## 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?* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?* * *Should their account be active?* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?* |
| **Authorization /authentication** | A computer named Up2-NoGud logged in at 10/03/2023 at 8:29:57 AM.  The IP address matches with the details of Robert Taylor Jr., Legal attorney, who was a former contractor for the company. The IP address of the computer used to login is 152.207.255.255. | The account had admin authorisation, although they were a legal professional and not a finance manager.  The account was closed on 27/12/19 so the account should no longer be active, but it accessed payroll systems in 2023. | The company should implement separation of duties and principle of least privilege.   * Users with roles that are not relevant to banking should not have admin access to the payroll systems. Contractors should also have lower privileges. * Regular audits should also be carried out to ensure that access is revoked when the user is no longer with the company or has a new role that does not require access to the payroll systems * User accounts should expire after a set amount of time (e.g., 30 days). * Enable MFA to prevent spoofing. |