Risk assessment activity

To complete the risk assessment activity, follow these steps to evaluate each risk and determine the likelihood, severity, and overall risk score. Here is a structured approach you can use:

### Risk Factors Description

1. \*\*Risk Factors\*\*: The bank's coastal location could expose it to natural disasters such as hurricanes, which might disrupt operations. The presence of 120 employees and a customer base of 2,200 accounts increases the number of potential attack vectors. Compliance with stringent financial regulations demands that the bank ensures high levels of data and funds security.

### Risks Evaluation

Assuming you are assessing five different risks, here’s how you might score them:

1. \*\*Risk 1: Natural Disaster (e.g., Hurricane)\*\*

- \*\*Likelihood\*\*: 3 (Moderate) – Coastal location increases the probability of such events.

- \*\*Severity\*\*: 5 (Critical) – Disruptions can severely impact bank operations and data integrity.

- \*\*Overall Risk Score\*\*: 15 (Likelihood 3 x Severity 5)

2. \*\*Risk 2: Data Breach due to Phishing\*\*

- \*\*Likelihood\*\*: 4 (High) – Many employees and customers could be targeted by phishing attempts.

- \*\*Severity\*\*: 4 (High) – A data breach can result in significant financial and reputational damage.

- \*\*Overall Risk Score\*\*: 16 (Likelihood 4 x Severity 4)

3. \*\*Risk 3: Insider Threat (e.g., Malicious Employee)\*\*

- \*\*Likelihood\*\*: 2 (Low) – Fewer opportunities for malicious insider activity.

- \*\*Severity\*\*: 5 (Critical) – Could lead to severe data and financial losses.

- \*\*Overall Risk Score\*\*: 10 (Likelihood 2 x Severity 5)

4. \*\*Risk 4: System Outage due to Software Failure\*\*

- \*\*Likelihood\*\*: 3 (Moderate) – Software systems are critical, and failures can occur.

- \*\*Severity\*\*: 3 (Moderate) – A system outage impacts operational efficiency but might be recoverable.

- \*\*Overall Risk Score\*\*: 9 (Likelihood 3 x Severity 3)

5. \*\*Risk 5: Regulatory Compliance Violation\*\*

- \*\*Likelihood\*\*: 2 (Low) – The bank has a strong compliance framework.

- \*\*Severity\*\*: 5 (Critical) – Non-compliance can result in severe legal and financial penalties.

- \*\*Overall Risk Score\*\*: 10 (Likelihood 2 x Severity 5)

### Summary

- \*\*Natural Disaster\*\*: Likelihood 3, Severity 5, Overall Risk Score 15

- \*\*Data Breach due to Phishing\*\*: Likelihood 4, Severity 4, Overall Risk Score 16

- \*\*Insider Threat\*\*: Likelihood 2, Severity 5, Overall Risk Score 10

- \*\*System Outage\*\*: Likelihood 3, Severity 3, Overall Risk Score 9

- \*\*Regulatory Compliance Violation\*\*: Likelihood 2, Severity 5, Overall Risk Score 10

The team should prioritize risks with higher overall scores, such as Data Breach due to Phishing, to ensure the bank’s security posture is adequately addressed.