**Risk Management Plan**

DHA Enterprise Inc. (DHAEI)

**

By : Sukhvir Kaur Sahota

# 

# Table of Contents

# 

[Executive Summary](#_rjpscud5ucvw) 2

[Introduction](#_3k2zzjd0affx) 3

[Purpose, Scope, and Users:](#_88af9fosom4i) 3

[Purpose:](#_yiq8fhbqmx2w) 3

[Scope:](#_rrz5dwy7dz3m) 4

[Users:](#_q28545z245ni) 4

[Risk Assessment](#_jcmmar4fqozc) 5

[The Process:](#_ef7ndalld4md) 5

[Assets, Vulnerabilities, and Threats:](#_v7smgvinz0z0) 6

[Assets](#_fka32a8conjl) 6

[Assets](#_ql639rl0sqbu) 8

[Vulnerabilities](#_9kjoz77dafjj) 8

[Threats](#_tgytorqz6txy) 9

[Determining the risk owners](#_scrdruibnax6) 10

[Impact and Likelihood](#_ugk4zwr4dxtw) 12

[Risk Acceptance Criteria](#_edxzfvfttylv) 13

[Risk Treatment](#_pcyvywe1eo0c) 13

[RMF Controls and Explanation](#_4icressrz0d4) 14

[Prioritization Rationale](#_bg1nlcm74css) 15

[Conclusion](#_unc02q8x3p8k) 15

[References](#_f4rhxu5l6q5l) 16

# 

# 

# Executive Summary

Cybersecurity risk management is the most important and ongoing process. It involves the identification, analysis, evaluation, and mitigation of potential threats. In this report, we present a Risk Management Plan specifically tailored for DHAEI, a software development company headquartered in Oshawa, Ontario, with multiple branch offices. Utilizing the ISO 27001 Risk Management Framework and RMF Controls, which are recognized as the leading international standard for information security management, DHAEI aims to safeguard its operations and infrastructure by addressing risks associated with its services.

The purpose of this RMP is to systematically identify, assess, manage, and monitor potential risks across DHAEI's operations and infrastructure, ensuring security, reliability, and continuity of services. From the main headquarters to remote users, this plan extends its reach, encompassing every IT asset and the information it holds. Its objectives are a shining shield against potential harm: minimize breaches, data loss, and disruptions; protect sensitive data and intellectual property; ensure confidentiality, integrity, and availability; uphold a sterling security reputation; and comply with industry regulations.

Through a continuous cycle of assessment, the plan identifies and prioritizes threats like phishing attacks, malware, data loss, and more. Brainstorming sessions gather diverse perspectives from IT, security, and management, building a comprehensive understanding of the risk landscape. Each threat is meticulously weighed, and its likelihood and potential impact are assessed, leading to a prioritized mitigation strategy. Ownership is assigned, ensuring clear accountability for implementing controls like strong passwords, security awareness training, robust backups, and swift vulnerability patching.

Among these threats, data loss stands as the most critical, demanding the highest priority. Backups and disaster recovery plans stand as a safety net, while encryption acts as a suit of armor for sensitive data. Intrusion detection systems stand guard, and vulnerability assessments continuously identify and patch weaknesses. Malware and ransomware, though less likely, are not ignored. A well-defined incident response plan serves as a rapid response force, while backups and patching provide a crucial defense. Security awareness training empowers employees to be vigilant against these digital foes.

By implementing this RMP, DHAEI builds a robust defense, proactively addressing risks and minimizing potential consequences. This not only safeguards its data but also ensures business continuity and a strong, unblemished reputation.

# Introduction

Cybersecurity threats are at an all-time high. In 2023 there were 3,025 data compromised with approximation of 353 million victims. (1) To mitigate those risks organizations hire professionals who build a Risk Management plan for the company.

Cybersecurity risk management is an ongoing process of identifying, analyzing, evaluating, and addressing your organization’s cybersecurity threats. Cybersecurity risk management is an ongoing process, not a one-and-done. Based on the findings from consistent monitoring and reporting, organizations can continue to adjust and configure new risk mitigation efforts as seen fit. (2)(4).

A popular way to think of a risk management plan is via the IT Risk Equation: *IT Risk = Threat x Vulnerability x Consequence. (3)*

In this report, we are developing a Risk management plan for *DHA Enterprise Inc. (DHAEI)* by using the ISO 27001 Risk Management Framework. ISO 27001 is the leading international standard for protecting and managing information security within an organization. This framework includes a combination of policies and procedures that revolve around CIA triads(4) DHAEi is a software development company with headquarters in Oshawa, Ontario, and several branch offices.

