# Vulnerability Assessment Report

1st December 2025

## 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 is used to guide the risk analysis of the information system.

## Purpose

The database server is a centralized system responsible for storing and managing large volumes of data. It houses customer, campaign, and analytics information that can be later evaluated to measure performance and support personalized marketing efforts. Because it is essential to daily marketing operations, securing this system is a high priority.

## Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Employee* | *Halt operations* | *2* | *3* | *6* |
| *Hacker* | *Delete info* | *2* | *3* | *3* |

## Approach

The assessed risks focused on the organization's data storage and management practices. Potential threat sources and events were evaluated based on the likelihood of a security incident, particularly considering the system's broad access permissions. The severity of these possible incidents was then analyzed in relation to their potential impact on daily operations.

## Remediation Strategy

Implement authentication, authorization, and auditing controls to ensure that only approved users can access the database server. This includes enforcing strong passwords, role-based access controls, and multi-factor authentication to restrict user privileges. Data in transit should be encrypted using TLS rather than SSL, and IP allow-listing should be applied so that only corporate office networks can connect to the database, preventing unauthorized internet access.