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	2	6
	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	2	2
	Supply chain disruption	*Delivery delays due to natural disasters.*	2	2	4
Notes	**Compromised/Leaked records and information** *Due to the critical functions that a bank holds, any breach of PII(Personal Identification Information) and SPI(Sensitive Personal Information)is considered to be a high-severity, the likelihood of such a breach is high due to the high amount of individual and commercial accounts. Since a large amount of cybercrime has been located within the country and targeted at high wealth institutions, the use of phishing(spear phishing, whaling, vishing) has become ever present, thus marking it as a very-high likelihood of occurrence.* **Theft** *Since the local area the bank resides in is a low crime area with a large number of employees(assuming that a good portion are security guards and cybersecurity professionals) The chances of theft are relatively low and the impact is not as critical as a breach in PII and SPI.*				

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