## 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.* | 3 | 3 | 9 |
| Compromised user database | *Customer data is poorly encrypted.* | 2 | 3 | 6 |
| Financial records leak | *A database server of backed up data is publicly accessible.* | 3 | 3 | 9 |
| Theft | *The bank's safe is left unlocked.* | 1 | 3 | 3 |
| Supply chain disruption | *Delivery delays due to natural disasters.* | 1 | 2 | 2 |
| Notes | *The source of a risk can range from malicious attackers to accidental human errors, natural or environmental hazards, structural failure or power outage. Taking into account all of these, a malicious attack would happen compromising emails/passwords or sensitive data, like ransomware. A former employee could leak any kind of information in a conversation or clicking on a malicious email. A power outage could get all the security electronic systems out, a theft could occur during this due to the fact that it is an area where the crime rates are low. Finally and environmentally speaking, the bank is in a coastal area which leads to being weaker to storms or tsunamis.* | | | | |

**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 |