

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> | 3 | 3 | 9 |
| | 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 | 1 | 2 |
| | Supply chain disruption | <i>Delivery delays due to natural disasters.</i> | 3 | 2 | 6 |
| Notes | <i>How are security events possible considering the risks the asset faces in its operating environment?</i> | | | | |

| | |
|--|--|
| | <p>Security events involving the bank's funds are possible due to the unique risks present in its operating environment. For instance, in the coastal area, the bank faces natural hazards like hurricanes, potentially leading to structural damage or power outages, which could disrupt financial operations. Additionally, the marketing partnerships and diverse customer base may expose the bank to business email compromise attempts or supply chain attacks, impacting the security of its financial records and funds. The number of employees, including remote workers, increases the attack surface, making the compromise of user databases a potential threat, further highlighting the need for robust security measures.</p> |
|--|--|

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 | Severity | | |
|------------|--------------|---------------|-------------------|
| | Low 1 | Moderate 2 | Catastrophic 3 |
| | Certain 3 | 6 | 9 |
| | Likely 2 | 4 | 6 |
| Rare 1 | 1 | 2 | 3 |