Vulnerability Assessment Report: Critical Database Access Control

Client: Tier-2 European Financial Institution (EU Bank)

Document Status: 1.0 (Executive Review)

Prepared For: CIO and Risk Committee

Date: February 2025

Assessor: Kwang yeon Lee, IT Compliance Manager

Focus: Non-Compliance with DORA and VAIT Mandates on Access Control

1. Executive Summary: Critical Regulatory Violation

This report outlines a **Critical (CVSS 10.0 equivalent)** security vulnerability rooted in a legacy configuration of the Bank's core remote database server. The vulnerability—leaving the server **open to the public internet**—directly violates fundamental regulatory principles across the EU financial services sector.

Conclusion: This exposure represents an **unacceptable regulatory risk** for the Bank. It constitutes a material breach of **DORA Article 10 (ICT Security Policies), VAIT AT 4.3 (Security Measures), and NIS2 Article 20 (Risk Management)**. Failure to remediate immediately exposes sensitive customer PII and financial transaction data to unauthenticated external access, threatening regulatory fines and severe reputational damage.

Immediate Action Mandate: Deploy a zero-trust architecture, commencing with immediate isolation (P1) and rapid implementation of a formal **Authentication, Authorization, and Accounting (AAA) Framework**.

2. Assessment Scope, Context, and Regulatory Alignment

2.1 Client Scenario and Business Context

The vulnerability was identified on a database server supporting the Bank's **Critical Function of Retail Transaction Processing.**

Detail	Description
Asset Assessed	Core Remote Database Server (Linux OS, MySQL DBMS)

Business Criticality	Supports the primary digital banking channel; **direct impact on customer PII and financial ledgers**. Failure triggers a DORA Level 1 Incident.
Vulnerability Origin	Server configured as "open to the public" for approximately 3 years, stemming from a **legacy setup during the integration of an Eastern European subsidiary**. This indicates a severe breakdown in **Post-Acquisition Governance**.
System Profile	Accessed by 20,000 remote employees (IT, Finance, and Risk) globally. Security is limited to SSL/TLS encryption for data in transit and password access.
Assessment Scope	CIA (Confidentiality, Integrity, Availability) of the data on the server, focusing on access control governance.
Methodology	**NIST SP 800-30 Rev.1** (Risk Assessment), supplemented by **DORA/VAIT** cross-referencing for financial sector impact scoring.

2.2 Regulatory Context and Gap Identification

The table below maps the technical vulnerability to the specific regulatory mandates it violates, confirming the **governance gap**:

Regulation / Standard	Relevant Mandate	Gap Identification (Violation)
DORA (Art. 10)	Requires robust ICT security policies concerning access control.	**FAILURE:** The configuration allows unauthorized external access, fundamentally violating the principle of restricted access.
VAIT (AT 4.3)	Demands strong security measures for access to IT systems, especially for critical data.	**FAILURE:** Critical financial data is not protected by network segmentation or strong authentication barriers.
NIS2 (Art. 20)	Requires organizations to implement risk management measures, including access control and encryption.	**FAILURE:** Lack of network isolation compromises the foundational security baseline required for network security.
ISO 27001 (A.5, A.14)	Requires a defined set of access control policies and secure system engineering practices.	**FAILURE:** The configuration demonstrates a severe breakdown in operational security change management and baseline controls.

3. Detailed Vulnerability Analysis and Remediation Plan

3.1 Critical Finding: External Attack Surface Exposure

Finding	Threat Source	Risk Score	Impact
Open to Public Internet	External Attack Surface Exposure	**Critical (10.0)**	**Data Exfiltration:** Unauthenticated access to PII and transactional data. **Regulatory Fine:** Direct violation of DORA/VAIT, risking severe enforcement action.
Analysis	The server's public IP address allows connection attempts from *any* internet location globally, exposing the authentication mechanism directly to brute-force and credential-stuffing attacks. This bypasses the first line of defense required for a financial institution. **Governance Gap:** This configuration was not identified or corrected during mandatory system reviews, indicating a failure in the **Internal Control System (ICS)** testing for new assets.		
Regulatory Ramification	**Direct DORA violation.** If a breach occurred, the regulator (e.g., BaFin) would cite this configuration as **Gross Negligence** concerning ICT risk management.		

3.2 High Finding: Shared Administrative Accounts and Weak Passwords

Finding	Threat Source	Risk Score	Impact
Shared Admin Accounts	Insider Threat / Lack of Accountability	**High (8.5)**	**Non-Repudiation Failure:** Inability to trace malicious or erroneous database changes back to an individual user, violating basic audit trails.

