Identify Access Control Assessment

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	• *The incident occurred on 10/03/23.* • *The user involved is identified as Legal/Administrator.* • *The IP address used for the login is 152.207.255.255.*	• *Robert Taylor Jr, who is not an admin, accessed the payroll systems despite his contract ending in 2019.* • *The access controls failed to restrict unauthorized access and prevent the incident.*	• *Implement an account expiration policy, where user accounts automatically expire after 30 days to remove access for terminated employees or contractors.* • *Restrict the access privileges of contractors, granting them only the necessary resources for their assigned tasks.* • *Enable Multi-Factor Authentication (MFA) to add an additional layer of security for user authentication and reduce the risk of unauthorized access.*

The activity involved assessing the access controls used by a business, analyzing their current process, identifying issues, and providing recommendations for improvement. My objective was to investigate a payment incident and prevent similar incidents in the future.

To solve the activity, I followed a step-by-step process:

- I reviewed the access log and took notes on key information such as the date, user role, and IP address involved in the incident.
- I identified authorization issues, including an unauthorized user accessing payroll systems and an expired contract.
- I made recommendations to mitigate future incidents, such as implementing account expiration policies, restricting access for contractors, and enabling Multi-Factor Authentication (MFA).

Overall, I successfully completed the activity by effectively analyzing the situation, identifying the issues with access controls, and providing practical recommendations for improving security practices.