approach [2]. It helps organizations like SKYREK identify threats, assess impact, and prioritize actions, enabling clear communication and informed decision-making to strengthen security measures.

Participants

ROLE	PARTICIPANT
Co-Founder	NIpuna Nadeeshan
Co-Founder	Malith Dilshan

2.4.Risk Assessment criteria

2.4.1.Risk Model

Risk = Impact x Probability, is the common formula**.**

2.4.2.Threat Impact Scale

Impact score	Definition	Range
High	Major disruption, serious consequences for business	From 7 to 10
Medium	Moderate impact, some disruption, but manageable.	From 3 to 6
Low	Minor impact, minimal disruption to operations.	From 1 to 2

2.4.3.Threat Probability Scale

Probability Score	Definition	Percentage
High	Very Likely to happen	80%
Medium	Likely to happen	50%
Low	Unlikely to Happen	25%

2.4.4.Risk Scale

Low Risk: Scores closer to 0.25–2.0

Medium Risk: Scores in the 2.0–4.5 range.

High Risk: Scores above 4.5, mainly focus on values 6.0–7.0.

2.4.5.Risk Calculation

The risk scores for the found assets were as follows,

Cloud Platform (AWS, Amazon S3) - 15.5 / 15

Company website (SkyRek.com) – 5.5 / 8.25

Company Email System - 11.2

Personal Workstation (BYOD) -13.5 / 14.4

Employee Information (on site PC) - 4

WhatsApp business Accounts – 5.5

2.5.Critical Asset Identification

Critical Assets	**Description**	**Security Requirements**
Cloud platform (AWS, Amazon S3)	The cloud platform (AWS) is where **Skyrek** stores its critical data, including client and project files, backups, and operational data. Amazon S3 provides scalable storage with high durability. [3]	• **Confidentiality**: High (Protect sensitive data such as client and project files). • **Integrity**: High (Ensure data is not altered without authorization). • **Availability**: High (Ensure data is accessible 24/7 with minimal downtime).
Skyrek.com website	The official website for **Skyrek**, provides customer-facing services, information, and interaction with potential clients. The website is critical for customer engagement and business reputation.	• **Confidentiality**: Medium (Publicly accessible, but user interactions should be secure). • **Integrity**: High (The website must maintain accurate and reliable content). • **Availability**: High (The website should be operational and accessible to customers at all times).
Business Email System	The business email system that employees use for internal and external communication, handling sensitive client information like project invoices and business correspondence. [4]	• **Confidentiality**: High (Emails may contain sensitive information such as client data and contracts). • **Integrity**: High (Emails must not be tampered with or forged). • **Availability**: Medium (Emails should be available but some temporary outages may be acceptable).
Personal employee workstations (BYOD)	**BYOD devices** used by employees to access company data, emails, and internal systems. These devices are owned by employees but used for business operations remotely.	• **Confidentiality**: High (Employee BYOD devices may access sensitive business data and should be secured). • **Integrity**: High (Ensure device security to prevent unauthorized tampering or malware). • **Availability**: Medium (Employees should have access to workstations but downtime can occur if devices fail or are not properly secured).
Employee information	Sensitive employee data (personal records, payroll, HR data) stored on a **onsite computer**. This data is critical	• **Confidentiality**: High (Employee information needs to be tightly controlled to prevent unauthorized access). • **Integrity**: High (Ensure accurate records,

	for HR management and business operations.	especially for payroll and benefits). • **Availability**: Low (Employee information does not need to be constantly available unless needed for HR processes).
WhatsApp Business Accounts	WhatsApp community is used by company Employees for project discussions and employee interactions.	• **Confidentiality**: Medium (WhatsApp may store customer communication but is not typically used for highly sensitive business data). • **Integrity**: Medium (Communications should not be tampered with, but minor errors may occur). • **Availability**: Medium (WhatsApp must be operational for client communication but is less critical than other systems).

