Risk Management Plan

DHA Enterprise Inc.

(ISO 27001 Framework)

Prepared by: Ifeanyi Christian Edeh

Cybersecurity Specialist

https://www.linkedin.com/in/ifeanyiedeh

Toolbox:

ISO 27001 Risk Management Framework

Date: March 19, 2025.

Table of Contents page

Executive Summary

DHA Enterprise Inc. (DHAEI) is a dynamic software development company based in Oshawa, Ontario, with several branch offices supporting an expanding client base. Since its founding in 2019, the company has focused on providing high-quality internet connectivity, web registration, and hosting services tailored to small office and home office (SOHO) users.

Over the years, DHAEI has built a strong digital presence that includes both on-premises infrastructure, primarily running Windows Server 2019, and cloud-based workloads hosted on Rackspace and Amazon Web Services (Amazon Web Services, 2023; Rackspace, 2023; Microsoft, 2023).

As the company continues to grow, it recognizes the importance of strong cybersecurity measures to maintain client trust and protect its operations. To address this, DHAEI is implementing a formal Risk Management Plan aligned with the ISO/IEC 27001 standard (ISO/IEC 27001, 2022). This framework will help the organization identify, evaluate, and manage potential vulnerabilities across all systems and locations.

The plan provides a clear roadmap for improving DHAEI's security posture. It highlights the most significant threats facing the company's infrastructure, including unauthorized data access and ransomware attacks, and assigns clear responsibilities for managing these risks from frontline security technicians to senior leadership (NIST, 2020). The plan also includes recommended measures to protect critical assets such as user data, physical and virtual servers, and cloud services. Each control is mapped to the relevant ISO 27001 requirements, ensuring compliance and alignment with recognized industry best practices (ISO/IEC 27001, 2022).

By integrating these strategies into everyday operations, DHAEI will strengthen its commitment to confidentiality, integrity, and availability. This proactive approach builds customer confidence and lays the foundation for continued growth and innovation.

1. Introduction

DHA Enterprise Inc. (DHAEI) is a dynamic software development organization headquartered in Oshawa, Ontario, with additional branch offices serving its growing client base. Established in 2019, the company delivers internet connectivity, web registration, and hosting services designed for small office/home office (SOHO) customers. DHAEI's environment comprises both on-premises Windows Server 2019 systems (Microsoft, 2023) and cloud workloads hosted on Rackspace and Amazon Web Services (AWS) (Amazon Web Services, 2023; Rackspace, 2023). Recognizing the importance of robust security, the company is now implementing a formal Risk Management Plan aligned with ISO/IEC 27001 standards (ISO/IEC 27001, 2022). This plan identifies critical risks, assigns responsibility for mitigating them, and details how each solution maps to relevant ISO 27001 controls (ISO/IEC 27001, 2022; NIST, 2020).

1.1 Purpose

- Establish a structured approach to identifying, assessing, and treating risks that threaten DHAEI's information systems.
- Ensure compliance with international standards, including ISO/IEC 27001.
- Protect critical assets and maintain stakeholder confidence in DHAEI's services.

1.2 Scope and Applicability

- Technical Scope: All servers (Windows Server 2019), workstations (Windows 10), domain controllers, cloud infrastructure (Rackspace, AWS), and supporting network infrastructure.
- Organizational Scope: Main office in Oshawa (1,500 users), multiple branch offices (200 users each), remote programmers (20) using L2TP VPN, and new Brampton branch requirements.
- Applicability: Management, IT, Security, and relevant branch technicians with direct involvement in risk identification, mitigation, and oversight.

1.3 Users and Stakeholders

- CEO (Alan Hake): High-level strategic oversight and final risk acceptance authority.
- CIO (Amanda Wilson): Aligns technology budgets and priorities with risk management.
- CISO (Paul Alexander): Oversees execution of the Risk Management Plan and ensures compliance.
- Security Technicians and Interns: Implement and manage security controls daily.
- Branch Office Technicians: Perform local maintenance and report on local security incidents.

2. Risk Assessment Methodology

DHAEI's approach is guided by ISO/IEC 27001, leveraging the following steps:

- Identify assets (tangible and intangible).
- Identify threats and vulnerabilities relevant to each asset.
- Analyze risk based on impact and likelihood.
- Determine risk ownership at various organizational levels.
- Define risk acceptance and treatment criteria.

2.1 Process and Involved Personnel

- **Process**:
    - Asset and Data Review: Catalog servers, endpoints, and services in main/branch offices and cloud environments.
    - Threat and Vulnerability Analysis: Evaluate potential risks (e.g., ransomware, insider threats, unauthorized data access, etc.).
    - Impact and Likelihood Assessment: Assign numerical values (0–10 for severity, 0–5 for probability).
    - Define Action: Accept, mitigate, transfer, or avoid each risk based on established thresholds.

