IT Compliance Risk Assessment Executive Report:

Strategic Operational Resilience

Client: Tier-2 European Financial Institution (EU Bank)
Document Version: 3.0 (Comprehensive Strategic Briefing)
Prepared For: Executive Board (Risk Committee) and Group CIO
Date: February 2025
Assessor: Kwang yeon Lee, IT Compliance and Governance Manager

1. Executive Summary: Prioritized Risk Posture

This comprehensive assessment evaluates five critical IT and cyber risks across the Bank's operational landscape, directly linking technical exposure to binding EU regulations (**DORA, VAIT, NIS2**).

The analysis, which covered the environment supporting **2 million** retail and **20,000** commercial accounts, confirms that systemic governance gaps in **Access Control** and **Third-Party Management** pose the highest immediate threat to the Bank's regulatory standing.

Risk ID	Risk Category	Priority Score (Out of 10)	Primary Regulatory Violation	Remediation Status
RA-01	**Uncontrolled Data Access**	**9 (Critical)**	DORA Art. 10 / VAIT AT 4.3	Immediate Isolation Complete (P1)
RA-02	**Compromised User Database**	**8 (High)**	NIS2 Art. 21 / ISO 27001 A.14	Requires Full AAA Framework Deployment
RA-03	**Insider Threat/BEC**	**7 (High)**	VAIT AT 5.2 (Awareness)	Susceptibility Reduced (42% -> 15%)
RA-04	**Supply Chain Dependency**	**7 (High)**	DORA Art. 28 (TPRM)	**Critical Gap - Requires Funded Program**
RA-05	**Physical Asset Loss**	**5 (Medium)**	ISO 27001 A.11 (Physical Security)	Policy Remediation Underway

Mandate: We must immediately allocate resources to deploy the **Authentication, Authorization, and Accounting (AAA) Framework** and fund the **DORA Third-Party Risk Management (TPRM)** Program to achieve a secure and compliant operational posture within the next 12 months.

2. Risk Taxonomy and Regulatory Context

2.1 Risk Quantification Methodology

Risks are prioritized using a quantitative model where the **Priority Score = Likelihood x Impact**. Impact specifically includes financial loss, reputational damage, and, most critically, **Regulatory Penalties** under DORA.

Risk ID	Likelihood (1-5)	Impact (1-5)	Priority Score (1-25)	Regulatory Focus
RA-01	5 (Very High)	4 (Major)	**20 (Critical)**	DORA, VAIT
RA-02	4 (High)	4 (Major)	**16 (High)**	NIS2, ISO 27001
RA-03	4 (High)	3 (Significant)	**12 (High)**	VAIT, ISO 27001
RA-04	3 (Medium)	4 (Major)	**12 (High)**	DORA Art. 28
RA-05	3 (Medium)	2 (Minor)	**6 (Medium)**	ISO 27001

3. Detailed Risk Analysis, Regulatory Alignment, and Remediation

3.1 RA-01: Uncontrolled External Data Access (Critical)

Risk Element	Analysis and Regulatory Alignment
Finding: Publicly Accessible Backup Server (7TB)	A critical server holding **7TB of unencrypted customer data** was found externally accessible due to a legacy misconfiguration from a recent subsidiary integration.
Regulatory Alignment:	**DORA Article 10 (ICT Security):** Direct failure to protect network access points. **VAIT AT 4.3 (Security Measures):** Unacceptable lack of basic access controls (firewall/VPN).
Impact & Figure:	**Estimated Exposure:** Potential regulatory fines could exceed **$10M** (due to DORA/GDPR overlap) plus remediation costs. The risk of **Data Integrity Compromise** is unacceptable.
Action & Resolution (Managerial):	**Immediate P1 Isolation:** Personally led the **Incident Response Team (IRT)** to apply an immediate **IP Allow-List** policy to the perimeter firewall. This eliminated the external attack surface within **90 minutes** of discovery. Created a **Security Exception Report** for the Risk Committee, documenting the failure and the rapid mitigation action to demonstrate proactive risk containment.

3.2 RA-02: Compromised User Database (High)

Risk Element	Analysis and Regulatory Alignment
Finding: Weak Authentication and Default Passwords	Audit identified multiple critical systems using shared, non-MFA privileged accounts and the use of default vendor credentials on development databases. Password hashing standards are outdated (SHA-1).
Regulatory Alignment:	**NIS2 Article 21 (Access Control):** Failure to ensure robust access control and encryption mechanisms. **ISO 27001 A.14 (System Acquisition):** Indicates a failure in secure development and default hardening procedures.
Impact & Figure:	**Risk:** A single breach of the system administrator database could grant an attacker access to **25%** of the Bank's core banking systems.
Action & Resolution (Forward Strategy):	**Project Charter: AAA Framework Deployment:** Initiate a dedicated project to deploy a complete **Authentication, Authorization, and Accounting (AAA)** framework. Upgrade all password storage to **Argon2 or bcrypt** and enforce mandatory **Multi-Factor Authentication (MFA)** for *all* privileged users within **180 days**.

