**Risk Management Plan for DHAEI**

**Presented by: Reniel Villahermosa**

**Table of Contents**

—----------------------------------------------------------------------------------------------------------------------------

Executive Summary……………………………………………………………………………………..3

1. Purpose, Scope and Users………………………………………………………………………… 4

2. Risk Assessment and Risk Treatment Methodology……………………………………………..5

* 2.1 Risk Assessment…………………………………………………………………………...5

1. The process…………………………………………………………………………….5
2. Assets, vulnerabilities and threats…………………………………………………...6
3. Determining the risk owners………………………………………………………….7
4. Impact and Likelihood…………………………………………………………………8
5. Risk Acceptance Criteria……………………………………………………………..9

* 2.2 Risk Treatment…………………………………………………………………………….10

3.Conclusion……………………………………………………………………………………………12

4. Citations………………………………………………………………………………………………13

# 

# 

# 

**Executive Summary**:

The Executive Summary for the Risk Management Plan of DHA Enterprise Inc. (DHAEI) encapsulates our strategic approach towards establishing a resilient and responsive cybersecurity posture that is vital for safeguarding our organizational assets. This plan describes our methodologies for identifying, evaluating, and mitigating risks across our comprehensive suite of software services, ensuring that our practices are in firm alignment with industry benchmarks such as ISO 27001 and NIST frameworks. It underscores the significance of protecting the confidentiality, integrity, and availability of our systems and data amidst an evolving threat landscape. Our commitment to rigorous risk management is integral to maintaining operational excellence, upholding client trust, and fostering robust growth. This document not only charts a path for navigating the complexities of information security but also serves as a testament to DHAEI’s dedication to a culture of continuous improvement and best in class service delivery.

**1. Purpose, Scope, and Users**

**Purpose**:

The purpose of DHAEI's Risk Management Plan is to fortify our organization's defenses against the spectrum of cyber risks that accompany the digital age. Rooted in industry best practices and regulatory standards, this plan is our blueprint for identifying and assessing threats, vulnerabilities, and the impact of potential security incidents on our operations. It outlines a structured approach to risk evaluation and treatment, ensuring that strategic decisions are made with a comprehensive understanding of our cyber risk landscape. By integrating risk management into the core of our business strategy, we aim to protect vital assets, maintain operational integrity, and instill an organizational culture aware to security mindfulness. This plan is not just a procedural document; it is a commitment to safeguarding the trust placed in us by our clients, employees, and stakeholders, thereby guaranteeing the continued success and resilience of DHA Enterprise Inc.

**Scope:**

The scope of DHAEI's Risk Management Plan encompasses every fpart of our technological infrastructure, operational processes, and human resources. It extends from our core IT systems, across networked and standalone devices, to the cloud services and software applications that drive our business forward. This comprehensive extent ensures that from our headquarters to remote work environments, every point of data exchange, storage, and processing falls within our protective measures. Furthermore, the plan covers the lifecycle of information handling within DHAEI, from creation and use to transmission and destruction, ensuring a holistic approach to risk management.

**Users**:

The users of this plan are as diverse as our operations, including every DHAEI employee, from top executives who leverage it for strategic oversight, to the IT staff who implement its guidelines daily. Additionally, our external partners, vendors, and clients interact with aspects of the plan through their engagement with our systems and protocols, necessitating their understanding and cooperation in our risk management efforts. By presenting clear roles, responsibilities, and expectations for each user group, the plan fosters a culture of security awareness and collective vigilance against cyber threats, making every stakeholder a custodian of DHAEI’s cybersecurity posture.

**2. Risk Assessment and Risk Treatment Methodology**

**2.1 Risk Assessment**:

a) *The process*

For the risk assessment process at DHA Enterprise Inc., a multi-layered approach is adopted, involving strategic planning, technical evaluation, and organizational alignment with business objectives. This in depth analysis involves key personnal who contribute unique expertise to the risk management framework.

