## Access controls worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | * Objective: The type of the event is "information," with event ID 1227, which occurred on 10/03/2023 at 8:29 AM. * The computer involved in the incident is named "Up2-NoGud," with an IP address of 152.207.255.255, and the payroll event that was added is "Faux\_Bank." | * **Objective:**After reviewing the employee directory, there's an issue with the authorization of company members where the issue lies in role-based access control. * Here, not every user should have admin access because it could potentially be a vulnerability that can be exploited. * The accounts of users who have left the company must be made inactive. * Another issue that could be resolved here is that we can limit users to accessing company resources only when present in the company network, which restricts any * potential threat actor outside of the network from accessing company resources. | **Objective:**   * I would recommend using role based access control which uplifts the principle of least privilege and separation of duties. * Enable MFA |