Vulnerability Assessment Report: Critical Database Access Control

Document Status: Final Draft for Executive Review

Prepared For: CIO and Risk Committee

Date: February 2025

Assessor: Kwang yeon Lee, IT Compliance Manager

Executive Summary

This report outlines a **Critical (CVSS 10.0 equivalent)** security vulnerability discovered on the Bank's core remote database server. The vulnerability stems from a legacy configuration that leaves the server **open to the public internet**, directly violating fundamental security principles outlined in **ISO/IEC 27001 (A.14) and the Digital Operational Resilience Act (DORA)**.

Immediate action is required to implement a zero-trust model. Failure to remediate this weakness exposes sensitive customer and financial data to unauthenticated access, resulting in an **unacceptable risk of data exfiltration and integrity compromise**, with potential regulatory fines and severe reputational damage. The primary threat identified is **External Attack Surface Exposure**, posing a "High" level risk.

1. Assessment Scope, Methodology, and Regulatory Alignment

Detail	Description
Asset Assessed	Core Remote Database Server (Linux OS, MySQL DBMS)
System Profile	Stores sensitive customer PII and financial transaction data. Accessed by 20000 remote employees globally.
Vulnerability Period	Server configured as "open to the public" for approximately 3 years.
Assessment Scope	CIA (Confidentiality, Integrity, Availability) of the data on the server.
Methodology	**NIST SP 800-30 Rev.1** (Risk Assessment) and **ISO/IEC 27001 Annex A** (Control Identification).
Regulatory Drivers	**DORA** (ICT Risk Management), **ISO 27001** (A.14: System Acquisition, Development and Maintenance), and **GDPR** (Data Protection by Design/Default).

2. Critical Findings and Risk Quantification

The most significant finding is the database server's **unrestricted exposure** to the public internet. This single vulnerability bypasses several layers of defense.

Finding ID	Vulnerability Description	Asset Impact	Likelihood	Risk Score
C-01	**Unrestricted Public Access:** Server access control is set *open to the public*, allowing initial connection attempts from any global IP address.	**Confidentiality, Integrity**	High (Inherent)	**Critical**
H-02	**Insufficient Authentication:** Reliance on basic username/password for 20000 global remote users across multiple jurisdictions.	**Confidentiality**	High	**High**
M-03	**Weak Authorization Policy:** Absence of a formalized Least Privilege or Role-Based Access Control (RBAC) structure.	**Integrity, Availability**	Medium	**Medium**

Detailed Analysis of Critical Finding (C-01)

The server's open configuration is an immediate and catastrophic failure of boundary protection.

- **Failure of DORA Compliance:** Directly contradicts DORA requirements for **ICT Risk Management** regarding the protection of network security and the maintenance of resilient ICT infrastructure.
- **Failure of ISO 27001 A.14:** Violates the principle of securing development/testing/operational environments and implementing system access control policies.
- **Analogy (Based on industry examples):** This is equivalent to leaving the vault door of a physical bank **permanently unlocked** and assuming the strong password on the safe inside is sufficient protection. No amount of internal control can compensate for the lack of a secure perimeter.

Detailed Analysis of High Finding (H-02)

Reliance solely on a single factor (username/password) for remote access by **20000 global employees** creates a vast attack surface highly susceptible to phishing and credential stuffing, elevating the risk from internal threat vectors.

- **Failure of ISO 27001 A.9 (Access Control):** The standard explicitly requires controls for secure log-on procedures. Relying on simple passwords fails to meet the expected security strength for a critical system.
- **GDPR Implications:** In the event of a breach, the lack of **Multi-Factor Authentication (MFA)** would be viewed by regulatory bodies as a clear negligence in implementing appropriate

technical and organizational measures (TOMs) to protect customer Personal Identifiable Information (PII).

- **Internal Threat Amplification:** Compromised user credentials (e.g., via a remote workstation breach) would grant an attacker unimpeded, authenticated access, bypassing any perimeter controls (once C-01 is fixed) and leading directly to data exfiltration or manipulation. This control deficiency exposes the bank to increased risk from advanced phishing campaigns targeting remote workers.

Detailed Analysis of Medium Finding (M-03)

The absence of a formalized **Role-Based Access Control (RBAC)** model and the failure to enforce the **Principle of Least Privilege (PoLP)** means that most, if not all, of the 20000 remote users likely have unnecessary or excessive permissions.

- **Failure of ISO 27001 A.9 (Access Control):** Violates the fundamental requirement to restrict access to information and application system functions based on the authorization policy.
- **Impact on Integrity:** A data integrity event (e.g., accidental deletion or modification of financial records) is highly likely because too many users have write/delete permissions for data they do not strictly need for their job functions.
- **Audit and Forensics Difficulty:** Without defined roles and documented privilege levels, conducting **forensic analysis** and fulfilling regulatory audit requests (especially under DORA's accountability provisions) becomes extremely difficult, as it is impossible to quickly isolate the source of an unauthorized action. This systemic weakness suggests a fundamental flaw in the Bank's governance structure for data ownership.

3. Remediation Strategy and Control Implementation

The remediation strategy must be immediate, prioritized, and documented under the governance of the IT Risk Committee.

Priority	Remediation Step	Policy/Control Standard	IT Compliance Manager Role
P1 - IMMEDIATE	**Isolate External Access:** Immediately restrict all external connections using **IP Allow-Listing** to specific corporate office IP addresses only. Close the external firewall ports to the public.	ISO 27001 A.13 (Communications Security)	**Directly manage the change control process** and secure sign-off from the CIO.
P2 - HIGH	**Enhance Authentication:** Mandate and deploy **Multi-Factor Authentication (MFA)** for all 20000 remote users accessing the database server.	DORA (Operational Resilience), ISO 27001 A.9 (Access Control)	**Coordinate the global MFA rollout** and create required user training and awareness documentation.

P3 - MEDIUM	**Implement Strong Authorization:** Enforce the principle of **Least Privilege** and implement a granular **Role-Based Access Control (RBAC)** model for all users (internal threat mitigation).	ISO 27001 A.9 (Access Control)	**Lead cross-functional workshop** with data owners and department heads to define and document the new RBAC structure.
P4 - LONG-TERM	**Adopt PKI and AAA:** Implement a **Public Key Infrastructure (PKI)** to verify all authorized devices and institute a robust **AAA Framework** (Authentication, Authorization, and Accounting) to audit access provision continuously.	DORA, ISO 27001 A.12 (Operations Security)	**Manage the governance project** for PKI deployment and integrate access audit logs into the central Security Information and Event Management (SIEM) system.

4. Governance and Reporting Requirements

To ensure sustainable risk mitigation and compliance with regulatory expectations for continuous improvement, the following governance measures are recommended:

1. **Risk Acceptance Policy:** Require formal, documented **risk acceptance** from the Executive Board for any delay in implementing P1/P2/P3 remediation actions.
2. **Risk Working Group:** Establish a dedicated, cross-functional working group (including IT Operations, Compliance, and Legal) to track the **Key Risk Indicators (KRIs)** associated with access control (e.g., percentage of users not yet enrolled in MFA).
3. **DORA Alignment:** Integrate the server's vulnerability and remediation status into the wider DORA-mandated **ICT Risk Management Framework**, ensuring that controls are continuously tested and reviewed.
4. **Executive Reporting:** Update the Executive Board monthly on the progress of P1-P4 deployment, highlighting remaining risks and resource needs.