## Access controls worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | **Objective:** Make 1-2 notes of information that can help identify the threat:  Looking at the event log we can gather the following information:   * The user is Legal/Administrator * The date happened was 10/03/2023 at 8:29:57 am * The 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?* * *Should their account be active?*   Robert Taylor Jr, the legal attorney was responsible for this, he has admin level access despite being a contractor and, his contract ended on the 27/12/2019 but he still has access to his account | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   All accounts should not have admin level privilege, they should follow least privilege.  All contractors’ accounts should expire after their contracts are complete or they should expire in a set amount of time.  All employees should use MFA, single sign on leaves all accounts vulnerable. |

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated