Access controls worksheet

	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 incident, according to the logs, claims to have been caused by the Legal/Administrator. This could be a case of session hijacking.* ● *When did it occur?* *This event seems to have occurred on 10/03/2023 at 8:29:57 AM.* ● *What device was used?* *The device was a Up2-NoGud, whose IP address is 152.207.255.255*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* *Robert Taylor Jr is an admin.* ● *Should their account be active?* *His contract ended in 2019, but his account accessed payroll systems in 2023.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* 1. *User accounts should expire after 30 days.* 2. *Multi-Factor Authentication needs to be implemented if not implemented yet.*