Bank Risk Assessment & Risk Register Report

1. Introduction

Risk assessments are a critical component of an organization's security strategy. This report documents a cybersecurity risk assessment conducted for a commercial bank to identify, evaluate, and prioritize risks that could impact financial assets and operations.

2. Operating Environment

The bank operates in a coastal region with low crime rates and employs both on-site and remote staff. It manages sensitive financial data for individual and commercial customers and must comply with strict regulatory requirements related to data protection and financial availability.

3. Risk Identification

The following risks to the bank's funds were evaluated:

- Business Email Compromise
- Compromised User Database
- Financial Records Leak
- Theft
- Supply Chain Attack

These risks originate from cyber threats, human error, environmental factors, and third-party dependencies.

4. Risk Assessment Methodology

Each risk was assessed using a qualitative risk scoring model:

- **Likelihood (1–3):** Probability of occurrence
- **Severity (1–3):** Potential business and regulatory impact
- **Priority Score:** Likelihood × Severity

Scores were assigned based on industry trends, operational context, and potential impact to confidentiality, integrity, and availability.

Bank Risk Assessment – Risk Priority

Risk	Likelihoo	Severity	Priority	Risk Level
Business Email Compromise	3	3	9	HIGH
Compromised User Database	2	3	6	MEDIUM
Financial Records Leak	2	3	6	MEDIUM
Theft	1	2	2	LOW
Supply Chain Disruption	1	2	2	LOW

6. Conclusion

This assessment demonstrates a structured approach to identifying and prioritizing risks in a regulated financial environment. The resulting risk register supports informed decision-making and helps focus security efforts on the most critical risks.

Prepared by: Sambou Kamissoko
LinkedIn: https://www.linkedin.com/in/sambouk/