Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** Make 1-2 notes 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?*

Notes:

1. The threat actor was Robert Taylor Jr., a former legal attorney contractor whose employment ended on 12/27/2019, but accessed the system on 10/03/2023 at 8:29:57 AM (over 3 years after termination)

2. The suspicious computer name "Up2-NoGud" and IP address 152.207.255.255 were used to attempt adding a fraudulent payroll event to "FAUX_BANK"

Issues:

1. Failed account deprovisioning: Robert Taylor Jr.'s account remained active with full Admin privileges 3+ years after his contract ended (12/27/2019)

2. Excessive privilege assignment: ALL employees have "Admin" authorization regardless of their role, violating the principle of least privilege (contractors, part-time, and seasonal workers have same access as full-time)

Recommendations:

1. Implement automated off-boarding procedures:
   - Immediate access revocation upon employment termination
   - Automatic account deactivation on contract end dates
   - Mandatory IT/HR checklist for departing employees

2. Enforce Role-Based Access Control (RBAC) with least privilege:
   - Create tiered authorization levels (User, Power User, Admin)
   - Restrict Admin access to essential personnel only
   - Implement need-to-know basis for sensitive systems like payroll

3. Deploy Multi-Factor Authentication (MFA) for all users, especially for financial transactions and administrative functions

4. Establish quarterly access reviews and audit procedures:
   - Regular review of all active accounts
   - Automatic alerts for dormant accounts (30+ days inactive)
   - Immediate investigation of suspicious access patterns