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.*	3	3	9
	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	2
	Supply chain disruption	*Delivery delays due to natural disasters.*	2	1	3
Notes	*- A threat actor attempting to collect confidential details about a business can only go so far without requiring passwords or PINs for* *- If user data is compromised, the integrity and trust placed in the bank will be negatively impacted, which may see a huge loss in customers and businesses* *- A leak of financial records would jeopardize the integrity of the bank, and the personal information of all of its clients, which would potentially lead to loss of customers and legal ramifications to ensue* *- The coastal area, with its low crime rate would likely not have residents committing theft at the bank, however if it were to occur, the financial lost could put the bank in debt and may incur some legal infractions as well* *- Natural disasters in a coastal area are heavily determined by the body of water, and are more likely to occur than in in-land areas. A disruption or delay in the supply chain, although inconvenient, will not result in more than a wave of disgruntled clients and complaints.*				

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