

# Vulnerability Assessment Report

27 December 2023

---

## 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 January 2024 to March 2024. [NIST SP 800-30 Rev. 1](#) is used to guide the risk analysis of the information system.

## Purpose

The purpose of this vulnerability assessment is to ensure the security and integrity of the database server, a critical asset for the business. The data on the database server can contain a multitude of data such as customer data, transaction data, business intelligence documentation, and maybe proprietary data. If the data is compromised due to a vulnerability, oversight can result in the loss of data, availability, and integrity.

## Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	Obtain sensitive information via exfiltration	3	3	9
Employee	Disrupt mission-critical operations	2	3	6
Customer	Alter/Delete critical information	1	3	3

## **Approach**

Risks that were measured considered the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents were weighed against the impact on 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.