Risk Register – Bank Operational Environment

Risk Register – Bank Operational Environment

Operational Environment:
The bank is located in a coastal area with low crime rates. It has 100 on-premise employees and 20 remote employees. The customer base includes 2,000 individual and 200 commercial accounts. It is marketed by a sports team and 10 local businesses. The bank must meet strict financial regulations, including cash reserve requirements.

Risk Table

Asset	Risk	Description	Likelihood (1-3)	Severity (1-3)	Priority (Score)
Funds	Business email compromise	An employee is tricked into sharing confidential information.	2 (Moderate)	3 (High)	6
Customer database	Compromised user database	Customer data is poorly encrypted.	3 (High)	3 (High)	9
Financial records	Financial records leak	A backup database server is publicly accessible.	2 (Moderate)	3 (High)	6
Funds	Theft	The bank’s safe is left unlocked.	1 (Low)	3 (High)	3
Business operations	Supply chain disruption	Delivery delays due to natural disasters.	2 (Moderate)	2 (Moderate)	4

Prioritization Summary

Priority Level	Risks
High (7–9)	**Compromised user database** (Priority: 9)
Medium (4–6)	**Business email compromise**, **Financial records leak**, **Supply chain disruption**
Low (1–3)	**Theft** (Safe left unlocked)

Notes

How are security events possible considering the risks the asset faces in its operating environment?

- **High data volume and multiple access points** (on-premise + remote employees) increase exposure to phishing and misconfiguration risks.
- **Backup systems** not properly segmented or secured could lead to data leaks.
- **Natural disasters** are plausible due to the **coastal location**, which may disrupt logistics and operations.
- Even with **low crime**, **human error** (like leaving a safe unlocked) can still lead to physical security breaches.