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.*	Two	Two	Four
	Compromised user database	*Customer data is poorly encrypted.*	Three	Three	Nine
	Financial records leak	*A database server of backed up data is publicly accessible.*	Three	Three	Nine
	Theft	*The bank's safe is left unlocked.*	One	Three	Three
	Supply chain disruption	*Delivery delays due to natural disasters.*	One	Two	Two
Notes	A financial records leak or the user database being compromised could lead to clients personal and financial information being stolen, and with multiple people and systems handling the bank's data the likelihood of this happening is the biggest risk facing the bank. Business emails being compromised also poses a risk, employees will need to be trained on how to recognize social engineering attacks and to report any suspicious activity to the I.T. department. A supply chain disruption is also a concern due to the possibility of tropical weather causing unsafe driving conditions that could prevent deliveries from being made. Theft isn't as likely of a risk for the bank due to the low crime rates in the area, but shouldn't be overlooked. Proper protocols need to be implemented and employees retrained to make certain that the bank's physical funds are protected.				

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**

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