**Vulnerability Assessment Report**

**20th November 2024**

Don Wickramanayake

# 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 October 2024 to December 2024. [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 a cornerstone of the business, supporting critical operations by storing and processing sensitive data, such as customer records, financial transactions, and operational metrics. Protecting this server is paramount to maintaining data confidentiality, integrity, and availability, which directly impact the organization’s reputation and operational continuity.

Without robust security measures:

* **Data Breaches**: Unauthorized access could lead to the exposure of confidential business information or personally identifiable information (PII), resulting in legal and financial repercussions.
* **Operational Disruptions**: A disabled or compromised server could halt business operations, delay decision-making, and interrupt service delivery to customers.
* **Financial Loss**: Downtime and data recovery efforts may incur significant costs, alongside potential fines for regulatory non-compliance.

Securing the database server through this assessment ensures the organization can identify vulnerabilities, prioritize remediation efforts, and maintain its business operations without compromising data security.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Malicious Insider/ unhappy employee* | *Unauthorized access to sensitive data* | *2* | *3* | *6* |
| *External Hacker/ fired employee* | *Exploit server vulnerabilities* | *2* | *3* | *6* |
| *Software Bug or Misconfigurations* | *Cause unintentional data exposure* | *3* | *2* | *6* |

# Approach

The risk assessment considered multiple threat sources likely to impact the company’s database server. Key threats identified include external competitors, malicious insiders, and potential vulnerabilities due to misconfigurations or open access.

1. **Competitors**: With the database accessible to external parties, there is a risk of competitors leveraging public data for their advantage, potentially undermining the company’s market position. This underscores the need for strict data access policies and encryption measures to protect sensitive information.
2. **Malicious Insiders**: A significant risk arises from the company's remote workforce, where an insider—whether intentionally or accidentally—might expose private business data. This highlights the importance of robust access controls, employee training, and monitoring mechanisms to mitigate internal threats.
3. **External Threat Actors**: An open public database increases the company's exposure to external threat actors who could exploit system vulnerabilities to introduce malicious software. These risks emphasize the necessity of regular vulnerability scans, timely patching, and firewall protections to secure the system.

By addressing these risks, the approach aims to enhance the database server's security, safeguarding the company’s operational integrity and reputation.

# Remediation Strategy

To address the risks identified, the following remediation strategies will be implemented:

1. **Strengthened Authentication and Authorization**:
   * Enforce strong password policies and require multi-factor authentication (MFA) to ensure secure access.
   * Implement role-based access controls (RBAC) to restrict user privileges based on job responsibilities, minimizing exposure to sensitive data.
2. **Data Encryption**:
   * Ensure all data in motion is encrypted using modern TLS protocols, replacing SSL to maintain industry-standard security for data transmissions.
3. **Network Access Restrictions**:
   * Configure IP allow-listing to permit access only from approved corporate office locations, reducing exposure to unauthorized users from the public internet.
4. **Monitoring and Auditing**:
   * Enable comprehensive auditing mechanisms to log and monitor database access and activities, providing visibility into potential unauthorized access attempts or insider threats.
5. **Vulnerability Management**:
   * Regularly perform vulnerability scans, promptly apply patches, and maintain system configurations to mitigate risks from software bugs and misconfigurations.

These strategies will reduce the likelihood of unauthorized access, protect sensitive business information, and ensure the resilience of the database server against internal and external threats.