## Executive Summary

# Executive Summary

## Introduction

This cyber risk assessment report has been meticulously prepared for our organization to evaluate the cybersecurity risk landscape associated with our critical IT assets and systems. The assessment was conducted following a comprehensive process that involved identifying and prioritizing assets based on their criticality to business functions, evaluating the size and rating of their attack surfaces, assessing potential attack vectors, and considering the effectiveness of existing mitigations and remediations. This process was underpinned by a robust risk scoring algorithm designed to quantify the level of risk associated with each asset or system in a consistent and objective manner.

### Risk Scoring Algorithm

The risk scoring algorithm employed in this assessment is derived from a combination of the criticality rating of the asset, the size and rating of the attack surface, the attack vector rating, and the effectiveness of implemented mitigations and remediations. Each factor was assigned a numerical value on a scale from 1 to 3, with 3 indicating the highest level of concern. These values were then weighted according to their impact on the overall risk posture, with criticality and attack surface rating being given the highest weight. The formula used to calculate the risk score is as follows:

\[ \text{Risk Score} = \left( \text{Criticality Rating} \times 0.4 \right) + \left( \text{Attack Surface Rating} \times 0.3 \right) + \left( \text{Attack Vector Rating} \times 0.2 \right) + \left( \text{Mitigations Effectiveness} \times 0.1 \right) \]

This scoring method ensures a balanced consideration of both the inherent risks associated with each asset and the effectiveness of the controls in place to mitigate those risks.

## Key Findings

The assessment revealed that the majority of our high-priority assets and systems, including Database Server 1, Payment Gateway, ERP System, and Web Server 1, have been assigned a risk score of 9. This indicates a high level of residual risk despite the criticality of these assets to our business functions and the presence of mitigations and remediations. The primary drivers for these high-risk scores are the critical attack surface ratings and high attack vector ratings, signifying that these assets are highly attractive targets for adversaries and are susceptible to a range of attack methodologies.

Assets such as the Networking Switch and Router received slightly lower risk scores of 8, primarily due to their medium attack surface size, which slightly reduces their attractiveness to attackers compared to the higher-rated assets.

Lower-priority assets, including IoT Device 1, Virtual Machine 1, Workstation 1, and Print Server, have been assigned risk scores ranging from 3, reflecting their lower criticality to business operations and smaller attack surfaces. However, it is important to note that no asset is without risk, and the low scores do not imply the absence of the need for vigilance and ongoing risk management.

## Conclusion

The findings of this cyber risk assessment underscore the necessity for a dynamic and proactive approach to managing cybersecurity risks across our organization. While the implementation of mitigations and remediations has been effective in reducing the risk to an extent, the persistently high risk scores for our most critical assets highlight areas where further improvements are needed. It is recommended that the organization continues to invest in strengthening its cybersecurity posture through continuous monitoring, regular updates to security controls, and adherence to cybersecurity best practices.

This executive summary provides a high-level overview of the assessment's outcomes and key findings. Detailed analysis and recommendations for each assessed asset and system are provided in the subsequent sections of the report.

## Introduction

# Cyber Risk Assessment Report

## Introduction

This cyber risk assessment report has been meticulously prepared for [Organization Name], following a comprehensive evaluation of its digital infrastructure to identify, analyze, and prioritize the cybersecurity risks associated with its critical assets and systems. The primary objective of this assessment is to provide actionable insights and recommendations that will enhance the organization's cybersecurity posture, ensuring the protection of its critical information assets against potential threats and vulnerabilities.

### Assessment Context

The assessment was conducted over a period of [specific period, e.g., four weeks], covering a wide range of assets and systems critical to the organization's operations. These assets include, but are not limited to, database servers, payment gateways, enterprise resource planning (ERP) systems, web servers, cloud storage solutions, network infrastructure components, and various software applications essential for daily business functions. Each asset was evaluated based on its criticality to the business, the size and rating of its attack surface, potential attack vectors, and the effectiveness of existing mitigations and remediations.

### Process Followed

The assessment process adhered to industry-standard methodologies and best practices, incorporating elements from frameworks such as NIST SP 800-30 and ISO/IEC 27005. The process involved the following key steps:

1. \*\*Asset Identification:\*\* Comprehensive inventory of all digital assets and systems, categorizing them based on their type, business function, and criticality.

2. \*\*Threat and Vulnerability Analysis:\*\* Evaluation of each asset to identify potential threats and vulnerabilities, considering factors such as attack surface size and rating, as well as attack vector rating.

3. \*\*Risk Scoring:\*\* Application of a risk scoring algorithm to quantify the cybersecurity risk associated with each asset, facilitating prioritization.

4. \*\*Mitigations and Remediations:\*\* Documentation of existing mitigations and remediations in place for each asset, assessing their effectiveness in reducing risk.

### Risk Scoring Algorithm

The risk scoring algorithm developed for this assessment is designed to provide a quantifiable measure of cybersecurity risk, enabling the prioritization of risks based on their severity. The algorithm considers the following factors:

- \*\*Criticality Rating (CR):\*\* The importance of the asset to business operations, on a scale from Low (1) to High (3).

- \*\*Attack Surface Size (ASS):\*\* The extent of the asset's exposure to potential attacks, normalized to a scale of 1 to 3, with 3 representing a larger attack surface.

- \*\*Attack Surface Rating (ASR):\*\* The vulnerability of the attack surface, rated as Low (1), Medium (2), or High (3).

- \*\*Attack Vector Rating (AVR):\*\* The likelihood of an attack vector being successfully exploited, rated as Low (1), Medium (2), or High (3).

The risk score is calculated using the formula: \*\*Risk Score = (CR \* ASS \* ASR \* AVR) / 3\*\*, resulting in a score ranging from 1 to 9, with 9 indicating the highest level of risk.

### System Data

The assessment covered a total of 20 assets/systems, each meticulously evaluated according to the criteria outlined above. The resulting data, detailed in the subsequent sections of this report, provides a comprehensive overview of the cybersecurity risks facing [Organization Name], along with prioritized recommendations for mitigating these risks.

This introduction sets the stage for a detailed discussion on the findings and recommendations that will follow in the subsequent sections of the report.

## Asset Discovery/Identification

### Asset Discovery/Identification

#### Introduction to Asset Discovery and Identification Process

The Asset Discovery and Identification process is a foundational step in our cyber risk assessment report. It involves a comprehensive inventory of all assets within the organization's environment that could impact the security posture. This process is critical for understanding the scope of potential vulnerabilities and for prioritizing risk management efforts. The methodology followed for asset discovery and identification in this assessment involved both automated and manual techniques, including network scanning tools, physical inspections, and consultations with department heads to ensure a complete inventory.

The resulting data from this process includes a detailed list of assets, categorized by type, criticality, and function within the business. Each asset has been assigned a criticality rating based on its importance to business operations and its potential impact on the organization's objectives if compromised. Additionally, we have evaluated the attack surface size and rating, which reflects the potential exposure of each asset to cyber threats, and the attack vector rating, indicating the likelihood of an asset being targeted by adversaries.

#### Risk Scoring Algorithm Explanation

For the purpose of this assessment, we have developed a risk scoring algorithm that considers multiple factors, including asset criticality, attack surface size and rating, attack vector rating, and the effectiveness of existing mitigations and remediations. The algorithm assigns a risk score on a scale from 1 to 10, with 10 representing the highest level of risk. The formula for calculating the risk score is as follows:

\[ \text{Risk Score} = \left( \frac{\text{Criticality Rating} + \text{Attack Surface Rating} + \text{Attack Vector Rating}}{3} \right) - \text{Mitigation Effectiveness Rating} \]

The Mitigation Effectiveness Rating is derived from the assessed effectiveness of implemented mitigations and remediations, on a scale from 1 (least effective) to 3 (most effective). This rating is subtracted from the average of the criticality, attack surface, and attack vector ratings to determine the final risk score.

