**Vulnerability Assessment Report**

**1st January 20XX**

# System Description

The system consists of a server with a high-performance CPU processor and 128GB of memory. It operates on the latest version of the Linux operating system and hosta MySQL database management system. The server has a stable network connection using IPV4 addresses and communicates with other servers within the organization’s network. The system employs SSL/TLS encryption to secure communications.

# Scope

This vulnerability assessment will focus on the current access controls of the system. The assessment period spans from June 20XX to August 20XX. NIST SP-800 -30 Rev. 1 guidelines will be applied to perform the risk analysis of the information system.

# Purpose

The database server is a critical business asset,providing storage for sensitive customer and business data. Securing the data on the server is vital to prevent unauthorized access and data breaches that could have significant financial and reputational impacts. If the server were disabled, the organization would face considerable operational disruption, potentially leading to lost revenue, legal consequences, and diminished customer trust.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Internal User(Privileged)* | *Alter/Delete critical information* | *2* | *3* | *6* |
| *External Attacker(Hacker)* | *Conduct Denial of Service (DoS) attacks* | *2* | *2* | *4* |

# Explanation of Risk Calculations:

# Exfiltration of Sensitive Information is identified as a moderate risk. Though a competitor’s threat source is unlikely, the impact of a successful exfiltration would be severe.

# Alteration/Deletion of Critical Information by an internal user with elevated privileges presents a higher risk due to the possibility of intentional or accidental data modification.

# Denial of Service (DoS) attacks are a moderate risk due to the likelihood of such attacks and the impact of temporary system downtime.

# Approach

The risks associated with the database server were evaluated by considering the data storage and management methods used by the business. The likelihood of threat occurrences and their impact on day-to-day operations were carefully weighed. The potential risks were evaluated to understand their possible consequences on business functions, particularly focusing on the integrity, availability and confidentiality of critical data.

# Remediation Strategy

To mitigate the identified risks and protect the database server, the following remediation and security measures should be implemented:

1. **Authentication and Authorization Controls**
   * **Multi-factor Authentication (MFA)**: Enforce multi-factor authentication for all users accessing the database server, particularly administrators and privileged users, to ensure stronger access control.
   * **Role-Based Access Control (RBAC)**: Implement RBAC to limit access to the server and sensitive data based on the principle of least privilege.
2. **Encryption**
   * Upgrade from SSL to **TLS (Transport Layer Security)** for encrypting data in motion, ensuring stronger security for communications between the server and external systems.
3. **Network Security**
   * **IP Allow-listing**: Restrict database access to only corporate office IP addresses to prevent unauthorized access from external sources or the internet.
   * **Firewall Configuration**: Set up firewalls to filter incoming traffic and prevent malicious attempts to reach the database.
4. **Auditing and Monitoring**
   * Implement **audit logs** to track user actions on the database, specifically focusing on access attempts, data modification, and deletion activities.
   * Set up real-time **intrusion detection systems (IDS)** to monitor for abnormal or suspicious activities.
5. **Regular Security Audits**
   * Conduct regular security audits and vulnerability assessments to identify and address emerging threats or weaknesses in the system.

This vulnerability assessment provides a comprehensive evaluation of potential risks to the database server and outlines actionable remediation strategies to secure the system and maintain business continuity. These measures will help mitigate the likelihood of security breaches, reduce the impact of potential attacks, and safeguard sensitive business data.