**Vulnerability Assessment Report**

**May 8, 2024**

# 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

* *How is the database server valuable to the business?   
  The database server is valuable as it stores critical business data, facilitating efficient management and informed decision-making.*
* *Why is it important for the business to secure the data on the server?  
  Securing data on the server is essential to protect sensitive information, comply with regulations, and maintain trust with customers.*
* *How might the server impact the business if it were disabled?  
  If the server were disabled, it could disrupt operations, lead to data loss, and impact customer satisfaction, potentially resulting in financial losses.*

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration Perform reconnaissance and surveillance of*  *the organization* | *1* | *3* | *3* |
| *Hardware / Software / Environment* | *Disrupt mission-critical operations through hardware failure / power outage / damaging physical servers due to environmental factors / vulnerable outdated software etc.* | *1* | *2* | *2* |
| *Hacker / APT* | *Conduct "man-in-the-middle" attacks. Conduct Denial of Service (DoS) attacks. Obfuscate future attacks. Craft counterfeit certificates. Install persistent and targeted network sniffers*  *on organizational information systems.* | *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. Moreover, long-term, human, and non-human impacts are also considered, since the server is present at a remote location.

# 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. Also, physical security protocols like defense-in-depth, and segregation of duties needed to be ensured at the physical location.