**Vulnerability Assessment Report**

**1st January 20XX**

# System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

# Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

The database server is a core asset to the business, serving as the primary system for storing and retrieving customer data. Because employees across the globe rely on it to identify and contact potential customers, ensuring continuous availability and integrity is vital. If the server were to be compromised or disabled, the organization would suffer immediate operational disruptions, customer trust erosion, and potentially severe financial loss. Securing the data on this server is essential for maintaining business continuity and regulatory compliance.

# Risk Assessment

| **Threat Source** | **Threat Event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| Hacker (external) | Exfiltrate sensitive customer information | 3 (High) | 3 (High) | 9 |
| Insider (privileged user) | Alter or delete critical customer records | 2 (Moderate) | 3 (High) | 6 |
| System failure (technological) | Denial of service due to resource exhaustion | 2 (Moderate) | 2 (Moderate) | 4 |

# Approach

The three selected risks represent highly relevant threats based on the server's current public accessibility and centralized function within the company. External hackers present a significant risk due to the lack of network access restrictions, increasing the likelihood of data breaches. Insider threats, while less probable, pose a high-impact risk due to their elevated privileges. Lastly, system-level failures were considered based on hardware load and global user demand. These risks were prioritized due to their potential to interrupt critical business operations.

# Remediation Strategy

To address these risks, the company should immediately implement an IP allowlist restricting access to known employee or corporate IP addresses. Multi-factor authentication (MFA) must be enforced for all administrative and data-access accounts. Role-based access control (RBAC) policies should be audited and limited strictly to business-justified roles. In addition, TLS 1.2 or higher must be used for data in transit, and logging should be configured to detect and alert on abnormal data access or deletion patterns. These measures directly mitigate the threats identified in the assessment.