Risk Assessment Report: Scoring Risks Based on Likelihood and Severity

Objective:
The goal of this project is to conduct a security risk assessment for a commercial bank by identifying and scoring the key risks to one of its primary assets—**funds**. The activity follows the principles of the NIST Cybersecurity Framework, which promotes the proactive identification, assessment, and prioritization of cybersecurity risks.

Scenario Summary:
The bank is situated in a **coastal region with low crime rates**, employing **100 on-premise and 20 remote staff**, and serving **2,000 individual** and **200 commercial** accounts. With strict **financial regulations**, including daily Federal Reserve compliance, and public marketing partnerships with a **professional sports team** and **local businesses**, the bank's data and funds must be well-protected against both internal and external threats.

Tasks Completed:

1. **Analyzed the operational environment** to understand contextual risk factors such as employee distribution, customer base, marketing exposure, regulatory requirements, and geographic vulnerabilities (e.g., hurricanes).

2. **Identified five key risks** to the bank's funds:

    - Business Email Compromise
    - Compromised User Database
    - Financial Records Leak
    - Theft
    - Supply Chain Disruption

3. **Scored each risk** using a **risk matrix**, assigning values (1–3) to:

    - **Likelihood**: How probable it is for the risk to occur based on the environment and past data.
    - **Severity**: The potential impact on the bank's operations, customers, finances, and regulatory standing.
    - **Priority**: A multiplication of Likelihood × Severity to guide mitigation focus.

4. **Provided a written risk analysis summary**, explaining how and why these risks are realistic threats based on the bank's operational environment.

Deliverables:

- A **risk register** table with completed Likelihood, Severity, and Priority scores.
- A **short explanation (40–60 words)** of how security events are possible within this specific bank environment.

Severity

Risk Register:

Asset	Risk(s)	Description	Likelihood	Severity	Priority (L X S)
Funds	Business email compromise	*An employee is tricked into sharing confidential information.*	3	3	9
	Compromised user database	*Customer data is poorly encrypted.*	2	3	6
	Financial records leak	*A database server of backed up data is publicly accessible.*	2	3	6
	Theft	*The bank's safe is left unlocked.*	1	3	3
	Supply chain disruption	*Delivery delays due to natural disasters.*	2	3	6
Notes	Security events are possible due to the nature of the bank's operational environment, which includes both physical and digital vulnerabilities. With a large number of employees managing sensitive data, the risk of human error—such as falling for phishing emails or misconfiguring server permissions—is significant. The coastal location increases the likelihood of natural disasters impacting the supply chain. Financial data leaks and thefts, though less frequent, can have catastrophic impacts due to regulatory, financial, and reputational consequences. Therefore, it is essential to address the highest scoring risks with immediate mitigation strategies.				

Sample risk matrix

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