

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.

| Asset | Risk(s) | Description | Likelihood | Severity | Priority |
|-------|---|--|------------|----------|----------|
| Funds | Business email compromise | <i>An employee is tricked into sharing confidential information.</i> | 2 | 2 | 4 |
| | Compromised user database | <i>Customer data is poorly encrypted.</i> | 2 | 3 | 6 |
| | Financial records leak | <i>A database server of backed up data is publicly accessible.</i> | 3 | 3 | 9 |
| | Theft | <i>The bank's safe is left unlocked.</i> | 1 | 3 | 3 |
| | Supply chain disruption | <i>Delivery delays due to natural disasters.</i> | 1 | 2 | 2 |
| Notes | <p><i>How are security events possible considering the risks the asset faces in its operating environment? Security events are possible because the funds are at risk of being accessed by malicious actors if an employee reveals confidential information, customer data is poorly encrypted, or a server of financial records data becomes publicly accessible. Additionally, leaving the bank's safe unlocked or experiencing delivery delays due to natural disasters places the funds physical availability at risk. A bank's operations could be terminated if they fail to comply with regulations.</i></p> <p><i>If a malicious actor manages to compromise the organization's business email or its user database, the resulting security event where confidential information is accessed and/or released could lead to reputational loss and compliance failures that could cause the bank to lose funds through the loss of customers, settlement of court cases, and payment of fines. A financial records leak would present the same risk of financial impact tied to the</i></p> | | | | |

| | |
|--|--|
| | <i>loss of customer trust and failure to meet regulatory requirements. A theft or supply chain attack presents a risk to the funds' physical availability, which could cause the bank not to meet the Federal Reserve's requirements for the amount of daily cash available.</i> |
|--|--|

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**

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 |