**Amanda Wilson (CIO): Strategic Alignment and Oversight**

Amanda Wilson, as the Chief Information Officer, plays a strategic role in the risk assessment process. Her responsibilities include setting the overall direction for the company’s cybersecurity initiatives, aligning IT security with business goals, and ensuring that the risk management strategies are proactive and responsive to the latest threat landscape. Amanda is tasked with integrating risk management into the broader business continuity planning, requiring her to collaborate closely with other executives to balance risk mitigation with operational efficiency and innovation. Her leadership in establishing and maintaining a security conscious culture is vital, as it directly impacts the enterprise’s resilience against cyber threats.

**Paul Alexander (CISO): Framework Definition and Risk Prioritization**

As the Chief Information Security Officer, Paul Alexander is at the core of the risk assessment execution. He is responsible for identifying the specific cybersecurity frameworks and standards, such as NIST or ISO/IEC 27001, that the organization will adopt. Paul leads the efforts in vulnerability identification and threat analysis, working with his team to conduct comprehensive evaluations of the enterprise’s digital assets. His role involves not only the identification of potential risks but also the development of a prioritized list of risks based on their likelihood and potential impact. This prioritization is crucial for efficient resource allocation and defines the focus areas for the technical teams. Paul’s expertise also guides the creation of response strategies and the development of a clear communication plan to report findings to the CIO and other stakeholders.

**William Freund (Manager of Systems): Technical Assessment and Mitigation Strategy Implementation**

William Freund oversees the practical aspects of the risk assessment process. As the Manager of Systems, he ensures that the technical environment is thoroughly scanned for vulnerabilities and that system defenses are both robust and adaptable. William’s team is responsible for implementing security controls based on the risk assessment outcomes and ensuring that all system patches and updates are deployed effectively to mitigate identified risks. He faces the challenge of managing the day-to-day security posture while also responding to emerging threats, requiring speed and a comprehensive understanding of both the organization’s technology stack and the evolving cybersecurity domain. His direct involvement is key in bridging the gap between strategic risk management goals and operational execution.

The combination of strategic, technical, and operational insights provided by Amanda, Paul, and William ensures a comprehensive risk assessment process at DHA Enterprise Inc. This collaborative approach ensures that risks are not only identified and evaluated but also that the mitigation strategies are effectively integrated into the company’s operations, reinforcing a robust cybersecurity posture that supports DHA Enterprise’s continued success.

b) *Assets, vulnerabilities, and threats*:

Considering the wide range of cyber threats facing modern enterprises, here are three significant threats that DHA Enterprise may encounter, along with the associated challenges in managing them:

1. **Advanced Persistent Threats (APTs):** APTs are sophisticated, long-term hacking processes where attackers infiltrate a network to steal information or monitor activities without being detected. For DHA Enterprise, the challenge with APTs lies in their stealth and persistence. Unlike other cyber attacks that seek immediate financial gain, APTs aim for long-term espionage, making them harder to detect and eradicate. Addressing APTs requires a robust security infrastructure, continuous monitoring, and the ability to rapidly respond to incidents, which can be resource-intensive.

2. **Supply Chain Attacks**: As enterprises increasingly rely on external vendors and service providers, the risk of supply chain attacks has escalated. These attacks occur when a trusted third-party is compromised, providing a backdoor into the primary target’s systems. The challenge for DHA Enterprise in managing this threat lies in the need to extend their cybersecurity practices beyond their immediate environment to their partners and suppliers. This involves conducting regular security assessments of partners, implementing stringent security requirements, and continuously monitoring the supply chain for potentil vulnerabilities.

3. **Cloud Storage/Data Breach**: As organizations migrate more of their operations and data storage to the cloud, the potential impact of breaches in these environments grows. For DHA Enterprise, the challenge is varied, involving the secure configuration of cloud services, ensuring that access controls are properly implemented, and that data is encrypted both at rest and in transit. Managing this threat requires a deep understanding of cloud architecture and the shared responsibility model of cloud security, as well as constant vigilance to adapt to new vulnerabilities and threats targeting cloud platforms.

