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?*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ● *Should their account be active?*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?*
	The source of the incident was AdsmEmployeeService used by a Legal/Administrator user. The incident occurred on 10/03/2023 at 8:29:57 am. The computer's name was Up2-NoGud, with an I.P. of 152.207.255.255.	*The user has admin access, along with every other user in the company, which is highly dangerous. Robert Taylor Jr. is the user, since they are the only legal/admin user, their last access date matches the incident, and the IP address also matches. They should not have any access since they last worked at the company in 2019.*	*The company should conduct user audits so that they can remove users who no longer work at the company, and adjust the privileges of the current users to prevent unauthorized access to the payroll info. Also, limiting contractors' access levels will keep company info safe.*