Risk register

Operational environment:

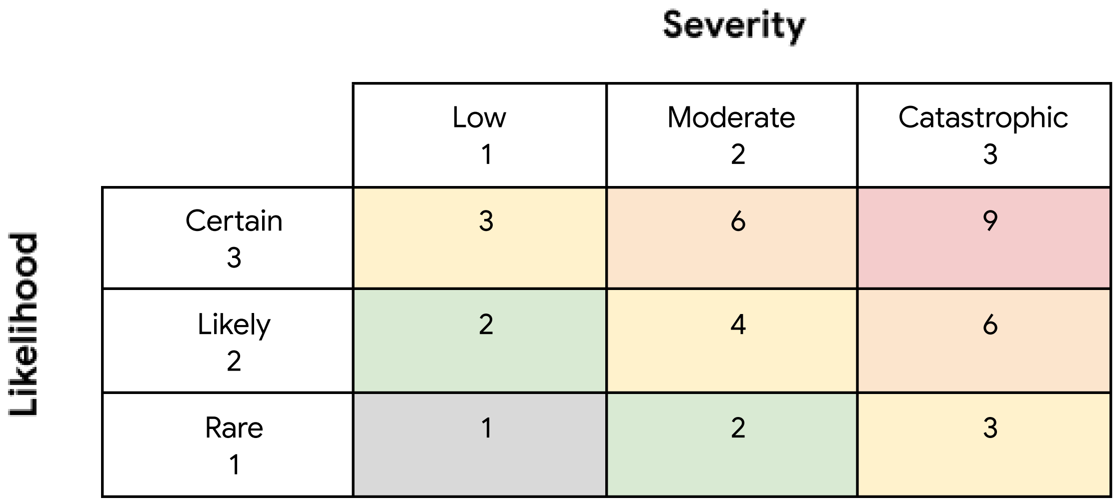
The bank is located in a coastal area with low crime rates. Many people and systems handle the bank's data—100 on-premise employees and 20 remote employees. The customer base of the bank includes 2,000 individual accounts and 200 commercial accounts. The bank's services are marketed by a professional 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.*	1	3	3
	Compromised user database	*Customer data is poorly encrypted.*	1	3	3
	Financial records leak	*A database server of backed up data is publicly accessible.*	1	3	3
	Theft	*The bank's safe is left unlocked.*	1	3	3
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	*How are security events possible considering the risks the asset faces in its operating environment?* *An improper password policy or firewall can compromise the business email, user database and financial records. Improper physical security to the bank's safe and vaults, such as absence of a CCTV camera or lesser number of security personnel, or even the people who have access to the safe key can play a fundamental role in the occurrence of a security event. As for supply chain disruption, and delays due to natural disasters; since the bank is located in a coastal area and may be prone to hurricanes, a few times in a year. Taking necessary precautions and being updated with the weather forecast may be an important step to prevent delays due to weather conditions and natural disasters.* *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.

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