## 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.* | 2 | 2 | 4 |
| Compromised user database | *Customer data is poorly encrypted.* | 2 | 3 | 6 |
| Financial records leak | *A database server of backed up data is publicly accessible.* | 2 | 3 | 6 |
| Theft | *The bank's safe is left unlocked.* | 1 | 3 | 3 |
| Supply chain disruption | *Delivery delays due to natural disasters.* | 1 | 3 | 3 |
| 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**

### **Notes**

Firstly, we assess the likelihood of each risk to the funds. Since employees could be easily tricked into giving confidential information, but a social attack like this is not very common, a likelihood of 2 is given. The likelihood of poorly encrypting customer’s data is not very much, since a bank should meet some security requirements before becoming a functional bank. However, this is not improbable, hence a likelihood of 2 would be good. The leakage of financial information could be as likely as the latter; therefore, a likelihood of 2. As we know, this area has a low crime rate; thus, a likelihood of 1 for theft. In the end, although the bank is located in a coastal area, the rate of hurricane or such natural disasters is not too high and the likelihood of supply chain disruption is low.

Secondly, we assess the severity of each risk based on the impact of the event on the reputation, finances, and regulation fines. Business email compromise cannot affect the bank’s finances or bring any fines, however it has a severe impact on the reputation; therefore a level 2 severity is chosen. For all the others, in case of an incident, the event will bring negative impact on all reputation, finances, and regulation fines; therefore, a level 3 severity is chosen.

Lastly, by multiplying the likelihood and severity, we conclude the risk assessment, finding the priority of each 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 |