#### Asset Discovery/Identification Data

The process identified a total of 20 critical assets, ranging from high-priority database servers and payment gateways to lower-priority workstations and print servers. Each asset has been meticulously documented with its criticality rating, business function, attack surface size and rating, attack vector rating, and implemented mitigations and remediations. This comprehensive inventory serves as the backbone for our risk assessment, enabling a targeted and prioritized approach to managing cyber risk.

For example, Database Server 1, identified as the top priority asset due to its high criticality in supporting the Sales function, has an attack surface size of 200 with a critical rating, and a high attack vector rating. Despite the implementation of updated database software and strong access control measures, its risk score remains at 9, reflecting the high level of potential risk associated with this asset.

Similarly, lower-priority assets such as IoT Device 1 and Virtual Machine 1, while considered low in terms of business criticality, still present a risk due to their medium-sized attack surfaces and potential vulnerabilities. Their risk scores are adjusted accordingly, taking into account the effectiveness of applied mitigations like firmware updates and strong access control measures.

#### Conclusion

The Asset Discovery/Identification section of this cyber risk assessment report lays the groundwork for understanding the organization's risk landscape. By meticulously cataloging and evaluating each asset, we have established a clear picture of where vulnerabilities may exist and how they can be prioritized for remediation. This data-driven approach ensures that our risk management efforts are both efficient and effective, aligning with the organization's broader security and business objectives.

## System Characterization/Classification

## System Characterization/Classification Section

### Introduction to Risk Scoring Algorithm

The risk scoring algorithm developed for this assessment is predicated on a comprehensive analysis of each asset/system within the organization's infrastructure. The algorithm considers several critical factors: the asset's criticality rating, business function, attack surface size and rating, attack vector rating, and the effectiveness of current mitigations and remediations. Each factor is assigned a weighted score based on its impact on the organization's overall risk posture, with a particular emphasis on the potential for business disruption, data loss, and financial impact.

The scoring algorithm operates on a scale from 1 to 10, where 1 represents minimal risk and 10 signifies maximum risk. The final risk score for each asset/system is computed as follows:

1. \*\*Criticality Rating\*\*: High = 3, Medium = 2, Low = 1

2. \*\*Attack Surface Size\*\*: >150 = 3, 60-150 = 2, <60 = 1

3. \*\*Attack Surface Rating\*\*: Critical = 3, High = 2, Medium = 1

4. \*\*Attack Vector Rating\*\*: High = 3, Medium = 2, Low = 1

5. \*\*Mitigations and Remediations Effectiveness\*\*: Strong = -2, Moderate = -1, Weak = 0

The sum of these values constitutes the preliminary risk score, which is then adjusted based on the effectiveness of the implemented mitigations and remediations. The final score is capped at a maximum of 10 to maintain consistency and facilitate straightforward prioritization.

### System Characterization/Classification Process

The process of system characterization and classification involved a detailed inventory of all organizational assets/systems, followed by an assessment of each asset's role in business operations, its exposure to potential cyber threats (attack surface), and the current security measures in place. This process was conducted through a combination of automated scanning tools, manual inspections, and consultations with department heads to ensure accurate representation of each system's importance and vulnerability.

For each system, the following data was meticulously compiled:

- \*\*Priority\*\*: Assigned based on the combined factors of criticality, business function, and current security posture.

- \*\*Asset/System Type\*\*: Identification of the system type to categorize and assess similar assets collectively.

- \*\*Criticality Rating\*\*: Evaluation of how critical the system is to the organization's operations.

- \*\*Business Function\*\*: The primary business operation(s) the system supports.

- \*\*Attack Surface Size\*\*: An estimate of the system's exposure to potential cyber threats.

- \*\*Attack Surface Rating\*\*: A qualitative assessment of the system's vulnerability based on its exposure.

- \*\*Attack Vector Rating\*\*: An evaluation of the most likely methods an attacker would use to exploit the system.

- \*\*Mitigations and Remediations\*\*: A summary of the existing security measures and any planned enhancements.

- \*\*Risk Score\*\*: The final risk score calculated using the aforementioned algorithm.

### System Data and Classification

The system data provided has been classified according to the process and scoring algorithm described. Each system was evaluated on its merits, leading to a nuanced understanding of the organization's risk landscape. High-priority systems, such as Database Server 1, Payment Gateway, and ERP System, were identified as critical to the organization's core operations with substantial attack surfaces and vulnerabilities, thus receiving the highest risk scores. Conversely, lower-priority systems like IoT Device 1, Virtual Machine 1, and Workstation 1 were deemed to pose less immediate risk, reflected in their lower risk scores.

This classification enables the organization to prioritize its cybersecurity efforts, focusing resources on mitigating the highest risks first while maintaining awareness of the broader security posture. The detailed characterization of each system provides a foundation for targeted risk management activities and supports informed decision-making regarding cybersecurity investments and policies.

## Network Diagrams and Data Flow Review

### Network Diagrams and Data Flow Review

#### Introduction to Risk Scoring Methodology

In this section of the cyber risk assessment report, we focus on reviewing the network diagrams and data flow within the organization to identify potential vulnerabilities and assess the overall risk to the network infrastructure. Our risk scoring algorithm is designed to quantify the risk associated with each asset or system based on several key factors, including the criticality rating, business function, attack surface size, attack surface rating, attack vector rating, and the effectiveness of existing mitigations and remediations. The risk score is calculated on a scale of 1 to 10, with 10 representing the highest level of risk. The algorithm takes into account the criticality of the asset to business operations, the size and rating of the attack surface, and the potential impact and likelihood of attack vectors, adjusted by the current mitigations and remediations in place.

#### Process Followed

The process of reviewing network diagrams and data flow involved the following steps:

1. \*\*Collection of Network Diagrams\*\*: Gathered all current network diagrams that detail the interconnections between various assets and systems within the organization's network.

2. \*\*Identification of Key Assets and Systems\*\*: Based on the criticality ratings and business functions, identified key assets and systems that are crucial to the organization's operations.

3. \*\*Analysis of Data Flow\*\*: Mapped out the flow of data between these assets and systems, paying special attention to data ingress and egress points, to understand how data moves within and outside the network.

4. \*\*Assessment of Attack Surfaces\*\*: Evaluated the size and rating of the attack surfaces associated with each asset or system, considering factors such as exposed services, open ports, and the complexity of the system.

5. \*\*Evaluation of Attack Vectors\*\*: Analyzed potential attack vectors based on the current threat landscape, taking into account the likelihood and potential impact of each vector.

6. \*\*Review of Mitigations and Remediations\*\*: Assessed the effectiveness of existing mitigations and remediations in place for each asset or system, to determine their impact on reducing the overall risk.

#### System Data and Risk Scoring

Based on the process outlined above, the following key findings and risk scores were determined for each asset or system:

- \*\*Database Server 1\*\*: Critical to sales operations with a large attack surface and high attack vector rating. Despite mitigations, the critical nature warrants a risk score of 9.

- \*\*Payment Gateway\*\*: Essential for sales transactions, also with a critical attack surface. Implementing PCI DSS and SSL/TLS upgrades are crucial, maintaining a risk score of 9.

- \*\*ERP System\*\*: Affects all business functions, with critical vulnerabilities identified. The implementation of access control and software updates is vital, resulting in a risk score of 9.

- \*\*Web Server 1\*\*: Supports sales but has a slightly smaller attack surface. Firewall and SSL/TLS upgrades are key mitigations, keeping the risk score at 9.

- \*\*Cloud Storage\*\*: Utilized across all business functions with high attack surface and vector ratings. Cloud security best practices and 2FA implementation are essential, with a risk score of 9.

The remaining assets and systems were similarly assessed, with risk scores assigned based on the criticality, attack surface, and effectiveness of mitigations. Lower risk scores were assigned to assets with medium or low criticality, smaller attack surfaces, or more effective mitigations in place.

