## Access controls worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | * The incident occurred on 10/03/2023 at 8:29:57 AM. * The IP address associated with the user is 152.207.255.255. * The user responsible for the payroll event is listed as Legal\Administrator. | 1. **Expired Authorization**: The user associated with the incident, Robert Taylor Jr., is a contractor whose contract ended on 27/12/2019, yet they still have admin privileges. This indicates that access to the system was not revoked after the end of their contract.    2. **Administrator Access**: Even though Robert Taylor Jr.'s role as a legal attorney would not typically require administrator access, he was granted admin privileges, allowing him to access and potentially misuse sensitive payroll functions. | 1. **Implement an Automated Access Revocation System**: The company should establish a policy that automatically revokes access to all systems, files, and privileges immediately after an employee or contractor’s contract ends. This would ensure that individuals like Robert Taylor Jr. do not retain access beyond their employment period, reducing the risk of unauthorized activity.  2. **Enforce Role-Based Access Control (RBAC)**: The business should implement RBAC to ensure employees and contractors are only given the minimum level of access required for their role. In this case, admin privileges should only be granted to employees who require it for their job functions, reducing the potential for misuse of sensitive functions like payroll. |