2.6.Threat Profile

Asset-Cloud Platform (AWS Amazon S3)		
Threat Analyze	**Impact**	**Mitigation**
Unauthorized access- • External attackers, internal employees, or third-party contractors may exploit misconfigured IAM roles/policies or use stolen credentials to gain unauthorized access to S3 resources	• Can lead to data theft, disclosure of sensitive information, modification of confidential data, and breach of client confidentiality	• Implement strict IAM policies with least privilege principle and regular permission reviews. • Use AWS CloudTrail and Config for monitoring and alerting on suspicious changes.
Publicly accessible resources- • Attackers use automated tools to scan for public buckets, exploit misconfigured ACLs, bucket policies, or leverage open endpoints • S3 buckets are particularly vulnerable as they're accessible through AWS endpoints from anywhere on the web	• This can result in data breaches, intellectual property theft, and financial losses through extortion or fraud.	• Enable S3 Block Public Access at account and bucket levels to prevent accidental exposures. • Implement automated alerts for any resource that becomes publicly accessible. • Apply least privilege IAM policies and restrict bucket policies to necessary users only.

Asset-WhatsApp Business Account		
Threat Analyze	**Impact**	**Mitigation**
Unauthorized access- • External attackers, or unauthorized employees may gain access.	. • Leads to unauthorized viewing or exfiltration of sensitive customer information, business messages, and files. • Results in severe reputational damage and loss of customer trust.	• Enable two-factor authentication (2FA) for all WhatsApp Business accounts. • Implement strong password policies and regularly update credentials.

Asset - Company Website (SKYREK.COM)		
Threat Analyze	**Impact**	**Mitigation**
a) **Protocol Downgrade** cause do to lack or misconfigurations of HSTS Header content.	Protocol downgrade attacks can force users from secure HTTPS connections to insecure HTTP, enabling attackers to intercept sensitive information, hijack sessions, inject malicious content, and compromise user credentials.	- Enforce HTTPS across all website pages. - Implement HTTP Strict Transport Security (HSTS). - Regularly test for protocol downgrade vulnerabilities. - Use strong TLS configurations and disable insecure protocols. - Monitor for suspicious traffic and attempted downgrades.

b) Cross-Site Scripting (XSS)	XSS attacks allow attackers to inject malicious scripts into web pages viewed by users, leading to theft of session cookies, user credentials, or sensitive data, as well as possible website defacement and loss of user trust.	- Implement strict input validation and output encoding. - Sanitize all user-supplied data and file uploads. - Apply Content Security Policy (CSP) headers. - Conduct regular vulnerability scanning and penetration testing.

Asset - Company Email System (SKYREK)		
Threat Analyze	**Impact**	**Mitigation**
a) Business Email Compromise (No SPF, DKIM, DMARC)	Attackers can spoof company email and act as legitimate employee of the organization, leading to unauthorized instructions, data theft, and phishing.	- Implement SPF, DKIM, and DMARC to authenticate outgoing emails and prevent spoofing. - Conduct regular security awareness training for employees. - Monitor and alert for suspicious email activity. - Enforce multi-factor authentication (MFA) for all email accounts.

Asset-personal workstations (BYOD)		
Threat Analyze	**Impact**	**Mitigation**
1) Unverified Applications (malware software)	• Data Theft: Malware may harvest login credentials or sensitive files. • Unauthorized Access: Keyloggers or backdoors can allow attackers to access corporate SaaS systems Leakage of confidential company data for personal gain.	• Require MDM/EDR (Endpoint Detection & Response) agents on all BYOD devices to detect unauthorized software in real time. • Restrict access to cloud systems from non-compliant devices using Zero Trust and conditional access policies

2) Inconsistent patching and updates	• Data breaches from unpatched BYOD vulnerabilities. • Cloud Access Compromise: Devices with security flaws may act as weak points when interacting with SaaS platforms	• Enforce mandatory auto-updates for OS and all business-critical applications • Deny access to core systems if patch status is out-of-date using remote compliance rules. • Integrate devices with cloud-based patch compliance monitoring (ex. Microsoft Intune, Jamf).

Asset-Employee Information (On site PC)		
Threat Analyze	**Impact**	**Mitigation**
1. Access or steal employee records of salary information	• Unauthorized access to sensitive employee data, including personal identification information, employment records and payroll data.	• Monitor user activity and logs of users. • Implement RBAC to limit access to certain sensitive data.

3.Technical Summary

The **SKYREK Information Security Risk Assessment Report** evaluates critical digital assets using the OCTAVE Allegro framework. The report identifies vulnerabilities across web applications, cloud infrastructure, business email, BYOD devices, WhatsApp Business accounts, and employee data systems. Key risks include protocol downgrade attacks, cross-site scripting (XSS), business email compromise due to lack of SPF/DKIM/DMARC, and unauthorized access to cloud storage and communications platforms. The assessment reveals gaps in secure coding practices, patch management, and incident response readiness.

