Risk Management Case Study

Prepared by: Anastasiya Gruneva
Date: January 14th, 2025

Table of Contents

Executive Summary 3
Risk Management Plan 5
Purpose, Scope, and Users 5
Risk Assessment and Risk Treatment Methodology 5
Risk Assessment 5
Risk Treatment 10
References 13

Executive Summary

Overview
This Risk Management Plan outlines DHA Enterprise Inc.'s (DHAEI) approach to identifying, assessing, and mitigating information security risks within its Information Security Management System (ISMS). Adhering to ISO 27001 standards, the plan ensures the confidentiality, integrity, and availability of sensitive information while addressing the dynamic challenges of a distributed work environment.

The analysis highlights key risks, prioritizes threats, and outlines actionable recommendations to safeguard DHAEI's operations, reputation, and compliance standing.

Risk Assessment and Identification
The risk assessment process involves identifying critical assets, vulnerabilities, and potential threats to DHAEI's information systems. These include centralized servers, network infrastructure, and endpoints, as well as human factors such as employee roles. The key risks identified are:

1. **Unauthorized Access**: A high-likelihood threat that jeopardizes data confidentiality and integrity, potentially compromising sensitive information or critical systems.
2. **Data Breaches**: While encryption measures reduce likelihood, this remains a significant risk to confidentiality due to the potential for reputational and financial losses.
3. **System Downtime**: Redundancy measures mitigate likelihood, but failures could impact service availability and productivity.

Each risk was assessed for its potential impact and likelihood, resulting in a priority ranking that supports effective resource allocation.

Recommendations for Risk Treatment
To address the identified risks, a tiered approach to mitigation is proposed, emphasizing alignment with best practices and industry standards.

1. **Mitigating Unauthorized Access (High Priority)**
   - Enforce **Multi-Factor Authentication (MFA)** across VPNs and critical systems.
   - Conduct **regular penetration testing** to identify vulnerabilities proactively.
   - Implement **network segmentation** to restrict access based on user roles.
2. **Reducing Data Breach Risks (Medium Priority)**
   - Apply **AES-256 encryption** to data at rest and in transit.

    - Deploy **endpoint protection solutions** to secure devices against unauthorized access.
    - Perform **data access audits** to monitor usage patterns and detect anomalies.
3. **Minimizing System Downtime (Low Priority)**
    - Establish **load balancing and clustering** for continuous service availability.
    - Implement **hardware health monitoring tools** to preemptively address failures.
    - Maintain a robust **backup and recovery plan** to ensure quick restoration of services.

Conclusion

This Risk Management Plan provides DHAEI with a structured approach to addressing its most pressing risks. By prioritizing resources to mitigate unauthorized access, enhancing encryption protocols, and ensuring operational redundancy, DHAEI can achieve a significant reduction in its overall risk exposure.

The recommendations align with DHAEI’s organizational objectives and commitment to security, ensuring operational continuity and maintaining client trust while meeting regulatory requirements. Implementing this plan will position DHAEI as a secure and resilient organization in the evolving digital landscape.

Risk Management Plan

Purpose, Scope, and Users

The purpose of this document is to define the methodology for assessment and treatment of information risks in DHA Enterprise Inc. (DHAEI), and to define the acceptable level of risk according to the ISO 27001 standard.

Risk Assessment and Risk Treatment are applied to the entire scope of the Information Security Management System (ISMS) (i.e., to all assets which are used within the organization or which could have an impact on information security within the ISMS), which includes includes the main office, branch offices, remote workers, and the planned Brampton branch office.

Users of this document are all employees of DHAEI, who take part in Risk Assessment and Risk Treatment.

Risk Assessment and Risk Treatment Methodology

Risk Assessment

The process

Risk Assessment is implemented through the Risk Assessment Table.

The risk assessment process involves (Secureframe's Guide on ISO 27001 Risk Assessment, retrieved 2025-01-14):

1. Identifying assets, vulnerabilities, and threats.
2. Evaluating the impact and likelihood of threats exploiting vulnerabilities.
3. Determining risk ownership and establishing a chain of command.

