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	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	*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. This information helps contextualize the risk assessment by considering external factors.*				

Likelihood:
Likelihood scores were estimated based on factors that could lead to a security incident. A range of 1, 2, or 3 on a risk matrix indicates rarity, likelihood, or certainty. For instance, the supply chain disruption, resulting from natural disasters, was rated as 1 due to the unpredictability of such events. In contrast, compromised data events were scored a 2 because they are more likely to occur given the possible causes.

Severity:

No risk received a severity score less than 2 because data breaches, like business email compromise, can have significant consequences. Customers trust the bank to safeguard their money and personal information, and regulatory non-compliance could lead to severe repercussions. Hence, risks were rated with a severity of 2 or higher.

Priority:
The financial records leak received the highest overall risk score of 9, signaling that this risk is almost certain to happen and would significantly impact the bank's ability to operate. This high overall score highlights the need for immediate attention, helping the security team prioritize remediation efforts for this risk before addressing those with lower scores.

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