**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

This database is valuable to the business because it contains information that is critical to business operations. It is important that the business secures the data on the server because unauthorized access could lead to data being stolen, or data being lost. If the database were disabled, business operations could be seriously impacted.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| Competitor | Competitor accesses business information and business plans. | 1 | 3 | 3 |
| Hacker | A hacker could potentially access and alter data in the database. | 3 | 3 | 9 |
| Supplier | Suppliers could alter data in the database to gather insight on contract prices and competition | 1 | 3 | 3 |

# 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. The risks listed were selected due to the ease of access that human threats have to the database. While unlikely that a competitor or supplier will attempt to gain access for the supposed reasons, it would be a critical security event. A hacker targeting the business will almost certainly target the database and gain access to the database, as it is publically available. This would be a critical security incident.

# 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.