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.*	1	3	3
	Financial records leak	*A database server of backed up data is publicly accessible.*	3	2	6
	Theft	*The bank's safe is left unlocked.*	1	3	3
	Supply chain disruption	*Delivery delays due to natural disasters.*	2	3	6
Notes	*How are security events possible considering the risks the asset faces in its operating environment?*				
	The risk factors involved with these assets range from human error to poor security posture for data to bad luck and timing. Supply chain disruption cannot be avoided amidst a natural disaster but is extremely impactful. Theft and email compromise is purely negligence on the responsible persons behalf. A safe being left open is extremely severe and confidential information being shared is severe but can be recovered from and secured. Access of data due to poor encryption is severe as well. Customer data being stolen due to poor encryption is extremely dangerous as well as financial records being publicly accessed.				

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