Risk register

Operational environment:

The commercial bank, situated in a coastal area with a workforce of 100 on-premise and 20 remote employees, serving 2,000 individual and 200 commercial accounts, and engaging in partnerships with a professional sports team and ten local businesses, the cybersecurity team conducts a risk assessment. The bank's daily operations are tightly regulated to meet Federal Reserve requirements, emphasizing the criticality of securing both data and funds. Factors such as the coastal location, diverse workforce, large customer base, marketing collaborations, and stringent financial regulations contribute to the complex risk landscape. The risk register identifies key risks, including business email compromise, compromised user databases, financial records leaks, theft, and supply chain attacks, each assessed for likelihood, severity, and prioritization to guide the cybersecurity team in focusing on the most vulnerable risks.

Asset	Risk(s)	Description	Likelihood	Severity	Priority
Funds	Business email compromise	*Unauthorised access to emails for malicious purposes*	2	2	4
	Compromised user database	*Risks associated with a potential breach of user databases*	3	2	6
	Financial records leak	*Risks related to potential leaks of sensitive financial data*	2	3	6
	Theft	*Risks associated with the theft of physical or digital assets*	1	2	2
	Supply chain disruption	*Risks associated with potential disruptions in the supply chain*	2	3	6
Notes	*Security events are possible in the bank's operating environment due to diverse risks, including potential supply chain disruptions from the coastal location, cyber threats like phishing targeting a varied workforce, data breaches from a large customer base, and additional access points through collaborations, all accentuated by strict financial regulations.*				

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