To mitigate these threats, the report recommends implementing secure protocols (HTTPS, HSTS), strong access controls, multi-factor authentication, regular vulnerability assessments, and employee security training. It also emphasizes enforcing mobile device management (MDM) for BYOD security, securing employee records, and strengthening cloud IAM policies. Overall, the report offers a structured roadmap for enhancing SKYREK's cybersecurity posture and ensuring the confidentiality, integrity, and availability of its critical systems and data.

4.References

References

[1] "MDN Web docs," 2 6 2025. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security.

[2] R. A. Caralli, "SEI Digital library," 1 6 2007. [Online]. Available: https://insights.sei.cmu.edu/library/introducing-octave-allegro-improving-the-information-security-risk-assessment-process/.

[3] M. Palankar, A. Iamnitchi, M. Ripeanu and S. Garfinkel, "Amazon S3 for Science Grids: a Viable Solution?," NPS scholorship, Boston, 2006/06.

[4] S. S. S. a. J. A. Ginige, "A Framework to Enhance Email based Business Processes," Colombo, 2008.

5.Appendix

5.1.Allegro worksheets for critical assets.

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Minimal negative feedback. Easily addressed without formal action.	Notable customer dissatisfaction Requires public communication or PR efforts	Significant damage leading to loss of client trust and potential business decline
Customer Loss	Less than 5% reduction in customers due to loss of confidence	5%-15% reduction in customers due to loss of confidence	More than 15% reduction in customers due to loss of confidence

Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than 5% of annual operating costs	Increase between 5– 15% of annual operating costs	Increase exceeding 15% of annual operating costs
Revenue Loss	Less than 5% annual revenue loss	5% to 15% annual revenue loss	Greater than 15% annual revenue loss
One-Time Financial Loss	One-time financial cost of less than LKR 50,000	One-time financial cost of LKR 50,000 to LKR 150,000	One-time financial cost is greater than LKR 150,000

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than 10% for 1 to 2 day(s).	Staff work hours are increased between 10% and 25% for 3 to 5 day(s).	Staff work hours are increased by greater than 25% for over 5 day(s).

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	**Low**	**Moderate**	**High**
Life	No threat to life	No threat to life	No threat to life
Health	No Health concerns	Noticeable stress and discomfort	Might lead to long term health issues
Safety	No safety concerns	Measurable safety impact on staff well-being	Critical safety violations leading to potential legal issues

Allegro Worksheet 5	RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES		
Impact Area	**Low**	**Moderate**	**High**
Fines	Less than LKR 50,000.	Between LKR 50,000 – 150,000	Greater than LKR 300,000
Lawsuits	Minor legal issues resolved without court action	Formal legal actions involving significant costs	Major lawsuits leading to substantial financial and reputational damage
Investigations	No regulatory attention	Low profile investigations by authorities	High profile investigations with potential for severe penalties

Allegro Worksheet 6	RISK MEASUREMENT CRITERIA – THIRD-PARTY DEPENDECY RISK		
Impact Area	**Low**	**Moderate**	**High**
Service Dependency	Minor delays from AWS services.	Temporary unavailability of AWS services requiring quick response	Long-term failure of critical AWS services halting operations
Control & Recovery	Easy switch to backup services	Moderate loss of control requiring workarounds	No fallback exists for critical operations tied to AWS services

Allegro Worksheet 7		IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	WEIGHT	IMPACT AREAS
1	**10**	**Reputation and Customer Confidence**
2	**8**	**Financial**
3	**6**	**Third-Party Dependency Risk**
4	**4**	**Fines and Legal Penalties**
5	**2**	**Productivity**
6	**1**	**Safety and Health**