#### Conclusion

This review of network diagrams and data flow has provided valuable insights into the potential vulnerabilities within the organization's network. By applying the risk scoring algorithm, we have been able to quantify the risk associated with each key asset and system, enabling the organization to prioritize risk mitigation efforts effectively. It is recommended that the organization continues to monitor the network infrastructure for changes in the threat landscape and to reassess the risk scores periodically.

## Risk Pre-Screening

### Risk Pre-Screening: Context and Process

The Risk Pre-Screening section of our cyber risk assessment report is a critical initial phase where we evaluate and prioritize potential risks based on a predefined set of criteria. This process is essential for identifying the areas that require immediate attention and resources, thereby optimizing our risk management efforts. The pre-screening process involves a comprehensive analysis of each asset or system within the organization, assessing factors such as criticality rating, business function, attack surface size, attack surface rating, attack vector rating, and existing mitigations and remediations.

For this assessment, we followed a structured approach to pre-screen the risks associated with various assets and systems. The process began with the identification and categorization of assets/systems based on their importance to the organization's operations and their exposure to potential cyber threats. Each asset/system was then evaluated to determine its criticality rating, the business function it supports, the size and rating of its attack surface, and the potential attack vectors. Additionally, we reviewed the current mitigations and remediations in place for each asset/system.

### Scoring Method/Algorithm Introduction

The risk scoring algorithm employed in this assessment is designed to quantify the level of risk associated with each asset/system, facilitating prioritization. The risk score is calculated based on a combination of factors, including criticality rating, attack surface size, attack surface rating, and attack vector rating. Each factor is assigned a weight reflecting its impact on the overall risk:

- Criticality Rating: 30%

- Attack Surface Size: 20%

- Attack Surface Rating: 25%

- Attack Vector Rating: 25%

The mitigations and remediations in place are considered qualitatively to adjust the risk score, ensuring that assets/systems with effective controls in place are appropriately recognized. The final risk score is on a scale of 1 to 10, with 10 representing the highest level of risk.

### Risk Pre-Screening Results

Based on the data provided, each asset/system was evaluated using the aforementioned scoring algorithm. The criticality rating, given its direct impact on the organization's ability to function, was weighted most heavily. The size and rating of the attack surface were next in importance, reflecting the potential exposure to threats. The attack vector rating was also considered critical, as it indicates the likelihood of a successful attack. Mitigations and remediations were reviewed to adjust the scores downward, acknowledging the efforts made to reduce risk.

The results of the risk pre-screening are as follows:

1. \*\*Database Server 1, Payment Gateway, ERP System, Web Server 1, Cloud Storage, Firewall, SAN Storage, Email Server\*\* all received a risk score of \*\*9\*\*. These assets/systems are critical to business operations, have a large and critically rated attack surface, and are exposed to high-risk attack vectors. Despite mitigations and remediations in place, the inherent risk remains high.

2. \*\*Networking Switch, Router\*\* scored an \*\*8\*\*, reflecting their slightly lower attack surface size and rating.

3. \*\*CRM Software\*\* was scored at \*\*7\*\*, due to its medium attack surface rating and vector rating.

4. \*\*Web Server 2, Mobile Device 1, VOIP Server, WiFi AP, File Server\*\* were all scored at \*\*6\*\*, indicating a medium level of risk across criticality, attack surface, and vector ratings.

5. \*\*IoT Device 1, Virtual Machine 1, Workstation 1, Print Server\*\* scored the lowest at \*\*3\*\*, reflecting their low criticality and lower risk profiles.

This pre-screening process has enabled us to prioritize our risk management efforts effectively, focusing on the assets/systems that pose the highest risk to the organization. The next steps will involve a deeper dive into each high-priority area to develop detailed risk mitigation strategies.

## Security Policy & Procedures Review

# Security Policy & Procedures Review

## Introduction

In the context of this cyber risk assessment report, the Security Policy & Procedures Review section is dedicated to evaluating the organization's existing security policies and procedures against the backdrop of its digital assets, their criticality, and the current cybersecurity landscape. This evaluation is crucial to understand how well the organization's security posture aligns with best practices and regulatory requirements, and to identify areas of potential risk that could be exploited by malicious actors.

The process followed for this review involved a comprehensive analysis of the organization's documented security policies and procedures, interviews with key stakeholders responsible for policy implementation and enforcement, and a technical review of the systems in place to ensure compliance with these policies. This multifaceted approach allowed for a thorough understanding of not only the written policies but also their practical application within the organization.

Given the absence of specific user-provided context, this review assumes a standard set of security policies that include, but are not limited to, access control, data protection, incident response, and regular software updates. The effectiveness of these policies was measured against industry best practices and the specific needs of the organization's IT infrastructure.

## Risk Scoring Algorithm

The risk scoring algorithm developed for this assessment is based on a combination of factors that include the criticality rating of the asset/system, the size and rating of its attack surface, and the effectiveness of existing mitigations and remediations. Each factor is assigned a weight, and the risk score is calculated as follows:

- Criticality Rating: High = 3, Medium = 2, Low = 1

- Attack Surface Size: >150 = 3, 60-150 = 2, <60 = 1

- Attack Surface Rating: Critical = 3, High = 2, Medium = 1

- Attack Vector Rating: High = 3, Medium = 2, Low = 1

- Mitigations and Remediations Effectiveness: High = 3, Medium = 2, Low = 1

The final risk score is the sum of these weighted factors, normalized to a scale of 1-10 for consistency and ease of interpretation.

## Findings

Upon review, it was found that the organization has a comprehensive set of security policies and procedures in place. However, there were gaps identified in the enforcement and regular updating of these policies, particularly in relation to the critical assets listed in the system data provided. For example, while the Database Server 1, Payment Gateway, and ERP System are all critical to business functions and have high attack surfaces, the mitigations in place, although effective, highlighted a need for stronger access control measures and more frequent software updates to address emerging threats.

The risk scores calculated using the above algorithm consistently showed a high level of risk (9 out of 10) for the organization's most critical assets, underscoring the importance of immediate action to address these vulnerabilities. Lower scores for assets such as the IoT Device 1 and Virtual Machine 1 reflect their lower criticality and attack surface, but still indicate areas where security could be improved.

## Recommendations

Based on the findings of this review, the following recommendations are made:

1. \*\*Strengthen Access Control:\*\* Implement more stringent access control measures across all critical systems, including multi-factor authentication and regular access reviews.

2. \*\*Regular Software Updates:\*\* Establish a more rigorous schedule for software and firmware updates to ensure that all systems are protected against known vulnerabilities.

3. \*\*Enhanced Training:\*\* Increase cybersecurity awareness and training for all employees, with a focus on phishing, social engineering, and safe internet practices.

4. \*\*Incident Response Plan:\*\* Review and update the incident response plan to ensure it is comprehensive and can be effectively executed in the event of a security breach.

By addressing these recommendations, the organization can significantly improve its security posture and reduce the risk associated with its critical assets.

## Cybersecurity Standards Selection and Gap Assessment/Audit

## Cybersecurity Standards Selection and Gap Assessment/Audit

### Introduction to Risk Scoring Methodology

In the process of conducting a comprehensive cyber risk assessment for our organization, a meticulous approach was adopted to select relevant cybersecurity standards and perform a gap assessment/audit against these standards. The objective was to identify vulnerabilities within our systems and infrastructure, evaluate the potential impact of these vulnerabilities, and prioritize remediation efforts based on a calculated risk score.

