## Access controls worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | **Objective:** List 1-2 pieces of information that can help identify the threat:   * *Legal\Administrator* * *10/03/2023 at 8:29:57 AM* * *PC named: “Up2-NoGud” with an IP of: 152.207.255.255* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *All employees have admin rights authorized for their accounts. Even the sales associates.* * *The account that started this incident should no longer be active as his end date was 12/27/2019 and this incident happened in October of 2023.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *A User provisioning audit should be launched to find any accounts that should be deprovisioned and any accounts with improper authorizations.* * *A Role-based access control (RBAC) should be implemented to insure that employees only have the resources they need based on their role* * *Any authorizations given outside of ones based on employee roles should be set with an expiration date and expire once it should be longer be needed.* |