1)**Asset- Cloud Platform**

- **Unauthorized access**

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?*
Cloud platform (AWS AMAZON S3)	AWS S3 stores critical organizational data and supports essential services such as backups, application hosting, and data analytics. Its high availability, scalability, and global access make it vital for business continuity, operational efficiency, and secure data management.	AWS provides a **secure and reliable infrastructure**, it is essential to understand **shared responsibility** and potential risks that arise from improper configurations, human error, or security lapses.
(4) Owner(s) *Who owns this information asset?*		
Co-founder		
Security Requirements		
❑ **Confidentiality**	Only authorized Skyrek personnel can view or access sensitive data on AWS. This includes sensitive customer information handled during custom software development. Access is enforced through strict IAM policies	
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	
❑ **Availability**	This asset must be available to authorized personnel to perform their job functions, with defined uptime requirements based on business needs	
	This asset must be available for 24 hours, 7days/week, 52 weeks/year.	
(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	Cloud platform (AWS AMAZON S3)		
	Area of Concern	*Unauthorized access*		
	(1) Actor *Who would exploit the area of concern or threat?*	Malicious external attackers or third-party contractors		
	(2) Means *How would the actor do it? What would they do?*	Exploiting misconfigured IAM roles/policies, using stolen credentials, or leveraging excessive permissions to gain access to sensitive data		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Breach of confidentiality		
	(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, loss of customer trust, potential legal penalties (GDPR/HIPAA), financial losses, and operational disruption	Reputation & Customer Confidence	9	4.5
	Financial	8	4
	Productivity	2	1
	Safety & Health	0	0
	Fines & Legal Penalties	4	2

		Third-Party Dependency Risk	6	3
			Relative Risk Score	**15.5**

(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?*
AWS S3 buckets and IAM (Identity and Access Management) configurations	**Administrative:** - Regularly review and update IAM roles and permissions. - Enforce least privilege principle for all users and services.
	Technical: - Enable Multi-Factor Authentication (MFA) for all privileged accounts. - Use AWS CloudTrail and Config for real-time monitoring and alerting on changes.
	Physical: - (Not directly applicable for cloud, but ensure secure management of physical devices used for access.)
	Residual Risk: - Some risk from zero-day vulnerabilities, sophisticated attacks, or human error may remain, but is minimized through regular reviews, monitoring, and best practices.

- **Publicly Accessible resources**

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**		
Information Asset Risk / Threat	Information Asset	Cloud platform (AWS AMAZON S3)	
	Area of Concern	*Publicly accessible resources*	
	(1) Actor *Who would exploit the area of concern or threat?*	• external attackers • Unintentional exposure by staff or third party.	
	(2) Means *How would the actor do it? What would they do?*	• Scanning for and identifying publicly accessible S3 buckets, databases, or other cloud resources using automated tools • Exploiting misconfigured access control lists (ACLs), bucket policies, or IAM roles to access or exfiltrate data • Leveraging open ports or public endpoints to gain unauthorized access	
	(3) Motive *What is the actor's reason for doing it?*	• Deliberate	
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**
	(5) Security Requirements *How would the information asset's security requirements be breached?*	• Breach of **confidentiality**	
	(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 and loss of customer trust	Reputation & Customer Confidence	8	4
		Financial	8	4
	• Financial losses (including extortion, fraud, or loss of business)	Productivity	2	1
		Safety & Health	0	0
	Regulatory penalties	Fines & Legal Penalties	4	2
		Third-Party Dependency Risk	6	3
			Relative Risk Score	**15**

(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?*
AWS S3 Buckets and other AWS cloud resources	- Enforce private-by-default settings for all S3 buckets and cloud resources. - Regularly audit resource permissions and public access using AWS Config, IAM Access Analyzer, and security tools. - Implement automated alerts for any resource that becomes publicly accessible. -.

