## 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?*   The incident was caused by Robert Taylor Jr. (a contractor of the business with a legal attorney role). His email is rt.jr@erems.net   * *When did it occur?*   According to the event log, the incident with ID event 1227 occurred at 8:29:57 am, 10/03/2023. This same timestamp appears in the last access of his account under the employee directory.   * *What device was used?*   The device used was hostname Up2-NoGud, with IP address 152.207.255.255, which is also registered under the employee directory on the same account. | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?*   This user has the highest level of authorization: Admin. The access should have been revoked from his account.   * *Should their account be active?*   This user started in the business 04/09/2019 and ended 27/12/2019. This account is supposed to be inactive. | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   It is recommended to improved the managerial control by revoking access to those accounts that has past end date. |