Involved Parties:

- Top Management: Responsible for approving the plan, providing resources, and ensuring alignment with organizational objectives - founder and CEO, Alan Hake, CIO, Amanda Wilson.
- Risk Owners: Individuals accountable for managing specific risks - Paul Alexander, Chief Information Security Officer (CISO).
- IT and Security Teams: Carry out technical controls and monitor risk mitigation measures - security personnel, IT staff, and branch office support technicians.

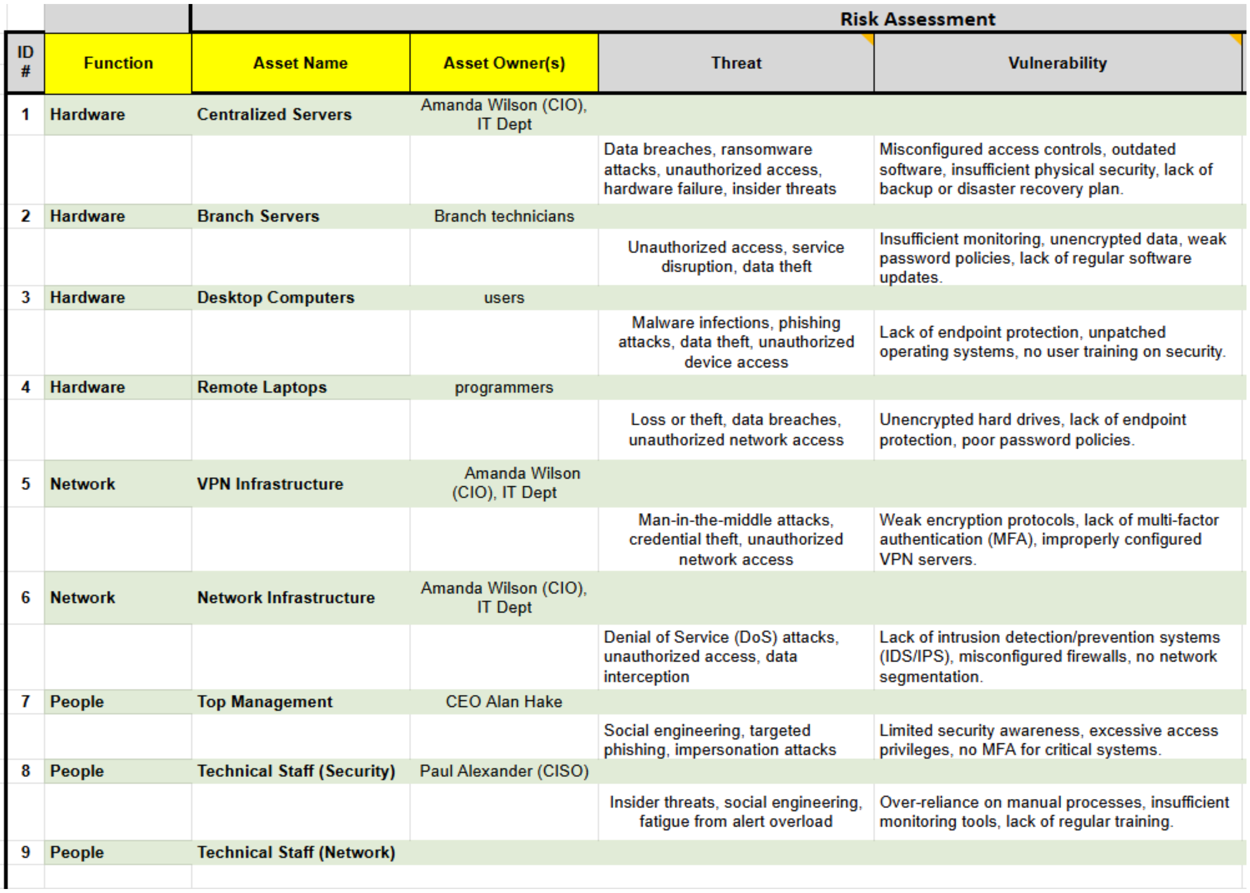
Assets, vulnerabilities, and threats

The first step in Risk Assessment is the identification of all assets in the ISMS scope (i.e., of all assets which may affect the confidentiality, integrity, and availability of information at DHAEI).

