**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 critical component of the organization’s IT infrastructure, storing vital data that supports internal operations and customer-facing services. Protecting this data is essential to ensure business continuity, prevent data breaches, and maintain customer trust. If the server were to become unavailable, it could severely disrupt operations, result in revenue loss, and damage the organization's reputation. This assessment aims to identify risks and vulnerabilities that could impact the availability, integrity, and confidentiality of information.

## Threat Sources

- External hacker  
- Malicious internal administrator  
- Hardware failure (technological)

## Threat Events

- Exfiltration of confidential information  
- Alteration or deletion of critical data  
- Disruption of operations due to disk failure

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| External hacker | Exfiltration of confidential information | *3* | *3* | *9* |
| Malicious internal admin | Alteration or deletion of critical data | *2* | *3* | *6* |
| Hardware failure | Disruption due to disk failure | *2* | *2* | *4* |

# Approach

This vulnerability assessment was conducted using a qualitative approach based on the NIST SP 800-30 Rev. 1 framework. The identified threats represent relevant risks to the operation of a public-facing database server. Both human and technological sources were considered. The selected threat events reflect significant business risks as they may compromise data integrity, operational continuity, and the organization’s reputation.

# Remediation Strategy

To mitigate the identified risks, it is recommended to implement robust security controls such as:  
- Multi-factor authentication (MFA) for database access, especially for administrators  
- Principle of least privilege, limiting user access by role  
- Strong encryption for data at rest and in transit (TLS 1.2+)  
- Continuous auditing and centralized logging to detect suspicious activities  
- Redundancy and automated backups to mitigate hardware failures  
These measures align with NIST guidelines and significantly reduce exposure to critical threats.