## 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 Event was caused by a system with User/Legal with IP address 152.207.255.255 cross referencing this IP with employee directory the IP address of the device belonged to a (Robert Taylor Jr) who’s working as contractor in Legal team*   * *When did it occur?*   *Event occurred on 10th March 2023 during the Morning at 8:29:57 A.M*   * *What device was used?*   *Computer with the Username Up2-NoGud* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?*   *The Threat actor had Admin level of access*   * *Should their account be active?*   *No , The user’s contract was expired on (12/27/2019) 3 years prior to this event but still the user’s access privilege is not revoked* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   *Upon Reviewing the employee directory i have observed the following points*   1. *All the Users are given Admin level of access regardless of their Nature , Role and Department they work on.* 2. *The Employees who left the organisation were still able to access the organisation system*   *Based on the observations , following recommendations are given to follow , in order to prevent future incidents*   1. *Only Security Analyst , Owner and Account Manager can be granted with Admin level of access and other employees shouldn’t be given such higher access* 2. *Other than these 3 , other users should have user level of access and should access only their department oriented resources* 3. *These access must be given with Managerial approval and not inherently* 4. *Part-time and Contract Employees should be given Limited access* 5. *It’s the duty of Security Analyst to Provide New User ID and delete the access to the employees who have left the organisation within 3 days of their LWD.* |