Risk register

Operational environment:

The bank operates in a low-crime coastal area with 100 on-premise and 20 remote employees, serving 2,000 individual and 200 commercial accounts. Marketing partnerships exist with a professional sports team and ten local businesses. The bank must comply with strict financial regulations regarding data security and cash reserves.

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.*	2	3	6
	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	3
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	*Notable considerations include increased data compromise risks from business partnerships and relatively lower priority of physical theft due to location. Risk priorities are calculated by multiplying likelihood (1-3) by severity (1-3), with higher scores indicating greater urgency for addressing the risk.*				

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
Certain 3	3	6	9
Likely 2	2	4	6
Rare 1	1	2	3

Likelihood