Analysis	Multiple privileged database users (e.g., DB_Admin_Ops) are shared by teams (IT Operations, DevOps, Finance). Furthermore, the password policy for these accounts is limited to 8 characters with no complexity checks. This fails the principle of **Segregation of Duties (SoD)** and increases the risk of **Business Email Compromise (BEC)** leading to privileged access.		
Regulatory Ramification	Violates **VAIT AT 4.3.1 (Individualized Access)** and **ISO 27001 A.5.15 (Access Control)**. Represents a fundamental weakness in our ability to perform post-incident forensic analysis.		

3.3 Medium Finding: Deficient Audit Logging and Monitoring

Finding	Threat Source	Risk Score	Impact
Decentralized Logs/No Review	Hidden Incidents / Compliance Failure	**Medium (6.5)**	**Delayed Detection:** Inability to detect a slow, targeted attack (e.g., data exfiltration over weeks) or monitor abnormal access patterns, failing DORA's incident management timeframes.
Analysis	Database access logs are stored locally on the server and are only reviewed on an ad-hoc basis (quarterly). There is no automated feeding of these logs into a central **Security Information and Event Management (SIEM)** system. This compromises the Bank's ability to meet the **NIS2** requirement for adequate monitoring and rapid incident detection.		
Regulatory Ramification	Directly violates **DORA Article 15 (ICT Incident Management)** and **NIS2 Article 21 (Monitoring)**, which mandate robust mechanisms for detecting anomalous activity impacting Critical Information Systems.		

4. Remediation Strategy, Control Implementation, and Governance

The remediation strategy is a phased program that tackles the technical findings through strategic **governance projects**, ensuring sustainable compliance.

4.1 Remediation Roadmap (4 Phases)

Priority	Phase / Action	Solution Steps & Concrete Work Example	Regulatory Alignment	Owner
P1 - IMMED.	**Isolation & Emergency Closure (Critical)**	**Immediate Firewall Deployment:** Apply a mandatory perimeter firewall policy blocking all non-corporate-VPN IP ranges. **Concrete Example:** Implement **IP Allow-Listing** policy validated by IT Security and approved by the CISO.	DORA Art. 10 (Network Security)	Head of IT Ops
P2 - SHORT-TERM	**Zero-Trust Enforcement (High)**	**Mandate MFA & Phased Decommission:** Implement Multi-Factor Authentication (MFA) for *all* remote users. Begin a 90-day project to **phase out all shared administrative accounts** (e.g., replace shared DB_Admin_Ops with individual privileged accounts managed by a PAM system).	VAIT AT 4.3 (Authentication)	IT Security
P3 - MEDIUM-TERM	**RBAC and Policy Overhaul (High/Medium)**	**Policy Overhaul:** Establish a formal, DORA-compliant **Access Control Policy**. Conduct a **Cross-functional workshop** with data owners to define the new **Role-Based Access Control (RBAC)** structure based on the **Principle of Least Privilege**.	ISO 27001 A.5 (Policies)	IT Compliance
P4 - LONG-TERM	**AAA Governance and Monitoring (Medium)**	**Centralized Logging & SIEM Integration:** Implement a log forwarding agent to push all database access logs to the Bank's central **SIEM system.**	NIS2 Art. 21 (Monitoring)	IT Governance/CISO

		Establish a formalized **Security Operations Center (SOC)** function to continuously monitor and report on anomalous access patterns (24/7 coverage).		

4.2 Control Implementation and Governance Requirements

To ensure these fixes are sustainable and meet the continuous compliance mandates of DORA and VAIT:

1. **Privileged Access Management (PAM) System:** Charter a project to procure and deploy a dedicated PAM solution. This will enforce MFA, session recording, and automatic credential rotation for all privileged access accounts, eliminating the risk of human error or shared credentials.

2. **Internal Control System (ICS) Integration:** The **P1-P4 remediation plan** must be formally integrated into the Bank's **ICS**. This requires mandatory, periodic **testing** by Internal Audit to verify that the firewall rules remain active and that MFA enrollment is 100% compliant.

3. **DORA-Specific Training:** Update the mandatory compliance training for **IT Operations staff** to include specific modules on DORA's Article 10 requirements regarding system hardening and access configuration.

4.3 Risk Management and Executive Reporting

1. **Risk Acceptance Policy:** Any delay exceeding the deadlines for P1 (3 days) or P2 (90 days) must be documented as a **material increase in regulatory risk** and requires formal, documented **risk acceptance** from the **Executive Board**.

2. **DORA Alignment:** Integrate the server's vulnerability and remediation status into the wider DORA-mandated **ICT Risk Management Framework**. The status of **P1 (Isolation)** is a Key Risk Indicator (KRI) that must be reported to the Board monthly until closed.

3. **Audit Readiness:** Upon completion of P4, perform a **Post-Implementation Review (PIR)** audit to certify that all controls meet the strict requirements of BaFin/ECB auditors, preparing the Bank for future DORA-related audits.