Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** Make 1-2 notes of information that can help identify the threat: ● *The event took place on 10/03/23.* ● *The user is Robert Taylor Jr. (Legal / Administrator)* *The IP address of the computer used to login is 152.207.255.255.*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *Robert Taylor Jr is an admin.* ● *His contract ended in 2019, but his account accessed payroll systems in 2023.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *User accounts should expire after 30 days.* ● *Contractors should have limited access to business resources.* ● *Enable MFA.*

Notes

- The event log indicates that the user "Legal\Administrator" initiated a payroll event on 10/03/2023 at 8:29:57 AM from the computer "Up2-NoGud" with IP address 152.207.255.255.
- Cross-referencing with the Employee directory, Robert Taylor Jr., a contractor with the role of Legal attorney, is associated with the same IP address (152.207.255.255) and has Admin authorization, with his last access recorded five days prior to the incident.

Issues

- All employees, including part-time, seasonal, and contractors like Robert Taylor Jr., have Admin-level access, which is excessive for their roles and increases the risk of unauthorized actions.

Recommendations

- Implement role-based access control (RBAC) to assign permissions based on job roles, limiting Admin access to only those who require it for their duties, such as the Owner or Office manager.
- Establish a process to promptly revoke access for employees upon termination or contract end, including regular audits to identify and deactivate stale accounts like Joanne Phelps.