Scenario

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.

Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	The event log shows that the employee, Robert Taylor Jr., with the IP address 152.207.255.255, was the cause of the incident. The event occurred on Date: 10/03/2023 At 8:29:57 AM.	Robert Taylor Jr. has administrative access to the organization's system. Robert's contract ended in 2019, yet his account wasn't deprovisioned.	Enable MFA: Technically, adding an extra layer should be required to approve transactions in the organization. Deprovisioning of user accounts when they no longer need access to systems. Termination of sessions after every 14 days. Enforcing the Principle of Least Privilege to ensure users only have access to the minimal resources they need with the right permissions. Integration of Role-based Access Control (RBAC). A system that controls what each user can access based on their role.