

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	<i>Business email compromise</i>	<i>An employee is tricked into sharing confidential information.</i>	2	2	4
	<i>Compromised user database</i>	<i>Customer data is poorly encrypted or left unencrypted.</i>	2	3	6
	<i>Financial records leak</i>	<i>A database server with complete backups is publicly accessible.</i>	3	3	9
	<i>Theft</i>	<i>A window or door is left unlocked, allowing a threat actor access to a building.</i>	1	3	3
	<i>Supply chain disruption</i>	<i>Delivery delays due to natural disasters.</i>	1	3	3
Notes	<p>How are security events possible considering the risks the asset faces in its operating environment?</p> <p><i>Thefts are unlikely due to the fact that the bank is in a low crime rate area. While the bank is in a coastal area, the likelihood of severe natural disasters is low, meaning that supply chain disruptions are not an imminent threat. Working with other companies increases risk due to higher rates of information exchange, including emails and documents, which could potentially lead to leaked information, phishing scams, or poorly configured permissions.</i></p>				

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