Asset-WhatsApp Business Account

- **Unauthorized Access**

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?*
WhatsApp business account	WhatsApp Business is a central channel for employee communications.	Contains about all the project updates, and internal coordination. It contains sensitive customer data and project discussions.
(4) Owner(s) *Who owns this information asset?*		
Co-Founder		
Security requirements		
❑ **Confidentiality**	Only authorized employees should have access to WhatsApp Business Accounts and the data within. Customer information, business messages, and shared files must be protected from unauthorized access or disclosure. End-to-end encryption is used, but risks remain if devices are lost, credentials are shared, or backups are not secured	
❑ **Integrity**	Only authorized personnel should be able to send, edit, or delete business messages and files. Controls are needed to prevent unauthorized modification of conversations, customer data, or business records, whether by accident or malicious intent	
❑ **Availability**	WhatsApp Business Accounts must be available to customer service and business teams during business hours to ensure uninterrupted communication with clients and partners. Service outages or account lockouts could disrupt operations and harm	
(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	Information Asset	WhatsApp Business Account		
	Area of Concern	*Unauthorized access to WhatsApp business account.*		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	External attackers		
	(2) Means *How would the actor do it? What would they do?*	Gaining access through stolen credentials, SIM swapping, phishing attacks, device theft, or exploiting weak authentication		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure**	❑ **Destruction**	
		❑ **Modification**	❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Breach of confidentiality: Unauthorized access allows viewing or exfiltration of sensitive customer information, business messages, and files.		
	(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 and loss of customer trust	Reputation & Customer Confidence	4	2
	Financial	3	1.5
• Financial losses (including extortion, fraud, or loss of business)	Productivity	2	1
	Safety & Health	0	0
Regulatory penalties	Fines & Legal Penalties	2	1
	Relative Risk Score		**5.5**

(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?*		
WhatsApp Business Account (and associated devices/applications)	**Administrative Controls:** - Enforce role-based access control: Only authorized staff may access WhatsApp Business accounts and sensitive communications. -		
	.**Technical Controls:** - Enable two-factor authentication (2FA) or two-step verification for all WhatsApp Business accounts Use strong, unique PINs and passwords for account access and regularly update them.		

Asset- Company Web site (SKYREK.COM)

- **Protocol Downgrade**

	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?***
Company Website (SKYREK.COM)	The SKYREK.COM website is the primary digital platform representing SKYREK, a company specializing in customized web solutions, business automation, and IT services. It is essential for client acquisition, service delivery, brand reputation, and business continuity.	**SKYREK.COM is the official company website, providing information about services (web development, mobile apps, software solutions, cybersecurity), showcasing the company's portfolio, and serving as a communication channel for prospects and clients. It also enables clients to go onboarding and acts as the main marketing and informational hub for the organization.**
(4) Owner(s) ***Who owns this information asset?***		
Co-Founder		
(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 (web admins, IT team) can access the website's backend, configuration, and sensitive data (e.g., client inquiries, admin credentials). Public content is visible to all, but administrative functions are restricted.**

Integrity	Only authorized personnel can modify this information asset, as follows:	**Only authorized personnel can modify website content, code, or configurations. Change management procedures must be enforced to prevent unauthorized or accidental alterations. All updates should be tracked and reviewed**
Availability	This asset must be available for these personnel to do their jobs, as follows:	
	The website must be available 24 hours/day, 7 days/week, 52 weeks/year	**As it is critical for business operations and client engagement. Downtime can lead to loss of business and reputational damage**
Other	This asset has special regulatory compliance protection requirements, as follows:	**The website must comply with any relevant data protection regulations if personal data is collected (e.g., GDPR for EU clients**

(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	Company Website (SKYREK.COM)
		Area of Concern	Protocol Downgrade (ex. forced HTTP, insecure communication), Web Vulnerabilities (ex, XSS, IDOR), Website Availability
		(1) Actor *Who would exploit the area of concern or threat?*	External attacker
		(2) Means *How would the actor do it? What would they do?*	• Exploits lack of forced HTTPS or secure protocol enforcement to downgrade user sessions to HTTP • Uses automated tools or manual techniques to intercept, modify, or steal data
		(3) Motive *What is the actor's reason for doing it?*	• To steal sensitive information (credentials, business data) • To disrupt business 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*	• Availability: Website must be accessible 24/7/365 for business continuity

		security requirements be breached?			
		(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	9	2.25
		Financial	6	1.5
		Productivity	3	0.75
		Safety & Health	0	0
		Fines & Legal Penalties	4	1

Relative Risk Score	5.5

- **Cross Site Scripting**

Allegro - Worksheet 10		**Information Asset Risk Worksheet**			
Information Asset Risk	**Threat**	Information Asset	Company Website (SKYREK.COM)		
		Area of Concern	*Cross-Site Scripting (XSS) via file upload and input fields*		
		(1) Actor *Who would exploit the area of concern or threat?*	External attacker		
		(2) Means *How would the actor do it? What would they do?*	• Submits malicious scripts through file uploads or input fields due to lack of input validation and sanitization • Exploits absence of Content Security Policy (CSP) headers and weak backend validation • Uses automated tools or manual testing to identify and exploit XSS vulnerabilities		
		(3) Motive *What is the actor's reason for doing it?*	• Deliberate		
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	• **Confidentiality:** Prevent unauthorized access to user data and credentials • **Availability:** Maintain uninterrupted access to the website and its services		
		(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	8	2
		Financial	7	1.75
		Productivity	5	1.25
		Safety & Health	1	1.75
		Fines & Legal Penalties	6	1.5
Relative Risk Score				**8.25**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
	Enforce strict input validation and output encoding on all user-supplied data		
	Implement file type validation and sanitization for uploads		

