Risk Register

Scenario

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 operates in a coastal region with low crime rates. Its data is managed by 100 on-premise employees and 20 remote employees. The customer base consists of 2,000 individual accounts and 200 commercial accounts. The bank's marketing partnerships include a professional sports team and ten local businesses. Compliance with financial regulations requires secure data management and sufficient cash reserves to meet Federal Reserve requirements.

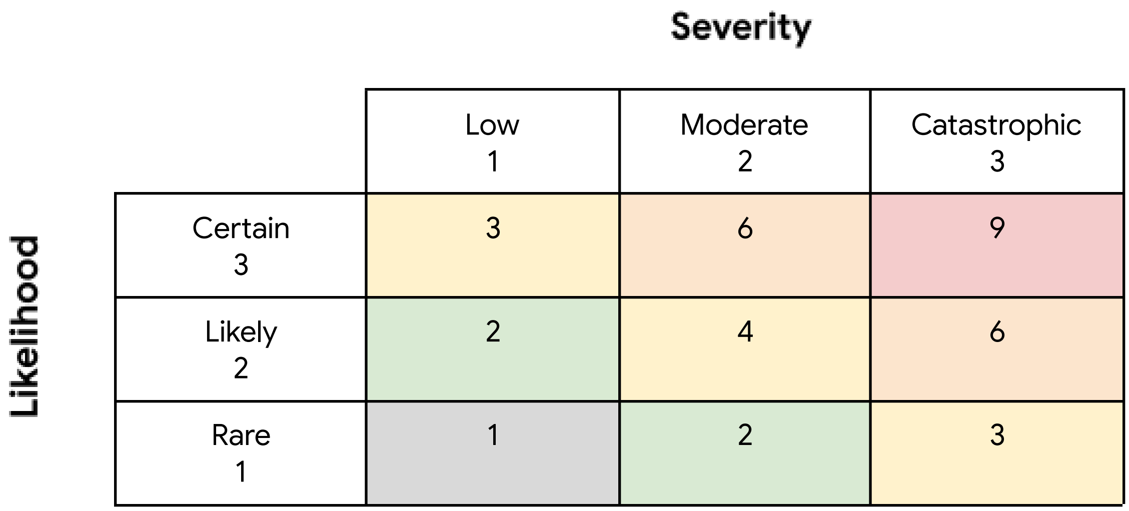
Asset	Risk(s)	Description	Likelihood	Severity	Priority
Funds	Business email compromise	*An employee is tricked into sharing confidential information.*	2	2	4
	Compromised user database	*Customer data is poorly encrypted.*	2	3	6

	Financial records leak	*A database server of backed up data is publicly accessible.*	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	• *Engaging in business partnerships increases the risk of data exposure due to additional attack vectors.* • *While theft remains a concern, its priority is lower due to the bank's low-crime location.*				

Risk Scoring Criteria:

- **Likelihood (1-3):** Assesses the probability of the risk being exploited (1 = low, 2 = moderate, 3 = high).
- **Severity (1-3):** Evaluates the potential damage to business operations (1 = low, 2 = moderate, 3 = high).
- **Priority Score:** Determined using the formula: **Likelihood × Severity = Risk Score**

Sample risk matrix



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