3.3 RA-03: Insider Threat via Social Engineering (High)

Risk Element	Analysis and Regulatory Alignment
Finding: High Phishing Susceptibility	Initial testing showed a **42% click-through rate** on phishing simulations, indicating a vulnerable "human firewall" across the international staff base.
Regulatory Alignment:	**VAIT AT 5.2 (Employee Awareness):** Mandates periodic and targeted training and a clear metric for effectiveness. **DORA Article 13 (Awareness):** Requires staff to be trained on resilience-relevant incidents.
Impact & Figure:	**Risk:** High likelihood of Business Email Compromise (BEC) leading to system access. **Cost:** Required investment for continuous training: **$250,000** annually to maintain compliance.
Action & Resolution (Managerial):	**Developed Continuous Training Program:** Designed and rolled out mandatory, role-specific **cybersecurity awareness training** and monthly phishing simulation drills across all **1,200 staff**. **Result:** Susceptibility rates dropped to **below 15%** within three months, measurably achieving the **VAIT** standard for awareness.

3.4 RA-04: Supply Chain Dependency (High)

Risk Element	Analysis and Regulatory Alignment
Finding: Single Point of Failure in Critical Third-Party Service	Operational continuity for the **Retail Transaction Processing Critical Function (CIF)** relies on a single logistics and cloud provider situated in a geopolitically vulnerable region.
Regulatory Alignment:	**DORA Article 28 (Third-Party Risk):** Requires identification and mitigation of single points of failure in the ICT supply chain. **VAIT AT 7.1 (Outsourcing):** Demands documented contingency plans for essential outsourced services.
Impact & Figure:	**Risk:** Potential for catastrophic service disruption (RTO breach) lasting **>48 hours** in the event of a regional incident. **Cost:** Estimated remediation budget for vendor diversification: **$1.2 Million**.
Action & Resolution (Forward Strategy):	**Program Charter Creation: DORA TPRM** Drafted the charter for the **DORA TPRM Remediation Program**. The next step requires the Board to authorize the **$1.2M** budget to secure alternative, geographically diverse service providers and integrate DORA-compliant audit/exit clauses into all critical contracts within **9 months**.

3.5 RA-05: Physical Asset Loss (Medium)

Risk Element	Analysis and Regulatory Alignment
Finding: Uncontrolled Access to Data Centers	Inconsistent access controls (e.g., lack of mandatory keycard systems, unmonitored server rooms) across satellite branch data closets expose physical servers to unauthorized access or theft.
Regulatory Alignment:	**ISO 27001 A.11 (Physical and Environmental Security):** Requires clear perimeter protection and defined security boundaries. **NIS2 Article 21 (Physical Security):** Requires physical and environmental protection of ICT systems.
Impact & Figure:	**Risk:** Potential for hardware loss or data tampering, affecting **Availability (A)**. **Mitigation Cost:** Initial budget for standardized CCTV and access control deployment: **$350,000**.
Action & Resolution (Managerial):	**Policy Harmonization:** Issued a global directive to harmonize the **Physical Security Policy** across all international branches, enforcing minimum standards for restricted areas (including mandatory access logging). Developed a **Physical Security Audit Checklist** for local IT teams to self-certify compliance monthly.

4. Conclusion and Strategic Investment Mandate

This report confirms that while we have demonstrated immediate capability in crisis management (RA-01), **sustained compliance requires strategic investment in governance projects.**

The Bank is currently exposed to systemic regulatory risk due to governance gaps in two primary areas: **Access Control (RA-02) and Supply Chain Resilience (RA-04).**

4.1 Strategic Recommendations and Call to Action

1. **Fund the DORA TPRM Program: Immediate authorization of the $1.2 Million budget** is required to mitigate Risk RA-04. This is a non-negotiable step to comply with **DORA Article 28** and eliminate the single point of failure in our critical service chain.

2. **Charter the AAA Framework Project:** Authorize the project to close Risk RA-02 by rolling out **MFA, PKI, and RBAC** across the enterprise. This investment secures our perimeter and ensures we meet the auditability requirements of **NIS2** and **VAIT**.

3. **Mandate Quarterly KRIs:** The Executive Board must define and approve the Bank's maximum **Risk Appetite** and receive mandatory quarterly reports on **Key Risk Indicators (KRIs)**, specifically tracking:

    - **Phishing Susceptibility Rate** (to ensure RA-03 stays below 15%).
    - **Mean Time to Patch (MTTP)** for all critical vulnerabilities.
    - **Coverage of Critical Assets by AAA/MFA** (target 100% within 12 months).

This is the decisive moment: Our success in the European financial sector depends on moving from reactive maintenance to proactive, governed resilience. Authorizing these two core projects (TPRM and AAA) will transform our compliance posture and demonstrate to regulators (BaFin, ECB) that the Bank is serious about managing its operational risks as mandated by DORA.

I urge the Board to approve the funding and program charters for the TPRM and AAA initiatives immediately.