## 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?*   *Based on the IP address comparison, the unauthorized transaction seems to have originated from the IP address "152.207.255.255", which belongs to* ***Robert Taylor Jr****, a contractor. He has used Up2-NoGud computer for the activity* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?* * *Should their account be active?*   *Robert Taylor has* ***Admin*** *privileges, which might be excessive for his role as a Contractor. Employees with these privileges should have more limited access to sensitive financial operations.*  *Taylor's account is currently active, and her last access was not recent, indicating no clear termination or restriction of access after completing certain tasks.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   *Admin privileges should only be granted to essential personnel. Taylor’s access should be reviewed, and her role as contractor should likely involve more limited access permissions.*  *The business should adopt a least-privilege policy where users only receive the access necessary for their role. Additionally, multi-factor authentication (MFA) should be implemented to prevent unauthorized access* |