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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

This vulnerability assessment aims to evaluate and enhance the access controls of the database server to protect critical business data. The server supports essential operations, and its security ensures data confidentiality, integrity, and availability. A compromise could lead to financial losses, downtime, and reputational damage. Guided by NIST SP 800-30 Rev. 1, the assessment will identify and mitigate risks, ensuring the server's reliability and resilience during the period from June to August 20XX.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Install persistent and targeted network sniffers on organizational information systems.*	*1*	*3*	*3*
Operating system(s)	*Disrupt mission-critical operations.*	*1*	*2*	*2*
Hacker	*Alter/Delete critical information*	*2*	*3*	*6*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

This qualitative vulnerability assessment evaluates risks based on the likelihood and severity of potential threats, leveraging security knowledge and judgment. The selected threats represent significant business risks due to their potential impact on critical data and operations. An employee installing persistent sniffers could compromise sensitive information, posing a major confidentiality breach. Operating system disruptions could halt mission-critical operations, leading to downtime and financial losses. A hacker altering or deleting critical information directly threatens data integrity and could harm organizational trust. These threats highlight vulnerabilities requiring prioritized mitigation to ensure operational resilience and data security.

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.

To mitigate risks identified in the assessment, specific security controls can be implemented. Adopting the **principle of least privilege** ensures employees only have access to the resources necessary for their roles, reducing the risk of insider threats like installing sniffers. Implementing **multi-factor authentication (MFA)** strengthens access control, making it harder for hackers to compromise accounts and alter/delete critical information. For operating system disruptions, employing **defense in depth**—with layered security measures like firewalls, intrusion detection systems, and backups—ensures mission-critical operations remain resilient. These controls collectively enhance the system's security posture and reduce vulnerabilities effectively.