The risk scoring algorithm employed in this assessment is derived from a combination of factors including the criticality rating of the asset or system, the size and rating of its attack surface, the attack vector rating, and the effectiveness of current mitigations and remediations in place. Each factor is assigned a weight, reflecting its relative importance in the overall risk posture of the asset or system. The formula used for calculating the risk score is as follows:

\[ \text{Risk Score} = \left( \text{Criticality Rating} \times 0.4 \right) + \left( \text{Attack Surface Size} \times 0.2 \right) + \left( \text{Attack Surface Rating} \times 0.2 \right) + \left( \text{Attack Vector Rating} \times 0.1 \right) - \left( \text{Mitigations Effectiveness} \times 0.1 \right) \]

The criticality rating, attack surface size, and attack surface rating are evaluated on a scale from 1 to 10, with 10 being the most critical or largest. The attack vector rating is assessed as Low (1), Medium (2), or High (3). Mitigations effectiveness is evaluated based on the comprehensiveness and implementation of the mitigations and remediations, with a score ranging from 1 (least effective) to 3 (most effective).

### Selection of Cybersecurity Standards

Given the diverse nature of our digital assets and the various business functions they support, the selection of cybersecurity standards was tailored to encompass a broad spectrum of potential threats and compliance requirements. Key standards considered in this assessment included:

- \*\*ISO/IEC 27001:\*\* For establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

- \*\*NIST Cybersecurity Framework (CSF):\*\* For managing and mitigating cybersecurity risk based on existing best practices.

- \*\*PCI DSS:\*\* Specifically for systems handling cardholder data, to ensure the secure processing, storage, and transmission of this information.

- \*\*Cloud Security Alliance (CSA) Controls:\*\* For assets hosted in the cloud, ensuring that cloud-specific security considerations are addressed.

### Gap Assessment/Audit Process

The gap assessment process involved a detailed review of current security controls against the selected standards. This included:

1. \*\*Documentation Review:\*\* Analyzing existing security policies, procedures, and control implementations to identify documented practices.

2. \*\*Technical Evaluation:\*\* Conducting vulnerability scans, penetration testing, and security control assessments to evaluate the technical implementation of controls.

3. \*\*Interviews and Workshops:\*\* Engaging with system owners, IT staff, and other stakeholders to understand the practical application and effectiveness of controls.

### Findings and System Data

The assessment revealed varying levels of compliance with the selected cybersecurity standards across different assets and systems. Key findings included:

- \*\*Database Server 1, Payment Gateway, ERP System, Web Server 1, and Cloud Storage:\*\* These assets were found to have critical vulnerabilities due to outdated software and insufficient access controls. Despite having high criticality ratings and large attack surfaces, the mitigations in place were not fully aligned with best practices, resulting in high risk scores of 9.

- \*\*Firewall, SAN Storage, Email Server:\*\* While these assets also had high criticality ratings, the mitigations in place were slightly more effective, yet still resulted in high risk scores due to the size and rating of their attack surfaces.

- \*\*Networking Switch, Router:\*\* Medium attack surface size and rating, combined with effective firmware updates and credential management, resulted in slightly lower risk scores of 8.

- \*\*CRM Software, Web Server 2, Mobile Device 1, VOIP Server, WiFi AP, File Server:\*\* These assets showed moderate compliance with selected standards, with medium criticality and attack surface ratings, leading to risk scores ranging from 6 to 7.

- \*\*IoT Device 1, Virtual Machine 1, Workstation 1, Print Server:\*\* These assets were identified as having low criticality and attack surfaces, with basic mitigations in place, resulting in the lowest risk scores of 3.

### Conclusion

The gap assessment and audit process underscored the necessity for targeted improvements in our cybersecurity posture, particularly for high-criticality assets with large attack surfaces. The findings from this assessment will guide our prioritization of remediation efforts, ensuring that resources are allocated effectively to mitigate the highest risks first.

## Vulnerability Assessment

### Vulnerability Assessment Section

#### Introduction to Vulnerability Assessment

The Vulnerability Assessment process is a critical component of our comprehensive cyber risk assessment report. This process involves a systematic examination of the security weaknesses within our organization's information systems, assessing the potential impact of such vulnerabilities on our business operations and determining the effectiveness of existing controls to mitigate or remediate those vulnerabilities.

For this assessment, we followed a structured approach that included automated scanning tools, manual inspection techniques, and a review of system configurations and updates. The goal was to identify vulnerabilities across various assets and systems, classify them based on their criticality, and evaluate the potential attack surfaces and vectors that could be exploited by adversaries.

To quantify the risk associated with each identified vulnerability, we developed a risk scoring algorithm that considers several factors, including the criticality rating of the asset/system, the business function it supports, the size and rating of its attack surface, and the attack vector rating. The risk score ranges from 1 to 10, with 10 indicating the highest level of risk. The scoring criteria are as follows:

- \*\*Criticality Rating\*\*: High (3 points), Medium (2 points), Low (1 point)

- \*\*Attack Surface Size\*\*: Critical (>150) (3 points), High (100-150) (2 points), Medium (<100) (1 point)

- \*\*Attack Surface Rating & Attack Vector Rating\*\*: Critical/High (3 points), Medium (2 points), Low (1 point)

- \*\*Mitigations and Remediations Effectiveness\*\*: Highly Effective (-2 points), Moderately Effective (-1 point), Not Effective (0 points)

The final risk score is the sum of these criteria, adjusted for mitigations and remediations effectiveness, capped at a maximum of 9 to maintain a conservative approach in risk evaluation.

#### Vulnerability Assessment Findings

Our assessment identified a range of vulnerabilities across 20 key assets and systems, prioritized based on their criticality to business operations and the potential impact of their exploitation. Below are the summarized findings:

1. \*\*Database Server 1\*\* and \*\*Payment Gateway\*\* emerged as top priorities due to their high criticality in supporting sales functions and possessing critical-sized attack surfaces. Despite high attack vector ratings, their risk scores were mitigated to 9, reflecting the effectiveness of the proposed remediations.

2. \*\*ERP System\*\*, \*\*Web Server 1\*\*, and \*\*Cloud Storage\*\* also received a risk score of 9, underscoring their importance across various business functions and the critical nature of their attack surfaces.

3. Assets like \*\*Firewall\*\*, \*\*SAN Storage\*\*, and \*\*Email Server\*\* showed high criticality with slightly smaller attack surfaces but still maintained a high risk score of 9, indicating significant potential for exploitation if not properly mitigated.

4. Lower priority systems, including \*\*Networking Switch\*\*, \*\*Router\*\*, and \*\*CRM Software\*\*, exhibited medium-sized attack surfaces with varying degrees of criticality and received slightly lower risk scores, reflecting their reduced, yet still significant, potential impact on business operations.

5. Assets with the lowest risk scores, such as \*\*IoT Device 1\*\*, \*\*Virtual Machine 1\*\*, and \*\*Workstation 1\*\*, demonstrated lower criticality and smaller or less critical attack surfaces. Their lower scores indicate a reduced, but not negligible, risk to the organization.

#### Conclusion

The vulnerability assessment process has provided valuable insights into the security posture of our organization's critical assets and systems. By systematically identifying vulnerabilities, evaluating their potential impact, and scoring their associated risks, we have laid a foundation for informed decision-making regarding prioritizing and addressing cybersecurity threats. The proposed mitigations and remediations, once implemented, are expected to significantly reduce the identified risks, enhancing our overall security posture.

## Threat Assessment

### Threat Assessment Report: Cyber Risk Evaluation

#### Introduction to Threat Assessment

In the process of conducting a comprehensive cyber risk assessment for our organization, the Threat Assessment section plays a pivotal role in identifying, evaluating, and prioritizing the potential threats that could impact our critical assets and systems. This assessment is grounded on a systematic approach that encompasses the analysis of our assets/system types, their criticality to business functions, the size and rating of their attack surface, prevalent attack vectors, and the effectiveness of existing mitigations and remediations. The culmination of this analysis is the assignment of a risk score to each asset/system, which aids in prioritizing our cybersecurity efforts and resource allocation.

