# Vulnerability Assessment Report

## 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 20-- to August 20--. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

## Purpose

This vulnerability assessment is conducted to evaluate the security of our business-critical database server, which stores valuable customer and business data. The database server is instrumental in daily operations, enabling employees to access and manage customer information. It is essential to secure the data on this server to protect the privacy and integrity of customer information. If the server were disabled or compromised, it could disrupt our daily business operations, result in data breaches, damage our reputation, and potentially lead to legal consequences.

## Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
|---|---|---|---|---|
| *Outsider* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Employee* | *Alter/Delete critical information* | *2* | *3* | *6* |
| *Hacker* | *Conduct Denial of Service (DoS) attacks* | *2* | *2* | *4* |

## Approach

The chosen threat sources and events are significant business risks for the following reasons:

- Outsider obtaining sensitive information: An external attacker could compromise the database server, leading to the exfiltration of sensitive customer data. This scenario is highly likely (Likelihood: 3) and has a severe impact (Severity: 3) as it could lead to data breaches, legal issues, and reputation damage.
- Employee altering/deleting critical information: Insider threats, such as employees, pose a risk of unauthorized changes to critical business data. While the likelihood is moderate (Likelihood: 2), the impact is severe (Severity: 3) because it could disrupt daily operations and integrity of data.
- Hacker conducting DoS attacks: This threat scenario involves a hacker sending excessive requests to overwhelm the server's capabilities. While the likelihood is moderate (Likelihood: 2), the impact is moderate (Severity: 2) as it might disrupt services temporarily.

## Remediation Strategy

To mitigate these identified risks, we propose the following security controls:

- Implement Principle of Least Privilege: Ensure that users, both internal and external, have the minimum level of access required to perform their duties. Limit access to sensitive data and critical system functions.
- Adopt Defense in Depth: Implement multiple layers of security controls, such as firewalls, intrusion detection systems, and access controls, to protect the database server from threats originating both internally and externally.
- Implement Multi-factor Authentication (MFA): Require users to provide multiple forms of identification to access the database server. This includes something they know (password) and something they have (e.g., a token or mobile app).
- Utilize Authentication, Authorization, and Accounting (AAA) Framework: Establish robust authentication mechanisms, set precise authorization rules, and maintain

comprehensive auditing. This ensures that only authorized users access the database server, limiting user privileges and tracking user activities.

By implementing these security controls, we aim to reduce the likelihood and impact of the identified threats and enhance the overall security of the database server.