MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

OCTOBER 2024 SEMESTER

IKB31503 INFORMATION SECURITY MANAGEMENT SYSTEMS

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AUDIT REPORT FOR OPERATIONS DEPARTMENT OF BRAHIM'S FOOD SERVICES SDN BHD (BFS)

(Academic Case Study)

PREPARED BY:

Nurin Nabeeha binti Azahari

(Team-based Academic Audit Project)

This document is a curated academic audit excerpt prepared for portfolio demonstration purposes. Sensitive operational details have been generalized.

Table of Contents

1.0 BACKGROUND OF THE COMPANY

Brahim's Food Services Sdn Bhd (BFS) is Malaysia’s top in-flight catering service provider and a major player in the global halal food services business. Formerly known as Brahims SATS Sdn Bhd (BSFS), the company is part of the Malaysian aviation industry and specializes in delivering halal-certified in-flight meals to airlines. With a decades-long history, BFS has gained a reputation for operational quality, innovation, and strict adherence to halal food preparation guidelines.

BFS runs the world’s largest halal-certified flight kitchen, preparing large volumes of meals daily for multiple international airline partners. The company operates 24 hours a day and seven days a week, using modern technology and a devoted staff to ensure constant quality and compliance with strict regulatory and safety standards.

BFS's flight kitchen is divided into three main departments: Production, Operations, and Equipment Services. The Operations Departments of BFS is a critical component of its business structure. It consists of several units, including Administration, Management Information, Operations Command Centre, Duty Room, Frontline Operations, Assembly and Cold Room Management, Duty Runner and Last-Minute Centre, Walkie Talkie and Hi Lift Key Management, and Newspaper and Magazine. This department is in charge of managing daily operational workflows, ensuring consistent service delivery, and maintaining equipment required to support aviation-related activities.

Given the critical importance of data accuracy, equipment security, and operational efficiency, BFS prioritizes the protection of sensitive information, physical assets, and procedures. To maintain its service excellence standards, the department uses a variety of technical tools, including biometric access control, GPS equipment tracking, and inventory management systems.

This Information Security Management System (ISMS) audit focuses on the Operations Department’s information security practices and compliance with ISO/IEC 27001 standards. The audit’s goal is to evaluate security controls, assess risks, and provide structured recommendations for improvement. BFS intends to maintain its commitment to safe, efficient, and secure operations by implementing proactive measures and strong ISMS frameworks, assuring the satisfaction of its airline partners and stakeholders.

2.0 SCOPE AND OBJECTIVE

2.1 Scope of the ISMS Audit

The scope of this Information Security Management System (ISMS) audit is focused on the Operations Department of Brahim's Food Services Sdn Bhd (BFS), a critical component of its business operations. This department oversees the coordination of daily workflows, equipment management, and service delivery, ensuring compliance with strict operational and regulatory standards.

The audit will evaluate processes, policies, and controls across the following units and areas of concern:

Units Involved

- Administration Unit
- Management Information Unit
- Operations Command Centre Unit
- Duty Room Unit
- Frontline Operations Unit
- Assembly and Cold Room Management Unit
- Duty Runner and Last-Minute Centre Unit
- Walkie Talkie and Hi Lift Key Management Unit
- Newspaper and Magazine Unit

Areas of Focus

1. **Physical Security**
    - Review physical access controls to sensitive areas (e.g., admin offices, secure storage areas) to ensure that only authorized personnel have access.

2. **Access Control:**
    - Assess mechanisms for controlling and verifying access to sensitive data, equipment, and operational areas, including badges, PINs, and biometric systems.

3. **Information Security:**
    - Evaluate how sensitive operational information (e.g., flight schedules, passenger load, and catering details) is stored, processed, and transmitted,

with a focus on encryption, secure communication channels, and access restrictions.

4. **Equipment Management:**
    - Review the tracking and management of critical equipment such as walkie-talkies and Hi Lift keys to prevent misuse or loss.

5. **Visitor Management:**
    - Assess procedures for managing visitors, ensuring they are properly supervised and restricted from accessing sensitive areas unless authorized.

6. **Incident and Emergency Preparedness:**
    - Evaluate protocols for handling security incidents, breaches, and emergency situations, ensuring staff are trained and aware of the procedures.

Exclusions

- Technical penetration testing and system-level vulnerability assessments were not conducted, as the audit was limited to procedural, administrative, and physical security controls within the defined academic scope.

2.2 Objective of the ISMS Audit

The key objectives of this ISMS audit are as follows:

1. **Assess Current Security Practices:**
    - Evaluate the current physical, administrative, and technical security controls in place, ensuring they align with Information Security Management System (ISMS) standards, particularly ISO/IEC 27001.

