Risk Register – Commercial Bank

Risk Assessment – Portfolio Activity:

Risk Factors

The bank's operating environment includes both on-premise and remote employees, increasing the potential for human error or phishing-based threats. Sensitive data, including financial records and customer databases, are prime targets for cybercriminals. Additionally, the bank must comply with strict financial regulations, making any data leak or fund disruption particularly damaging.

Risk	Description	Likelihood	Severity	Priority (L x S)
Business Email Compromise	Attackers may impersonate executives or vendors to initiate fraudulent transactions.	3	3	9
Compromised User Database	Hackers gain access to the bank's database, exposing user credentials and PII.	2	3	6
Financial Records Leak	Sensitive financial documents are unintentionally leaked or exfiltrated.	2	3	6

Theft	Physical or digital theft of customer funds due to internal or external actors.	2	2	4
Supply Chain Disruption	A vendor's system is compromised, allowing attackers' indirect access to the bank.	1	3	3

This color-coded matrix summarizes the cybersecurity risk assessment for a commercial bank.

Each cell shows the risk score calculated as: Likelihood x Severity.

Colors indicate risk levels:

- Green: Low (1-3)
- Yellow: Medium (4-6)
- Red: High (7-9)

Risk Matrix

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