

Risk register

You've joined a new cybersecurity team at a commercial bank. The team is conducting a risk assessment of the bank's current operational environment. As part of the assessment, they are creating a risk register to help them focus on securing the most vulnerable risks.

A **risk register** is a central record of potential risks to an organization's assets, information systems, and data. Security teams commonly use risk registers when conducting a risk assessment.

Your supervisor asks you to evaluate a set of risks that the cybersecurity team has recorded in the risk register. For each risk, you will first determine how likely that risk is to occur. Then, you will determine how severely that risk may impact the bank. Finally, you will calculate a score for the severity of that risk. You will then compare scores across all risks so your team can determine how to prioritize their attention for each risk.

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> | 2 | 3 | 6 |
| | 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 | 3 | 3 |
| | Supply chain disruption | <i>Delivery delays due to natural disasters.</i> | 1 | 2 | 2 |

| | |
|-------|---|
| Notes | <i>Doing business with other companies might increase the risks to data since it presents other avenues for the information to be compromised. The risk of theft is important, but might not be a priority because the bank is in an area with low crime rates.</i> |
|-------|---|

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