## 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 | *An employee is tricked into sharing confidential information.* | Moderate (2) | High (3) | 2 x 3 = 6 |
| Compromised user database | *Customer data is poorly encrypted.* | Low (1) | High (3) | 1 x 3 = 3 |
| Financial records leak | *A database server of backed up data is publicly accessible.* | Moderate (2) | High (3) | 2 x 3 = 6 |
| Theft | *The bank's safe is left unlocked.* | Low (1) | Moderate (2) | 1 x 2 = 2 |
| Supply chain disruption | *Delivery delays due to natural disasters.* | Moderate (2) | Moderate (2) | 2 x 2 = 4 |
| Notes | *How are security events possible considering the risks the asset faces in its operating environment?* | | | | |

**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





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

**Asset Risks Analysis:**

#### Funds Business Email Compromise

* Asset: Financial funds
* Risk Description: Employee tricked into sharing confidential information
* Likelihood: Moderate (2)
* Severity: High (3)
* Priority: 2 x 3 = 6

#### Compromised User Database

* Asset: Customer data
* Risk Description: Poorly encrypted customer data
* Likelihood: Low (1)
* Severity: High (3)
* Priority: 1 x 3 = 3

#### Financial Records Leak

* Asset: Financial records
* Risk Description: Publicly accessible database server with backed-up data
* Likelihood: Moderate (2)
* Severity: High (3)
* Priority: 2 x 3 = 6

#### Theft - Unlocked Safe

* Asset: Physical cash in the bank's safe
* Risk Description: Safe left unlocked
* Likelihood: Low (1)
* Severity: Moderate (2)
* Priority: 1 x 2 = 2

#### Supply Chain Disruption - Delivery Delays

* Asset: Operational continuity
* Risk Description: Delivery delays due to natural disasters
* Likelihood: Moderate (2)
* Severity: Moderate (2)
* Priority: 2 x 2 = 4

### **Interpretation:**

* The highest priority risks are the Funds Business Email Compromise and the Financial Records Leak, both with a priority score of 6.
* These risks have a higher likelihood of occurring and would result in severe damage if exploited.

### **Security Events and Possibility:**

* The Business Email Compromise and Financial Records Leak might occur due to phishing attempts or lax security protocols, exploiting human error.
* The Compromised User Database and Publicly Accessible Server could stem from insufficient encryption or misconfiguration of databases, making them susceptible to breaches.
* Theft due to an unlocked safe might happen due to human negligence or lack of proper security protocols.
* Supply chain disruptions can happen due to the bank's dependence on external factors like natural disasters affecting deliveries.

Addressing these risks involves implementing measures such as robust employee training on cybersecurity, encryption protocols for databases, strict physical security protocols for the safe, regular supply chain risk assessments, and contingency plans for potential disruptions.

Prioritizing and addressing these risks will help the bank mitigate potential security incidents and uphold its regulatory requirements.

#### **Business Email Compromise**

Employees may fall victim to phishing emails, leading to unauthorized access to financial systems or fraudulent fund transfers.

#### **Compromised User Database**

Weak encryption or database vulnerabilities can be exploited, granting unauthorized access to sensitive financial information.

#### **Financial Records Leak**

Improperly secured servers or misconfigured access controls may lead to the exposure of crucial financial records to unauthorized entities.

#### **Theft**

Lax physical security measures or negligence could result in unauthorized access to the bank's funds, leading to potential theft.

#### **Supply Chain Attack**

#### Disruptions in the supply chain due to external factors, like natural disasters, may impact the availability of funds or financial services, affecting the bank's operations.

### **Risk Likelihood Assessment:**

#### **Business Email Compromise**

* Once a day: Low (1)
* Once a month: Moderate (2)
* Once a year: Moderate (2)
* Description: Phishing attempts could occur sporadically, potentially impacting daily operations if successful.

#### **Compromised User Database**

* Once a day: Low (1)
* Once a month: Low (1)
* Once a year: Moderate (2)
* Description: Vulnerabilities might be exploited, but frequent occurrences are less likely.

#### **Financial Records Leak**

* Once a day: Low (1)
* Once a month: Moderate (2)
* Once a year: Moderate (2)
* Description: Misconfigurations or breaches could happen occasionally, impacting financial data security.

#### **Theft**

* Once a day: Low (1)
* Once a month: Low (1)
* Once a year: Moderate (2)
* Description: Lax security measures could lead to sporadic incidents of theft.

#### **Supply Chain Attack**

* Once a day: Low (1)
* Once a month: Low (1)
* Once a year: Moderate (2)
* Description: Disruptions in the supply chain due to events like hurricanes could happen infrequently but significantly impact fund availability.

These likelihood scores are based on the frequency and probability of each risk occurring within different timeframes, considering the nature of the threats and the bank's operational environment.

### **Severity Assessment:**

#### **Business Email Compromise**

* Severity: 3 (High)
* Description: Potential financial loss, compromise of sensitive data, regulatory violations, and damage to the bank's reputation could severely impact operations and trust.

#### **Compromised User Database**

* Severity: 2 (Moderate)
* Description: While it could lead to a breach of customer data and regulatory concerns, the immediate financial impact might be lower than other risks.

#### **Financial Records Leak**

* Severity: 3 (High)
* Description: The leak of financial records can directly impact financial stability, regulatory compliance, and damage the bank's reputation significantly.

#### **Theft**

* Severity: 2 (Moderate)
* Description: While it can lead to financial loss and customer trust issues, the immediate impact might be less severe than a large-scale data breach.

#### **Supply Chain Attack**

* Severity: 2 (Moderate)
* Description: Disruptions in the supply chain can affect the availability of funds and services, impacting operations and customer trust, but may have a more localized impact compared to direct data breaches.

These severity scores are based on the potential consequences each risk poses to the bank's financial stability, regulatory compliance, operational continuity, and reputation.

**let's calculate the priority score for each risk using the formula: Likelihood x Severity = Priority**

### **Calculating Priority Scores:**

#### **Business Email Compromise**

* Likelihood: 2 (Moderate)
* Severity: 3 (High)
* Priority: 2 x 3 = 6

#### **Compromised User Database**

* Likelihood: 1 (Low)
* Severity: 2 (Moderate)
* Priority: 1 x 2 = 2

#### **Financial Records Leak**

* Likelihood: 2 (Moderate)
* Severity: 3 (High)
* Priority: 2 x 3 = 6

#### **Theft**

* Likelihood: 1 (Low)
* Severity: 2 (Moderate)
* Priority: 1 x 2 = 2

#### **Supply Chain Attack**

* Likelihood: 1 (Low)
* Severity: 2 (Moderate)
* Priority: 1 x 2 = 2

The priority scores help in determining the order in which these risks should be addressed or mitigated. Higher priority scores indicate risks that need immediate attention and allocation of resources to minimize their potential impact.