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.*	3	3	9
	Compromised user database	*Customer data is poorly encrypted.*	3	3	9
	Financial records leak	*A database server of backed up data is publicly accessible.*	2	3	6
	Theft	*The bank's safe is left unlocked.*	1	3	3
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	**Business Email Compromise:** Since the bank collaborates with several local businesses and a professional sports team, an attacker could use spear phishing techniques targeting these partners or remote employees to access corporate emails. This could allow the theft of confidential information or the distribution of ransomware that directly affects the bank's funds. **Compromised user database:** With 2,200 active accounts and multiple employees handling data, a database breach could allow unauthorized access. Attackers could illicitly transfer funds or sell information to third parties. Remote employees, if not properly protected, also increase the attack surface.				

	Financial Records Leakage: Access by many employees and systems to financial records exposes the bank to the risk of accidental or malicious leaks. A simple human error or improper access could reveal critical information, affecting both individual and business accounts and violating financial regulations. **Theft:** The bank must maintain daily cash in accordance with Federal Reserve requirements. If a physical or digital theft were to occur, it could be deprived of the necessary funds, impacting its daily operations. Its coastal location and low crime rate do not eliminate the possibility of internal attacks or external organized crime. **Supply chain attack:** Reliance on external systems and suppliers can be exploited through attacks on third-party software or hardware. A disruption could leave customers without service, eroding public confidence and damaging the bank's reputation, as well as affecting the immediate availability of funds.

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