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?* ● The unauthorized payroll entry (Event ID 1227, "Payroll event" added. FAUX_BANK") was logged 10/03/2023 at 8:29:57 AM from IP 152.207.255.255, under the account "Legal\Administrator." ● That same IP address belongs to Robert Taylor Jr., a Legal attorney contractor whose access end date was 12/27/2019 - almost four years before this login.	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ● *Should their account be active?* ● Robert Taylor Jr.'s contract ended 12/27/2019, yet his account was never deactivated and was still able to log in and post a payroll transaction almost four years later. ● Every employee in the directory - including part-timers, seasonal staff, and contractors - is listed with full Admin authorization on the shared cloud drive, so a former contractor had the same broad access as full-time staff,	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* ● (Operational) Create a formal offboarding procedure that revokes account access the moment an employee's or contractor's end date is reached and run periodic access audits to catch any accounts that were missed. ● (Technical/Managerial) Apply the principle of least privilege by assigning role-based access levels instead of Admin for everyone and require multi-factor

	Note(s)	Issue(s)	Recommendation(s)
		violating least privilege.	authentication plus dual approval for sensitive actions like payroll changes.