	Apply Content Security Policy (CSP) headers
	Regular vulnerability scanning and penetration testing
	Secure coding practices and code reviews
	- Security awareness training for developers and admins - Incident response plan

Asset- Email System

- **Business Email Compromise**

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?*

Email System	The email system is essential for internal and external communication, sharing sensitive business and client information, and supporting daily operations. Compromise could lead to data breaches, phishing, reputational damage, and business disruption.	Email System is a cloud-based platform used by all staff for business correspondence, client communication, and sharing internal documents. It contains confidential project information, invoice details.
(4) Owner(s) *Who owns this information asset?*		
Nipuna Nadeeshan, Co-Founder		
(5) Security Requirements *What are the security requirements for this information asset?*		
Confidentiality	Only authorized personnel can view this information asset, as follows:	Only authorized personnel can access email accounts and content. Access to sensitive emails is restricted based on job roles.
Integrity	Only authorized personnel can modify this information asset, as follows:	Only authorized users can send, receive, or modify emails. Email content and attachments must not be altered by unauthorized parties.
Availability	This asset must be available for these personnel to do their jobs, as follows:	

	The website must be available 24 hours/day, 7 days/week, 52 weeks/year	The email system must be available 24 hours/day, 7 days/week, 52 weeks/year to ensure uninterrupted business operations.
Other	This asset has special regulatory compliance protection requirements, as follows:	The system should comply with anti-phishing and anti-spoofing standards (DMARC, DKIM, SPF); Data Loss Prevention (DLP) controls are required to prevent accidental or malicious data leakage.

(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	Information Asset	Email System (Skyrek)		
	Area of Concern	*Phishing, Email Spoofing, Data Leakage*		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	External attacker		
	(2) Means *How would the actor do it? What would they do?*	• Sends phishing emails to employees to steal credentials or deliver malware • Spoofs legitimate company email due to lack of DMARC, DKIM, SPF • Insider forwards sensitive information to unauthorized recipients due to lack of DLP		
	(3) Motive *What is the actor's reason for doing it?*	• Deliberate •		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **destruction** ❑ **Modification** ❑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	• **Confidentiality: Prevent unauthorized access to email content and attachments** • **Integrity: Ensure emails are not altered or tampered with** • **Availability: Email system must be continuously accessible for business operations**		
	(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	6	4.8

		Financial	2	1.6
		Productivity	1	0.8
		Safety & Health	0	0
		Fines & Legal Penalties	5	4
			Relative Risk Score	**11.2**

(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?*
	- Implement DMARC, DKIM, and SPF to prevent spoofing
	Enable Data Loss Prevention (DLP) policies
	- Regular phishing awareness training for staff
	- Multi-factor authentication (MFA) for all accounts
	- Centralized logging and monitoring of email activity

Asset- Personal Employee Workstation (BYOD)

- **Unverified Applications (Malware)**

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?*
Personal Employee Workstation (BYOD)	BYOD allows employees to work flexibly, increasing productivity and reducing hardware costs for Skyrek. However, these devices access sensitive company data (ex. emails, client info), making them critical to protect against data breaches, loss, or misuse.	The BYOD asset includes employees' personal devices used to access Skyrek's corporate network, applications, and data. These devices store and process sensitive information like customer data, internal communications, and proprietary business information.
(4) Owner(s) *Who owns this information asset?*		
Individual Employees		
(5) Security Requirements *What are the security requirements for this information asset?*		
Confidentiality	Only authorized personnel can view this information asset, as follows:	Employees must use secure authentication (e.g., multi-factor authentication) and encryption to access company data on BYOD devices to prevent unauthorized access. **Devices must have endpoint security software (e.g., antivirus, anti-malware) and company-approved apps to ensure data integrity and prevent**

		unauthorized changes.
Integrity	Only authorized personnel can modify this information asset, as follows:	Devices must have endpoint security software (e.g., antivirus, anti-malware) and company-approved apps to ensure data integrity and prevent unauthorized changes.
Availability	This asset must be available for these personnel to do their jobs, as follows:	
	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:	Compliance with GDPR and CCPA is required since BYOD devices may handle personal data of customers and employees.

