Internal Security Audit & Compliance Report:

DORA Compliance and Operational Resilience

Client: EU Retail Bank (Tier-2 Financial Institution)
Document Version: 2.0 (Executive Briefing for DORA Gap Closure)
Prepared For: Executive Board (Risk Committee) and Global IT Compliance Office
Date: February 2025
Assessor: Kwang yeon Lee, IT Compliance Manager

1. Executive Summary: DORA Compliance and Risk Imperatives

This internal audit assesses the IT compliance and operational resilience posture of the EU Retail Bank against mandatory financial regulations, specifically the **Digital Operational Resilience Act (DORA)** and **VAIT** (German requirements).

Key Conclusion: The Bank's existing governance structure and resilience framework are **Critically Non-Compliant** with DORA's core mandates, primarily concerning **ICT Third-Party Risk Management** and System Resilience Testing. The failure to define and map Critical Functions creates an unacceptable risk of regulatory enforcement action.

Immediate Action Mandate: The Board must immediately sanction the **DORA Gap Closure Program**. The highest priority is to establish a verified **ICT Third-Party Register** and formally adopt the required **Digital Operational Resilience Strategy**.

2. Audit Scope, Goals, and Workflow

2.1 Audit Goals

The primary goals of this assessment were to:

1. **Verify DORA Compliance:** Evaluate alignment with DORA Articles 4, 15, and 28 concerning Governance, Incident Reporting, and Third-Party Risk.

2. **Assess VAIT/ISO Alignment:** Confirm that existing controls meet the required standard for an EU financial institution (VAIT, ISO 27001).

3. **Map Critical Functions:** Identify and document the criticality of business processes to underpin **Business Continuity Planning (BCP).**

2.2 Assessment Scope

The scope focused on the **Governance, Documentation, and Testing** of the Bank's core digital infrastructure and data assets as required by DORA.

Component	Scope Status	Assessment Focus
Governance Structure	In Scope	Board responsibility, IT Steering Committee oversight, Risk Taxonomy integration.
ICT Third-Party Register	In Scope	Completeness, critical function mapping, contractual resilience clauses.
Operational Resilience	In Scope	Testing protocols (e.g., threat-led penetration testing), RTO/RPO definitions.
Branch/Physical Security	Out of Scope	Focused solely on ICT infrastructure and governance controls.

2.3 Audit Workflow: Professional Methodology

The assessment followed a structured, risk-based methodology used in my prior experience at the IMF and Coupang:

1. **DORA Gap Analysis:** Reviewed artifacts against mandatory DORA requirements (e.g., Art. 4—Governance, Art. 15—Incident Management).

2. **Control Gap & ICS Testing:** Assessed the effectiveness of internal controls (ICS) using a sample-based testing approach, aligning findings to **VAIT and ISO 27001 Annex A.**

3. **Risk Quantification:** Assigned scores based on the likelihood of regulatory fine (high) and the impact on financial stability (critical).

4. **Executive Reporting:** Delivered a prioritized, phased remediation roadmap for Board review.

3. Control Assessment: Critical DORA and VAIT Gaps

The audit identified deficiencies across three critical control domains, highlighting significant non-compliance risk.

3.1 Administrative Controls (DORA and Governance)

Finding ID	Finding Description	Risk Score	Recommended Control (DORA Art. 4 & VAIT AT 3.1)
D-01	**No Formal DORA Strategy:** The **Board** has not formally adopted the mandatory **Digital Operational Resilience Strategy**, nor has it fully defined or approved the **Risk Appetite** for ICT resilience.	**Critical**	**Board Mandate**: Formal adoption of the DORA Strategy and clear assignment of ICT roles/responsibilities to the management body.
D-02	**Immature Incident Management:** Incident response procedures are documented but have **not been tested end-to-end** for critical functions, failing DORA's Article 15 requirements.	**High**	Implement a mandatory, quarterly program of **Threat-Led Penetration Testing (TLPT)** exercises, fully documenting and reporting outcomes to the Board.
D-03	**Missing Critical Function Mapping:** Business and IT have not collaborated to definitively identify and map **Critical or Important Functions (CIF),** undermining RTO/RPO definition.	**High**	Launch a **Cross-Functional Working Group** to map the entire operational risk taxonomy to the required **CIF** definitions.