Each of these threats presents unique challenges, requiring DHA Enterprise to deploy a combination of technical safeguards, procedural policies, and continuous education to protect against sophisticated cyber adversaries. The key to managing these threats effectively lies in adopting a complete and adaptive security strategy that considers not just the technology, but also the human and procedural aspects of cybersecurity.

c) *Determining the risk owners*:

Creating a "chain" of risk ownership from the ground level to the senior executive level involves describing clear roles and responsibilities across various tiers of the organization. Here’s an in-depth approach tailored for DHA Enterprise:

1. **Ground Level - IT Support Staff/Technicians**(Harold Fry): Individuals in this role are at the forefront of risk detection. Their daily interactions with technology make them pivotal in spotting anomalies. They contribute to the chain of risk ownership by implementing and adhering to operational security protocols, reporting incidents, and ensuring that the first line of defense against cyber threats is robust.

2. **Middle Management - IT Managers/Cybersecurity Analysts (Paul Alexander CISO)**: This group translates the company’s cybersecurity policies into actionable procedures and oversees the implementation of security measures. They play a key role in risk ownership by monitoring the effectiveness of security protocols, coordinating security initiatives, and providing training to lower-level staff. They are the anchor in communicating upward and downward to ensure that security measures are understood and enacted effectively.

3. **Senior Management - Chief Information Security Officer (CISO)**: The CISO is responsible for the overall cybersecurity posture of the organization. In terms of risk ownership, the CISO develops the overarching cybersecurity strategy, aligns it with the organization's business objectives, and ensures that risks are managed according to regulatory and compliance requirements. They are tasked with the strategic distribution of resources to mitigate risks and must be prepared to communicate the state of cybersecurity to other C-level executives and the board.

4. **Executive Level - CEO/Board of Directors (Amanda Wilson (CIO)**: At the top of the risk ownership chain, the CEO and Board of Directors have the ultimate responsibility for the risk management framework as it relates to the organization’s strategic vision and objectives. They ensure that cybersecurity is given due consideration in all business decisions and that sufficient resources are allocated for its implementation. Their understanding of risk assessments and management plans is critical for making informed decisions that could impact the entire organization.

In this structured chain, each level contributes by executing their specific roles, maintaining constant communication, and ensuring that cybersecurity is integrated into all business processes. This collaborative approach ensures that risk ownership is not siloed but is a shared responsibility across the organization, fostering a culture where cybersecurity is a fundamental aspect of every role.

d) *Impact & Likelihood*:

This table outlines the potential effects of these risks on the confidentiality, integrity, and availability (CIA) of DHA Enterprise’s systems and data, quantifying the extent of impact from 0 (no impact) to 10 (maximum impact), and assessing the likelihood of occurrence from 0 (unlikely) to 5 (almost certain). Each risk has been carefully analyzed to reflect DHA Enterprise’s specific operational context, providing a clear prioritization basis for addressing the most critical threats first.

| **Threat/Risk** | **Impact on Confidentiality (0-10)** | **Impact on Integrity (0-10)** | **Impact on Availability (0-10)** | **Likelihood (0-5)** |
| --- | --- | --- | --- | --- |
| Advanced Persistent Threat (APT) | 9 | 7 | 6 | 4 |
| Supply Chain Attack | 8 | 8 | 7 | 3 |
| Cloud Data Breach | 7 | 7 | 9 | 4 |

Explanation on threats/risks:

To deeply understand the impact on Confidentiality, Integrity, and Availability (CIA) for each identified threat in DHA Enterprise Inc., we consider how each component of CIA could be compromised:

**Advanced Persistent Threats (APTs)**:

- **Confidentiality**: The stealthy nature of APTs often targets the unauthorized access and exfiltration of sensitive information. With an impact score of 9, this threat can lead to significant breaches of confidentiality as attackers gain prolonged, unauthorized access to company secrets, client data, and intellectual property.

- **Integrity**: At 7, the impact on integrity is notable due to APTs’ potential to alter data covertly. This manipulation can have profound effects on business decisions, financial reporting, and trust in the integrity of the systems.

- **Availability**: With an impact score of 6, APTs can also disrupt services by utilizing network resources for data exfiltration or by corrupting systems as part of their attack, although their primary goal is often not to disrupt operations but to remain undetected.

**Supply Chain Attacks:**

- **Confidentiality**: This risk is given an 8 for impact on confidentiality since attackers often compromise the supply chain to infiltrate an organization’s network and steal sensitive information passed along the supply chain.

