**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 critical to the functioning of the company’s systems, managing large amounts of data. It stores data like customer and inventory information, as well as important metrics that are later used for analytics.

If the server was to become disabled, the company operations would be severely impacted, maybe even completely halted temporarily; and potential exfiltration of data could be harmful for compliance and business reasons. Because of these factors, it is crucial to secure this asset.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Customers* | *Alter/delete critical information* | *1* | *2* | *2* |
| *Employees* | *Alter/delete critical information* | *1* | *3* | *3* |
| *Employees* | *Spill sensitive information* | *2* | *2* | *4* |
| *System administrators* | *Alter/delete critical information* | *3* | *3* | *9* |
| *Hacker* | *Alter/delete critical information* | *2* | *3* | *6* |
| *Hacker* | *Conduct DoS atacks* | *3* | *3* | *9* |
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Temperature and humidity controls* | *Damage hardware* | *2* | *2* | *4* |
| *Natural hazards* | *Interrupt normal operations* | *2* | *3* | *6* |

# Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

# Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.