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	*In this coastal bank with a substantial employee base and strict financial regulations, risks like business email compromise and theft are heightened due to the high value of funds and data. The involvement of external parties, such as sports teams and local businesses, increases exposure to supply chain attacks and financial records leaks.* **Notes on Risk Factors:** The bank's funds are at significant risk due to high-value targets and external exposure. Risks like business email compromise and theft are particularly relevant given the bank's substantial employee base and community marketing efforts. **Likelihood Scores:** 1. Business email compromise: 2 2. Compromised user database: 2 3. Financial records leak: 3				

	4. Theft: 1 5. Supply chain attack: 1 **Severity Scores:** 1. Business email compromise: 2 2. Compromised user database: 3 3. Financial records leak: 3 4. Theft: 3 5. Supply chain attack: 2 **Overall Risk Scores:** 1. Business email compromise: 4 (Likelihood 2 × Severity 2) 2. Compromised user database: 6 (Likelihood 2 × Severity 3) 3. Financial records leak: 9 (Likelihood 3 × Severity 3) 4. Theft: 3 (Likelihood 1 × Severity 3) 5. Supply chain attack: 2 (Likelihood 1 × Severity 2)

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

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