## 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?*   *This incident was caused by Robert Taylor Jr.; this is the user corresponding to the IP analyzed in the event log.*   * *When did it occur?*   *The event was on the following date: 8:29:57 AM.*   * *What device was used?*   *The device was Up2-NoGud.* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?*   *The user was Legal\Administrator. But if we check the employee directory we can see that he is a Contractor with Admin permissions.*   * *Should their account be active?*   *His account needs to be deactivated because this employee no longer works for the company. If we look at the event log, we can see that it occurred outside this person's contract dates.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   *Mainly, accounts should be deactivated once individuals no longer work for the company. Afterward, special permissions should be configured according to the position of the people within the department. It's not necessary for all users in the department to have* ***Administrator permissions****.* |