(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	Information Asset	Personal workstation (BYOD)		
	Area of Concern	Unverified Applications		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	Hackers(external)		
	(2) Means *How would the actor do it? What would they do?*	Malicious unverified apps installed via phishing or unofficial stores steal data or disrupt devices.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Availability (device downtime); Confidentiality (data leaks)		
	(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**
Data breaches (GDPR/CCPA fines)	Reputation & Customer Confidence	8	4
	Financial	6	3
Productivity loss	Productivity	6	3
	Safety & Health	1	0.5
Reputational damage	Fines & Legal Penalties	6	3
	Relative Risk Score		**13.5**

(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?*
Risk 1: Unverified Applications Container: BYOD Devices	• **Tech:** Encryption, remote wipe, 6-digit PIN/biometrics, geolocation. • **Physical:** Anti-theft accessories, tracking apps.
Risk 2: Loss/Theft of BYOD Device Container: BYOD Devices	• **Tech:** Encryption, remote wipe, PIN/biometrics, geolocation. • **Physical:** Anti-theft accessories, tracking apps.

Asset – Employee Personal Workstation (BYOD)

- **Inconsistent Patching and Updates**

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk / Threat	Information Asset	Employee personal workstations (BYOD)		
	Area of Concern	Inconsistent Patching and Updates		
	(1) Actor *Who would exploit the area of concern or threat?*	External		
	(2) Means *How would the actor do it? What would they do?*	Exploit unpatched OS/apps via malware or remote attacks		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Confidentiality (data leaks); Availability (device downtime)		
	(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**
Data breaches (GDPR/CCPA fines)	Reputation & Customer Confidence	2	1.6
	Financial	7	5.6
Productivity loss	Productivity	6	4.8
	Safety & Health	0	0

	Reputational damage	Fines & Legal Penalties	3	2.4
			Relative Risk Score	**14.4**

(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?*		
Risk: Inconsistent Patching and Updates Container: BYOD devices.	• **Admin:** Mandate updates, monthly reminders, training. • **Tech** MDM enforces updates, blocks non-compliant devices, and EDR for vulnerabilities. .		

Asset- Employee information (on site PC)

- Access or steal Employee personal information

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 information (on site PC)	This pc stores employee information , records and salary information.	This pc stores employee information , records and salary information.
(4) Owner(s) *Who owns this information asset?*		
Co-founder		

(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view employee information.	
❑ **Integrity**	Only authorized personnel can modify the employee details and salary information and salary calculations.	
❑ **Availability**	Not needed to be always available. Enough if it is available for needed times.	

(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	Information Asset	Employee Information (on site pc)	
	Area of Concern	Access or Steal Employee Records or Salary Information	
Threat	(1) Actor *Who would exploit the area of concern or threat?*	malicious insiders	
	(2) Means *How would the actor do it? What would they do?*	Exploit BYOD vulnerabilities (e.g., weak authentication, malware) to access or steal employee records/salary info stored or accessed on the device.	
	(3) Motive *What is the actor's reason for doing it?*	Deliberate	
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**

		(5) Security Requirements *How would the information asset's security requirements be breached?*	Confidentiality (unauthorized access to sensitive data)		
		(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**
Data breach leading to GDPR/CCPA fines	Reputation & Customer Confidence	5	2.5
	Financial	2	1
Reputational damage	Productivity	1	0.5
	Safety & Health	0	0
Employee trust issues, Potential legal action	Fines & Legal Penalties	0	0
		Relative Risk Score	**4**

(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?*
Risk 1: Access or Steal Employee Records or Salary Information via BYOD Vulnerabilities Container: BYOD devices	• **Admin:** Enforce strict access controls (least privilege), train employees on data handling, audit access logs quarterly. • **Tech:** MDM to enforce encryption, MFA for sensitive data, DLP to block unauthorized sharing, containerization for records. accepted