## 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?* * *When did it occur?* * *What device was used?* * *Eg:* * *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?* * *Eg:* * *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?* * *Eg:* * *prevent this kind of incident:* * *User accounts should* * *expire after 30 days.* * *Contractors should* * *have limited access to* * *business resources.* * *Enable MFA.* |