**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 is valuable to the business as it contains all customer data/information as well as information on the company and its employees. It is important for the business to secure the data on this server as any alterations or loss of data would not only harm the company’s reputation but its customers and employees as well. If the server were to be altered or disabled in any way, the business could lose all its customers and/or not be able to operate the business normally.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Employee* | *Alter/delete critical information* | *2* | *3* | *6* |
| *Hacker* | *Disrupt mission-critical operations.* | *3* | *3* | *9* |

# Approach

I selected the three above threat events as these pose the most significant risk to the business and its operations with the current database being open to the public. The company’s information should be kept private, but with it being public it would be easy for anyone to perform any of the above listed threat events. Still I listed a competitor, hacker, and employee as the source of these threats as they would be most likely to carry out such threat events. Although with the current setup, it really could be anyone.

# Remediation Strategy

First and foremost the business needs to implement the principle of least privilege, meaning only the people who need to have access to the information have it, with only the necessary privileges. I would also use authentication, authorization and auditing mechanisms to ensure that only authorized users can access the database server. This includes using multi-factor authentication, strong passwords and role-based access controls to limit user privileges. I would also encrypt the data in motion using TLS instead of SSL. I would use IP allow-listing to only the employees of the business to prevent random users outside the company from connecting to the database.