**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

The database server is essential for storing business-critical data. Securing it protects sensitive information and ensures business continuity. If the server is disabled, operations could be disrupted, leading to financial loss and reputational damage.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Hacker Outsider* | *DDOS Attack* | *2* | *1* | *3* |
| *Insider Employee* | *Bypass access control and leak data* | *1* | *1* | *2* |

# Approach

This assessment focuses on three significant threat events: data exfiltration, denial of service (DoS), and insider threats. These were selected due to their high potential impact and relevance to publicly accessible database servers. Data exfiltration poses a severe risk to sensitive information, while DoS attacks can disrupt operations and affect service availability. Insider threats are often overlooked but can be highly damaging due to privileged access. Each was chosen based on likelihood and severity, using expert judgment and known industry trends.

# Remediation Strategy

To mitigate the risk of data exfiltration, implementing public key infrastructure (PKI) and encrypting sensitive data in transit and at rest is essential. For denial of service attacks, deploying intrusion detection systems (IDS) and rate-limiting controls can help prevent network overload. Enforcing the principle of least privilege and multi-factor authentication (MFA) will reduce insider threat risks by limiting user access to only necessary resources. These layered controls follow a defense-in-depth approach to protect the system across multiple threat surfaces.