## 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?* * *When did it occur?* * *What device was used?*  1. ***The event happened on March 3, 2023, at 08:29:57 5 days prior*** 2. ***This user is Legal/Administrator*** 3. ***IP 152.207.255.255*** | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?* * *Should their account be active?*  1. ***Robert Taylor had Administer Privileges*** 2. ***There account should not be active as his contracted ended in 2019 but his account had payroll account access in 2023.*** | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*  1. ***Enable Multifactor Authentication*** 2. ***Contractors should not have the same access privileges to business resources.*** 3. ***User Accounts should expire after not being used for 30 days*** |