# Risk Register

## 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 their data and funds, like having enough cash available each day to meet Federal Reserve requirements.

## Notes

Security events are possible due to a variety of risk factors in the bank's operating environment. With a large number of employees handling sensitive data, phishing attacks or human errors could lead to business email compromise. Remote employees increase the risk of compromised user databases through weak security practices. Financial records leaks and theft could result from both internal and external threats, while supply chain disruptions due to coastal location hazards could impact banking operations.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Risk(s) | Description | Likelihood (1-3) | Severity (1-3) | Priority (Likelihood × Severity) |
| Funds | Business email compromise | An employee is tricked into sharing confidential information. | 3 | 3 | 9 |
| 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. | 2 | 3 | 6 |
| Funds | Theft | The bank's safe is left unlocked. | 1 | 3 | 3 |
| Funds | Supply chain disruption | Delivery delays due to natural disasters. | 1 | 2 | 2 |