# Vulnerability Assessment Report

1st January 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 June 2022 to August 2022. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

## Purpose

The database server serves as the central hub for storing and managing extensive volumes of critical data. This includes customer information, campaign data, analytics, and essential business records. Its security is paramount due to its integral role in marketing operations and its function as the backbone of data management. Boasting a robust CPU and 128GB memory, the server efficiently handles complex queries and serves as the primary repository for vital business data, facilitating informed decisions, data analysis, and strategic planning.

Securing the database server is of utmost importance. It safeguards sensitive customer PII, financial records, and aligns with compliance regulations that vary by industry. A breach could lead to operational disruptions, revenue loss, customer dissatisfaction, and increased data recovery costs. It's crucial to mitigate these risks to ensure seamless business operations and data 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

Assessment focused on data storage and management procedures, analyzing risks. 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.

## Risk Evaluation

Evaluation centered on business data methods. Threat likelihood and potential impact were assessed against operational risks. Securing server data is vital for compliance, continuity, reputation, and financial safety. Server disruption could lead to major disruptions and legal consequences.

## 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. Implementing robust security measures and conducting regular vulnerability assessments are crucial to mitigating risks and ensuring the server's reliability and integrity.