# Purpose, Scope, and Users:

## Purpose:

The Risk Management Plan for DHAEI is proposed to systematically identify, assess, manage, and continuously monitor potential risks associated with its operations and infrastructure, ensuring the security, reliability, and continuity of its services. By addressing these risks, DHAEI Organisation aims to following :

* Minimize the likelihood of security breaches, data loss, and business disruptions.
* Protect sensitive data, including customer information and intellectual property.
* Ensure the confidentiality, integrity, and availability of critical IT systems and resources.
* Maintain a strong reputation for security and reliability.
* Comply with any relevant industry regulations or data protection laws.

## Scope:

This RMP encompasses the entire organization of DHAEI, including its main office in Oshawa, Ontario, currently running branch offices, newly planned office in Brampton, Mississauga, and remote workforce, focusing on technical, security, and user-related risks. It also includes employees, contractors, and any other individuals who access or use the company's IT systems and data.

The following aspects are in main consideration for business operations :

* IT infrastructure and systems (servers, network devices, desktops, laptops, software applications)
* Data storage and management practices
* User access controls and security protocols
* Physical security measures for IT equipment and facilities
* Business continuity and disaster recovery procedures
* Third-party vendor relationships (if applicable)

## Users:

This RMP is intended for use by the management team at DHAEI, including the CEO, CIO, Chief Information Security Officer (CISO), IT staff, and support technicians responsible for implementing risk management strategies. We can categorize them into the following

* **IT Department:** IT personnel will utilize the RMP to identify and prioritize IT-related risks, develop mitigation strategies, and implement security controls.
* **Security Team:** The security team will leverage the RMP to assess security vulnerabilities, recommend appropriate security measures, and conduct security awareness training for employees.
* **Management:** Executives and managers will use the RMP to understand the overall risk landscape, allocate resources for risk mitigation efforts, and make informed decisions regarding IT security investments.
* **All Employees:** By understanding the identified risks and mitigation strategies outlined in the RMP, all DHAEI employees can play a crucial role in maintaining a secure IT environment.

# Risk Assessment

ISO 27001 requires organizations to conduct a risk assessment to identify and evaluate information security risks. It emphasizes the need to assess the likelihood and potential impact of risks and prioritize them for treatment.

### The Process:

DHAEI will adopt a cyclical risk assessment process involving continuous monitoring and updates. We have decided to have 5 steps in the risk assessment process for DHAEI management.

1. ***Brainstorming sessions*:** The very first step is deciding on a team, based on the requirements of DHAEI the team should consist of the following to identify potential threats across all DHAEI's operations.

* IT Staff
* Network Security Team
  + ***Harold Fry*** - Security Tech
  + ***Lewis Mableton*** - Intern
* Management personnel
  + Founder and CEO, ***Alan Hake.***
  + The CIO, ***Amanda Wilson***
  + ***Paul Alexande*r** as Manager of Information Security and Chief Information Security.

1. ***Threat identification*:** Based on the brainstorming session discussion all mentioned users will contribute to creating a list of potential internal and external threats they think could impact their organization. They can do a consideration based on :

* User access management (weak passwords, lack of MFA)
* Phishing attacks targeting employees
* Malware and ransomware infections
* Hardware failures or data loss incidents
* Business continuity disruptions due to power outages or natural disasters
* Security vulnerabilities in software applications used by employees
* Physical security risks at branch offices

1. ***Risk prioritization*:** Evaluate each identified risk using a risk matrix that considers likelihood and potential impact (financial, reputational, operational).

* ***Likelihood*:** How probable is the threat to occur, considering user behavior, current security measures, and industry trends? (5)
* ***Impact*:** How severe would the consequences be if the threat materializes? This could involve financial loss, data breach, reputational damage, or disruption to business operations. (5)

1. ***Risk ownership assignment*:** Management will be assigning ownership of each risk to a specific individual or department responsible for mitigation strategies. The reason behind this step is to ensure accountability for implementing mitigation strategies and monitoring risks.

* User-related risks like phishing awareness might be assigned to the It and Security Team for training initiatives
* Risks concerning branch office security procedures might be owned by branch office managers.
  + Maybe by Paul and/or Amanda in our case.

1. ***Documentation*:** All Identified risks, assessments related to them, and all mitigation plans should be documented.

