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.*	2	3	6
	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	1	1
Notes	*How are security events possible considering the risks the asset faces in its operating environment?* If a business email is compromised, this could lead to a threat actor impersonating an employee and gaining access to confidential information. This has a large human component of risk associated with it and thus is more likely than the other scenarios. This has a chance of severely impacting business operations and is ranked as the highest priority. With a compromised user database, a threat actor could access confidential or restricted data and is ranked at the highest severity. As the threat actor would have to gain access to the database first, the likelihood is ranked at moderate.				

	If a financial records leak occurred and restricted data was made public this would constitute a very high severity rating. The likelihood of this happening is ranked at moderate due to the restricted nature of the data. If the bank's safe was left unlocked, this would lead to a highly severe scenario where the bank would not have the cash required by the Federal Reserve, not to mention the loss of assets. I ranked this as a low likelihood of happening as the bank is located in a low crime rate area and there would be many procedures to prevent this. A supply chain disruption has a low likelihood of occurring and would delay bank operations for a couple days. Because this does not directly impact the bank's assets, I would rank this as a low severity scenario.

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