## 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?*   *The event occured at 08:29:57 by Robert Taylor from a computer device containing the same ip address as the log record which 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?*   *The user seems to posssess adminsitrator access which is a high privilge level, this seems to be too much access than necessary. This is a risk as human errors and misuse of access can pose an internal threat to assests and external thrats from bad actors taking control of the account to gain access to data and financial information.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   *Future recommendation would be to apply principle of least privilege restricting access to a minimum for what the user requires to perform their tasks.*  *Furthrmore, every user has admin rights which is bad practice the only user to have admin rights should be the security analyst George Harris. It is highly suggested to implement an access control model (RBAC) identify birth right accesses for everyone next group accesses by team adding members to those groups* |