## 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?* * *When did it occur?* * *What device was used?* * Unauthorized user w/ Legal/Administrator account * An unknown computer/server using IP address 152.207.255.255 * Activity conducted 10/3/23 | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?* * *Should their account be active?* * (Legal) admin account   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:   * *Which technical, operational, or managerial controls could help?*   To prevent this kind of incident from happening again, the principle of least privilege should be implemented:   * User accounts should expire 30 days * Enable MFA * Audit users who have access to these files especially when employee/contractor is no longer with company |