Access controls worksheet

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.

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● *Who caused this incident?* - *The user is Legal\Administrator with a IP Address of 152.207.255.255* - *(Robert Taylor Jr)* ● *When did it occur?*	**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*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* - *Enable MFA* - *Contractors should have limited access to business resources.*

	- *October 3, 2023 at approximately 8:29am* ● *What device was used?* - *Computer Up2-NoGud*		