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	*How are security events possible considering the risks the asset faces in its operating environment?* ***Business Email Compromise*** *The combination of 100 on-premise employees and 20 remote employees increases the risk of business email compromise, as attackers can target both local and remote communication channels. Low crime rates might reduce physical threats but do not mitigate cyber threats, necessitating robust email security protocols.* ***Compromised User Database***				

	With 2,200 accounts (individual and commercial), a compromised user database could have severe financial and reputational impacts. The involvement of many people and systems handling data heightens the risk of breaches, particularly if security measures are not uniformly enforced across on-premise and remote environments. ***Financial Records Leak*** *Strict financial regulations demand the bank secure its financial records, making a leak highly detrimental. A large customer base and external marketing partners increase the number of potential access points, necessitating stringent access controls and regular audits to ensure compliance and data integrity.* ***Theft*** *While the coastal location and low crime rates might reduce physical theft risk, the internal threat remains due to the significant number of employees handling funds and data. Robust internal controls and employee monitoring are essential to prevent and detect any fraudulent activities.* ***Supply Chain Attack*** *Dependence on ten local businesses for marketing and possibly other services introduces vulnerabilities through supply chain attacks. Ensuring these partners adhere to strong security practices is crucial, as any compromise within the supply chain can directly affect the bank's operations and data security.*

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