* There are multiple ways to document it but creating a playbook is one of the effective approaches to doing it.
* All users involved in the risk assessment process will contribute to ensuring the register accurately reflects user-related concerns and mitigation strategies

### 

### Assets, Vulnerabilities, and Threats:

#### Assets

An asset is anything that has current or future economic value to a business. For DHAEI the assets can be categorized into 3 groups

1. **Data:**

* **Customer Information:** According to The Personal Information Protection and Electronic Documents Act (PIPEDA) it is essential for DHAEI to make use of customer data. This includes but is not limited to details of customers such as
  + Names,
  + contact details,
  + financial information (if applicable) of DHAEI's clients.
* **Intellectual Property:** Intellectual property (IP) refers to documents, designs, symbols, names, and images used in commerce.
  + *Proprietary software code* - This refers to software programs developed by DHAEI that are protected by copyright law.
  + *Development tools* - These are resources, frameworks, libraries, or software applications used by DHAEI's developers to create and maintain software products
  + *Confidential information* that gives DHAEI a competitive advantage -This includes any sensitive or proprietary information that DHAEI possesses, such as trade secrets, customer data, business strategies, or research and development findings.
* **Company Data:** Company data, including financial records, employee information, and internal documents, is a vital asset for DHAEI's operations and success.
  + Financial records: It could be related to transactions, including income, expenses, assets, liabilities, and cash flow
  + Employee information: Employee information includes personal and professional data about DHAEI's workforce, such as names, addresses, contact details, employment history, compensation, performance evaluations, and benefits.
  + Internal documents: These may include company plans, project proposals, product specifications, marketing materials, legal contracts, policies and procedures, meeting minutes, memos, etc.

1. **IT Infrastructure:**

* **Servers:** Physical or virtual machines that store data, run applications, and provide network services.
  + 2 domain controllers named DCI and DC2
  + One file server named FSI
  + Windows Software Update Services (WSUS) server named WSUSI
  + An infrastructure server named DHADNS provides DNS services to the network
* **Network Devices:** Routers, switches, and firewalls that enable communication and data flow within the network and to the internet.
* **Client Computers:** Desktops and laptops used by employees to perform their work.
  + 1,500 users in the main office (all use desktop computers)
  + 200 branch users use desktops
  + 20 Programmers use Laptops
* **Software Applications:** Operating systems, productivity tools, development software, and any other programs essential for DHAEI's business processes.

1. **Reputation:**

* DHAEI's reputation is also a valuable asset. A data breach or security incident could damage its reputation and lead to lost business.
* A positive reputation brings trust among customers, partners, investors, and other stakeholders, which is very essential for business growth.

| **Assets** | | **Vulnerabilities** | | **Threats** |
| --- | --- | --- | --- | --- |
| **Data** | * Customer Information * Intellectual Property * Company Data | **Data Vulnerabilities** | * Unauthorized Access * Data Breaches | * Security Incidents * Data Loss * Malware and Ransomware |
| **IT Infrastructure** | * Servers * Network Devices * Client Computers * Software application | **IT Infrastructure Vulnerabilities** | * Unpatched Systems * Weak Security   Configuration   * Malware and Ransomware * Hardware Failure |
| **Reputation** | | **Reputational Vulnerabilities** | * Security Incidents * Data Loss * System Outages * Negative Publicity |

#### Vulnerabilities

Every asset of the Company comes up with so many vulnerabilities. Based on the assets of DHAEI, the following vulnerabilities could be identified.

1. **Data Vulnerabilities:**

* **Unauthorized Access:** Weak passwords, lack of MFA, and phishing attacks can allow unauthorized users to access confidential data.
* **Data Breaches:** Security vulnerabilities in DHAEI's systems or applications could be exploited to steal or leak sensitive data.

1. **IT Infrastructure Vulnerabilities:**

* **Unpatched Systems:** Outdated software and operating systems with known vulnerabilities can be easily exploited by attackers.
* **Weak Security Configuration:** Incorrect security settings on servers, network devices, and applications can leave them vulnerable to attacks.
* **Malware and Ransomware:** Malicious software can infect DHAEI's systems, encrypting data, disrupting operations, and demanding ransom for decryption.
* **Hardware Failure:** Hardware components like storage drives can malfunction, leading to data loss or downtime.

1. **Reputational Vulnerabilities**

* **Security Incidents:** Any data breach, malware infection, or other security incident can damage DHAEI's reputation and lead to negative publicity.
* **Data Loss:** Losing customer data or other sensitive information can erode trust and damage DHAEI's reputation for reliability.
* **System Outages:** Frequent outages or downtime can disrupt customer service and damage DHAEI's image of reliability.
* **Negative Publicity:** Media reports about security vulnerabilities or data breaches can significantly harm DHAEI's reputation.

