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 event was caused by a user at the IP address: 152.207.255.255 and occurred on the computer Up2-NoGud at 8:30 AM.*	**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 associated with this issue was Robert Taylor Jr. who had admin level access along with every other past or present employee despite the fact they were no longer employed and thus should have had a deactivated account.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* *The simplest control to prevent this incident would be implementing the principle of least privilege there by revoking admin access from all the employees and implicitly removing all access of terminated employees.*