Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** Make 1-2 notes of information that can help identify the threat: ● *At 8:29 AM, on 10/03/2023.* ● *The number of this Event ID for this event is "1227".* ● *The event occurred in relation to the payroll event "FAUX_BANK".* ● *The IP address used to log in was 152.207.255.255* ● *The incident occurred from a computer with the name of "Up2-NoGud".* ● *The Legal/Administrator is the user and the employee's name is Robert Taylor Jr.*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *The user should not have access to make payroll transactions as he is a Legal Attorney.* ● *The user's authorization is set to Admin, this should be removed.* ● *He was a contractor whose contract ended in 2019. His access to all systems should be revoked upon termination and in accordance with Termination Policies.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Implementation of Termination Policies (remove access upon termination).* ● *Implementation of Password Policies can prevent year old passwords from being used.* ● *Principle of least privilege for roles. Implement RBAC to ensure contractors have only necessary roles.* ● *Periodic access audits could catch any current or terminated employees with inappropriate access.* ● *Enabling MFA can ensure that unwanted access is prevented.*