Date: August 2, 2024

Prepared by: Junaid Shakoor,

Purpose: This report presents a risk assessment of the commercial bank's operational environment, focusing on potential risks to its financial assets. The assessment aims to identify and prioritize vulnerabilities to inform the development of effective mitigation strategies.

Operational Environment:

The bank operates in a coastal region with historically low crime rates. However, its extensive digital infrastructure, a workforce of 100 on-premise and 20 remote employees, and a diverse customer base of 2,000 individual and 200 commercial accounts create a complex environment susceptible to various cyber threats. Additionally, the bank's location in a coastal area exposes it to the risk of supply chain disruptions due to natural disasters.

Risk Assessment Methodology:

A risk register was developed to identify and assess potential risks. Each risk was evaluated based on its likelihood of occurrence and potential severity of impact, using a scale of 1 (low) to 3 (high). The overall risk priority was calculated by multiplying the likelihood and severity scores.

**Asset	Risk(s)	Description	Likelihood	Severity	Priority**
Funds	Business email compromise	An employee is tricked into sharing confidential information.	2	3	6
Funds	Compromised user database	Customer data is poorly encrypted.	2	3	6
Funds	Financial records leak	A database server of backed up data is publicly accessible.	1	3	3
Funds	Theft	The bank's safe is left unlocked.	1	2	2
Funds	Supply chain disruption	Delivery delays due to natural disasters.	1	2	2

Findings and Recommendations:

The highest priority risks are **business email compromise** and a **compromised user database**, both with a risk score of 6. These risks require immediate attention and mitigation strategies.

Recommended Actions:

- **Business email compromise:**
    - Implement robust email security measures, including spam filters, phishing awareness training, and multi-factor authentication.
    - Establish clear procedures for verifying the authenticity of financial transactions.
- **Compromised user database:**
    - Review and strengthen data encryption practices for customer information.
    - Conduct regular vulnerability scans and penetration testing to identify and address potential weaknesses in the database security.

The remaining risks, while lower in priority, should not be ignored. Measures should be taken to strengthen physical security, monitor for unauthorized access to backup servers, and develop contingency plans for supply chain disruptions.

Conclusion:

This risk assessment provides a snapshot of the current threat landscape facing the bank. By proactively addressing the identified risks and implementing recommended mitigation strategies, the bank can significantly enhance its security posture and protect its financial assets. Regular risk assessments and continuous monitoring are essential to adapt to the evolving threat landscape and ensure ongoing security.