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.

Event Information:

Event Type: Information
Event Source: AdsmEmployeeService
Event Category: None
Event ID: 1227
Date: 10/03/2023
Time: 8:29:57 AM
User: Legal\Administrator
Computer: Up2-NoGud
IP: 152.207.255.255
Description:
Payroll event added. FAUX_BANK

Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** Make 1-2 notes of information that can help identify the threat: ● *Who caused this incident?* *Robert Taylor Jr. [Role: Legal attorney]* ● *When did it occur?* *8:29:57 AM on 10/03/2023* ● *What device was used?* *Computer: Up2-NoGud* *IP Address: 152.207.255.255*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* *Admin* ● *Should their account be active?* *No. His contract ended in 2019, but he still can access payroll systems in recent few days (2023).*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* - *Limiting access for contractors to business resources.* - *Apply SSO and MFA*