#### Threats

Based on the case study and the analysis of Assets and their vulnerabilities, we picked 4 main threats for DHAEI.

**Main Threats:**

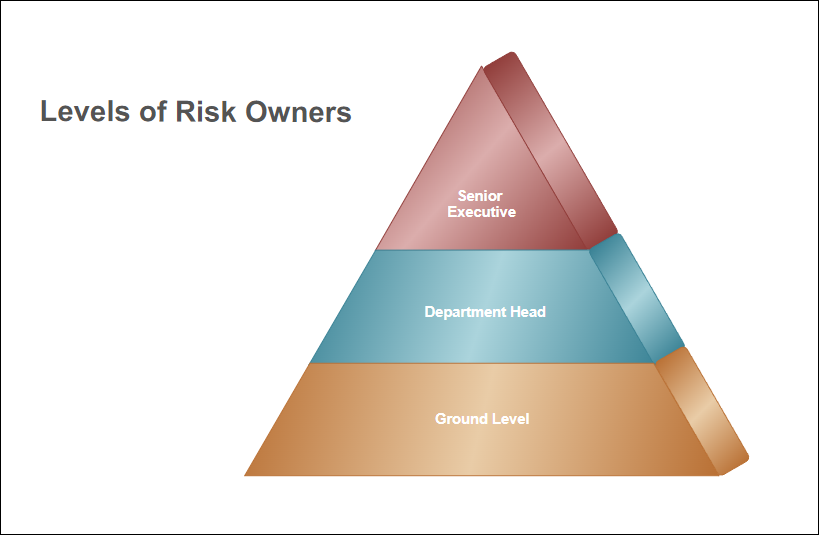
* **Security Breach ( via Phishing attack):** Unauthorized access to sensitive data (customer information, intellectual property) due to weak security practices or vulnerabilities.
* **Data Loss or Disruption:** Hardware failure, cyberattacks, or human error leading to data loss or disruption of critical operations. Potential weaknesses in network infrastructure leading to service disruptions.
* **Malware and Ransomware:** Malicious software that can infect DHAEI's systems, encrypt data, disrupt operations, and demand ransom for decryption.

**Challenges in Managing Threats:**

* **Limited Resources:** Balancing security needs with budget constraints for personnel, training, and equipment.
* **Remote Access Security:** Maintaining secure access for remote workers.
* **Branch Office Security:** Ensuring adequate security measures at branch offices with potentially less stringent protocols compared to the main office.
* **Data Transfer:** Minimizing risks during data migration from the main office to the Brampton branch server.

### Determining the risk owners

We have Categorized the risk owners into 3 categories. These individuals play crucial roles in mitigating each risk:



1. **Ground Level:** These individuals perform the initial detection, response, and implementation of security controls or recovery procedures.
2. **Department Head:** These individuals oversee the overall strategies and procedures related to security, data management, or business continuity.
3. **Senior Executive:** These individuals hold ultimate responsibility for the company's security posture, data integrity, and business continuity. They allocate resources and ensure that the necessary plans and procedures are in place.

| **Type of Risk** | **Ground Level** | **Department Head** | **Senior Executive** |
| --- | --- | --- | --- |
| **Security Breach (Phishing)** | ***Harold Fry***- Security Technician | ***Paul Alexander*** - Chief Information Security Officer (CISO) | ***Amanda Wilson*** - Chief Information Officer (CEO) |
| **Data Loss or Disruption** | ***Lewis Mableton and Harold Fry*** -IT Support Technician | ***William Freund*** -System Manager  ***Scotty Doohan*** - Application Manager | ***Richard Xavir*** - Chief Operating Officer (COO) |
| **Data Loss or Disruption** | ***Harold Fry - Security Tech***  ***Susan Carter- Shift Supervisor***  ***Edward Michael*** - Shift supervisor | ***Paul Alexander***- Chief Information Security Officer (CISO) | ***Alan Hake***-Chief Executive Officer (CEO) |

1. **Risk:** Security Breach (Phishing)

* **Ground Level:** Monitors for suspicious activity and implements security controls.
  + ***Harold Fry****- Security Technician*
* **Department Head:** Oversees information security policies and procedures.
  + ***Paul Alexander*** *- Chief Information Security Officer (CISO)*
* **Senior Executive:** Holds ultimate responsibility for data security and company reputation.
  + ***Amanda Wilson*** *- Chief Information Officer (CEO)*

