## Access controls worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | **Objective:** List 1-2 pieces of information that can help identify the threat:   * *Who caused this incident?*   *AdsmEmployeeService who has Legal/Administrator access caused this incident.*   * *When did it occur?*   *The incident occurred on 10/03/2023 in the morning 8:29:57 AM.*   * *What device was used?*   *The device that was used in the incident in Up2-NoGud. And its IP address is 152.207.255.255.* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?*   *Robert Taylor Jr. has an*  *Admin level of access. He is the legal attorney of the organization.*   * *Should their account be active?*   *His contract ended in 2019. But his account accessed the payroll system in 2023. His account should not be active.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*  1. *Revoke access to files when an employee is no longer with the company.* 2. *Enable MFA.* 3. *Contractors should*   *have limited access to*  *business resources.* |