Risk Assessment Report Summary

Financial Institution IT Compliance Risk Assessment and Mitigation

---

Prepared by: Kwang yeon Lee, IT Compliance Manager
Date: 10/1/2025

Introduction:

This risk assessment evaluates vulnerabilities within the financial institution's IT and physical security environment, focusing on **protecting critical data assets, ensuring stringent regulatory compliance**, and **mitigating risks of operational disruption**.

The analysis is grounded in the bank's operational profile, which serves a customer base of **2 million individual and 20,000 commercial accounts** and is supported by **1,200 staff** across on-premise and remote setups. Operating in a coastal area under strict mandates, including Federal Reserve requirements for daily cash availability, necessitates a proactive security posture. This assessment identifies and prioritizes key risks to guide strategic security investments and compliance efforts.

Executive Summary:

As the **IT Compliance Manager**, I spearheaded a comprehensive, data-driven risk assessment to identify, evaluate, and prioritize vulnerabilities threatening the bank's critical assets, customer data, and operational stability. The assessment focused on five key areas: **Financial Records Leaks, Compromised User Databases, Physical Theft, Business Email Compromise (BEC)**, and **Supply Chain Disruption**.

Key Outcomes:

- **Identified and remediated a Critical High-Risk vulnerability** (Priority Score: 9) involving a publicly accessible backup server, significantly reducing exposure to a multi-million dollar regulatory fine.
- **Strengthened core security controls** by implementing AES-256 encryption, Multi-Factor Authentication (MFA), and biometric physical security measures.
- **Enhanced human firewall capability**, cutting employee phishing susceptibility from 42% to below 15% through mandatory training.

Risk Assessment Methodology and Register:

The IT Compliance team is conducting a formal risk assessment of the bank's current operational environment. As part of this process, the team is tasked with creating a **Risk Register**, which serves as a central, living record of potential risks to the organization's assets, information systems, and data.

My task was to evaluate a set of high-impact risks previously recorded in this register. For each risk, I needed to:

1. Determine the **Likelihood** of the occurrence.
2. Determine the **Severity** of the risk towards the bank (operational, reputational, or financial impact).

3. Prioritization: The **Priority** score was calculated as Likelihood × Severity, allowing for an objective, focused allocation of risk mitigation resources.
4. Compliance: All recommendations and remediation projects were strictly aligned with leading frameworks, including ISO 27001 controls, GDPR requirements, and applicable financial regulatory frameworks

Risk Register:

The following five primary risks, originating from various sources including malicious attacks, human error, and environmental hazards, were evaluated:

Primary Risks	Description
Financial Records Leak	Unauthorized disclosure of sensitive financial data.
Compromised User Database	Unauthorized access to customer data due to weak encryption.
Theft	Physical loss of cash assets due to security failures.
Business email compromise (BEC)	Social engineering attack leading to confidential data sharing or fraudulent wire transfers.
Supply chain disruption	Operational delays due to vendor or environmental failure.

Risk Assessment

Risks were evaluated using a quantitative methodology: Priority = Likelihood (1-3) × Severity (1-3).

Asset	Risk	Description	Likelihood (1~3)	Severity (1~3)	Priority
Funds/Data	Financial Records Leak	*A database server of backed up data is publicly accessible.*	3	3	9 (High)
Customer Data	Compromised User Database	*Customer data encryption is based on outdated protocols.*	2	3	6 (Moderate)
Physical Assets	Theft	*Physical security weakness with unsecured bank safes during off-hours.*	2	3	6 (Moderate)
Information/ Funds	Business email compromise (BEC)	*An employee is tricked into sharing confidential information.*	2	2	4 (Low-Moderate)
Operations	Supply chain disruption	*Delivery delays to operational centers due to natural disasters.*	1	2	2 (Low)

Key Risk Areas and Findings:

1. Financial Records Leak - Priority Score: 9 (High Risk)

Finding: A critical security gap was identified where a backup server held multi-terabyte financial datasets spanning 2,200 accounts and was publicly accessible over the network. This exposure represented a significant breach of GDPR and ISO 27001 standards, posing a risk of regulatory fines estimated at $4-5 million USD and severe reputational damage.

Action & Resolution:

- Led the immediate project to **migrate all backups** to encrypted cloud storage with robust **Role-Based Access Controls (RBAC).**
- Implemented mandatory **quarterly penetration testing** for all data repositories.
- **Result**: Projected **80%+ reduction** in breach likelihood, establishing full regulatory compliance and significantly enhancing customer trust.

2. Compromised User Database – Priority Score: 6 (Moderate Risk)

Finding: Customer data was protected using outdated AES-128 encryption, which was insufficient against modern, evolving attack vectors and represented a critical compliance vulnerability.

Action & Resolution:

- Collaborated with the database security team to implement **AES-256 encryption** and mandatory **Multi-Factor Authentication (MFA)** for all database access points.
- Conducted system audits and vulnerability testing post-implementation.
- **Result**: Encryption robustness improved by an estimated **60%**, successfully closing a major compliance gap with GDPR and local financial regulations.

3. Theft Risk – Priority Score: 6 (Moderate Risk)

Finding: Physical security protocols were inadequate, evidenced by instances of unsecured bank safes during off-hours, posing a direct threat to physical cash assets.

Action & Resolution:

- Recommended and oversaw the installation of **biometric locking mechanisms** and 24/7 CCTV surveillance.
- Established a process for regular compliance audits of physical security protocols.
- **Result**: Theft risk exposure is estimated to be **reduced by over 70%,** substantially bolstering compliance with internal control and asset protection standards.

4. Business Email Compromise (BEC) – Priority Score: 4 (Low-Moderate Risk)

Finding: Initial organizational assessment revealed a high phishing susceptibility rate of **42%** among employees, indicating a weak human firewall.

Action & Resolution:

- Developed and rolled out mandatory, continuous **cybersecurity awareness training** and periodic **phishing simulation drills.**
- **Result**: Susceptibility rates dropped to **below 15%** within three months, significantly enhancing the human firewall and reducing the potential for social engineering breaches.

5. Supply Chain Disruption – Priority Score: 2 (Low Risk)

Finding: Operational continuity was threatened by seasonal natural disasters (hurricanes) affecting critical vendor logistics.

Action & Resolution:

- Partnered with key vendors to **diversify supply routes** and develop formal, documented contingency plans.
- **Result**: Ensured operational continuity during the last two hurricane seasons with **zero disruption incidents**, safeguarding the bank's operational stability.

Conclusion:

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.

By personally spearheading key remediation projects and fostering collaboration with stakeholders across the organization, I successfully fortified our defenses against data breaches, strengthened physical security, and measurably enhanced overall organizational cyber resilience. This established framework ensures continuous compliance and positions the bank to meet evolving regulatory and operational challenges with confidence.