**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?*
* *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** |
| --- | --- | --- | --- | --- |
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Competitor* | *Alter/Delete critical information* | *1* | *3* | *3* |
| *Employee* | *Disrupt mission-critical operations* | *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.

The chosen threat sources and event are significant business risks for the following reasons:

* Hacker obtaining sensitive information: An external attacker could compromise the database server, leading to exfiltration of sensitive information by installing malicious software on organizational systems to locate and acquire the sensitive information. The scenario is high for likelihood (3) and severity (3) with risk point at 9.
* Competitor altering or deleting critical information: Competitor disguised as a customer and doing an attack based on the database server is open to the public from a competitor could lead to a threat to delete or alter that is critical to day-to-day business operations. The scenario is low for likelihood (1) and high for severity (3) with risk point at 3.
* Employees disrupt mission-critical operations. An internal threat from employees to compromise the integrity of information in such a way that prevents the business from carrying out critical operations. The scenario is moderate for likelihood (2) and high for severity (3) with risk point at 6.

# Remediation Strategy

* implement the principles of least privilege: ensuring that all of the users both internal and external have least or the minimum level of access required based on their roles to perform their duties.
* Implement the principle of defense in depth: implement multiple layers of security controls, such as firewall, intrusion detection system, access control, and continuous security audit to protect the database from internal or external threats.
* Implement MFA: require users to provide multiple forms of identification to access the database server. This includes something they know such as a password, something that they have such as access token for user ID and something the user has such as face recognition.
* Implement the AAA (authentication, authorization, and accounting) framework