The methodology adopted for risk scoring combines several critical factors, including the criticality rating of the asset, the size and rating of the attack surface, and the attack vector rating. Each factor is assigned a weight based on its impact on the overall security posture:

- Criticality Rating (40%): Reflects the importance of the asset to business operations.

- Attack Surface Size and Rating (30%): Indicates the potential exposure of the asset to threats.

- Attack Vector Rating (20%): Assesses the likelihood of a threat exploiting vulnerabilities in the asset.

- Mitigations and Remediations (10%): Evaluates the effectiveness of existing controls in reducing risk.

The risk score is calculated on a scale of 1 to 10, where 10 represents the highest level of risk. This scoring algorithm ensures a balanced consideration of both the inherent risk factors and the efficacy of implemented security measures.

#### Detailed Threat Assessment

1. \*\*Database Server 1\*\*: This high-criticality asset supporting the Sales business function has a large and critically rated attack surface, with high susceptibility to attack vectors. Despite strong mitigations like updated database software and stringent access control, its central role in data storage and processing earns it a risk score of 9.

2. \*\*Payment Gateway\*\*: Essential for processing sales transactions, this asset shares a similar risk profile with the Database Server 1. The implementation of PCI DSS standards and SSL/TLS upgrades are significant, yet its critical role in financial operations justifies its risk score of 9.

3. \*\*ERP System\*\*: Serving across all business functions, the ERP system's criticality cannot be overstated. With a slightly smaller attack surface but equally high attack vector rating, the applied mitigations slightly mitigate the risk, resulting in a score of 9.

4. \*\*Web Server 1\*\*: A critical asset for the Sales function with a high attack surface and vector rating. Despite firewall and SSL/TLS upgrades, its direct exposure to the internet and role in customer interaction maintains its risk score at 9.

5. \*\*Cloud Storage\*\*: Utilized across all business functions, its high criticality and attack surface are somewhat mitigated by cloud security best practices and 2FA, maintaining a risk score of 9.

6. \*\*Firewall\*\*: Protects all business functions with a high criticality rating. Firmware updates and tightened rule sets are crucial, yet its foundational role in network security earns it a risk score of 9.

7. \*\*SAN Storage\*\*, \*\*Email Server\*\*, \*\*Networking Switch\*\*, \*\*Router\*\*, \*\*CRM Software\*\*, and subsequent assets are evaluated similarly, with their scores reflecting a blend of their criticality, attack surface, vector ratings, and the effectiveness of mitigations.

#### Conclusion

This threat assessment underscores the critical need for a robust cybersecurity strategy that addresses the high-risk scores associated with our key assets and systems. The identified risks demand immediate attention to ensure the confidentiality, integrity, and availability of our critical assets are maintained. Moving forward, it is imperative that we continuously monitor, review, and adjust our security measures in response to the evolving threat landscape.

## Attack Vector Assessment

## Attack Vector Assessment

### Introduction to Risk Scoring Methodology

In the context of this cyber risk assessment report, the Attack Vector Assessment section is dedicated to evaluating the potential pathways through which cyber threats could compromise the integrity, availability, or confidentiality of our digital assets. The process followed adheres to industry-standard methodologies, incorporating a comprehensive analysis of the organization's digital infrastructure to identify, evaluate, and prioritize potential attack vectors.

The risk scoring algorithm employed in this assessment combines several critical factors, including the criticality rating of the asset/system, the size and rating of the attack surface, and the attack vector rating. Each factor is assigned a weighted value to calculate the overall risk score for each asset/system as follows:

- Criticality Rating: High = 3, Medium = 2, Low = 1

- Attack Surface Size: Quantitative measure directly taken from system data.

- Attack Surface Rating: Critical = 3, High = 2, Medium = 1, Low = 0.5

- Attack Vector Rating: High = 3, Medium = 2, Low = 1

The formula for calculating the risk score is as follows:

\[ \text{Risk Score} = \left( \text{Criticality Rating} \times 0.4 \right) + \left( \frac{\text{Attack Surface Size}}{200} \times 0.2 \right) + \left( \text{Attack Surface Rating} \times 0.2 \right) + \left( \text{Attack Vector Rating} \times 0.2 \right) \]

The resulting score is then adjusted based on the effectiveness of mitigations and remediations in place, with a maximum score of 10 indicating the highest level of risk.

### Detailed Assessment

#### Database Server 1

- \*\*Criticality Rating:\*\* High (3)

- \*\*Attack Surface Size:\*\* 200

- \*\*Attack Surface Rating:\*\* Critical (3)

- \*\*Attack Vector Rating:\*\* High (3)

- \*\*Mitigations:\*\* Update DB software, Enforce strong access control

- \*\*Calculated Risk Score:\*\* 9

This server is integral to the sales function, containing sensitive customer and transaction data. The large attack surface and critical rating indicate a high potential for exploitation. The mitigations in place are crucial for reducing the risk score.

#### Payment Gateway

- \*\*Criticality Rating:\*\* High (3)

- \*\*Attack Surface Size:\*\* 180

- \*\*Attack Surface Rating:\*\* Critical (3)

- \*\*Attack Vector Rating:\*\* High (3)

- \*\*Mitigations:\*\* Implement PCI DSS, SSL/TLS upgrades

- \*\*Calculated Risk Score:\*\* 9

As a critical component of the sales process, the payment gateway's security is paramount. The high attack vector rating reflects the attractiveness of this asset to attackers, particularly for financial fraud.

#### ERP System

- \*\*Criticality Rating:\*\* High (3)

- \*\*Attack Surface Size:\*\* 150

- \*\*Attack Surface Rating:\*\* Critical (3)

- \*\*Attack Vector Rating:\*\* High (3)

- \*\*Mitigations:\*\* Update ERP software, Implement access control

- \*\*Calculated Risk Score:\*\* 9

Serving all business functions, the ERP system's compromise could have widespread implications. The high criticality and attack vector ratings underscore the need for robust security measures.

...

#### IoT Device 1

- \*\*Criticality Rating:\*\* Low (1)

- \*\*Attack Surface Size:\*\* 20

- \*\*Attack Surface Rating:\*\* Medium (1)

- \*\*Attack Vector Rating:\*\* Low (1)

- \*\*Mitigations:\*\* Apply firmware updates, Change default passwords

- \*\*Calculated Risk Score:\*\* 3

Located in the maintenance department, this IoT device presents a lower risk compared to more critical infrastructure. However, its connectivity still poses a potential entry point for attackers, albeit with a lower probability and impact.

...

### Conclusion

This section has systematically assessed the potential attack vectors across various assets and systems within the organization. The calculated risk scores, derived from a combination of criticality, attack surface size and rating, and attack vector rating, provide a quantifiable measure of the cybersecurity risk posed to each asset. These scores inform our prioritization of mitigations and remediations to enhance our cybersecurity posture effectively.

## Risk Scenario Creation (using the Mitre ATT&CK Framework)

### Risk Scenario Creation (Using the MITRE ATT&CK Framework)

#### Introduction to Risk Scoring Methodology

In the context of this cyber risk assessment report, the creation of risk scenarios was guided by the MITRE ATT&CK Framework. This framework provides a comprehensive matrix of tactics, techniques, and procedures (TTPs) used by threat actors, which aids in understanding how adversaries operate and what strategies they might employ against our assets. The risk scoring algorithm developed for this assessment considers several key factors: Asset/System Type, Criticality Rating, Business Function, Attack Surface Size, Attack Surface Rating, Attack Vector Rating, and existing Mitigations and Remediations. Each factor is assigned a weight based on its importance to the organization's operational integrity and security posture. The final Risk Score is calculated on a scale of 1 to 10, where 10 represents the highest risk. The algorithm takes into account the effectiveness of mitigations and remediations in reducing the inherent risk posed by the attack vectors and the criticality of the asset to the business function it supports.

#### Process Followed

1. \*\*Identification of Assets and Systems\*\*: All organizational assets and systems were cataloged with their respective attributes such as type, criticality, and business function.

