## 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?* * *Legal\Admin* * *When did it occur?* * *10/03, 8:30-3PM* * *What device was used?* * *Up2-NoGud 150.207.255.255* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?* * *Everyone has admin rights* * *Should their account be active?* * *Some accounts don’t have a lease on session* * *Amanda has a 1 IP address* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?* * *Mitigate user and admin access based on role* * *Add a lease rule on session* * *Enforce a VPN to confirm the IP* |