Activity Overview

In this activity, you will practice performing a risk assessment by evaluating vulnerabilities that commonly threaten business operations. Then, you will decide how to prioritize your resources based on the risk scores you assign each vulnerability.

You might recall that the purpose of having a security plan is to be prepared for risks. Assessing potential risks is one of the first steps of the **NIST Cybersecurity Framework (CSF)**, a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Risk assessments are how security teams determine whether their security operations are adequately positioned to prevent cyber attacks and protect sensitive information.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

Review the following scenario. Then complete the step-by-step instructions.

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.

Step-By-Step Instructions

Follow the instructions and answer the question below to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

Step 2: Understand 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

Step 4: Score risks based on their likelihood

Step 5: Score risks based on their severity

Step 6: Calculate an overall risk score

What to Include in Your Response

Be sure to address the following criteria in your completed activity:

- 2-3 sentences describing the risk factors
- 5 likelihood scores
- 5 severity scores
- 5 overall risk scores