## Access controls worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | **Objective:** List 1-2 pieces of information that can help identify the threat:   * *The incident was caused by the user "Legal\Administrator".* * *The incident occurred on October 3, 2023, at 8:29:57 AM.* * *The event was triggered from the computer named "Up2-NoGud" with the IP address 152.207.255.255.* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *User "Legal\Administrator" had access to add payroll events, but exact level not in log.* * *Account status of "Legal\Administrator" unclear due to limited info; depends on role, responsibilities, and org policies.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Tighten access controls per user roles.* * *Monitor and audit for prompt anomaly detection.* * *Add MFA, role-based access, and training for security.* |