NIST Risk Assessment of Financial Institution

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.*	2	3	6
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	*Risk of financial records leak: With 200 commercial accounts that the bank holds, there are elevated risks of data leak. The bank holds its financial records in publicly accessible database server, and dealing with many third parties would increase the attack surface potentially resulting in security incidents of sensitive financial information leak that are beyond the bank's control.* *Risk of compromised user database: With 2200 customer accounts that are poorly encrypted, there are added risks of data compromise. Further investigation of data encryption method would be needed to fully assess the risk.* *Risk of theft: The risk of theft is very important as customers trust the bank to safeguard their assets; the consequences could severely jeopardize the business operations. There is an added risk of theft as the bank's safe is left unlocked. The likelihood remains moderate as the bank is in an area with low crime rates.* *Risk of business email compromise: With 120 employees working for the bank, there are added risks of business email compromise that could lead to attacks of phishing and social engineering. We have*				

	learned that an employee had been tricked into sharing confidential information; the security team should investigate the incident to assign the severity level more accurately. *Risk of supply chain disruption: This risk is regarded as unlikely due to the unpredictability of natural disasters. Being located in a coastal area, there is a likelihood that the bank may experience supply chain disruption caused by hurricanes; the threat is more pronounced in certain hurricane seasons.* *Severity: All risks received a severity score equal to or higher than 2 because they could lead to serious consequences such as difficulties in business continuity and potential fines and lawsuits. Furthermore, the customers trust the bank to protect their information and assets; breaking this trust could jeopardize the bank's reputation.* *Priority: The risk of financial records leak received the highest overall risk score of 9. This indicates that this risk is almost certain to happen and it would greatly affect the bank's ability to operate. The high score indicates that the security team should prioritize remediating any issues related to this risk before resolving risks that scored lower.*

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 (rare), a 2 means there's a moderate likelihood (likely), and a 3 means there's a high likelihood (certain).
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**