DHAEI Risk Management Plan

Violet Figueroa

Executive Summary

This Risk Management Plan outlines the key risks, vulnerabilities, and mitigation strategies for DHA Enterprise Inc. (DHAEI), a software development company with a main office in Oshawa, Ontario, several branch offices, and remote employees. The plan was developed to align with ISO/IEC 27001 standards and addresses the organization's need to protect its information assets while meeting technical, security, and user requirements.

Overview of Risk Assessment

The risk assessment process identified critical assets, threats, and vulnerabilities across DHAEI's infrastructure. Three primary risks were highlighted:

1. Unauthorized Access to Sensitive Data
   - Threat: Cyberattacks exploiting weak authentication mechanisms.
   - Vulnerability: Lack of multi-factor authentication (MFA) and inconsistent access control policies.
2. Data Loss Due to System Failures
   - Threat: Hardware failures or natural disasters affecting servers.
   - Vulnerability: Limited redundancy in branch office servers and insufficient backup policies.
3. Phishing Attacks Targeting Employees
   - Threat: Social engineering attacks compromising user credentials.
   - Vulnerability: Lack of employee awareness training on identifying phishing attempts.

Each risk was analyzed for its potential impact on confidentiality, integrity, and availability (CIA) of information assets, as well as its likelihood of occurrence. Risks were prioritized based on their scores to focus on the most critical issues.

Key Findings

- The highest-priority risk is phishing attacks, which pose a significant threat to confidentiality due to the potential for compromised credentials leading to data breaches.
- Unauthorized access risks are also high-priority due to their impact on both confidentiality and integrity.
- Data loss risks are medium-priority, as existing backups provide partial mitigation; however, improvements in redundancy are necessary for long-term resilience.

These findings highlight three critical risks that require immediate attention based on their likelihood and impact scores (IT Governance, 2024).

Recommended Risk Treatments

To address these risks, the following mitigations are proposed:

1. Unauthorized Access:
   - Implement multi-factor authentication (MFA) for all systems.
   - Enforce strong password policies and conduct regular access reviews.
   - Priority: High
2. Data Loss:
   - Deploy automated backup solutions and implement server redundancy at branch offices.

  - Establish disaster recovery protocols to ensure business continuity.
  - Priority: Medium
3. Phishing Attacks:
   - Conduct regular employee training sessions on recognizing phishing emails.
   - Deploy advanced email filtering tools to detect and block malicious messages.
   - Priority: High

Next Steps

The implementation of these treatments will require collaboration across DHAEI’s management team, IT security personnel, and branch office technicians. Regular monitoring of risks and periodic reviews of the Risk Management Plan will ensure that DHAEI remains resilient against emerging threats while supporting its planned expansion into Brampton, Mississauga.

Purpose

To systematically identify, assess, and address risks that could impact DHA Enterprise Inc. (DHAEI) in achieving its business objectives, particularly in maintaining the confidentiality, integrity, and availability (CIA) of its information assets. This plan aims to minimize potential damages caused by security incidents through the application of effective risk treatment strategies while ensuring compliance with ISO/IEC 27001 standards (Sprinto, 2024; IT Governance, 2024).

This document will guide DHAEI in safeguarding its infrastructure, including its main office in Oshawa, Ontario, branch offices, and remote operations. It will also address risks associated with planned changes, such as the establishment of a new branch office in Brampton, Mississauga. By identifying vulnerabilities and threats across DHAEI's digital and physical environments, this plan will enable the organization to implement prioritized controls and ensure continuity of operations.

The Risk Management Plan will serve as a foundation for informed decision-making by DHAEI's management team and technical staff. It will also provide a clear framework for addressing risks associated with existing systems (e.g., Active Directory domain, VPN connections, file servers) and meeting technical, security, and user requirements. This version aligns with the assignment's requirements and incorporates details specific to DHAEI's context.