1. **Risk:** Data Loss or Disruption

* **Ground Level:** Provides technical support and assists with data recovery processes.
  + ***Lewis Mableton and Harold Fry*** *-IT Support Technician*
* **Department Head:** Oversees data backup and disaster recovery procedures.
  + ***William Freund*** *-System Manager*
  + ***Scotty Doohan*** *- Application Manager*
* **Senior Executive:** Ensures operational continuity and data integrity.
  + ***Richard Xavir*** *- Chief Operating Officer (COO)*

1. **Risk:** Malware and Ransomware

* **Ground Level:** Monitors systems for suspicious activity that might indicate malware infection. Responds to malware incidents by isolating infected systems, containing the threat, and reporting it to the security team.
  + **Harold Fry** - *Security Tech*
  + **Susan Carter**- *Shift Supervisor*
  + **Edward Michael** - *Shift supervisor*
* **Department Head:** Implements security measures like email filtering and web content filtering to prevent the spread of malware. Analyzes malware incidents to identify attack vectors and implement preventive measures.
  + ***Paul Alexander***- *Chief Information Security Officer (CISO)*
* **Senior Executive:** Makes critical decisions during ransomware attacks, considering factors like data recovery options, negotiation strategies, and potential legal implications.
  + ***Alan Hake***-*Chief Executive Officer (CEO)*

### Impact and Likelihood

| **Threat** | **Impact**  **(C I A)** | **Extent**  **(0-10)** | **Likelihood**  **(0 - 5)** | **Risk**  **(= I \* L)** |
| --- | --- | --- | --- | --- |
| **Security Breach (Phishing)** | C- High  I- Medium  A- Medium | 7 | 3 | 21 |
| **Data Loss or Disruption** | C- High  I- High  A- High | 9 | 4 | 36 |
| **Malware and Ransomware** | C- High  I- High  A- Medium | 8 | 3 | 24 |

**Impact (C, I, A):** This column indicates the potential impact of the threat on Confidentiality (C), Integrity (I), and Availability (A) of DHAEI's data and systems.

**Extent (0-10)**: This score reflects the severity of the impact on each affected area (C, I, A). A score of 10 represents the most significant potential damage.

**Likelihood (0-5)**: This score represents the estimated probability of the threat occurring within a given timeframe. A score of 5 indicates a very high likelihood.

**Risk Score (= I \* L)**: This is calculated by multiplying the Impact extent by the Likelihood score (Risk = Likelihood x Impact). It provides a quick overview of the overall risk level associated with each threat.

### Risk Acceptance Criteria

1. **Security Breach (Phishing): Medium**

No Doubt that phishing attacks pose a significant risk, their impact might be more localized depending on the compromised accounts or systems. However, the potential for data breaches and reputational damage necessitates strong security measures against phishing attempts.

1. **Data Loss or Disruption**: **High**

This threat has the highest risk score due to its potential for widespread and severe consequences across all three aspects of the CIA triad, making it the top priority for risk mitigation.

1. **Malware and Ransomware**: **High ( Can be Minimized to Midum)**

The impact of malware and ransomware attacks can be severe, but their likelihood might be mitigated through proactive security measures like anti-malware solutions and employee training. However, it's still crucial to have robust incident response plans in place to address such threats effectively.

By understanding the potential impact and likelihood of each threat, DHAEI can prioritize its risk mitigation efforts and allocate resources accordingly to protect its critical assets and ensure business continuity.

# Risk Treatment

For the 3 Threats, the following are the recommendations based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This framework provides a set of guidelines for managing cybersecurity risks, including identification, protection, detection, response, and recovery. The following are the Recommended Controls for the mitigation of threats.

## RMF Controls and explanation

1. **Security Breach (Phishing) (Medium Risk)**

* ***RMF Control: AC-2 (Account Management):*** Enforce strong password policies and multi-factor authentication (MFA) for all user accounts to mitigate the risk of unauthorized access via phishing attacks.
* ***RMF Control: AC-3(7)(Access Control):*** Implement email filtering and web content filtering solutions to block phishing attempts and prevent unauthorized access to sensitive information.
* ***RMF Control: AC-18 (Security Awareness and Training):*** Conduct regular security awareness training to educate employees on identifying and avoiding phishing attacks, enhancing their ability to protect against security breaches.
* ***RMF Control: CM-2 (Baseline Configuration)***: Patch systems and software promptly to address known vulnerabilities that attackers might exploit through phishing attacks.

