## 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?*   *Robert Taylor Jr. – Legal Attorney*   * *When did it occur?*   *8:29 AM, October 3, 2023*   * *What device was used?*   *Computer: Up2-NoGud*  *IP Address: 152.207.255.255.* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?*   *The user has Admin access, and so does every other user in the company, which should not be the case.*   * *Should their account be active?*   *No their account should not be active since Robert Taylor Jr.’s role at the company is a Legal Attorney also his employment date ended in 12/27/2019 but because of the access to his account not expiring, it was used to access payroll.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   *-The principle of least privilege should be enacted, since every employee at the company has admin privileges when they don’t need to.*  *-Also, employees need to stick to their respective roles, and the concept of separation of duties needs to be followed, and instead of the Attorney handling invoices the person who is actually employed to do so should be doing it, like the account manager.*  *-Also, people who have left the company should still not have access/ authorization, there were 3 ex-employees who still have admin privileges.*  *-Direct hires to the company shouldn’t have much access within the company.*  *-MFA should be enabled* |