Scope

The scope includes protecting the confidentiality, integrity, and availability of information assets across DHAEI's main office and branch offices (NIST SP 800-30, 2012). The assessment aims to identify, evaluate, and address risks that could impact DHAEI's ability to meet its technical, security, and user requirements while ensuring compliance with ISO/IEC 27001 standards.

Users

1. Alan Hake (Founder and CEO)
    - Role: Oversees overall business operations and strategic decision-making.
    - Importance: Provides executive support for the risk management process and ensures alignment with the company's goals.
2. Amanda Wilson (CIO)
    - Role: Responsible for managing the organization's IT infrastructure and ensuring its security.
    - Importance: Leads the implementation of technical and security requirements, including risk assessment and treatment.
3. Paul Alexander (Chief Information Security Officer)
    - Role: Manages the information security team and oversees all security-related activities within DHAEI.

- Importance: Directly responsible for identifying risks, proposing mitigations, and ensuring compliance with ISO/IEC 27001.

4. Information Security Team (Security Technicians and Intern)
   - Role: Conducts technical assessments, implements security controls, and monitors systems for vulnerabilities.
   - Importance: Provides hands-on expertise in identifying threats and vulnerabilities across DHAEI's infrastructure.
5. Branch Office Support Technicians
   - Role: Handles local maintenance of branch office servers and ensures operational continuity.
   - Importance: Key to implementing risk treatments at branch office locations.
6. IT Department Staff (Central Technology Department)
   - Role: Manages day-to-day IT operations, including server maintenance, updates, and VPN configurations.
   - Importance: Ensures that technical requirements are met and supports risk mitigation efforts.
7. Remote Programmers (20 Work-from-Home Employees)
   - Role: Develop software using company-issued laptops while connecting to the main office via VPN.
   - Importance: Their devices and connections represent potential risks that need to be managed effectively.
8. End Users (Main Office and Branch Office Employees)
   - Role: Utilize desktop computers for daily tasks across all offices.
   - Importance: Their adherence to security policies is critical in mitigating insider threats or accidental breaches.
9. External Auditors or Consultants (if applicable)
   - Role: Assess compliance with ISO/IEC 27001 standards and provide recommendations for improvement.
   - Importance: Offers an unbiased evaluation of DHAEI's risk management practices.

Risk Assessment

Process

The risk assessment process for DHA Enterprise Inc. (DHAEI) will follow a systematic approach to identify, evaluate, and prioritize risks to its information assets.

Assets, Vulnerabilities, and Threats

Based on DHAEI's environment, the following are three main threats the organization faces:

1. Unauthorized Access to Sensitive Data:
   - Vulnerability: Weak password policies or lack of multi-factor authentication (MFA).
   - Threat: Cyberattacks targeting user credentials or exploiting unprotected systems.
2. Data Loss Due to System Failures:
   - Vulnerability: Lack of redundancy in branch office servers or inadequate backup processes.
   - Threat: Hardware failures or natural disasters impacting data availability.
3. Phishing Attacks on Employees:
   - Vulnerability: Lack of employee awareness or training on recognizing phishing emails.
   - Threat: Phishing attacks represent a significant threat to DHAEI's information security due to their ability to compromise credentials through social engineering tactics (MITRE ATT&CK, 2024).

Challenges in managing these threats include ensuring consistent security practices across branch offices, addressing technical limitations in remote environments, and maintaining employee compliance with security policies.

Risk Owners

For each identified risk, a "chain" of ownership from ground-level personnel to senior executives will be established:

1. Unauthorized Access to Sensitive Data:
   - Ground Level: IT Security Technicians—Monitor access logs and enforce password policies.
   - Mid Level: Paul Alexander (CISO)—Oversees implementation of MFA and system hardening.
   - Senior Level: Amanda Wilson (CIO)—Approves resource allocation for security enhancements.
2. Data Loss Due to System Failures:
   - Ground Level: Branch Office Support Technicians—Ensure proper server maintenance.

