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.

<table>
<tr><th>Asset</th><th>Risk(s)</th><th>Description</th><th>Likelihood</th><th>Severity</th><th>Priority</th></tr>
<tr><td rowspan="5">Funds</td><td>Business email compromise</td><td><i>An employee is tricked into sharing confidential information.</i></td><td>2</td><td>2</td><td>4</td></tr>
<tr><td>Compromised user database</td><td><i>Customer data is poorly encrypted.</i></td><td>2</td><td>3</td><td>6</td></tr>
<tr><td>Financial records leak</td><td><i>A database server of backed up data is publicly accessible.</i></td><td>3</td><td>3</td><td>9</td></tr>
<tr><td>Theft</td><td><i>The bank's safe is left unlocked.</i></td><td>1</td><td>3</td><td>3</td></tr>
<tr><td>Supply chain disruption</td><td><i>Delivery delays due to natural disasters.</i></td><td>1</td><td>2</td><td>2</td></tr>
<tr><td>Notes</td><td colspan="5"><i>How are security events possible considering the risks the asset faces in its operating environment?</i>
Security events are possible due to the combination of technical, human, and environmental risks present in the organization’s operating environment.
Business email compromise (BEC) is a significant risk if employees use weak passwords, reuse credentials, or fail to follow secure email practices such as recognizing phishing attempts. Without strong authentication controls and user awareness, attackers can gain unauthorized access and exploit email systems to commit fraud or steal sensitive information.
Databases and financial records are also vulnerable if proper access controls, encryption, and monitoring parameters are not strictly implemented and enforced. Misconfigured</td></tr>
</table>

	permissions or lack of role-based access controls can lead to unauthorized exposure of confidential client and financial data. Physical and identity-based threats are another concern. As a client-facing business managing over 2,000 individual accounts, improper customer identification or insufficient access restrictions could result in identity fraud, account takeover, or data theft. Strong identity verification and least-privilege access are critical due to the sensitive nature of customer information. Finally, supply chain and operational disruptions pose a risk due to the bank's coastal location. Natural disasters or regional infrastructure failures could impact availability of systems, third-party services, or physical facilities, potentially leading to service outages or data availability issues if adequate resilience and contingency planning are not in place.

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