Sri Lanka Institute of Information Technology

Information Security Risk Management

IE3052

GROUP ASSIGNMENT

IT	NAME
IT22284334	Kezothran G
IT22090126	Kowshick S N
IT22257536	Kajan S
IT22122346	Farhan R

Table of Contents

1. Executive Summary

Jungle Kitchen, a growing food manufacturer, needs stronger cybersecurity to protect its digital assets, including customer data, secret recipes, supplier agreements, and employee devices. Currently, the company faces risks like ransomware attacks, weak access controls exposing confidential recipes, inadequate backups leading to data loss, and unsecured devices vulnerable to phishing. To address these issues, we recommend implementing secure automatic backups, stronger login protections, device security software, and employee training. These measures will ensure business continuity, regulatory compliance, and customer trust while keeping Jungle Kitchen's tropical vegan products safe.

2. Purpose

The purpose of this risk assessment is to evaluate the current cybersecurity risks faced by Jungle Kitchen as it moves toward greater digitalization. Using the OCTAVE Allegro framework, we aim to identify critical information assets, assess vulnerabilities related to cloud storage, BYOD devices, and weak security controls, and recommend appropriate mitigation strategies. This assessment will help Jungle Kitchen enhance its cybersecurity posture, protect its sensitive data, ensure business continuity, and support its ongoing growth in a secure and resilient manner.

3. Key Issue and Recommendations

Lack of Access Control and Privilege Management

- Implement Role-Based Access Control (RBAC) ensuring employees access only necessary systems/data for their roles.

Absence of Regular Data Backups and Disaster Recovery Testing

- Establish automated secure backups (cloud and local) and conduct regular disaster recovery simulations.

No Cybersecurity Awareness Training for Employees

- Launch mandatory cybersecurity awareness training sessions focused on phishing, safe device usage, and data handling.

Inadequate Incident Response Preparedness

- Develop and document an Incident Response Plan (IRP), define team roles, and conduct regular breach simulation exercises.

No Network Traffic Monitoring or Activity Logging

- Deploy network monitoring solutions (IDS/IPS systems) to detect malicious activities and abnormal traffic patterns.

Reliance on BYOD Without Strong Security Controls

- Enforce a BYOD policy requiring device encryption, antivirus installation, strong authentication, and patch management.

Limited Control Over Cloud Storage Access

- Configure cloud storage platforms (e.g., Google Drive) with MFA, audit logging, and role-based permission settings to prevent unauthorized access**.**

No Monitoring or Control of External Device Connections

- Restrict and monitor the use of external devices (USB drives) through endpoint protection software and device management policies.

Inconsistent Secure Storage Practices Across Devices

- Standardize secure storage practices across all employee devices, ensuring that sensitive data is encrypted both at rest and in transit.

4. OCTAVE – allegro Framework and Methodology

The OCTAVE Allegro Framework was chosen for this project due to its effectiveness in assessing organizational information security risks without requiring extensive technical infrastructure or external expertise. OCTAVE Allegro emphasizes a risk assessment approach that focuses on information assets, their containers, and the operational context in which they exist, making it particularly suitable for small businesses like Jungle Kitchen.

Reasons for using OCTAVE Allegro:

- **Simplicity:** It is easier to apply for small teams without large cybersecurity departments
- **Asset-focused:** Focuses on protecting critical information rather than only technology infrastructure.
- **Self-directed:** Can be conducted internally by employees with basic cybersecurity awareness.
- **Cost-effective:** Reduces the need for expensive external risk consultants.
- **Customizable:** The process can be tailored to fit the organization's specific operational needs.

5. Appraisal receivers

ROLE	NAME	SIGNIFICANCE	DEPARTMENT
CEO	M.manukulasuriya	Executive	Overall
MANAGER	Ayesha jayamini	Administration	Overall
IT MANAGER	Vidura de silva	Technical	IT Department
ACCOUNTANT	Githmi danuska	Administration	Accounting Department

6. Risk Model

The Risk Assessment Criteria - Quantitative Analysis

RISK = Value of Impact * Probability

To make the computation of the total risk easier, the degree of risk will be evaluated using the previously given formula. This is the conventional method for determining risk.