- Mid Level: IT Security Team—Implement backup solutions and redundancy measures.
- Senior Level: Amanda Wilson (CIO)—Approves funding for infrastructure upgrades.

3. Phishing Attacks on Employees:
    - Ground Level: Employees—Participate in security awareness training.
    - Mid Level: Paul Alexander (CISO)—Develops training programs and monitors incidents.
    - Senior Level: Alan Hake (CEO)—Promotes a culture of security awareness across the organization.

Impact and Likelihood

Risks are evaluated using a matrix that considers both likelihood and impact to prioritize treatment options effectively (Secureframe, n.d.)

Threat	Impact on CIA	Impact Rating (0–10)	Likelihood Rating (0–5)	Risk Score (= Impact × Likelihood)
Unauthorized Access	C, I	8	4	32
Data Loss Due to System Failures	A	9	3	27
Phishing Attacks	C	7	5	35

Risk acceptance criteria

The highest-risk item identified is Phishing Attacks, with a risk score of 35. This poses a significant threat to confidentiality due to potential data breaches caused by compromised credentials. This risk must be prioritized for immediate mitigation through employee training and technical controls like email filtering. Risks with low likelihood and minimal impact may be accepted if they fall within DHAEI's risk tolerance levels (Sprinto, 2024).

Risk Treatment

These are the recommended mitigations for the three main threats identified above:

Threat	Recommended Mitigation	Priority	Justification
Unauthorized Access	Implement MFA, enforce strong password policies, conduct regular access reviews(Sprinto, 2024; Secureframe, n.d.).	High	Prevents unauthorized access to sensitive systems, reducing exposure to cyberattacks.
Data Loss Due to System Failures	Deploy automated backups, implement server redundancy at branch offices.	Medium	Ensures availability of critical data even in case of hardware failures or disasters.
Phishing Attacks	Conduct regular employee training sessions; deploy advanced email filtering tools.	High	Reduces likelihood of successful phishing attacks by improving user awareness.

Prioritization Justification

1. Phishing attacks are prioritized as high due to their high likelihood and potential impact on confidentiality.
2. Unauthorized access is also a high priority as it directly threatens both confidentiality and integrity.
3. Data loss is medium priority because existing backups provide partial mitigation. However, redundancy improvements are necessary for long-term resilience.

References and Citation

1. MITRE ATT&CK. (2024). MITRE ATT&CK Framework. Retrieved January 21, 2025, from https://attack.mitre.org
2. National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments (SP 800-30 Rev. 1). Retrieved January 21, 2025, from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
3. Sprinto. (2024). ISO 27001 Risk Assessment: A Complete Guide. Retrieved January 21, 2025, from https://sprinto.com/blog/iso-27001-risk-assessment/
4. Secureframe. (n.d.). How to Do an ISO 27001 Risk Assessment. Retrieved January 21, 2025, from https://secureframe.com/hub/iso-27001/risk-assessment
5. IT Governance Ltd. (2024). 5 Steps to an Effective ISO 27001 Risk Assessment. Retrieved January 21, 2025, from https://www.itgovernance.co.uk/iso27001-risk-assessment-tool
6. ISO/IEC. (2022). ISO/IEC Standard: Information Security Management Systems. Retrieved January 21, 2025, from https://www.iso.org/standard/27001
7. Trellix. (2024). What Is the MITRE ATT&CK Framework?. Retrieved January 21, 2025, from https://www.trellix.com/security-awareness/cybersecurity/what-is-mitre-attack-framework/
8. SISA Information Security. (2024). Comparison between ISO 27005, OCTAVE & NIST SP 800-30. Retrieved January 21, 2025, from https://www.sisainfosec.com/blogs/comparison-between-iso-27005-octave-nist-sp-800-30-sisa-blog/
9. Drata. (n.d.). ISO 27001 Risk Assessment: A Step-by-Step Guide. Retrieved January 21, 2025, from https://drata.com/grc-central/iso-27001/risk-assessment