Key Assets:

- Centralized servers (DC1, DC2, FSI, WSUSI, DHADNS).
- Branch servers (DHADNS).
- Desktop computers and remote laptops for programmers.
- VPN and network infrastructure.
- Employees (Top management, Technical staff - security, network, programmers, General staff)

The next step is to identify all threats and vulnerabilities associated with each asset. Every asset may be associated with several threats, and every threat may be associated with several vulnerabilities (Kosutic, retrieved 2025-01-14).



		Risk Assessment			
ID #	Function	Asset Name	Asset Owner(s)	Threat	Vulnerability
1	Hardware	Centralized Servers	Amanda Wilson (CIO), IT Dept		
				Data breaches, ransomware attacks, unauthorized access, hardware failure, insider threats	Misconfigured access controls, outdated software, insufficient physical security, lack of backup or disaster recovery plan.
2	Hardware	Branch Servers	Branch technicians		
				Unauthorized access, service disruption, data theft	Insufficient monitoring, unencrypted data, weak password policies, lack of regular software updates.
3	Hardware	Desktop Computers	users		
				Malware infections, phishing attacks, data theft, unauthorized device access	Lack of endpoint protection, unpatched operating systems, no user training on security.
4	Hardware	Remote Laptops	programmers		
				Loss or theft, data breaches, unauthorized network access	Unencrypted hard drives, lack of endpoint protection, poor password policies.
5	Network	VPN Infrastructure	Amanda Wilson (CIO), IT Dept		
				Man-in-the-middle attacks, credential theft, unauthorized network access	Weak encryption protocols, lack of multi-factor authentication (MFA), improperly configured VPN servers.
6	Network	Network Infrastructure	Amanda Wilson (CIO), IT Dept		
				Denial of Service (DoS) attacks, unauthorized access, data interception	Lack of intrusion detection/prevention systems (IDS/IPS), misconfigured firewalls, no network segmentation.
7	People	Top Management	CEO Alan Hake		
				Social engineering, targeted phishing, impersonation attacks	Limited security awareness, excessive access privileges, no MFA for critical systems.
8	People	Technical Staff (Security)	Paul Alexander (CISO)		
				Insider threats, social engineering, fatigue from alert overload	Over-reliance on manual processes, insufficient monitoring tools, lack of regular training.
9	People	Technical Staff (Network)			

Figure 1. Example of Risk Assessment Table for DHEI.

Top Threats and Challenges for DHAEI:

1. **Unauthorized Access:** Vulnerabilities in VPNs or RODCs could allow unauthorized access.

   Challenge: Ensuring strong authentication without affecting user productivity.

2. **Data Breaches:** Risk of sensitive data being compromised from stolen file servers or drives.

   Challenge: Implementing encryption effectively across all devices.

3. **System Downtime:** Potential hardware failures leading to service interruptions.

   Challenge: Ensuring redundancy and quick recovery.

Determining the risk owners

For each risk, the chain of ownership is as follows (Kosutic, 2022):

1. Ground Level: Security Technicians – Monitor and report incidents. Security technicians have direct access to systems and tools for monitoring and incident reporting. Their expertise is critical for identifying threats and vulnerabilities in real-time.
2. Mid-Level: CISO – Develop and enforce risk management policies. The CISO role is designed to translate technical risks into business terms, enforce policies, and prioritize risk treatments that align with organizational goals.
3. Executive Level: CIO – Allocate resources and approve mitigation strategies. The CIO is responsible for aligning cybersecurity with the organization's overall strategy, ensuring adequate funding and approval of initiatives that address identified risks.

