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.*	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	*How are security events possible considering the risks the asset faces in its operating environment?* ● *2-3 sentences describing the risk factors* ● *5 likelihood scores* ● *5 severity scores* ● *5 overall risk scores* *The risk factors include compromise to business email due to human error, compromised user database because of poor encryption, leak of financial records due to a compromised database server, theft due to physical insecurity and supply chain disruption due to coastal location and the likelihood of natural disaster.* ***1)*** *Business email could be compromised occasionally, most likely due to human error. The priority is comparatively low, because the*				

	severity of impact on the business is moderate - confidence in the business and regulatory violations are all aspects which make priority moderate but less severe because no financial information was exposed. ***2)*** *A compromised user database as a result of poor encryption is moderately likely - encryption methodology can be revised but threat actors can change tactics. This won't happen daily but it's not a rare occurrence. Reputation and failure to follow regulation in data protection makes priority moderately high but again, no financial information has been compromised.* ***3)*** *However, if a database server of backed up data becomes publicly accessible the priority is highest due to the high likelihood and high severity level of impact - compromised data, financial information and reputation make this a higher priority.* ***4)*** *It is hoped that employees are very well practiced in physical security procedures so open access to physical assets is uncommon. This compromises confidence in security, the customer assets themselves, as well as access to money as per Federal Reserve requirements, however because its likelihood is so rare, priority is relatively low.* ***5)*** *Finally, supply chain disruption due to natural disaster can occur in this coastal region, but it is comparatively low in occurrence and while it may disrupt business, customers data and finances are not breached as a result meaning priority is low.*

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