**Vulnerability Assessment Report**

**26th January 2024**

# 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

This analysis serves a critical role in safeguarding the integrity and confidentiality of the customer data and financial information at XYZ Financial Services. The database server is the backbone of our business and we hold a legal and ethical obligation to maintain the integrity of our customer’s information. A security breach would have far reaching consequences including losing the trust of our customers. If the server were to be disabled business continuity would be disrupted, and there would be a significant financial loss as well as a negative impact on our customer’s confidence in our security.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Disgruntled employee* | *Conduct Denial of Service (DoS) attacks* | *3* | *4* | *12* |
| *Malicious software* | *Alters or deletes data that is critical*  *to day-to-day business operations.* | *3* | *5* | *15* |

# 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. There was also a cost benefit analysis made as well as a realistic timeline for implementation.

# Remediation Strategy

Firstly, ensure that only authorized users can access the database server. This includes using 2FA, strong passwords, and role-based access controls. Access control audits should be performed regularly to identify and rectify over-permissioned accounts. It is also important to enhance employee awareness of cybersecurity threats and best practices. In order to ensure timely application of security patches there should be a patch management team assembled as well as automated patch deployment implemented to streamline the patch management process. The network should be properly secured through proper segmentation. This will be done by implementing firewalls as well as regularly reviewing the network architecture. Finally, encryption and data protection measures should be taken. Sensitive data should be encrypted at rest as well as in transit. Encryption protocols should be regularly updated and data should be classified according to sensitivity and encrypted accordingly.