Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: • Legal/Admin user caused this incident. They have the IP address 152.207.255.255 • It occurred on 10/03/2023 at 8:29:57 AM. • The device that was used was Up2-NoGud.	**Objective:** Based on your notes, list 1-2 authorization issues: • The user was the legal attorney. He has admin privileges. • His account should not be active because he stopped working at the company in 2019.	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: • Deprovisioning of users, users accounts should expire after 30 days. • Principle of least privilege: Contractors should have limited access to systems. • Enable MFA.