1. Value of Impact

Impact level	Value (out 0 to 10)	Description
High	7- 10	a major incident capable of significant damage to the company
Medium	4 – 6	an incident resulting in some but not major harm to the company.
Low	1 – 3	An incident with minor influence on the company

2. Probability of Occurrence

Probability level	Value	Description
High	75	An event a high chance to happen
Medium	50	An event that has a medium chance to happen
Low	20	An event that has a low chance of happening (does not happen usually)

3. Risk Calculation

Impact /Probability	High – 1.0	Medium – 0.5	Low – 0.1
High – 0.75	0.75 * 1 = 0.75	0.75 * 0.5 = 0.375	0.75 * 0.1 = 0.075
Medium – 0.5	0.5 * 1 = 0.5	0.5 * 0.5 = 0.25	0.5 * 0.1 = 0.05
Low – 0.2	0.2 * 1 = 0.2	0.2 * 0.5 = 0.1	0.2 * 0.1 = 0.02

4. Quantitative Analysis Parameter

Variable	Description
Exposure Factor (EF)	The evaluated threat scenario's proportion of asset loss varies from 0% to 100%.
Single Loss Expectancy (SLE)	The possible loss or damage that can be predicted because of a single risk is represented by the variable "Asset Value x EF".

Annualized Rate Occurrence (ARO)	The frequency of a danger during a period of one year. How likely is it that the risk scenario will materialize over the course of a year?
Annualized Loss Expectancy (ALE)	The result of ARO and SLE. The risk value indicates the anticipated damage to the asset over a one-year period because of the incident.
Safeguard Cost / Benefit	(ALE before safeguard) – (ALE After Safeguard) – (Annual Cost of Safeguard)

7. Asset Profile / Identification of Critical Assets

Critical Asset	**Description**	**Security Requirements (C.I.A.)**	**Appropriate Value (LKR)**
Customer Database	Personal details of customers (name, address, order history, payment records) stored in Google Drive and accessed via BYOD.	Confidentiality: High Integrity: High Availability: Medium	**LKR 400,000 (As per the company's data)**
Product Recipes and Formulations	Unique vegan recipes and product secrets critical for Jungle Kitchen's brand identity.	Confidentiality: Very High Integrity: High Availability: Low	**LKR 600,000 (As per the company's data)**
Supplier Contracts and Financial Documents	Supplier agreements, pricing documents, and business financial records.	Confidentiality: High Integrity: High Availability: Medium	**LKR 300,000 (As per the company's data)**
Employee Email Accounts	Email accounts used for internal/external communication. Vulnerable to phishing and unauthorized access.	Confidentiality: High Integrity: Medium Availability: High	**LKR 250,000 (As per the company's data)**
Cloud Storage Accounts (Google Drive, OneDrive)	Storage of sensitive business documents, recipes, contracts, HR information.	Confidentiality: High Integrity: High Availability: Very High	**LKR 400,000 (As per the company's data)**
BYOD Devices (Employee Laptops and Phones)	Personal devices used for company work, exposing business data to risks like malware and theft.	Confidentiality: High Integrity: Medium Availability: High	**LKR 200,000 (As per the company's data)**

Payroll and HR Records	Digital records of employee salaries, contracts, and personal data.	Confidentiality: Very High Integrity: High Availability: Medium	**LKR 350,000 (As per the company's data)**
Backup Storage Devices (Portable Hard Drives)	Hard drives used for backup storage of important business data.	Confidentiality: Medium Integrity: High Availability: Medium	**LKR 150,000 (As per the company's data)**

5. Threat Profile and Mitigation Plan

Critical Asset: Customer Database

Field	Details
Threat	Phishing attack or weak password breach of customer data
Actor	Outsider (hacker), Insider (employee mistake)
Motive	Financial fraud, identity theft
Outcome	Disclosure
Impact	High
Probability	Medium