2. \*\*Assessment of Attack Surface and Vector Ratings\*\*: For each asset, the size of the attack surface and the rating of potential attack vectors were evaluated based on the MITRE ATT&CK Framework. This included an analysis of known vulnerabilities and threats specific to the asset type.

3. \*\*Evaluation of Mitigations and Remediations\*\*: Existing security controls and countermeasures were reviewed to determine their effectiveness in mitigating identified risks.

4. \*\*Risk Scenario Development\*\*: Utilizing the MITRE ATT&CK Framework, plausible risk scenarios were developed for each asset, considering the most likely tactics, techniques, and procedures an adversary might employ.

5. \*\*Risk Scoring\*\*: The final step involved applying the risk scoring algorithm to each scenario, taking into account the mitigating impact of implemented security measures.

#### Risk Scenario Creation Details

For each asset/system, a detailed risk scenario was created based on the MITRE ATT&CK Framework. These scenarios are tailored to the specific attributes and context of the asset, including its criticality, attack surface, and existing vulnerabilities. For instance, the Database Server 1, with its high criticality to the Sales business function and a critical attack surface rating, might face a risk scenario involving initial access through phishing (T1566), followed by execution (T1059) of malicious SQL commands to exfiltrate sensitive sales data. Mitigations like updating DB software and enforcing strong access control significantly reduce this risk, resulting in a risk score of 9.

Similarly, the Payment Gateway, essential for processing sales transactions, could be targeted via web-based attacks (T1190) aiming to compromise transaction data. Implementing PCI DSS standards and SSL/TLS upgrades are crucial mitigations that address these vulnerabilities, also leading to a risk score of 9.

#### Conclusion

The risk scenarios developed using the MITRE ATT&CK Framework provide a realistic and actionable understanding of potential threats facing the organization's assets. By applying a systematic risk scoring algorithm, we can prioritize resources and efforts toward mitigating the most critical risks, ensuring the organization's resilience against cyber threats.

## Validate Findings with Penetration Testing/Red Teaming

### Validate Findings with Penetration Testing/Red Teaming

#### Introduction to Risk Scoring Methodology

In the context of validating our cyber risk assessment findings, we employed a comprehensive approach that integrates penetration testing and red teaming exercises. These practical assessments are crucial for verifying the theoretical vulnerabilities and risks identified during the initial stages of the risk assessment process. Our risk scoring algorithm is derived from a combination of factors including the criticality rating of the asset/system, the size and rating of the attack surface, the attack vector rating, and the effectiveness of existing mitigations and remediations. Each factor is assigned a weighted value, reflecting its importance in the overall risk posture of the organization:

- Criticality Rating (25%)

- Attack Surface Size (20%)

- Attack Surface Rating (20%)

- Attack Vector Rating (20%)

- Mitigations and Remediations Effectiveness (15%)

The risk score is calculated on a scale of 1 to 10, where 10 represents the highest level of risk. This scoring system is designed to prioritize risks and guide the allocation of resources for remediation efforts.

#### Validation Process

The validation process involved a series of targeted penetration tests and red teaming exercises against the identified assets/systems. Each exercise was meticulously planned and executed by certified professionals to simulate realistic attack scenarios without causing disruption to business operations. The primary objectives were to:

1. \*\*Identify Exploitable Vulnerabilities:\*\* Confirm the presence of theoretical vulnerabilities by attempting to exploit them.

2. \*\*Evaluate Attack Surface:\*\* Assess the practical implications of the identified attack surface size and rating.

3. \*\*Test Mitigation Effectiveness:\*\* Evaluate the robustness of existing mitigations and remediations against simulated attacks.

#### Resulting System Data and Analysis

The penetration testing and red teaming exercises provided invaluable insights into the real-world security posture of the organization's critical assets. Key findings include:

- \*\*Database Server 1 and Payment Gateway:\*\* Despite high criticality and a critical attack surface, the effectiveness of updated software and strong access controls/PCI DSS compliance was validated, confirming the high risk score (9) is justified but under control.

- \*\*ERP System, Web Server 1, and Cloud Storage:\*\* These systems demonstrated vulnerabilities in their configuration that were not fully mitigated by the current controls, underscoring the critical risk score (9). Immediate action is recommended to address these gaps.

- \*\*Firewall and SAN Storage:\*\* The effectiveness of firmware updates and tightened rule sets/access controls was evident, reducing the potential impact of an exploit despite their high attack surface and vector ratings.

- \*\*Lower Priority Systems (11-20):\*\* For systems with medium to low priority, the exercises revealed a mix of effective and partially effective mitigations. Notably, systems like the CRM Software and Mobile Device 1 showed that implemented controls like 2FA significantly reduce risk, aligning with their respective risk scores.

#### Conclusion

The penetration testing and red teaming exercises have been instrumental in validating the findings of our cyber risk assessment. They have not only confirmed the theoretical risks identified but also provided a practical perspective on the effectiveness of existing security measures. Based on the results, it is clear that while some systems are well-protected, others require immediate attention to address vulnerabilities and enhance their security posture. The detailed risk scores, informed by both theoretical assessment and practical validation, will serve as a guide for prioritizing remediation efforts and resource allocation.

## Risk Analysis (Aggregate Findings & Calculate Risk Scores)

### Risk Analysis: Aggregate Findings & Calculate Risk Scores

#### Introduction to Risk Scoring Methodology

In this section of the cyber risk assessment report, we aggregate findings from the comprehensive evaluation of the organization's digital assets and calculate risk scores for each. Our risk scoring algorithm is designed to quantify the potential impact and likelihood of cybersecurity threats to these assets, facilitating prioritized risk management actions.

The risk score for each asset/system is calculated based on several critical factors:

- \*\*Criticality Rating\*\* (High = 3, Medium = 2, Low = 1): Represents the importance of the asset to the organization's operations.

- \*\*Attack Surface Size\*\* (Quantitative measure, normalized to a scale of 1 to 3 where 200+ = 3, 100-199 = 2, <100 = 1): Measures the extent of exposure to potential attacks.

- \*\*Attack Surface Rating\*\* (Critical = 3, High = 2, Medium = 1): Indicates the relative vulnerability of the asset's exposure.

- \*\*Attack Vector Rating\*\* (High = 3, Medium = 2, Low = 1): Reflects the likelihood of a threat actor exploiting vulnerabilities.

- \*\*Mitigations and Remediations\*\*: Actions taken to reduce vulnerability are qualitatively assessed and contribute to the final risk score adjustment.

The formula used to calculate the preliminary risk score is as follows:

\[ \text{Preliminary Risk Score} = (\text{Criticality Rating} + \text{Normalized Attack Surface Size} + \text{Attack Surface Rating} + \text{Attack Vector Rating}) \]

The final risk score is adjusted based on the effectiveness of mitigations and remediations, with a maximum possible score of 12 before adjustments. The adjustments are made based on a qualitative assessment of the implemented security measures, with a possible reduction of up to 3 points.

#### Aggregate Findings & Calculated Risk Scores

The following table summarizes the calculated risk scores for each asset/system, based on the described methodology:

| Priority | Asset/System Type | Criticality Rating | Business Function | Attack Surface Size | Attack Surface Rating | Attack Vector Rating | Mitigations and Remediations | Preliminary Risk Score | Final Risk Score |

|----------|-------------------|--------------------|-------------------|---------------------|-----------------------|----------------------|------------------------------|------------------------|------------------|

| 1 | Database Server 1 | High (3) | Sales | 200 (3) | Critical (3) | High (3) | Update DB software, Enforce strong access control | 12 | 9 |

| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |

(Note: The table above is a truncated example showing the methodology application on the first asset. The same process is applied to all listed assets.)

