## Access controls worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | The IP address belongs to Robert Taylor Jr., a contractor who no longer works there. The event occurred 5 days ago but the contractor has not worked there in 4 years and should not have access. **Objective:** List 1-2 pieces of information that can help identify the threat:   * *Who caused this incident?* * *When did it occur?* * *What device was used?* | Robert Taylor Jr. no longer works for the company and should not have any access to company accounts or data. Furthermore, all employees/contractors have admin privileges - the company does not practice Principle of Least Privilege which increases the risk of attack. **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?* * *Should their account be active?* | Employees and contractors who no longer work at the company should have all access disabled/removed immediately. This practices Least Privilege.  Not everyone should have Admin authorization, only those that need it. When Admin use-cases are complete, those rights should be revoked.  **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?* |