- **Integrity**: An impact score of 8 is assigned as these attacks can introduce tampered hardware or software into the enterprise’s environment, leading to the potential for malicious actors to manipulate operations or data flows without immediate detection.

- **Availability**: Supply chain attacks have an impact score of 7 on availability, as they can disrupt operations not just within a single organization but across multiple entities that are part of the supply chain.

**Cloud Data Breaches**:

- **Confidentiality**: With an impact of 7, cloud data breaches directly threaten the privacy and security of information stored off-premises. In cases where sensitive data is exposed, this can lead to significant loss of customer trust and potential regulatory penalties.

- **Integrity**: Similarly, the integrity score of 7 denotes the potential for compromised data within the cloud to be altered or deleted, which could disrupt the business processes that depend on this data.

- **Availability**: With the highest impact score of 9, the availability concerns with cloud data breaches stem from the potential for extensive downtime or loss of access to critical data and applications, which can halt business operations and incur substantial financial losses.

The likelihood scores for these threats are derived from an evaluation of the current threat landscape and the specific vulnerabilities present within DHA Enterprise Inc.’s systems. APTs and Cloud Data Breaches both score a 4 out of 5 in likelihood due to the increasing prevalence of sophisticated cyber-attacks and the growing reliance on cloud infrastructure. Supply Chain Attacks are given a slightly lower likelihood score of 3, which still signifies a significant risk, especially given recent high-profile incidents in the global supply chain.

This assessment underscores the need for a robust cybersecurity framework at DHA Enterprise Inc., where protective measures are continuously evaluated and updated in response to an evolving threat landscape. It also highlights the need for incident response plans and business continuity strategies to mitigate the potential impact on the organization’s CIA.

e) *Risk Acceptance criteria:*

In the context of risk management for DHA Enterprise, the acceptance criteria for risks involve determining which risks can be tolerated based on their impact and likelihood, balanced against the cost and effort required for mitigation. It’s a decision that must take into account the organization’s risk appetite, the potential impact on business objectives, and the feasibility of control measures.

For example, the most likely and highest impact risk identified might be a Cloud Data Breach, given its significant potential impact on Availability (rated 9 out of 10), with a relatively high likelihood of occurrence (rated 4 out of 5). Such a breach could lead to extensive service downtime, loss of customer trust, regulatory repercussions, and financial losses, directly affecting DHA Enterprise’s core operations and reputation. Therefore, this risk might be prioritized for active treatment measures such as implementing robust encryption, regular security audits, and comprehensive incident response planning.

Conversely, certain lower-impact or lower-likelihood risks might be candidates for acceptance or minimal action. For instance, suppose a risk is identified with a low impact on the organization's CIA and low likelihood of occurrence, such as a minor system glitch that causes negligible downtime. In that case, the cost of mitigating this risk might outweigh the benefit. The decision to “ignore” or minimize action on such risks is based on a thorough understanding that not all risks can or should be fully eliminated, but rather managed in accordance with the organization’s capacity to absorb and respond to them.

This nuanced approach to risk acceptance must be documented and regularly reviewed, ensuring it aligns with DHA Enterprise's evolving business strategies and the dynamic nature of cyber threats. Such a policy allows for efficient resource allocation and ensures that management efforts are focused on the most significant risks, while minor risks are monitored but not necessarily eliminated.

**2.2 Risk Treatment**

In embracing these responses, we interweave the technical with the human element. It's about creating an environment where technology serves as the formidable wall, and our people are the gatekeepers. It's a continuous journey of vigilance, learning, and adaptation, ensuring that DHA Enterprise stands resilient in the face of cyber threats. The explanation of the threats are as follows:

**1. Advanced Persistent Threats (APTs)**:

**Priority**: High

**Mitigation and Response**: To counter APTs, implement robust network monitoring and endpoint protection systems that leverage behavioral analysis to detect anomalies indicative of such threats. Regularly update and patch systems and conduct comprehensive network security audits. For APTs that evade initial defenses, an incident response plan should be in place, developed following NIST SP 800-61 guidelines, which emphasize the importance of preparation, detection, analysis, containment, eradication, and recovery.

