Vulnerability Assessment Report

1st January 20XX

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 holds valuable business data, such as customer records, which are crucial for business operations and revenue generation.*
- *Securing this data is critical to maintaining the business's reputation and customer trust, as data breaches could lead to legal liabilities, customer loss, and financial damage.*
- *If the server is disabled or compromised, daily operations would be significantly disrupted, impacting employee productivity and customer satisfaction.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk (Likelihood * Severity)
Internal Employee	*Unauthorized data access or sharing of critical data*	*2*	*3*	*6*
Competitor	*Data exfiltration to gain a business edge or release critical*	*3*	*4*	*12*

	information to gain strategic advantages			
Cybercriminals/ Hackers	*SQL injection to extract sensitive and critical information*	*4*	*5*	*20*

Approach

This risk assessment focuses on threats specifically chosen due to the database's exposure and potential accessibility to external parties. Internal employees, while typically trusted, may intentionally or unintentionally access or share critical data without authorization. Competitors could target the organization through data exfiltration to gain a strategic advantage, especially if sensitive information provides insights into operations or products. Cybercriminals are particularly concerning due to their likelihood of employing techniques like SQL injection, a common method for extracting sensitive data from vulnerable databases. 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.