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?* *This incident was caused by an employed contractor identified as Robert Taylor Jr. on 10/03/2023 at 8:29:57 AM. The device used was labeled as "Up2-NoGud".*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ● *Should their account be active?* *The user had Legal/Administrator access despite having an end date of 12/27/2019. Following a review of current and prior employee access, all users (including seasonal and no longer employed) have active administrator access.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* *The organization should restrict user access according to the Principle of least privilege and separation of duties. Users should be audited to determine appropriate access as business needs and employee roles change. Additionally, MFA should be utilized as this would prevent a threat actor from gaining access to a user's account, which may have been the case here.*