Risk Assessment and Mitigation Summary

Field	Details
Asset Value	LKR 400,000
Exposure Factor (EF)	30%
Single Loss Expectancy (SLE)	LKR 120,000 (400,000 × 30%)
Annualized Rate of Occurrence (ARO)	0.3
Annualized Loss Expectancy (ALE)	LKR 36,000 (120,000 × 0.3)
Mitigation Plan	- Implement Multi-Factor Authentication (MFA) - Strengthen password policies - Provide phishing awareness training
Cost of Mitigation	LKR 20,000
Expected New ALE	LKR 6,000
Risk Benefit	LKR 10,000 saved annually (36,000 – 6,000 – 20,000)

Critical Asset: Product Recipes and Formulations

Field	Details
Threat	Theft of secret recipes via unauthorized access
Actor	Insider (employee)
Motive	Sell secrets, competitive advantage
Outcome	Disclosure
Impact	Very High
Probability	Low

Risk Assessment and Mitigation Summary

Field	Details
Asset Value	LKR 600,000
Exposure Factor (EF)	40%
Single Loss Expectancy (SLE)	LKR 240,000 (600,000 × 40%)
Annualized Rate of Occurrence (ARO)	0.1
Annualized Loss Expectancy (ALE)	LKR 24,000 (240,000 × 0.1)
Mitigation Plan	- Encrypt all recipe files - Restrict access to recipe documents (role-based)
Cost of Mitigation	LKR 25,000
Expected New ALE	LKR 4,000
Risk Benefit	LKR -5,000 (small cost, but brand protection is critical)

Critical Asset: Supplier Contracts and Financial Documents

Field	Details
Threat	Unauthorized access or data leak
Actor	Outsider (attacker), Insider mistake
Motive	Financial fraud
Outcome	Disclosure
Impact	High
Probability	Medium

Risk Assessment and Mitigation Summary for Financial Documents

Field	Details
Asset Value	LKR 300,000
Exposure Factor (EF)	25%
Single Loss Expectancy (SLE)	LKR 75,000 (300,000 × 25%)
Annualized Rate of Occurrence (ARO)	0.3
Annualized Loss Expectancy (ALE)	LKR 22,500 (75,000 × 0.3)
Mitigation Plan	- Use encryption for financial documents - Implement sharing restrictions on cloud storage
Cost of Mitigation	≈ LKR 15,000
Expected New ALE	≈ LKR 5,000
Risk Benefit	LKR 2,500 saved (22,500 – 5,000 – 15,000)

Critical Asset: Employee Email Accounts

Field	Details
Threat	Phishing attacks leading to business email compromise
Actor	Outsider
Motive	Unauthorized access, fraud
Outcome	Disclosure
Impact	High
Probability	High

Risk Assessment and Mitigation Summary for Financial Documents

Field	Details
Critical Asset	Cloud Storage Accounts
Asset Value	LKR 250,000
Exposure Factor (EF)	20%
Single Loss Expectancy (SLE)	LKR 50,000 (250,000 %)
Annualized Rate of Occurrence (ARO)	0.5
Annualized Loss Expectancy (ALE)	LKR 25,000 (50,000 × 0.5)
Mitigation Plan	- Configure SPF, DKIM, DMARC policies - Run quarterly phishing awareness programs
Cost of Mitigation	≈ LKR 20,000
Expected New ALE	≈ LKR 5,000
Risk Benefit	Break even (25,000 – 5,000 – 20,000) but critical protection

Critical Asset: Cloud Storage Accounts

Field	Details
Threat	Unauthorized data access or misconfiguration leak
Actor	Outsider, Insider
Motive	Theft, sabotage
Outcome	Disclosure
Impact	Very High
Probability	Medium

