**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/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) 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?*

*The database can hold sensitive information regarding employees and customers personal data and also include all the companies data. All of these are assets to the company and is needed for the company to function,*

* *Why is it important for the business to secure the data on the server?*

*The company needs to secure data on the server to stop a variety of threat actors from looking at what the data is at; it may be vital for the business operations or could be needed to hold employees and customers' sensitive personal information.*

* *How might the server impact the business if it were disabled?*

*If the server was disabled the business may not be operational as all the data they need to run whether that is data being collected or employee accounts to be accessible for them to carry out their job role.*

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Employee/customer* | Alter/Delete critical information | *2* | *3* | *6* |
| *Hacker* | Craft counterfeit certificates. | *1* | *3* | *3* |

# 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.

A competitor would gain an advantage by having information from the businesses database that could include sensitive records such as marketing strategies or even new products that are not currently patented meaning they could steal the ideas and make it their own product. Also they can just leak this information for the business to get bad press as it would be a data leak and would damage the reputation of the company.

Employees and customers could alter or delete critical information from the database if the right access controls are not in place this would be bad for the company as it could show false records of whatever information is stored and this would not comply with government or organisational compliance as it could go against things such as GDPR as all data should be accurate and stored safely.

Hackers could craft counterfeit certificates in order to obtain access to the database if the right access controls are not in place. They could create a certificate thats valid for them to access the company database as there may not be and external filtering on who can access the database.

# Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorised 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.