3.2 Technical Controls (ISO 27001 and Resilience)

Finding ID	Finding Description	Risk Score	Recommended Control (ISO 27001 A.12 & VAIT AT 4.2)
T-01	**Unsecured Privileged Access: Multi-Factor Authentication (MFA)** is absent on all non-client-facing critical infrastructure	**High**	Mandate **MFA** for all privileged access accounts. Implement a Privileged Access Management

	(e.g., core banking database servers, privileged admin jump boxes).		**(PAM)** solution with session recording.
T-02	**Untested Disaster Recovery: The Disaster Recovery Plan (DRP)** is documented but the last recorded **full system restoration test** was 18 months ago, failing DORA's requirement for regular testing.	**High**	Schedule **mandatory, documented DRP failover testing** twice annually, with results reviewed by the Risk Committee.
T-03	**Unmanaged Legacy Systems:** Several core banking and data warehousing systems are running on **End-of-Life (EoL)** operating systems, presenting unpatchable vulnerabilities.	**Medium**	Charter a dedicated project to **decommission or migrate** all EoL systems within 12 months, in line with VAIT requirements for system lifecycle management.

3.3 Third Party and Physical Controls

Finding ID	Finding Description	Risk Score	Recommended Control (DORA Art. 28)
P-01	**Incomplete Third-Party Register:** The mandatory **ICT Third-Party Register** is incomplete; it lacks full identification of sub-service providers and critical dependencies required by DORA Article 28.	**Critical**	**ICT Third-Party Vetting**: Immediately complete the Register and conduct a due diligence review on all critical vendors, ensuring DORA-compliant termination clauses.
P-02	**Branch Control Variation:** Significant variance in physical access and monitoring controls across international branch offices (e.g., varying standards for CCTV and secure data destruction).	**Medium**	Harmonize the **Physical Security Policy** globally, enforcing minimum standards for restricted areas via the Internal Control System (ICS).

4. Compliance Checklist: Regulatory Status

This status update provides a clear-cut view of the Bank's regulatory posture, highlighting the mandates of particular interest to the German regulator (BaFin).

Regulation / Standard	Requirement Status	Critical Gap Description	Action Mandate
DORA (EU)	**Non-Compliant**	Failure to adopt **DORA Strategy** and implement required **Third-Party Risk (Art. 28)** and **Resilience Testing (Art. 24)**.	*Immediate Board Oversight and Program Charter*
VAIT (Germany)	**GAP**	Non-adherence to requirements for **System Lifecycle (AT 4.2)** due to EoL systems and lack of documented **Internal Audit** cycles.	*IT Governance Program Implementation*
ISO 27001	**Immature**	Lack of a formalized, end-to-end **Information Security Management System (ISMS)** charter and associated policy library.	*ISMS Implementation Project (Foundational)*
GDPR (EU)	**Medium Risk**	General Data Protection Regulation requirements are addressed on the client side, but internal **Data Classification** and **Data Masking** standards require enforcement.	*Data Governance Policy Enforcement*

5. Stakeholder Memorandum: Prioritization and DORA Gap Closure Program & Accountability

TO: Executive Board (Risk Committee)
FROM: Kwang yeon Lee, IT Compliance and Governance Manager
Date: February 2025

SUBJECT: URGENT: Post-Deadline DORA Non-Compliance Remediation Plan

The findings confirm that the Bank is currently operating in a state of **Regulatory Non-Compliance** following the mandatory DORA application date of January 2025. This is no longer a matter of preparation; it is one of material **regulatory exposure** and poses a direct threat to the Bank's license to operate.

We must immediately launch a high-priority, dedicated **DORA Remediation Program** to shift from a posture of non-compliance to one of regulatory defense.

