## 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 event was caused by a user tagged Legal/Administrator. Robert Taylor Jr. He last logged into the system 5 days ago on the 10/03/2023 at 8:29:57.*  *He logged in using the Up2-NoGud computer with an IP address of 152.207.255.255.* | **Objective:** Based on your notes, list 1-2 authorization issues:  *Regarding access, every user in the company has administrator level access regardless of their job role and position within the company. This presents a serious security risk.*  *The user in question should have their account deactivated since their contract with the company ended two years ago.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   1. *Implementing the least privilege principle will ensure employees have only the essential permissions they need to fulfil their job role.* 2. *User deprovisioning: users accounts must be audited regularly to make sure that users who longer need access to systems are removed. User accounts should expire after 30 days of inactivity.* 3. *Multi-factor authentication must be enabled to reduce risks of password hijacking.* |