- **Personnel:**
    - **Amanda Wilson** (CIO): Authorizes budgets and final strategic directions.
    - **Paul Alexander** (CISO): Conducts overarching risk analysis and orchestrates security measures.
    - **Security Technicians**: Provide technical data on vulnerabilities and assist in implementing mitigations.
    - **Branch Technicians**: Offer local insights into infrastructure status and user patterns.

2.2 Assets, Vulnerabilities, and Threats

Key Assets

- Active Directory Domain Controllers (DC1, DC2, RODCs)
- File Servers (FSI) and Branch Office Servers
- Cloud Services (AWS, Rackspace)
- VPN Infrastructure (L2TP for remote workers)

Potential Vulnerabilities

- Misconfiguration in domain controllers
- Inadequate encryption on file servers
- Weak credentials for remote access
- Insufficient patch management for servers and endpoints

Top 3 Threats

- Ransomware Attacks
    - Challenges: Could disrupt operations across multiple branches; branch technicians might lack advanced incident response training.
- Data Breaches/Unauthorized Access
    - Challenges: Regulatory compliance issues, especially with storing or transmitting data across main/branch offices and cloud.
- Service Disruption/Outage (e.g., DDoS or system failure)
    - Challenges: Potential downtime affecting 1,500 plus users in the main office, plus 200 in each branch.

2.3 Risk Ownership

Each risk has a defined chain of ownership:

- **Ground Level**:
    - Branch Technicians: Monitor local security events, apply OS patch updates, escalate issues.
    - Security Technicians: Perform vulnerability scanning, remediate findings, log incidents.
- **Mid-Level**:
    - Paul Alexander (CISO): Coordinates risk response strategies, ensures consistent control implementation.
- **Senior Executive**:
    - Amanda Wilson (CIO): Approves budget and major security changes, escalates to CEO if high-level acceptance is required.
    - CEO (Alan Hake): Holds ultimate responsibility for risk acceptance, especially for strategic or high-impact risks.

2.4 Impact and Likelihood

Risk	Confidentiality (0-10)	Integrity (0-10)	Availability (0-10)	Severity (0-10)	Likelihood (0-5)
Unauthorized Data Access	**9**	**8**	**7**	**9**	**4**
Malware / Ransomware	**8**	**9**	**10**	**9**	**3**
Infrastructure Failure	**5**	**6**	**10**	**8**	**3**

- **Severity: 0 = Minimal impact; 10 = Severe impact**
- **Likelihood: 0 = Unlikely; 5 = Highly Likely**

2.5 Risk Acceptance Criteria

DHAEI will prioritize risk treatment as follows:

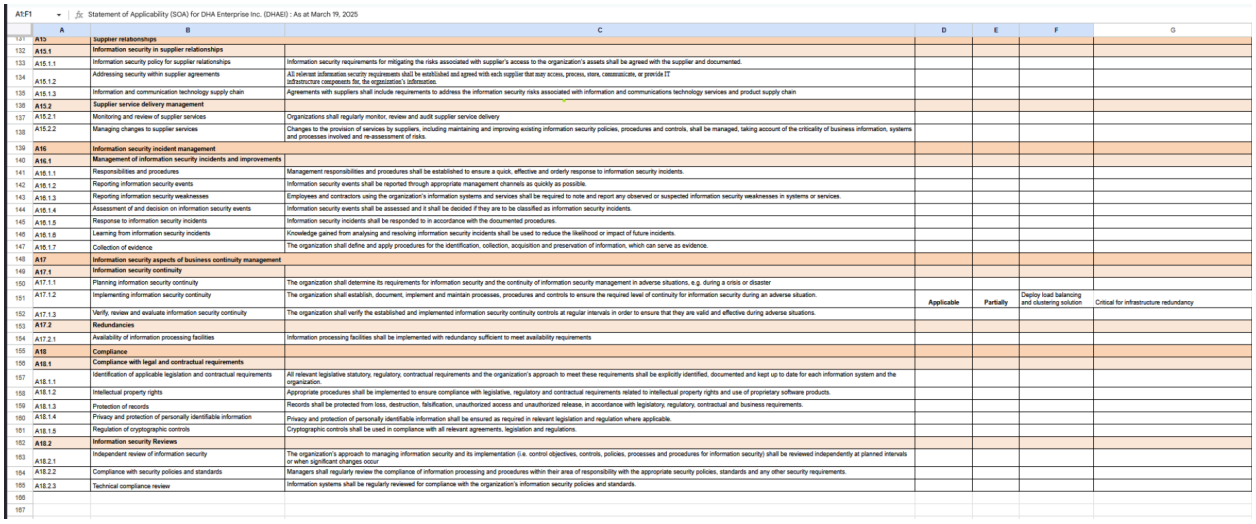
- High-Severity Risks (Score ≥ 8): Require immediate action (mitigate or transfer) due to major operational/financial impact.
- Moderate Risks (Score ~ 5–7): Addressed based on resource availability and operational priorities.
- Low Risks (Score ≤ 4): May be accepted if cost of mitigating exceeds potential loss or if controls are impractical.