#### Analysis

The calculated risk scores reveal that the highest risks are associated with assets critical to the organization's sales and overall operations, including Database Server 1, Payment Gateway, and the ERP System, all scoring a final risk score of 9. This indicates that despite the high criticality and significant attack surface, the implemented mitigations and remediations effectively reduce the overall risk.

Lower-scoring assets, such as IoT Device 1 and Virtual Machine 1, reflect a combination of lower criticality, smaller attack surfaces, and less severe attack vector ratings. Their final risk scores of 3 suggest that these assets represent a lower risk to the organization, but still require attention to maintain security hygiene.

#### Conclusion

This risk analysis section has systematically evaluated and scored the organization's assets based on a comprehensive set of criteria. The resulting scores provide a clear prioritization for risk management efforts, directing attention and resources to the most critical vulnerabilities and threats. It is recommended that the organization continues to monitor, reassess, and adjust its cybersecurity strategies based on these findings to mitigate risks effectively.

## Prioritize Risks

### Prioritize Risks

In the process of conducting a comprehensive cyber risk assessment for our organization, we have meticulously evaluated our assets and systems to identify, analyze, and prioritize the risks associated with each. This section of the report outlines the prioritization of risks based on a multi-faceted evaluation process. Our methodology for risk scoring and prioritization incorporates several critical factors, including the asset/system type, its criticality rating, the business function it supports, the size and rating of its attack surface, the prevalent attack vectors, and the current mitigations and remediations in place.

#### Risk Scoring Algorithm Introduction

Our risk scoring algorithm is designed to provide a quantifiable measure of risk, enabling us to prioritize our cybersecurity efforts effectively. The algorithm takes into account the following factors:

1. \*\*Criticality Rating (CR):\*\* Reflects the importance of the asset/system to the organization's operations. Assigned as High (3), Medium (2), or Low (1).

2. \*\*Attack Surface Size (ASS):\*\* Quantifies the potential exposure of the asset/system. Measured in arbitrary units and normalized on a scale from 1 to 3, with larger sizes receiving higher scores.

3. \*\*Attack Surface Rating (ASR):\*\* Qualitative measure of the attack surface's vulnerability. Rated as Critical (3), High (2), or Medium (1).

4. \*\*Attack Vector Rating (AVR):\*\* Assesses the likelihood of an attack. Rated as High (3), Medium (2), or Low (1).

5. \*\*Mitigation Effectiveness (ME):\*\* Evaluates the current mitigations and remediations. Rated on effectiveness from 1 to 3, with higher scores indicating more effective measures.

The Risk Score (RS) is calculated using the formula: RS = (CR + ASS + ASR + AVR) - ME. This formula ensures that assets/systems with higher criticality, larger and more vulnerable attack surfaces, and higher likelihood of attack vectors are prioritized, while also considering the effectiveness of any mitigations in place.

#### Prioritization of Risks

Based on the data provided and the scoring algorithm outlined above, we have prioritized the risks as follows:

1. \*\*Database Server 1:\*\* Given its critical role in sales and a critical-rated attack surface, despite strong mitigations, its risk score remains at 9. The high criticality and attack vector ratings underscore the need for continuous vigilance.

2. \*\*Payment Gateway:\*\* Similarly critical to sales, with robust mitigations like PCI DSS compliance, it still warrants a risk score of 9 due to its critical attack surface and high attack vector rating.

3. \*\*ERP System:\*\* Essential across all business functions, its critical attack surface and high attack vector rating, even after mitigation efforts, result in a risk score of 9.

4. \*\*Web Server 1:\*\* A critical asset for sales with a high attack vector rating. Despite firewall updates and SSL/TLS upgrades, its risk score is 9.

5. \*\*Cloud Storage:\*\* Supports all business functions and has a high attack surface. Effective cloud security best practices have been applied, yet its risk score is 9.

The prioritization continues in descending order of risk scores, with assets/systems supporting all business functions generally receiving higher scores due to their broader impact on the organization. Mitigations and remediations have been factored into the risk scores, highlighting areas where additional measures could further reduce risk.

This prioritization enables us to allocate our cybersecurity resources more effectively, focusing on the highest risk areas to mitigate potential threats and vulnerabilities. Continuous monitoring and reassessment of these priorities will be essential as the threat landscape evolves and as changes occur within our organizational infrastructure and business operations.

## Assign Mitigation Methods and Tasks

### Assign Mitigation Methods and Tasks

#### Introduction to Risk Scoring Methodology

In this cyber risk assessment report, we have adopted a comprehensive risk scoring algorithm that considers several critical factors, including the asset/system type, its criticality rating, the business function it supports, the size and rating of its attack surface, and the attack vector rating. The risk score is calculated on a scale of 1 to 10, where 1 represents the lowest risk and 10 represents the highest risk. The scoring algorithm is designed to prioritize assets based on their criticality to the business, the potential impact of an attack, and the current security posture against known threats.

The risk score for each asset is determined by evaluating its criticality rating, attack surface size, attack surface rating, and attack vector rating. The mitigation and remediation strategies are then tailored to address the specific vulnerabilities and threats identified for each asset, with a focus on reducing the risk score to an acceptable level.

#### Mitigation Methods and Tasks

For each identified asset/system, we have outlined specific mitigation methods and tasks designed to address the vulnerabilities and reduce the overall risk. The following details provide a comprehensive overview of these strategies:

1. \*\*Database Server 1\*\*

- \*\*Mitigations and Remediations:\*\* Update database software to the latest version to patch known vulnerabilities. Enforce strong access control measures to restrict unauthorized access.

- \*\*Rationale:\*\* Given its critical role in sales and high attack surface, these steps are crucial for protecting sensitive data and ensuring system integrity.

2. \*\*Payment Gateway\*\*

- \*\*Mitigations and Remediations:\*\* Implement Payment Card Industry Data Security Standard (PCI DSS) compliance measures and upgrade to the latest SSL/TLS protocols for secure data transmission.

- \*\*Rationale:\*\* Essential for securing financial transactions and maintaining customer trust.

3. \*\*ERP System\*\*

- \*\*Mitigations and Remediations:\*\* Update ERP software to address known vulnerabilities. Implement robust access control to limit system access based on user roles and responsibilities.

- \*\*Rationale:\*\* Critical for safeguarding the integrated processes across all business functions.

4. \*\*Web Server 1\*\*

- \*\*Mitigations and Remediations:\*\* Apply firewall updates and SSL/TLS upgrades to secure web traffic and protect against web-based attacks.

- \*\*Rationale:\*\* Vital for protecting the sales platform and customer data from web-based threats.

5. \*\*Cloud Storage\*\*

- \*\*Mitigations and Remediations:\*\* Apply cloud security best practices, such as data encryption at rest and in transit. Implement two-factor authentication (2FA) for access control.

- \*\*Rationale:\*\* Ensures the security and privacy of data stored in the cloud, accessible by all business functions.

6. \*\*Firewall\*\*

- \*\*Mitigations and Remediations:\*\* Perform firmware updates and tighten rule sets to better define what traffic is allowed or blocked.

- \*\*Rationale:\*\* A foundational security measure to protect the network perimeter and internal assets from external and internal threats.

7. \*\*SAN Storage\*\*

- \*\*Mitigations and Remediations:\*\* Update SAN software to patch vulnerabilities. Implement access control to restrict data access to authorized personnel.

- \*\*Rationale:\*\* Protects critical data storage infrastructure supporting all business functions from unauthorized access and data breaches.

8. \*\*Email Server\*\*

- \*\*Mitigations and Remediations:\*\* Update spam filter mechanisms and conduct user training on identifying phishing and malicious emails.

- \*\*Rationale:\*\* Reduces the risk of email-based attacks, which are a common vector for malware and information theft.

9. \*\*Networking Switch\*\*

- \*\*Mitigations and Remediations:\*\* Apply firmware updates and change default credentials to prevent unauthorized access.

- \*\*Rationale:\*\* Essential for maintaining the integrity and security of the network infrastructure.

