## 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?*   *Finance manager says they didn’t make that transaction*  *A desposit was made from the business to an unknown bank account*  *Checked event says the user was Legal/Administrator*  *The event took place on 10/03/23.*  *The user is Legal/Administrator.*  *The IP address of the computer used to login 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?*   *Legal/Administrator was the user who had access to the business bank account to make a transaction*  *There should be an employee name attached to those kinds of actions*  *Robert Taylor Jr is an admin.*  *His contract ended in 2019, but his account accessed payroll systems in 2023.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   *More control and accountability*  *Having a name attached to these transactions*  *Restrict access to only those who need it*  *User accounts should expire after 30 days.*  *Contractors should have limited access to business resources.*  *Enable MFA.* |