

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.

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.