DORA Gap Closure Program: Phased Action Plan

This plan prioritizes mandatory governance and third-party risk (DORA Articles 4 and 28) and allocates resources to urgent technical remediation and testing (DORA Article 24).

I recommend the immediate allocation of resources to launch the following three-phase project:

Phase 1: Immediate Remediation & Accountability (0-6 Months)
Focus: Establishing legal and governance defense mechanisms.

Action	DORA Article / Finding Addressed	Concrete Deliverables	Owner
1.1 Formalize Governance & Strategy	Art. 4 (Governance) / D-01	**Immediate Board Resolution** formally adopting the Digital Operational Resilience Strategy, backdated and documented with a clear remediation path. **Designation of a single Executive Board member accountable** for closing the compliance gap.	CEO / Board
1.2 Critical Function Mapping	Art. 11 (Business Functions) / D-03	Finalized **Critical and Important Functions (CIF)** register. Documented **RTOs** and **RPOs** signed off by Business Unit Heads, demonstrating structured risk identification.	CRO / Compliance
1.3 ICT Third-Party Remediation	Art. 28 (Third-Party Risk) / P-01	**100% completion of the ICT Third-Party Register.** Urgent review and remediation of contractual clauses with all Critical Service Providers to enforce DORA-mandated audit and termination rights.	Procurement / Legal

Phase 2: Technical Hardening and Validation (6-12 Months)

Focus: Implementing technical controls required for sustained resilience.

Action	DORA Article / Finding Addressed	Concrete Deliverables	Owner
2.1 Enhanced Access Control	Art. 10 (Access) / T-01	Deployment and mandatory enforcement of **Multi-Factor Authentication (MFA)** for all privileged access. Full implementation of a **Privileged Access Management (PAM)** solution across critical infrastructure.	CISO / IT Security
2.2 DRP Testing & Validation	Art. 24 (Testing) / T-02	Execution of **First Full DRP Failover Test** based on CIF RTOs. This is a non-negotiable regulatory requirement; results must be documented, and presented to the Risk Committee.	Head of Infrastructure
2.3 TLPT Implementation	Art. 26 (TLPT) / D-02	Scoping and commencement of the **Threat-Led Penetration Testing (TLPT) program**, focusing on the newly mapped CIFs.	IT Audit / CISO

Phase 3: Sustainment, Audit, and Maturity (12+ Months)

Focus: Achieving a demonstrable and auditable state of compliance.

Action	DORA Article / Finding Addressed	Concrete Deliverables	Owner
3.1 Legacy System Decommission	VAIT AT 4.2 / T-03	Full retirement or migration of all identified **End-of-Life (EoL)** operating systems and applications to eliminate unpatchable systemic risk.	Project Management Office (PMO)
3.2 Compliance Training	Art. 13 (Awareness) / A-03	Launch of mandatory, role-specific **DORA and Cyber Awareness Training program**, targeting international subsidiaries and Board members.	HR / Compliance
3.3 Continuous Reporting	Art. 15 (Incident Reporting)	Implementation of a **Quarterly Resilience Dashboard** for the Executive Board, tracking key DORA metrics (RTO breaches, incident volumes, third-party compliance status) and providing transparency on remediation progress.	IT Compliance

Conclusion: A Call to Fiduciary Responsibility

The gaps identified in this report constitute **a failure of our fiduciary duty** to safeguard the Bank's operational continuity as mandated by EU law. Every day we operate without a formal DORA Strategy or a validated Third-Party Register, we compound our regulatory liability.

The time for planning has passed. The time for decisive action is now.

We recommend the Executive Board immediately **sign off on this Remediation Plan and allocate the necessary funding** to close these critical gaps within the next 12 months. This investment is not discretionary; it is an **urgent risk containment measure** essential to protect our capital, our reputation, and our legal standing with the supervisory authorities.

We must shift from compliance effort to compliance defense. Our regulatory status depends on the Board's commitment today.