Access controls worksheet

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 reoccur.

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	• The incident was triggered by the `Legal\Administrator` account. • It occurred on October 3, 2023, at 8:29 AM. • The activity came from a device named `Up2-NoGud`, not known to be used by the finance department.	• Robert Taylor Jr is an admin. • His contract ended in 2019, but his account accessed payroll systems in 2023.	• Implement role-based access control to ensure only authorized finance personnel can access payroll systems. • Disable or audit legacy administrator accounts not tied to active users. • Enable MFA and maintain access logs with regular reviews to detect unauthorized activity early.