2. **Identify Security Risks and Vulnerabilities:**
    - Identify potential vulnerabilities, weaknesses, or non-compliance issues in the department's processes and security measures, focusing on sensitive information, access controls, and equipment management.

3. **Enhance Operational Security:**
    - Provide actionable recommendations for improving security controls to reduce the risks of unauthorized access, data breaches, and security incidents affecting department operations.

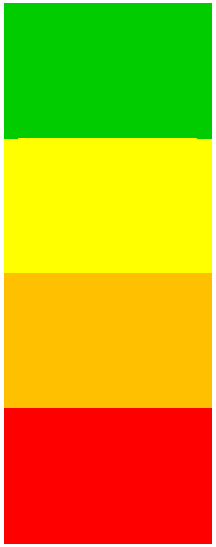
4. **Ensure Compliance:**
    - Verify the department's adherence to internal security policies, procedures, and relevant industry regulations to maintain compliance with corporate and regulatory standards.

5. **Increase Security Awareness:**
    - Raise awareness among personnel regarding best practices in security, emphasizing the importance of protecting sensitive areas, data, and equipment

Risk Level = Likelihood value x Consequences / Impact value

5	LOW	MED	HIGH	EXT	EXT
4	LOW	MED	HIGH	HIGH	EXT
3	LOW	MED	MED	HIGH	HIGH
2	LOW	LOW	MED	MED	MED
1	LOW	LOW	LOW	LOW	LOW
LIKELIHOOD	1	2	3	4	5
CONSEQUENCE					

L X C	
Score 0 – 5	= Low
Score 6 – 10	= Medium
Score 12 – 16	= High
Score 20 – 25	= Extreme



If Risk = Green = Low Risk = Accept

If Risk = Yellow = Medium Risk = Accept or Treat

If Risk = Orange = High Risk = Treat

If Risk = Red = Extreme Risk = Treat

Likelihood description:

Likelihood	Rating	Criteria
Almost certain	5	The threat is very likely to occur based on current vulnerabilities. This threat is expected to happen frequently or with high probability.
Likely	4	The threat has a high probability of occurring, and the vulnerabilities present make it probable that the threat will exploit these weaknesses.
Possible	3	The threat is not highly probable, but there is a reasonable chance that it could occur, particularly if certain conditions align.
Unlikely	2	The threat is unlikely to occur based on existing controls, but it is still possible under certain circumstances.
Almost certain not to happen	1	The threat is highly unlikely, and current controls are robust enough to make this occurrence very rare or improbable.

Impact description:

Consequence	Rating	Criteria / Examples
Catastrophic	5	The consequence of the threat materializing would result in severe damage, including major financial loss, irreparable damage to the organization’s reputation, or legal/regulatory consequences.
Major	4	Significant damage would occur, potentially affecting operations or causing substantial financial loss. Recovery would be time-consuming and costly, and the organization's reputation may suffer.
Moderate	3	The impact would be noticeable but manageable. While operations may be affected, the damage is controllable and would not result in significant long-term consequences.
Minor	2	The threat would cause minimal disruption, with manageable financial impact and little to no long-term effect. The organization can recover quickly with little resource expenditure.
Insignificant	1	The impact of the threat would be negligible, with no meaningful effect on operations or finances. The issue can be resolved swiftly at the department level.

9.0 CONCLUSIONS

The Information Security Management System (ISMS) audit of the Operations Department demonstrates that foundational security controls are in place to support operational continuity and regulatory compliance. The department shows structured implementation of access controls, physical security safeguards, and defined operational procedures.

However, opportunities for improvement were identified to further strengthen the organization's security posture. Areas recommended for enhancement include strengthening authentication mechanisms, improving monitoring and tracking controls, modernizing encryption practices, and refining incident response procedures to align with evolving security standards.

Additionally, increased automation in visitor and equipment management processes could further reduce human error and improve traceability. Continuous staff awareness training and periodic policy reviews were also recommended to ensure long-term alignment with ISO/IEC 27001 best practices.

Overall, the audit findings suggest that while existing controls provide a reasonable level of protection, proactive enhancements will further improve resilience against emerging operational and cybersecurity risks. By implementing structured improvements, the department can enhance governance, risk mitigation capability, and long-term information security maturity.

By addressing these vulnerabilities and continuously improving its security infrastructure, the Operations Department can significantly enhance its resilience against evolving threats and safeguard its operations, assets, and sensitive information.