Risk management Plan and SOA

The Risk management Plan identifies specific actions and controls needed to mitigate the risks outlined in the risk assessment.

The Statement of Applicability (SOA) then documents which of these controls are implemented, partially implemented, or not yet implemented, and provides details on their objectives, applicability, and status.

Together, they ensure that risk management efforts are systematically applied, monitored, and aligned with organizational policies and ISO 27001 standards.

Risk management plan

1 . Purpose, Scope, and Users

Purpose: To identify, assess, and manage risks associated with DHAEI’s IT systems and operations, ensuring that potential threats are mitigated and organizational objectives are met.

Scope: Includes all critical IT assets, including servers, network infrastructure, and remote work setups, across the main and branch offices.

Users: The plan will be used by DHAEI's IT and security teams, including the CIO, IT managers, and security personnel, to guide risk management efforts and ensure compliance with security policies.

2 . Risk Assessment and Risk Treatment Methodology

2.1 Risk Assessment

The Process:

- List all critical assets and their functions.
- Determine weaknesses and potential threats to the assets.
- Evaluate the likelihood and impact of each threat on the assets.
- Assign responsibilities for managing each risk.
- Create a risk assessment table and risk treatment plan.

Individuals or Groups to Involve:

- IT Security Manager: To provide insights into technical vulnerabilities and security controls.
- Operations Manager: To assess operational impacts and resource requirements.
- CIO: For strategic oversight and alignment with organizational objectives.

Assets, Vulnerabilities, and Threats:

Two Main Threats:

- Data Breaches: Unauthorized access to sensitive information.
- Physical Theft: Theft of equipment or servers.

Challenges:

- Rapid Evolution of Threats: Keeping up-to-date with emerging threats.
- Resource Constraints: Limited budget and personnel for implementing security measures.
- Integration of New Systems: Ensuring new systems are secure and compliant.

Determining Risk Owners:

Risk 1: Data Breaches

- IT Security Manager: Manages data protection and access controls.
- Compliance Officer: Ensures adherence to data protection regulations.
- CIO: Oversees overall data security strategy.

Risk 2: Physical Theft

- Facilities Manager: Implements physical security measures.
- IT Security Manager: Ensures equipment is securely stored.
- CIO: Reviews physical security policies and resource allocation.

Impact and Likelihood Table

Threat/Risk	Impact (0-10)	Likelihood (0-5)	Effect on C/I/A
Data Breaches	8	3	Confidentiality, Integrity
Physical Theft	6	2	Availability, Confidentiality

2.2 Risk Treatment

Summary of Threats:

- Data Breaches: Moderate impact; affects confidentiality and integrity.
- Physical Theft: Lower likelihood; impacts availability and confidentiality.

Recommended Mitigations:

1 . Data Breaches:

- Mitigations: Enhance data encryption, enforce strict access controls, and conduct regular security training.
- Priority: Medium, as it’s critical but less frequent.

- References: ISO 27001 controls, NIST SP 800-53.
    - According to isms.online, "Data leakage is a frequent issue for organisations that manage large amounts of data, ranging from different classifications, on multiple distinct and interconnected IT systems, applications and file servers. ISO 27001:2022 Annex A 8.12 pertains to ICT operations which are conducted with system administrator access, and come under the umbrella of network management and maintenance."

2 . Physical Theft:

- Mitigations: Strengthen physical security measures, use asset tracking systems, and implement secure storage practices.
- Priority: Low, given the lower likelihood but still important.
- References: ISO 27001 Annex A controls, physical security standards.
    - According to isms.oneline, "ISO 27001:2022 Annex A 7.1 guarantees an organisation can show it has suitable physical security boundaries in place to stop unauthorised physical access to information and other related assets."

Statement of Applicability (SOA)

1 . Control Objectives and Controls

For each control, we will have a control object and specific measures outlined.

A . Access Control

Control Objective: Protect information by managing access.

- Control : A.9.1.1: Access Control Policy
    - Measures: Establish and enforce policies for user access management.
- Control : A.9.2.3 Management of Privileged Access Rights
    - Measures: Implement procedures for use of privledged access.
- Control : A.9.4.1: Information Access Restriction
    - Measures: Restrict information access based on roles and responsibilities.

