Scenario

You've joined a new cybersecurity team at a commercial bank. The team is conducting a risk assessment of the bank's current operational environment. As part of the assessment, they are creating a risk register to help them focus on securing the most vulnerable risks.

A **risk register** is a central record of potential risks to an organization's assets, information systems, and data. Security teams commonly use risk registers when conducting a risk assessment.

Your supervisor asks you to evaluate a set of risks that the cybersecurity team has recorded in the risk register. For each risk, you will first determine how likely that risk is to occur. Then, you will determine how severely that risk may impact the bank. Finally, you will calculate a score for the severity of that risk. You will then compare scores across all risks so your team can determine how to prioritize their attention for each risk.

Steps

Step 2: Understanding the operating environment

When conducting a risk assessment, it's important to consider the factors that could cause a security event. This often starts with understanding the operating environment.

In this scenario, your team has identified characteristics of the operating environment that could factor into the bank's risk profile:

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.

step 3: consider potential risks to assets

Security events are possible when assets are at risk. The source of a risk can range from malicious attackers to accidental human errors. A risk source can even come from natural or environmental hazards, such as a structural failure or power outage.

The bank's funds are one of its key assets. Your team has listed five primary risks to the bank's funds:

- Business email compromise
- Compromised user database
- Financial records leak
- Theft
- Supply chain attack

Consider these potential risks in relation to the bank's operating environment. Then, write 2-3 sentences (40-60 words) in the Notes area of the template describing how security events are possible considering the risks facing the funds in this operating environment.

Step 4: score risks based on their likelihood
As you might recall, risk can be calculated with this simple formula:

Likelihood x Impact = Risk

In order to calculate the score for a security risk, you must first estimate and score the likelihood of the risk causing a security event. The likelihood of a risk can be based on available evidence, prior experience, or expert judgment. A common way to estimate the likelihood of the risk is to determine the potential frequency of the risk occurring:

- Could the risk happen once a day?
- Could the risk happen once a month?
- Could the risk happen once in a year?

For example, the bank must have enough funds available each day to meet its legal requirements. A potential risk that could prevent the bank from replenishing its funds is a supply chain disruption. Being located in a coastal area, there's a likelihood that the bank may experience supply chain disruptions caused by hurricanes. However, a hurricane might only impact the bank every few years, so you can score the likelihood as low.

In this instance, the team is scoring the likelihood of an event on a scale of 1-3:

- 1 represents an event with a low chance of occuring.
- 2 represents an event with a moderate chance of occuring.
- 3 represents a high chance of occuring.

Review the **Risk(s), Description**, and **Notes** of the risk register template. Refer to the risk matrix and use it to estimate a likelihood score for each risk. Then, enter a **score (1-3)** for each risk in the **Likelihood** column of the register.

step 5: score risks based on their severity

A severity score is an estimate of the overall impact that might occur as a result of an event. For example, damage can occur to a company's reputation or finances and there may be a loss of data, customers, or assets. Evaluating the severity of a risk helps businesses determine the level of risk they can tolerate and how assets might be affected.

When evaluating the severity of a risk, consider the potential consequences of that risk occurring:

- How would the business be affected?
- What's the financial harm to the business and its customers?
- Can important operations or services be impacted?
- Are there regulations that can be violated?
- What is the reputational damage to the company's standing?

Use the top row of the risk matrix and consider the potential impact of each risk. Estimate a severity score for each risk. Then, enter a score (1-3) for each risk in the Severity column of the register:

- 1 (low severity)
- 2 (moderate severity)
- 3 (high severity)

For example, a leak of financial records might lead to a loss of profits, a loss of customers, and heavy regulatory fines. A risk such as this might receive a severity score of 3 because it greatly impacts the bank's ability to operate.

step 6: calculate an overall risk score

Ultimately, the goal of performing a risk assessment is to help security teams prioritize their efforts and resources.

Using the risk formula, multiply the likelihood and severity score for each risk. Then, enter a priority **score (1-9)** for each of the risks in the **Priority** column of the register.