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?* ● *When did it occur?* ● *What device was used?*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ● *Should their account be active?*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?*

According to the Accounting Exercise Spreadsheet, the event occurred on **October 3rd, 2023 (assuming date format is MM/DD/YYYY)** The device that was used was a Computer with name **Up2-NoGud** under User: **Legal\Administrator** with IP address: **152.207.255.255**. According to our records, we do not have an authorized device under that computer name nor that IP address.

Seems that the User had Administrator privileges as they were able to add in new Payroll deposit information for a transaction about to be deposited (thankfully our IDPS and SIEM tools have flagged and stopped the deposit before it was processed and finalized). User\LegalAdministrator either shouldn't exist or if legitimate user, should not have privileges to sign off on deposits. For proper control mechanisms to avoid errors, the Finance Manager can create the deposit request, and the Accounts Manager should review the request and double-check that all details are correct and legitimate and then approve it before funds leave the account.

User accounts should expire after 30 days of termination. Robert Tayler Jr was an old employee. Also enable MFA