Highest priority will be given to unauthorized data access and ransomware threats due to severe business and regulatory implications. Infrastructure failures are important but can be addressed progressively based on cost-benefit analyses.

3. Statement of Applicability (SOA)

As part of the information security risk management project for DHA Enterprises Inc., I conducted a comprehensive controls assessment and documented the status of security measures in a formal Statement of Applicability (SoA). The process and findings are visually supported by the following SoA file screenshots:

Figure 1: This screenshot displays how we mapped supplier management, incident handling, and compliance controls, identifying areas where controls were fully in place or needed further development.



A1:F1 | Statement of Applicability (SOA) for DHA Enterprise Inc. (DHAEI) : As at March 19, 2025

	A	B	C	D	E	F	G
131	**A15**	**Supplier relationships**					
132	**A15.1**	**Information security in supplier relationships**					
133	A15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.				
134	A15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.				
135	A15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain				
136	**A15.2**	**Supplier service delivery management**					
137	A15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery				
138	A15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.				
139	**A16**	**Information security incident management**					
140	**A16.1**	**Management of information security incidents and improvements**					
141	A16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.				
142	A16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.				
143	A16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.				
144	A16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.				
145	A16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.				
146	A16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.				
147	A16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.				
148	**A17**	**Information security aspects of business continuity management**					
149	**A17.1**	**Information security continuity**					
150	A17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster				
151	A17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	**Applicable**	**Partially**	Deploy load balancing and clustering solution	Critical for infrastructure redundancy
152	A17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.				
153	**A17.2**	**Redundancies**					
154	A17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements				
155	**A18**	**Compliance**					
156	**A18.1**	**Compliance with legal and contractual requirements**					
157	A18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.				
158	A18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.				
159	A18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.				
160	A18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.				
161	A18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.				
162	**A18.2**	**Information security Reviews**					
163	A18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur				
164	A18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.				
165	A18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.				
166							
167							

Figure 2: Here, you can see the evaluation of operational procedures, asset management, and network security controls, with clear indications of partial implementations and improvement needs.

A1:F1 | Statement of Applicability (SOA) for DHA Enterprise Inc. (DHAEI) : As at March 19, 2025

	A	B	C	D	E	F	G
76	A11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.				
77	A11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorisation.				
78	A11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.				
79	A11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.				
80	A11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.				
81	A11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.				
82	**A12**	**Operations Security**					
83	**A12.1**	**Operational procedures and responsibilities**					
84	A12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.				
85	A12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.				
86	A12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.				
87	A12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.				
88	**A12.2**	**Protection from malware**					
89	A12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.				
90	**A12.3**	**Backup**					
91	A12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	**Applicable**	**Partially**	Implement offsite encrypted backups	Required for recovery from ransomware or malware
92	**A12.4**	**Logging and monitoring**					
93	A12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.				
94	A12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.				
95	A12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.				
96	A12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.				
97	**A12.5**	**Control of operational software**					
98	A12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.				
99	**A12.6**	**Technical Vulnerability Management**					
100	A12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.				
101	A12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.				
102	**A12.7**	**Information systems audit considerations**					
103	A12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.				
104	**A13**	**Communications security**					
105	**A13.1**	**Network security management**					
106	A13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.				
107	A13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.				
108	A13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.				
109	**A13.2**	**Information transfer**					
110	A13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.				
111	A13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.				
112	A13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.				
113	A13.2.4	Confidentiality or non- disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.				

Figure 3: This final screenshot highlights our review of access control management, cryptographic controls, and physical security, offering a detailed look at our user management and data protection practices.

A1:F1 | Statement of Applicability (SOA) for DHA Enterprise Inc. (DHAEI) : As at March 19, 2025

	A	B	C	D	E	F	G
47	A9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.				
48	A9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.				
49	A9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.				
50	A9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.				
51	A9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.				
52	**A9.3**	**User responsibilities**					
53	A9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.				
54	**A9.4**	**System and application access control**					
55	A9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.				
56	A9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Applicable	Partially	Expand MFA to all privileged accounts	Required to reduce unauthorized data access
57	A9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.				
58	A9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.				
59	A9.4.5	Access control to program source code	Access to program source code shall be restricted.				
60	**A10**	**Cryptography**					
61	**A10.1**	**Cryptography controls**					
62	A10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.				
63	A10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.				
64	**A11**	**Physical and environmental security**					
65	**A11.1**	**Secure areas**					
66	A11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.				
67	A11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.				
68	A11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.				
69	A11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.				
70	A11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.				
71	A11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.				
72	**A11.2**	**Equipment**					
73	A11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.				
74	A11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.				
75	A11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.				
76	A11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.				
77	A11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorisation.				
78	A11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.				
79	A11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.				
80	A11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.				
81	A11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.				
82	**A12**	**Operations Security**					
83	**A12.1**	**Operational procedures and responsibilities**					
84	A12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.				
85	A12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.				
86			The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance				

These referenced SOA screenshots illustrate the rigorous approach taken to evaluate, document, and prioritize security controls, ensuring DHA Enterprises Inc. meets both operational needs and regulatory requirements in its risk management efforts.

