**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](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg#heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose**

Consider the following questions to help you write:

# The database server is a critical asset, as it stores and manages essential data for the business, including customer, employee, and company information. Securing this data is vital to prevent financial losses, legal issues, and damage to the company's reputation. If the server were disabled, it could severely disrupt operations.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Employee* | *Disrupt operations* | *2* | *3* | *6* |
| *Customer* | *Change critical information* | *1* | *3* | *3* |

# **Approach**

# The approach involved assessing risks related to the business's data storage and management procedures. Potential threat sources and events were identified based on the likelihood of a security incident. The severity of these incidents was evaluated in relation to their potential impact on company’s daily operations.

# **Remediation Strategy**

Implement authentication, authorization, and auditing mechanisms to ensure only authorized users can access the database server. This includes enforcing strong passwords, role-based access controls, and multi-factor authentication to restrict user privileges. Use TLS for encrypting data in motion, and apply IP allow-listing to corporate offices to prevent unauthorized internet users from connecting to the database.