

# Vulnerability Assessment Report

1<sup>st</sup> 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?*

“The database server is a centralized computer system that stores and manages large amounts of data. The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations.”

## Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	Obtain sensitive information via exfiltration	3	3	9

<i>Employee</i>	<i>Disrupt mission-critical operations</i>	<i>2</i>	<i>3</i>	<i>6</i>
<i>Customer</i>	<i>Alter/Delete critical information</i>	<i>1</i>	<i>3</i>	<i>3</i>

## Approach

This section documents the approach used to conduct the vulnerability assessment report. It is important to be clear and concise when writing your approach. A transparent summary of your approach helps stakeholders understand that the assessment is credible and that the results can be used to make informed decisions.

Consider the following questions to help you write an approach section:

- *What was your rationale for selecting the risks that you evaluated?*
- *How were you deriving the likelihood and severity scores of each risk?*
- *What were the limitations of the assessment?*

*“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.”*

## Remediation Strategy

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. Any recommendations that you make should be realistic and achievable. Overall, the remediation section of a vulnerability assessment report helps to ensure that risks are addressed in a timely and effective manner.

Consider the following questions to help you write a remediation strategy:

- *Which technical, operational, or managerial controls are currently implemented to secure the system?*
- *Are there security controls that can reduce the risks you evaluated? What are those controls and how would they remediate the risks?*
- *How will the results of the assessment improve the overall security of the system?*

*“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.”*