Please refer to the link below for the complete Statement of Applicability (SOA).

Statement of Applicability (SOA) for DHA Enterprise Inc. (DHAEI)

4. Risk Treatment

4.1 Threats and Recommended Mitigations

Threat 1: Ransomware Attack (High Severity)

- **Mitigation Strategies:**
  - Endpoint Detection and Response (EDR) solutions on all workstations.
  - Encrypted, regular backups (onsite/offsite).
  - Enhanced staff training on phishing awareness.

Threat 2: Data Breach/Unauthorized Access (Moderate–High Severity)

- **Mitigation Strategies:**
  - Implement MFA for remote and privileged logins.
  - Enforce strict AD Group Policies (password complexity, account lockouts).
  - Use file-level or volume-level encryption (BitLocker on Windows Server 2019).

Threat 3: Service Disruption/Outage (Moderate–High Severity)

- **Mitigation Strategies:**
  - Redundant network links; load balancing for critical systems (e.g., DC1/DC2).
  - Implement cluster management for the RODC environment to reduce single points of failure.
  - Regular testing of DR/BCP (Disaster Recovery/Business Continuity Plan).

4.2 Prioritization and Justification

- **Ransomware Attack** – Highest priority: Potential to halt operations across multiple branches.
  - ❖ **Rationale:** Malware significantly impacts availability and integrity of critical business data, causing operational disruption (ISO/IEC 27001 Controls A.12.3.1, A.12.2.1).
- **Data Breach** – Equally critical from a regulatory standpoint, but immediate operational impact may be lower than ransomware.
  - ❖ **Rationale:** Regulatory compliance requirements and severe reputational damage if data is compromised (ISO/IEC 27001 Control A.9.4.2).
- **Service Outage** – Infrastructure disruptions are highly impactful but can be mitigated with robust redundancy and DR strategies.
  - ❖ **Rationale:** Ensuring continuous business operation reduces customer dissatisfaction risks, but can be phased in based on budgetary constraints (ISO/IEC 27001 Control A.17.1.2)

Conclusion

This ISO 27001-aligned Risk Management Plan offers DHA Enterprise Inc. (DHAEI) a clear and methodical framework for safeguarding its information systems and digital assets against emerging cybersecurity threats (ISO/IEC 27001, 2022). By prioritizing ransomware prevention, stringent unauthorized access controls, and robust infrastructure redundancy, DHAEI positions itself effectively to sustain uninterrupted operations and proactively meet the evolving demands of its growing user base (NIST, 2020; Microsoft, 2023).

Moreover, this plan underscores the company's strong commitment to upholding recognized industry best practices and actively mitigating potential vulnerabilities across both on-premises and cloud environments, including workloads hosted on AWS and Rackspace (Amazon Web Services, 2023; Rackspace, 2023). Regular review and updates to this Risk Management Plan ensure DHAEI remains agile, resilient, and capable of seamlessly adapting to the challenges inherent in expanding its branch offices and deepening its reliance on cloud-based services.

Ultimately, the continued success of DHAEI hinges upon its capability to secure mission-critical data, maintain compliance with ISO 27001 standards, and consistently deliver reliable services to its clients (ISO/IEC 27001, 2022). This comprehensive Risk Management Plan not only addresses immediate cybersecurity concerns but also establishes a foundational framework for ongoing cybersecurity excellence, vital to DHAEI's long-term innovation, stability, and growth.

References

1. Amazon Web Services. (2023). *AWS security best practices*. Retrieved from https://aws.amazon.com/security/

2. ISO/IEC 27001. (2022). *Information security management systems – Requirements (ISO/IEC 27001:2022)*. International Organization for Standardization. Retrieved from https://www.iso.org/standard/27001

3. Microsoft. (2023). *Windows Server security best practices*. Retrieved from https://learn.microsoft.com/en-us/windows-server/security/

4. National Institute of Standards and Technology. (2020). *NIST SP 800-53 (Rev.5) – Security and Privacy Controls for Federal Information Systems and Organizations.* Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

5. Rackspace. (2023). *Security and compliance for Rackspace products*. Retrieved from https://docs.rackspace.com/security/