REPORT
Bank Risk Register Analysis

v1.0.2

Author:

Eldon Gabriel

June 12, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/15/2025	Eldon G.	Initial draft.
v1.0.1	02/22/2025	Eldon G.	Added cover, table of contents, and revision history.
v1.0.2	06/12/2025	Eldon G.	Added hierarchical section numbering and TOC structure update.

SECTION 1.0: RISK REGISTER ANALYSIS OVERVIEW

1.1 Incident Overview

Operational Environment: The bank is located in a coastal area with low crime rates. Many people and systems handle the bank's data—100 on-premise employees and 20 remote employees. The customer base of the bank includes 2,000 individual accounts and 200 commercial accounts.

The bank's services are marketed by a professional sports team and ten local businesses in the community. There are strict financial regulations that require the bank to secure its data and funds, like having enough cash available each day to meet Federal Reserve requirements.

1.2 Risk Analysis Details

Asset	Risk(s)	Description	Likelihood	Severity	Priority
Funds	Business email compromise	*An employee is tricked into sharing confidential information.*	2	3	6
	Compromised user database	*Customer data is poorly encrypted.*	2	3	6
	Financial records leak	*A database server of backed-up data is publicly accessible.*	3	3	9
	Theft	*The bank's safe is left unlocked.*	1	3	3
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	Employees may fall victim to phishing attacks, exposing confidential data, while poor encryption on user databases increases the risk. Additionally, unlocked safes within the bank's premises pose a security vulnerability. The risk level depends on the bank's location, considering both crime rates and susceptibility to natural disasters, which may further threaten physical and data security.				

1.3 Risk Assessment Criteria and Scoring Methodology

Asset: The asset at risk of being harmed, damaged, or stolen.

Risk(s): A potential risk to the organization's information systems and data.

Description: A vulnerability that might lead to a security incident.

Likelihood: Score from **1-3** of the chances of a vulnerability being exploited. A **1** means there's a low likelihood, a **2** means there's a moderate likelihood, and a **3** means there's a high likelihood.

Severity: Score from **1-3** of the potential damage the threat would cause to the business. A **1** means a low severity impact, a **2** is a moderate severity impact, and a **3** is a high severity impact.

Priority: How quickly a risk should be addressed to avoid the potential incident. Use the following formula to calculate the overall score: **Likelihood x Impact Severity = Risk**

1.4 Sample Risk Matrix

Severity

Likelihood	Low 1	Moderate 2	Catastrophic 3
Certain 3	3	6	9
Likely 2	2	4	6
Rare 1	1	2	3

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

The risk analysis conducted for the bank's operational environment revealed several high-priority concerns. Among the most critical were:

- A **financial records leak** from a publicly accessible backup database.
- **Business email compromise (BEC)** scenarios resulting from social engineering attacks.
- **Compromised customer data** due to weak encryption practices.

Additional risks, such as **physical theft** from an unlocked safe and **supply chain disruptions**, were identified as lower in priority but still relevant, particularly given the bank's coastal location and dependence on external vendors.

This assessment highlights the importance of combining both technical and physical security measures in a banking environment governed by strict financial regulations.

2.2 Recommendations for Risk Mitigation

Based on the findings, the following risk mitigation strategies are recommended:

- **Secure backup systems and databases** by removing public access and enforcing strict access control policies.
- **Implement advanced email security protections**, such as SPF, DKIM, and DMARC, to reduce BEC risk, and conduct regular phishing awareness training.
- **Upgrade encryption protocols** for customer databases to meet industry standards (e.g., AES-256, proper key management).
- **Improve physical security controls**, ensuring bank safes are locked at all times and monitored with security systems.
- **Develop a business continuity plan** that addresses supply chain disruptions, including alternative delivery routes and vendor risk assessments.

Applying these recommendations will help the bank reduce its overall risk exposure, comply with regulatory standards, and protect both financial assets and customer trust.