# Vulnerability Assessment Report

**1st January 20XX**

### **System Description**

The server is equipped with a high-performance CPU processor and 128GB of memory. It operates on the latest version of the Linux operating system and hosts a MySQL database management system. The system maintains a reliable network connection using IPv4 addressing and communicates with other servers within the company’s network infrastructure. Security configurations currently include SSL/TLS-encrypted connections to protect data in transit.

### **Scope**

This vulnerability assessment focuses on evaluating the **current access controls** and security configurations of the database system. The assessment covers a three-month period, from **June 20XX to August 20XX**, and follows the risk assessment framework outlined in **NIST SP 800-30 Rev. 1**.

### **Purpose**

The database server functions as a centralized repository that stores and manages large volumes of data, including customer details, campaign results, and analytical information. This data is essential for tracking business performance and personalizing marketing strategies.  
 Because the system supports key marketing and analytics operations, maintaining its security is vital. Any compromise of this server could lead to the exposure of sensitive customer data, disruption of ongoing marketing activities, and potential reputational damage to the company.

### **Risk Assessment**

| **Threat Source** | **Threat Event** | **Likelihood (1–3)** | **Severity (1–3)** | **Risk (L × S)** |
| --- | --- | --- | --- | --- |
| Hacker | Obtain sensitive information via data exfiltration | 3 | 3 | 9 |
| Employee | Disrupt mission-critical operations | 2 | 3 | 6 |
| Customer | Alter or delete critical information | 1 | 3 | 3 |

*Scale: 1 = Low, 2 = Medium, 3 = High.*

**Summary:** The highest risk is associated with potential **unauthorized access and data exfiltration by external attackers**, due to the system’s open access configuration. Insider threats and accidental data alterations also pose moderate risks to the integrity and availability of the system.

### **Approach**

This assessment evaluated risks related to the organization’s data storage and management practices. Potential threat sources and events were analyzed based on the **likelihood of occurrence** given the system’s current access permissions and security controls. The **severity of each potential incident** was then weighed against its likely impact on daily business operations. This approach ensures that the company can prioritize high-impact vulnerabilities while maintaining operational continuity.

### **Remediation Strategy**

To strengthen the database server’s security posture, the following remediation measures are recommended:

1. **Access Control and Authentication**
   * Implement strong authentication and authorization mechanisms to restrict access to approved users only.
   * Enforce the use of **strong passwords**, **multi-factor authentication (MFA)**, and **role-based access controls (RBAC)** to minimize user privileges.
2. **Encryption and Data Protection**
   * Replace outdated **SSL** connections with **TLS (Transport Layer Security)** to ensure robust encryption for data in motion.
   * Regularly review encryption certificates and ensure secure key management practices.
3. **Network Restriction**
   * Apply **IP allow-listing** to restrict database access to corporate offices and authorized remote networks.
   * Block all unauthorized or public internet access to the database server.
4. **Auditing and Monitoring**
   * Enable detailed **audit logs** to monitor access patterns and detect unauthorized activities.
   * Regularly review audit records and integrate monitoring with a centralized security information system (SIEM).