Risk register

Operational environment:

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.

Asset	Risk(s)	Description	Likelihood	Severity	Priority
Funds	Business email compromise	*An employee is tricked into sharing confidential information.*	2	2	4
	Compromised user database	*Customer data is poorly encrypted.*	2	3	6
	Financial records leak	*A database server of backed up data is publicly accessible.*	3	3	9
	Theft	*The bank's safe is left unlocked.*	1	3	3
	Supply chain disruption	*Delivery delays due to natural disasters.*	1	2	2
Notes	*How are security events possible considering the risks the asset faces in its operating environment?* *MY RESPONSE:* *When I work with other companies, I recognize that it increases data risks by opening new avenues for compromise. While I consider theft a risk, I don't prioritize it as much due to the bank's location in a low-crime area. I also need to account for the number of companies interacting with the bank, as they can introduce risks beyond my control, impacting both customers and operations.* *For likelihood, I score risks on a scale of 1-3. I rate supply chain attacks caused by natural disasters as a 1 (unlikely), but I consider data breaches more likely, so I score them a 2. In terms of severity, I never score risks lower than 2, given the serious consequences of data*				

breaches like email compromises. I know that such incidents could seriously harm customer trust and disrupt operations.
Finally, I prioritize risks based on their overall score. A financial records leak receives the highest score of 9, signaling that I need to address it first. Regular risk assessments help me stay ahead of threats and keep the bank secure.

NOTES:
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.
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. *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.* *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.* *For this practice activity, your estimations for 'Likelihood' and 'Severity' should be based on a reasonable interpretation of the provided 'Operational Environment' and 'Risk*

Description,' applying general industry knowledge about common vulnerabilities and their potential impact. While real-world assessments involve extensive data, here you are practicing the process of evaluating risk.

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.

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.*

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*

Notes

Some risk factors to have considered might have been the number of other companies that interact with the bank. These sources of risk might introduce incidents beyond the bank's control. Also, the risk of theft is important to consider because of the number of customers and the operational impact it could have to the business.

Likelihood

A range of likelihood scores were estimated based on factors that could lead to a security incident. Each risk was scored as a 1, 2, or 3 on a risk matrix, meaning the chances of occurring were rare, likely, or certain. A supply chain attack caused by natural disaster was

	scored with a 1, meaning it was regarded as unlikely due to the unpredictability of those events. On the other hand, compromised data events were scored a 2 because they are likely to occur given the possible causes. **Severity** No risk received a severity score less than 2 because risks that involve data breaches such as business email compromise, can have serious consequences. Customers at a bank trust the businesses to protect their money and personal information. Also, the bank's operations could be terminated if they fail to comply with regulations. **Priority** A financial records leak received the highest overall risk score of 9. This indicates that this risk is almost certain to happen and would greatly impact the bank's ability to operate. Such a high overall score signals the security team to prioritize remediating, or resolving any issues related to that risk before moving on to risks that scored lower. **Key takeaways** Risk assessments are useful for identifying risks to an organization’s information, networks and systems. Security plans can benefit from regular risk assessments as a way of highlighting important concerns that should be addressed. Additionally, these assessments help keep track of any changes that can occur in an organization's operating environment. Thank you for completing this activity! Risk assessments help businesses ensure that they're prepared to prevent or mitigate situations that could be harmful to them, their partners, or their customers. You are likely to be involved in a risk assessment that evaluates your operational environment and identifies critical risks that require attention. Go to the next course item to compare your work to a completed exemplar.

Asset: The asset at risk of being harmed, damaged, or stolen.
Risk(s): A potential risk to the organization's information systems and data.
Description: A vulnerability that might lead to a security incident.
Likelihood: Score from 1-3 of the chances of a vulnerability being exploited. A 1 means there's a low likelihood, a 2 means there's a moderate likelihood, and a 3 means there's a high likelihood.
Severity: Score from 1-3 of the potential damage the threat would cause to the business. A 1 means a low severity impact, a 2 is a moderate severity impact, and a 3 is a high severity impact.
Priority: How quickly a risk should be addressed to avoid the potential incident. Use the following formula to calculate the overall score: **Likelihood x Impact Severity = Risk**

Sample risk matrix

Severity

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