## 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-likely | 3 | 6 |
| Compromised user database | *Customer data is poorly encrypted.* | 2-likely | 3 | 6 |
| Financial records leak | *A database server of backed up data is publicly accessible.* | 3-certain | 3 | 9 |
| Theft | *The bank's safe is left unlocked.* | 1-rare | 3 | 3 |
| Supply chain disruption | *Delivery delays due to natural disasters.* | 1-rare | 2 | 2 |
| Notes | *How are security events possible considering the risks the asset faces in its operating environment?*  *The risk of business email compromise is at the priority of 6 due to its likelihood and severity, typically a person is the weakest link in security and can fall for Phishing emails in which this poses a big threat for a bank as the following things that an attacker can do with compromising an email could be significant.*  *Compromised user databases where in the database the encryption is poor can also lead to a significant impact on customer data and an attacker may gain access to a clients bank account and their money which is why it has a priority of 6.*  *Financial records leak with a priority of 9 needs to be addressed as all backup database data is publicly accessible in which with combination of poorly encrypted data an attacker will be able to gain information of all customers/clients*  *Theft is at a priority of 3 this is because its not likely to happen even though the assets may be at risk its unlikely that the safe is left unlocked and even if it is, it is the last line of defense in a banks security where there will be many more security measures in place like security cameras, security guards, access controls to stop a physical threat so it is unlikely a theft will happen.*  *Supply chain disruption has a priority of 2 as natural disasters are rare and most are predictable even though services could go down during one the event in which one happens is very unlikely.* | | | | |

**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 |