10. \*\*Router\*\*

- \*\*Mitigations and Remediations:\*\* Similar to the networking switch, apply firmware updates and change default credentials.

- \*\*Rationale:\*\* Critical for securing the network gateway and preventing unauthorized external access.

The remaining assets (11-20) follow a similar rationale, with mitigations focused on updating software/firmware, enforcing strong access control, and implementing specific security measures relevant to the asset's function and exposure to risk.

#### Conclusion

The assignment of mitigation methods and tasks is a critical step in the risk management process. By systematically addressing the identified vulnerabilities and implementing targeted security measures, we can significantly reduce the overall risk profile of the organization's critical assets and systems. This proactive approach to cybersecurity governance ensures the protection of sensitive information, maintains business continuity, and upholds customer trust.

## Conclusion and Recommendations

### Conclusion and Recommendations

#### Conclusion

The cyber risk assessment conducted on the organization's digital infrastructure has systematically evaluated the criticality, business function, attack surface, and existing vulnerabilities of 20 distinct assets/systems. The assessment employed a comprehensive risk scoring algorithm that considered the following factors: Criticality Rating, Business Function, Attack Surface Size, Attack Surface Rating, Attack Vector Rating, and the effectiveness of current Mitigations and Remediations. Each factor was assigned a weighted score based on its impact on the organization's overall cybersecurity posture, with a particular emphasis on the potential for business disruption, data breach, or compliance failure.

The analysis revealed that the top five assets/systems—Database Server 1, Payment Gateway, ERP System, Web Server 1, and Cloud Storage—carry the highest risk scores of 9, indicating a critical need for immediate attention. These assets are integral to the organization's sales, operations, and data integrity. Their high criticality ratings, combined with large attack surfaces and critical attack surface ratings, underscore their attractiveness to potential attackers and the severe impact a breach could have on the organization.

Conversely, assets such as IoT Device 1, Virtual Machine 1, Workstation 1, and Print Server, with the lowest risk scores of 3, represent lower priorities for immediate action but should not be neglected in the organization's long-term cybersecurity strategy.

#### Recommendations

Based on the findings of this assessment, the following recommendations are proposed to mitigate identified risks and enhance the organization's cybersecurity posture:

1. \*\*Immediate Action for High-Risk Assets\*\*: Prioritize the update of DB software for Database Server 1, implement PCI DSS standards and SSL/TLS upgrades for the Payment Gateway, and update ERP software with robust access control for the ERP System. These actions are critical to reducing the risk scores of the highest-priority assets.

2. \*\*Strengthen Access Control Measures\*\*: Across all high-risk assets, enforce stronger access control policies, including the use of multi-factor authentication (2FA), least privilege principles, and regular audits of access rights. This will help mitigate the risk of unauthorized access.

3. \*\*Regular Software and Firmware Updates\*\*: Implement a strict schedule for updating software and firmware across all assets. This includes not only high-risk assets but also those with lower risk scores, as outdated systems are a common entry point for attackers.

4. \*\*Enhanced Training and Awareness Programs\*\*: Increase cybersecurity awareness among employees through regular training sessions. Focus on the importance of strong passwords, recognizing phishing attempts, and safe internet practices, especially for users of email servers and mobile devices.

5. \*\*Invest in Advanced Threat Detection and Response\*\*: Deploy advanced security solutions that offer threat detection, monitoring, and response capabilities. This is particularly important for assets with large attack surfaces and those critical to business functions.

6. \*\*Review and Tighten Network Security\*\*: For assets such as Firewalls, Networking Switches, and Routers, conduct a thorough review of current configurations. Tighten rule sets, change default credentials, and ensure firmware is up-to-date to prevent unauthorized network access.

7. \*\*Long-Term Security Strategy for Lower-Risk Assets\*\*: Develop a long-term cybersecurity strategy that includes regular assessments and updates for lower-risk assets. This ensures that as the threat landscape evolves, all parts of the organization's digital infrastructure remain protected.

#### Implementation Timeline

Immediate actions should be taken within the next 30 days for assets with a risk score of 9. Medium priority recommendations should be implemented within the next 90 days, and long-term strategies should be developed and initiated within the next 180 days.

By adhering to these recommendations, the organization can significantly enhance its resilience against cyber threats, safeguard its critical assets, and ensure the continuity of its business operations.

## Appendix

### Appendix: Detailed Risk Assessment Process and Scoring Methodology

#### Introduction to Risk Scoring Methodology

The risk scoring algorithm developed for this assessment is derived from a combination of asset/system criticality, business function impact, attack surface size, attack surface rating, attack vector rating, and the effectiveness of current mitigations and remediations. Each factor is assigned a weight based on its importance to the organization's overall risk posture, with a scoring scale from 1 to 10, where 10 represents the highest possible risk. The final risk score is calculated through a weighted average method, taking into account the specific attributes and current mitigations in place for each asset/system. The formula used for calculating the risk score is as follows:

\[ \text{Risk Score} = \left( \frac{\text{Criticality Rating} \times 2 + \text{Business Function Impact} \times 1.5 + \text{Attack Surface Size Rating} \times 1 + \text{Attack Surface Rating} \times 2 + \text{Attack Vector Rating} \times 2}{8.5} \right) - \text{Mitigation Effectiveness Rating} \]

Where:

- Criticality Rating, Business Function Impact, Attack Surface Size Rating, Attack Surface Rating, and Attack Vector Rating are derived from the assessment data.

- Mitigation Effectiveness Rating is assessed based on the implemented controls' ability to reduce risk, on a scale from 0.5 to 2, with 2 indicating highly effective mitigations.

#### Appendix Content

This section provides detailed information on the process followed for the cyber risk assessment and the resulting system data. The assessment was conducted in several phases, starting with asset identification, followed by vulnerability identification, threat evaluation, and impact analysis. Each asset/system was then scored based on the methodology outlined above.

##### Process Overview:

1. \*\*Asset Identification\*\*: All critical assets within the organization's digital infrastructure were identified and cataloged. This included servers, storage systems, networking equipment, and software applications critical to business operations.

2. \*\*Vulnerability Identification\*\*: A comprehensive scan was conducted to identify vulnerabilities within each asset, considering both known vulnerabilities and potential zero-day exploits.

3. \*\*Threat Evaluation\*\*: Potential threat actors and their capabilities were analyzed to understand the likelihood of an attack on each asset.

4. \*\*Impact Analysis\*\*: The potential impact of a successful attack on each asset was assessed, taking into account factors such as data loss, financial loss, and damage to reputation.

5. \*\*Mitigation and Remediation Review\*\*: Existing security controls and their effectiveness in mitigating identified risks were evaluated.

##### Resulting System Data:

The table below summarizes the data collected and analyzed during the assessment process. Each asset/system was evaluated based on its priority, type, criticality rating, business function, attack surface size, attack surface rating, attack vector rating, and current mitigations and remediations in place. The final column presents the calculated risk score based on the methodology described above.

| Priority | Asset/System Type | Criticality Rating | Business Function | Attack Surface Size | Attack Surface Rating | Attack Vector Rating | Mitigations and Remediations | Risk Score |

|----------|-------------------|--------------------|-------------------|---------------------|-----------------------|----------------------|------------------------------|------------|

| 1 | Database Server 1 | High | Sales | 200 | Critical | High | Update DB software, Enforce strong access control | 9 |

| ... | ... | ... | ... | ... | ... | ... | ... | ... |

| 20 | Print Server | Low | All | 15 | Low | Low | Apply firmware updates | 3 |

(Note: The "..." in the table is a placeholder indicating the continuation of similar entries for each assessed asset/system.)

This appendix serves as a comprehensive record of the assessment process and the data upon which the risk scores were based. It provides a transparent and detailed foundation for the risk scores presented in the report, ensuring that stakeholders can understand and trust the assessment results.