The specter of APTs is akin to a constant shadow looming over our digital corridors – silent, persistent, and potentially devastating. Given the high priority of this threat, our response must be multifaceted and unwavering. We'll deploy state-of-the-art intrusion detection systems to serve as our digital sentinels, ever-watchful for the subtle indicators of a breach. Our team will engage in regular 'cyber fire drills,' following the meticulous protocols set forth in the NIST guidelines, to ensure readiness and resilience. We will not only safeguard our systems but also cultivate a culture where every employee is a vigilant guardian of our digital domain, capable of recognizing and reporting the faintest whisper of an anomaly.

**2. Supply Chain Attacks**:

**Priority**: High

**Mitigation and Response**: Establish rigorous security protocols for all vendors, including periodic security assessments as per ISO/IEC 27001 requirements, to ensure compliance with your security standards. Implement a segmented network architecture to limit the spread of any potential breaches, and employ continuous monitoring of network traffic to and from third-party systems. Use threat intelligence services to stay informed of potential supply chain threats and encourage a policy of transparency and quick communication with vendors.

In today’s interconnected world, a risk to our suppliers is a risk to us – the chain is only as strong as its weakest link. Thus, managing supply chain attacks is high on our agenda. Our strategy extends beyond our immediate network, ensuring that every partner weaves security into their fabric as tightly as we do ours. We'll conduct thorough security assessments and demand transparency, establishing a mutual commitment to safeguard our shared digital ecosystem. It's about nurturing a symbiotic relationship where security is a shared value, and every alert from our partners is treated with the same urgency as our own.

**3. Cloud Data Breaches**:

**Priority**: High

**Mitigation and Response:** Leverage encryption for data at rest and in transit, following best practices outlined in NIST SP 800-145. Ensure that access controls are in place to limit data exposure to unauthorized users, guided by the principle of least privilege. Employ Cloud Access Security Brokers (CASBs) to enforce policy across cloud environments and conduct regular vulnerability assessments of cloud resources. Furthermore, establish a comprehensive cloud security governance framework that includes backup and recovery procedures, as recommended by ISO/IEC 27017, which focuses on the security of cloud services.

The cloud is our sky-high fortress of data, yet it's vulnerable to storms of cyber threats. Protecting this realm is paramount, so we treat cloud data breaches with the highest priority. Our strategy encompasses encryption that's akin to an unbreakable seal on our treasure clutter of data, and access controls that serve as the judicious gatekeepers. We adopt the wisdom of ISO/IEC 27017 to craft a security governance model that's both robust and nimble, adapting to the cloud’s ever-changing winds. We recognize the trust our clients place in us to safeguard their data and uphold that trust with unwavering commitment and state-of-the-art security measures.

**Conclusion**

In treating these risks, it's crucial to prioritize based on the potential impact on the organization’s operations and the likelihood of occurrence. High-priority risks such as APTs and Cloud Data Breaches necessitate immediate and continuous attention due to their severe implications and the evolving nature of these threats. The recommended responses are not static; they require ongoing evaluation and adaptation in line with emerging threats and technological advancements. This dynamic approach ensures DHA Enterprise maintains a strong security posture and resilience against cyber threats.

In embracing these responses, we interweave the technical with the human element. It's about creating an environment where technology serves as the formidable wall, and our people are the gatekeepers. It's a continuous journey of vigilance, learning, and adaptation, ensuring that DHA Enterprise stands resilient in the face of cyber threats.

**Citations**

* National Institute of Standards and Technology. (2020). Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 (5th ed.). <https://doi.org/10.6028/NIST.SP.800-53r5>
* International Organization for Standardization. (2013). ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements.
* National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing, NIST Special Publication 800-145. <https://doi.org/10.6028/NIST.SP.800-145>
* International Organization for Standardization. (2015). ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
* Imperva. (n.d.). Cyber Threats: Protecting Your Organization from Cyber Crime. Retrieved 2024, April, from <https://www.imperva.com/learn/data-security/cybersecurity-risk-management/>
* To cite the GetApp webpage in APA format, you would structure the citation as follows:
* GetApp. (n.d.). Reviewing the 5 Stages of the Cybersecurity Lifecycle. Retrieved 2024, April, from <https://www.getapp.com/resources/cybersecurity-lifecycle/>