Impact and likelihood

Once risk owners have been identified, it is necessary to assess impacts for each combination of threats and vulnerabilities for an individual asset if such a risk materializes. After the assessment of consequences, it is necessary to assess the likelihood of occurrence of such a risk (i.e., the probability that a threat will exploit the vulnerability of the respective asset). By entering the values of consequence and likelihood into the Risk Assessment Table, the level of risk is calculated automatically by adding up the two values.

Threat/Risk	Effect on CIA	Extent (0-10)	Likelihood (0-5)	Risk (Extent + Likelihood)	Description
Unauthorized Access	C, I	8	4	12	Could expose sensitive data and allow attackers to modify or misuse critical systems.
Data Breaches	C	9	3	12	Compromised data from stolen servers or drives could lead to reputational and financial loss.
System Downtime	A	7	3	10	Hardware failures could disrupt services, affecting productivity and customer satisfaction.

Figure 2. Impact and Likelihood of Three Top Risks for DHAEI.

Notes:

- Extent: Represents the potential severity of the impact (0 = no impact, 10 = catastrophic impact).
- Likelihood: Reflects the probability of the risk occurring (0 = highly unlikely, 5 = highly likely).

This table helps prioritize mitigation strategies based on the severity and probability of each risk affecting the organization.

Risk acceptance criteria

Most Likely / Highest Risk: Unauthorized Access

Risk Level: 12 (Extent: 8, Likelihood: 4)
Impact on DHAEI:
Unauthorized access poses a critical threat to DHAEI because it directly compromises Confidentiality (C) and Integrity (I).

- Confidentiality Impact: Unauthorized users could gain access to sensitive data, such as intellectual property or user credentials, resulting in potential data leaks or breaches.

- Integrity Impact: Malicious actors could alter or corrupt data, undermining the reliability and accuracy of systems.

For DHAEI, the risks from unauthorized access could:

- Undermine Client Trust: A breach of client data could damage the company's reputation, resulting in client attrition.
- Cause Compliance Issues: If DHAEI fails to secure sensitive data, it may face regulatory penalties.
- Operational Costs: Recovery from such incidents could be costly, involving technical fixes and potential legal actions.

Why Some Items May Be "Ignored" or "Minimized"

1. Data Breaches (Risk Level: 12, Extent: 9, Likelihood: 3)
   Although it shares the same risk level as unauthorized access, the likelihood of a data breach is slightly lower because DHAEI already uses encryption and plans to strengthen it further. If encryption is robustly implemented, the threat can be significantly mitigated, making this less urgent than unauthorized access.
2. System Downtime (Risk Level: 10, Extent: 7, Likelihood: 3)
   While downtime is impactful to Availability (A), DHAEI has redundancy and recovery mechanisms planned (e.g., load balancing and cluster management). The likelihood is lower due to these measures, and any incidents can likely be resolved quickly with minimal long-term effects.

Unauthorized Access emerges as the most pressing risk because it affects Confidentiality and Integrity. If left unchecked, it could cascade into other risks like data breaches.
In contrast, risks like System Downtime can be deprioritized if DHAEI continues to develop robust backup and redundancy strategies. Similarly, Data Breaches may be minimized with proper encryption and secure file storage protocols.

The prioritization of risks aligns with their likelihood and extent of impact. By focusing resources on addressing unauthorized access, DHAEI can significantly reduce its overall risk exposure.

Risk Treatment

1. Unauthorized Access

- Threat Description: Vulnerabilities in VPNs or RODCs could allow unauthorized access to sensitive data or systems.
- Impact: High on Confidentiality (C) and Integrity (I); Likelihood is high due to remote work and branch office setups.