Reference for access controls : https://www.isms.online/iso-27001/annex-a-9-access-control/

B . Cryptography

Control Objective: Protect data confidentiality and integrity through encryption.

- Control : A.10.1.1: Cryptographic Controls
    - Measures: Use encryption for data at rest and in transit.
- Control : A.10.1.2: Key Management

    - Measures: Manage encryption keys securely.

References : https://www.isms.online/iso-27001/annex-a-10-cryptography/

C . Physical and Environmental Security

Control Objective: Protect physical assets and infrastructure from threats.

- Control : A.11.1.1: Physical Security Perimeter
    - Measures: Implement physical security measures for office and branch locations.
- Control : A.11.2.1 Equipment Siting & Protection
    - Measures: Secure equipment with access controls and surveillance.

References : https://www.isms.online/iso-27001/annex-a-11-physical-and-environmental-security/

D . Operations Security

Control Objective: Ensure secure and effective operation of IT systems.

- Control : A.12.2.1 Controls Against Malware
    - Measures: Implement malware controls and user awareness beyond just anti-virus software.
- Control : A.12.4.1: Event Logging
    - Measures: Monitor and log events for security purposes.

References : https://www.isms.online/iso-27001/annex-a-12-operations-security/

E . Communications Security

Control Objective: Secure internal and external communications.

- Control : A.13.1.1: Network Controls
    - Measures: Manage and control networks to protect information based on business needs.
- Control : A.13.2.1: Information Transfer Policies and Procedures
    - Measures: Establish secure procedures for data transfer.

References : https://www.isms.online/iso-27001/annex-a-13-communications-security/

F . Compliance

Control Objective: Ensure adherence to legal and regulatory requirements.

- Control : A.18.1.1: Identification of Applicable Legislation and Contractual Requirements
    - Measures: Comply with legal and contractual obligations.
- Control : A.18.2.1 Independent Review of Information Security

    - Measures: Conduct regular security reviews and audits.

References : https://www.isms.online/iso-27001/annex-a-18-compliance/

2 . Applicability

List of ISO 27001 controls relevant to DHAEI based on the risk assessment and organizational needs.

- Access Control: Necessary due to critical role in managing user access and authentication.
- Cryptography: Essential for protecting data confidentiality and integrity.
- Physical and Environmental Security: Needed to protect physical assets and infrastructure.
- Operations Security: Required to maintain secure and effective operation of IT systems.
- Communications Security: Important for securing data communications.
- Compliance: Ensures adherence to regulatory requirements and internal policies.

3 . Responsibility

IT Security Manager:

- Responsible for implementing and maintaining access control and cryptographic measures.

Operations Manager:

- Oversees operations security and monitoring.

Facilities Manager:

- Ensures physical security and equipment protection.

Compliance Officer:

- Manages compliance with legal and regulatory requirements.

4 . Monitoring and Review

Monitoring Procedures:

- Access Control:
    - Regular audits and access reviews.
- Cryptographic Controls:
    - Key management audits and encryption validation.
- Physical Security:
    - Surveillance and access logs.
- Operations Security:

    - Event logs and patch management reviews.
- Communications Security:
    - Network traffic analysis and VPN security reviews.
- Compliance: Periodic
    - compliance audits and policy reviews.

Review Frequency:

- Monthly:
    - Access control audits
    - Patch management reviews
    - Network security assessments
- Quarterly:
    - Cryptographic controls review
    - Event logging analysis
    - Physical security inspections
- Annually:
    - Compliance reviews
    - Overall information security assessments

References

1. ISO 27001:2022 annex A 8.12 – data leakage prevention. ISMS.online. (n.d.-b). https://www.isms.online/iso-27001/annex-a/8-12-data-leakage-prevention-2022/#what-is-annex-a-8-12
2. ISO 27001:2022 annex A 7.1 – physical security perimeters. ISMS.online. (n.d.). https://www.isms.online/iso-27001/annex-a/7-1-physical-security-perimeters-2022/