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?* ● *When did it occur?* ● *What device was used?* ● *The incident's IP address was the contracted legal attorney who left the company 4 years ago* ● *It happened 5 days ago from his past user account*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ● *Should their account be active?* ● *User accounts have access to all company resources through the shared cloud drive* ● *The past contracted legal attorney's account should have been deactivated after they left the company*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* ● *Implement an IAM system to manage user privileges to resources and adhere to separation of duties* ● *Immediately remove past user accounts from the shared drive after they leave the company*