Recommended Mitigations:

1. Implement Multi-Factor Authentication (MFA):
   - Ensure MFA is mandatory for VPN and RODC access.
   - Aligns with NIST SP 800-53 IA-2 (Identification and Authentication) and ISO/IEC 27001 A.9.4 (Access Control).
2. Conduct Regular Penetration Testing:
   - Identify potential vulnerabilities in VPN and RODC configurations.
   - Supports NIST SP 800-53 CA-8 (Penetration Testing) and ISO/IEC 27001 A.18.2.3 (Technical Compliance Testing).
3. Use Network Segmentation:
   - Restrict access to sensitive systems based on user roles.
   - References NIST SP 800-53 AC-4 (Information Flow Enforcement) and ISO/IEC 27001 A.13.1 (Network Security).

Priority: High

This risk is prioritized because a successful exploit could compromise the entire network and sensitive data.

2. Data Breaches

- Threat Description: Sensitive data on file servers or stolen drives could be compromised.
- Impact: Significant on Confidentiality (C); Likelihood is moderate with existing security plans.

Recommended Mitigations:

1. Encrypt Data at Rest and In Transit:
   - Use AES-256 encryption for stored and transmitted data.
   - Aligns with ISO/IEC 27001 A.10 (Cryptographic Controls) and NIST SP 800-53 SC-12 (Cryptographic Key Establishment).
2. Implement Endpoint Protection Solutions:
   - Secure file servers and endpoints against unauthorized access.
   - Supports NIST SP 800-53 SI-3 (Malicious Code Protection) and ISO/IEC 27001 A.12.6.2 (Detection).

3. Perform Regular Data Audits:
    - Track access to and use of sensitive data to detect unusual patterns.
    - References NIST SP 800-53 AU-6 (Audit Review and Analysis) and ISO/IEC 27001 A.16.1.4 (Monitoring).

Priority: Medium

This risk is critical, but planned mitigations (encryption and audits) reduce its likelihood, placing it below unauthorized access.

3. System Downtime

- Threat Description: Hardware failures could cause service interruptions, affecting productivity.
- Impact: High on Availability (A); Likelihood is relatively low due to planned redundancy.

Recommended Mitigations:

1. Implement Load Balancing and Clustering:
    - Distribute workloads to ensure continuous service availability.
    - Aligns with ISO/IEC 27001 A.12.1.3 (Capacity Management) and NIST SP 800-53 CP-7 (Alternate Processing Sites).
2. Monitor Hardware Health Proactively:
    - Use tools to predict and prevent failures.
    - References NIST SP 800-53 MA-3 (Maintenance Tools) and ISO/IEC 27001 A.12.1.2 (Monitoring).
3. Establish a Backup and Recovery Plan:
    - Schedule regular backups and store them securely offsite.
    - Supports NIST SP 800-53 CP-9 (Information Backup) and ISO/IEC 27001 A.12.3 (Backup).

Priority: Low

With redundancy and backup plans in place, this risk has a lower immediate impact compared to others.

Prioritization Explanation

- Unauthorized Access: Highest priority due to its potential to undermine overall network security.
- Data Breaches: Medium priority since encryption reduces immediate exposure but still requires careful monitoring.

- System Downtime: Lowest priority given the mitigation measures already in place.

Applying these mitigations in alignment with NIST and ISO/IEC standards ensures a structured and compliant risk treatment approach.

References

National Institute of Standards and Technology (NIST). (retrieved 2025-01-14). NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. Retrieved from https://csrc.nist.gov

International Organization for Standardization. (retrieved 2025-01-14). ISO/IEC 27002:2022 Information security, cybersecurity, and privacy protection — Information security controls. Retrieved from https://www.iso.org

MITRE. (retrieved 2025-01-1). ATT&CK Framework. Retrieved from https://attack.mitre.org

Kosutic, D. (2022-04-07) Risk owners vs. asset owners in ISO 27001:2013 https://advisera.com/27001academy/knowledgebase/risk-owners-vs-asset-owners-in-iso-270012013/

Secureframe's Guide on ISO 27001 Risk Assessment (retrieved 2025-01-14) https://secureframe.com/hub/iso-27001/risk-assessment

Kosutic, D. (retrieved 2025-01-14) ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/