**Vulnerability Assessment Report**

# 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 to August. [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 very valuable to our organization as we have numerous employees that work remotely in different locations of the world. It is very important to secure the data on the server because all information has been stored in a remote database that has been open to the public since the launch of the company three years ago. The server can cause all business operations to halt if it comes to a point where it is disabled.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| Competitor | Obtain sensitive information via exfiltration | *1* | *3* | *3* |
| Hacker | Alter/Delete critical information | *3* | *3* | *9* |
| Customer | Disrupt mission-critical operations | *2* | *2* | *4* |

# Approach

Competitors, Hackers, and Customers all pose the title of a threat source. These threat sources were decided upon considering the nature of the public access to the organization’s remote database. The severity of potential incidents were weighed against the impact on day-to-day operational needs.

# Remediation Strategy

Applying the AAAframework can ensure that only authorized users have the proper access to the remote database server. This involves multi-factor authentication and role-based access controls. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.