IT Compliance Risk Assessment Executive Report

Document Version: 1.0 (Executive Briefing)
Prepared For: Executive Board and Group Risk Committee
Date: February 2025
Assessor: Kwang yeon Lee, IT Compliance Manager

Executive Summary

This report provides a data-driven summary of the critical IT and cyber risks threatening the Bank's operational resilience, customer data confidentiality, and adherence to stringent regulatory mandates (including **DORA, VAIT, and Federal Reserve** requirements).

The assessment, which covered the operating environment for **2 million individual and 20,000 commercial accounts**, identified three high-priority risks requiring immediate strategic mitigation investment: **Uncontrolled External Data Access** (Critical), **Insider Threat via Social Engineering** (High), and **Geographic Supply Chain Dependency** (Medium).

By personally spearheading the remediation projects, we have already successfully reduced the susceptibility rate to social engineering from **42% to below 15%** and eliminated the critical data breach vulnerability, positioning the Bank for sustained compliance and operational stability.

1. Assessment Context and Regulatory Alignment

1.1 Scope and Operational Profile

The assessment evaluated the full attack surface—physical and virtual—supporting the Bank's operations across its coastal headquarters and remote staff (1,200 employees). The focus was on protecting the **CIA (Confidentiality, Integrity, and Availability)** of critical data assets, which is paramount given the Bank's obligation to maintain daily cash availability and strict Federal Reserve reporting mandates.

1.2 Methodology and Governance Standards

The analysis utilized the **NIST SP 800-30 Rev.1** Risk Assessment framework. All identified control deficiencies and recommended remediation are mapped directly to relevant industry standards and regulatory frameworks:

- **DORA (Digital Operational Resilience Act):** Specifically addresses the resilience of our ICT infrastructure and third-party risk management (TPRM).
- **VAIT (Versicherungsaufsichtliche Anforderungen an die IT):** Provides the standard for the security of IT systems within the financial/insurance sector (relevant for German regulatory alignment).
- **ISO/IEC 27001:** Provides the control set for information security management.

2. Comprehensive Risk Register and Mitigation Strategy

The analysis identified five distinct risks, which we have grouped into three priority areas based on their potential impact and likelihood.

Risk ID	Risk Title (Original Category)	Threat Vector	Inherent Risk Score	Mitigation Status
RA-01	**Critical Data Leak** (Financial/User Database)	External Hacking/Unauthenticated Access	**Critical (9)**	Remediated (95% Complete)
RA-02	**Insider Threat** (Business Email Compromise)	Phishing/Credential Theft	**High (7)**	Control Enhanced
RA-03	**Physical Asset Loss** (Theft)	Unauthorized Access/Physical Security Lapse	**Medium (5)**	Control Implemented
RA-04	**Supply Chain Dependency** (Operational Disruption)	Natural Disaster/Geographic Concentration	**Medium (5)**	Control Implemented
RA-05	**Compromised User Database** (Addressed in RA-01)	External Hacking/Unauthenticated Access	**Critical (9)**	Remediated (95% Complete)

Detailed Analysis and Action for All Five Threats

Strategic Priority 1: External Attack Surface & Data Confidentiality (RA-01 & RA-05)

Finding (RA-01 & RA-05): A critical **High-Risk vulnerability** was identified where a legacy backup server containing non-encrypted **Financial Records and PII (Compromised User Database)** was **publicly accessible** on the internet via an outdated firewall configuration. This posed an immediate and unacceptable risk of **data exfiltration** and integrity compromise.

Regulatory Violation: Direct breach of **GDPR** (Article 32 – TOMs), **DORA** (ICT Risk Management), and **ISO 27001 A.13** (Communication Security).

Action & Resolution: I immediately managed the cross-departmental incident response. This included emergency firewall configuration changes, securing the server behind a **Virtual Private Cloud (VPC)**, and confirming data-at-rest encryption. **Result:** The risk was reduced from **Critical (9)** to **Low (2)** within 48 hours, fully eliminating the threat of a public-facing data breach.

Strategic Priority 2: Insider Threat & Human Resilience (RA-02)

Finding (RA-02): The initial audit revealed a staff **vulnerability rate of 42%** among 1,200 employees in phishing simulation drills, indicating a severely weak "human firewall" and a high risk of **Business Email Compromise (BEC)**, the primary vector for ransomware and credential harvesting.

Regulatory Focus: Failure to meet **DORA** requirements for operational resilience through lack of adequate staff training and awareness.

Action & Resolution: Developed and rolled out mandatory, continuous **cybersecurity awareness training** and periodic, targeted phishing simulation drills. **Result:** Susceptibility rates dropped to **below 15%** within three months, measurably reducing the potential for successful social engineering breaches and fulfilling DORA's people-related resilience mandates.

Strategic Priority 3: Physical & Operational Resilience (RA-03 & RA-04)

Finding (RA-03 - Physical Theft): The assessment identified a physical security lapse concerning remote access cards and laptop disposal procedures, posing a risk of **Physical Theft** of unencrypted assets from decommissioning or loss of access tokens outside secure zones.

Action & Resolution (RA-03): Implemented a formal, mandatory **Asset Disposal Policy** requiring triple-pass data erasure and secure, two-person chain-of-custody for all retiring equipment. All remote access cards were immediately swapped for MFA-secured YubiKeys.

Finding (RA-04 - Supply Chain): Operational continuity was threatened by reliance on a single-source vendor whose primary logistics hub was located in a coastal region susceptible to natural disasters (hurricanes).

Regulatory Focus (RA-04): Critical failure of **DORA's Third-Party Risk Management (TPRM)** and a gap in **Business Continuity Planning (BCP)**.

Action & Resolution (RA-04): Partnered with key vendors to formally **diversify supply routes** and develop documented contingency plans (including contractual fail-over agreements). **Result:** Ensured operational continuity during the last two hurricane seasons with **zero disruption incidents**, safeguarding the bank's stability.

3. Conclusion and Strategic Recommendations

This rigorous risk assessment underscores the value of a proactive and integrated IT compliance program that combines technical controls, regulatory adherence, and continuous employee training. My direct leadership in these high-priority projects demonstrates a comprehensive capability to transform compliance requirements into measurable operational improvements. To transition from reactive fixes to sustained, mature governance, I recommend the following for Executive Board review:

1. **Formalize Risk Appetite:** Define and approve the Bank's maximum **Risk Appetite** for data integrity and operational resilience, aligning it with **DORA** mandates.
2. **Continuous KRIs:** Mandate the quarterly reporting of **Key Risk Indicators (KRIs)**—specifically the phishing susceptibility rate and Mean Time to Patch (MTTP)—to the Risk Committee.
3. **Third-Party Review:** Launch a full-scope audit of all critical third-party vendors to assess compliance with the new **DORA** standards and secure alternative service providers for single points of failure.