

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	<i>An employee is tricked into sharing confidential information.</i>	3	2	1
	Compromised user database	<i>Customer data is poorly encrypted.</i>	2	3	1
	Financial records leak	<i>A database server of backed up data is publicly accessible.</i>	1	3	2
	Theft	<i>The bank's safe is left unlocked.</i>	1	2	1
	Supply chain disruption	<i>Delivery delays due to natural disasters.</i>	1	2	3
Notes	<i>The bank deals with a high volume of accounts including personal and commercial accounts and has a higher profile due to being used by local businesses and a professional sports team. This amount of client traffic and marketing increases the attack surface of the bank and would make this bank a prime target to attackers or human error. This also increases the impact of the vulnerability being exploited.</i>				

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**

Email: $3 * 2 = 6$

Database: $2 * 3 = 6$

Records Leak: $1 * 3 = 3$

Theft: $1 * 2 = 2$

Supply Chain: $1 * 2 = 2$

Sample risk matrix

Li
ke
li
ho
o
d

Severity

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