1. **Data Loss or Disruption (High Risk)**

* ***RMF Control: CP-2 (Data Backup)***: Implement a robust backup and disaster recovery (DR) plan with regular backups stored off-site to ensure data integrity and availability.
* ***RMF Control: CP-15 (Backup of Information)***: Regularly test backup and recovery procedures to ensure functionality and effectiveness in restoring data in the event of data loss or disruption.
* ***RMF Control: SC-13 (Cryptographic Protections)***: Employ data encryption to protect sensitive data at rest and in transit, mitigating the risk of unauthorized access and data breaches.
* ***RMF Control: SI-4 (Intrusion Detection)***: Implement intrusion detection and prevention systems (IDS/IPS) to monitor for suspicious activity and prevent unauthorized access, reducing the risk of data loss or disruption.
* ***RMF Control: RA-5 (Vulnerability Scanning)***: Conduct regular vulnerability assessments and penetration testing to identify and remediate system weaknesses, minimizing the risk of exploitation by attackers.

1. **Malware and Ransomware (Medium Risk)**

* ***RMF Control: AC-21 (User Training)***: Develop and implement an incident response plan for handling malware and ransomware attacks, ensuring a timely and effective response to mitigate the impact of such incidents.
* ***RMF Control: CP-18 (Backup of Information)*** : Description: Back up data regularly to facilitate recovery in case of ransomware attacks, minimizing the risk of data loss and enabling business continuity.
* ***RMF Control: CM-6 (Software Patch Management)*** : Description: Patch systems and software promptly address known vulnerabilities that attackers might exploit through malware and ransomware attacks.
* ***RMF Control: AC-18 (Security Awareness and Training)***: Conduct regular security awareness training to educate employees on identifying and avoiding malware and ransomware threats, reducing the likelihood of successful attacks.

## Prioritization Rationale

The prioritization is based on the risk assessment scores, considering both the impact and likelihood of each threat:

1. **Security Breach (Phishing):**

* **Priority:** Medium-High.
* Medium-high risk score due to the potential for significant financial losses, reputational damage, and data breaches.

1. **Data Loss or Disruption:**

* **Priority:** High
* This risk score is High due to its potential for severe and widespread consequences across confidentiality, integrity, and availability.

1. **Malware and Ransomware:**

* **Priority**Medium
* The risk score is medium due to the potential for disruption and financial losses, but the likelihood might be mitigated through proactive security measures.

By focusing on mitigating the highest risk first (data loss or disruption), DHAEI can significantly improve its overall security posture and minimize the potential for devastating consequences. Addressing the other threats with appropriate measures further strengthens their security framework.

# Conclusion

Implementing this RMP will significantly enhance DHAEI's preparedness for potential threats. By proactively addressing risks and implementing mitigation strategies, DHAEI can protect its sensitive data, ensure business continuity, and safeguard its reputation.

# References

1. Tns. (2024, February 23). *2023 will go down for a Record-Setting number of data breaches*. Governing. <https://www.governing.com/management-and-administration/2023-will-go-down-for-record-setting-number-of-data-breaches#:~:text=There%20were%203%2C205%20data%20compromises,information%20and%20consumer%20data%20in>
2. Knowles, M. (2024, January 22). *Cybersecurity Risk Management: Frameworks, plans, & best practices*. Hyperproof. <https://hyperproof.io/resource/cybersecurity-risk-management-process/#:~:text=What%20is%20Cybersecurity%20Risk%20Management,has%20a%20role%20to%20play>.
3. *How to develop a cybersecurity Risk Management Plan*. (2023, October 24). Packetlabs. <https://www.packetlabs.net/posts/how-to-develop-a-cybersecurity-risk-management-plan/>
4. Rodrigues, J. (2023, November 23). *How to create an effective Cybersecurity Risk Management Plan*. TitanFile. <https://www.titanfile.com/blog/how-to-create-an-effective-cybersecurity-risk-management-plan/>
5. Chatterton, C. (2023, August 16). The Ultimate Guide to Risk Prioritization. Hyperproof. <https://hyperproof.io/resource/the-ultimate-guide-to-risk-prioritization/>
6. Cybersecurity Framework | NIST. (2024, April 25). NIST. <https://www.nist.gov/cyberframework>
7. Force, J. T. (2020). Control baselines for information systems and organizations. <https://doi.org/10.6028/nist.sp.800-53b>
8. Hanna, K. T. (2022, December 13). *ISO 27001*. WhatIs. <https://www.techtarget.com/whatis/definition/ISO-27001>