Activity Overview

In this activity, you will assess the access controls used by a business. You'll analyze their current process, identify issues, and make recommendations to improve their security practices.
Previously, you learned that access controls are security controls that manage access, authorization, and accountability of information. Authentication controls are used to verify who someone is, whereas authorization controls are used to grant a user permissions and set limits on the things they're allowed to do. When done well, access controls are the key to decreasing the likelihood of a security risk.
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 scenario below. Then complete the step-by-step instructions.
You're the first cybersecurity professional hired by a growing business.
Recently, a deposit was made from the business to an unknown bank account. The finance manager says they didn't make a mistake. Fortunately, they were able to stop the payment. The owner has asked you to investigate what happened to prevent any future incidents.
To do this, you'll need to do some accounting on the incident to better understand what happened. First, you will review the access log of the incident. Next, you will take notes that can help you identify a possible threat actor. Then, you will spot issues with the access controls that were exploited by the user. Finally, you will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs.

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
To use the template for this course item, click the link below and select *Use Template*.
Link to template: Access control worksheet
OR
If you don't have a Google account, you can download the template directly from the attachment below.
Access control worksheet
DOCX File

Step 2: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.
To use the supporting materials for this course item, click the link below and select "Use Template."
Note: The spreadsheet for this supporting resource has two tabs.
Link to template: Accounting exercise
OR

If you don’t have a Google account, you can download the supporting materials directly from the attachment below.
Accounting exercise
XLSX File

Step 3: Review the event log of this payroll incident

Event logs contain information related to the operation and usage of a system. They can be utilized to identify suspicious activity, detect vulnerabilities, and track users.
Find the Event log tab of the *Accounting exercise* spreadsheet. Carefully review the event log of this incident to start your investigation. Notice the *Event Type*, *Date*, *Time*, and *IP Address* of the user in the log details.
Make 1-2 notes of information that you learned about the user from reviewing the *Event log* details. Add your notes to the Notes column of the access control worksheet.

Step 4: Identify access control issues that led to the incident

Log details tell you a lot about a specific moment in time. You can find other useful details about an event by cross referencing that information with other sources.
This business has a range of different employees. They all currently manage company resources using a shared cloud drive.
Find the Employee directory tab of the *Accounting exercise* spreadsheet. Compare the information found in the *Employee directory* tab with the information in the *Event log* tab. Notice any similarities between the details in the *Event log* and the details in the *Employee directory*.
Then, list 1-2 issues that you discover with how the business handles employee access in the Issues column of the *Access control worksheet*.

Step 5: Recommend mitigations that can prevent a future breach

You’ve completed your accounting of the strange payment and discovered flaws with how the business handles their information.
Find the Recommendation(s) column of the *Access control worksheet*. Make at least 2 recommendations of mitigations the business can implement to prevent incidents like this in the future.
For example, one recommendation might be to have procedures in place to revoke access to files when an employee is no longer with the company.

What to Include in Your Response

Be sure to include the following elements in your completed activity:

- 1-2 notes about the user
- 1-2 access control issues
- 2 recommendations for access control mitigations