Risk Assessment and Mitigation Summary for Financial Documents

Field	Details
Asset Value	LKR 400,000
Exposure Factor (EF)	30%
Single Loss Expectancy (SLE)	LKR 120,000 (400,000 × 30%)
Annualized Rate of Occurrence (ARO)	0.2
Annualized Loss Expectancy (ALE)	LKR 24,000 (120,000 × 0.2)
Mitigation Plan	- Enable full audit logs - Implement strict folder-level access permissions
Cost of Mitigation	≈ LKR 20,000
Expected New ALE	≈ LKR 4,000
Risk Benefit	LKR 0 (Neutral, but protection is essential)

Critical Asset: BYOD Devices

Field	Details
Threat	Malware infection, data leakage through unsecured personal devices
Actor	Employee negligence or cybercriminals
Motive	Theft, espionage
Outcome	Disclosure, Interruption
Impact	High
Probability	High

Risk Assessment and Mitigation Summary for Financial Documents

Field	Details
Asset Value	LKR 200,000
Exposure Factor (EF)	30%
Single Loss Expectancy (SLE)	LKR 60,000 (200,000 × 30%)
Annualized Rate of Occurrence (ARO)	0.5
Annualized Loss Expectancy (ALE)	LKR 30,000 (60,000 × 0.5)
Mitigation Plan	- Enforce security policies for BYOD (encryption, antivirus) - VPN access for remote work
Cost of Mitigation	≈ LKR 15,000
Expected New ALE	≈ LKR 5,000
Risk Benefit	LKR 10,000 saved (30,000 – 5,000 – 15,000)

Critical Asset: Payroll and HR Records

Field	Details
Threat	Insider data theft or accidental disclosure
Actor	Insider (employee mistake or malicious)
Motive	Financial fraud, privacy violations
Outcome	Disclosure
Impact	Very High
Probability	Medium

Risk Assessment and Mitigation Summary for Financial Documents

Field	Details
Asset Value	LKR 350,000
Exposure Factor (EF)	35%
Single Loss Expectancy (SLE)	LKR 122,500 (350,000 × 35%)
Annualized Rate of Occurrence (ARO)	0.2
Annualized Loss Expectancy (ALE)	LKR 24,500 (122,500 × 0.2)
Mitigation Plan	- Store payroll files with encryption - Restrict access to HR manager only
Cost of Mitigation	≈ LKR 20,000
Expected New ALE	≈ LKR 4,000
Risk Benefit	LKR 500 saved (24,500 – 4,000 – 20,000)

Critical Asset: Backup Storage Devices

Field	Details
Threat	Theft or loss of backup drives
Actor	Outsider
Motive	Data theft
Outcome	Disclosure, loss
Impact	Medium
Probability	Low

Risk Assessment and Mitigation Summary for Audit and Access Controls

Field	Details
Asset Value	LKR 150,000
Exposure Factor (EF)	30%
Single Loss Expectancy (SLE)	LKR 45,000 (150,000 × 30%)
Annualized Rate of Occurrence (ARO)	0.1
Annualized Loss Expectancy (ALE)	LKR 4,500 (45,000 × 0.1)
Mitigation Plan	- Encrypt backup hard drives - Physically secure backup devices
Cost of Mitigation	≈ LKR 10,000
Expected New ALE	≈ LKR 1,000
Risk Benefit	Small loss, but huge data safety (4,500 – 1,000 – 10,000)

Summary

Using the OCTAVE Allegro framework, this report offers a thorough information security risk assessment for Jungle Kitchen. The Customer Database, Product Recipes, Supplier Contracts, Employee Email Accounts, Cloud Storage, BYOD Devices, Payroll and HR Records, and Backup Storage Devices are among the important information assets that are evaluated.

Major security threats were identified by the assessment, including insider data leaks, phishing attacks, cloud storage unauthorized access, inadequate BYOD security controls, and a lack of formal incident response protocols. A quantitative understanding of the possible financial impact was ensured by performing risk calculations using Single Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO), Exposure Factor (EF), and Annualized Loss Expectancy (ALE).

For every critical asset, a mitigation plan was created that included cost-effective tactics such as requiring multi-factor authentication, putting in place strict access control guidelines, safeguarding data storage, educating people about cybersecurity, and securing endpoints and networks with the right technical solutions.