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 purpose of this vulnerability assessment is help better secure the organization's database server, a valuable business asset that holds valuable hardware and is used to store important data. By helping to secure the data on the server we can better ensure that no breaches are made in the perceivable future. If a breach were to occur or systems were to shutdown, a disabling of this data server would be detrimental to the organization's workflow and credibility to its shareholders.

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?*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk

E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Unknown Threat Actor	Threat actors install network sniffers to collect traffic information.	*2*	*3*	*6*
Employee	Has enough authorization privileges to pose risk to company's security.	*3*	*3*	*9*

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.

For a data server as important as this it is important to look at both outsider and insider threat possibilities. A competitor poses a large risk to an organization in that they of all people would benefit from obtaining confidential information for financial reasons. Another outsider threat is an unknown threat actor; threat actors can perform attacks on an organization's network which is why it's important to scan this for vulnerabilities. An insider threat would be an employee with too many authorization privileges; this would be a common violation of the principle of least privilege and separation of duties standards. I ranked likelihood based on the chance that such attack would occur at some point soon and the organization would have to deal with it. I then ranked severity based off of the impact the attack would have on the organization if successful. Together these two scores gave me the risk factor. My only limitations for this assessment were that I do not know much about this companies' current security structure and their internal framework or how updated all of their security software is.

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?*