## 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 initiated by Legal/Administrator * The event took place on 10/3/2023 at 8:29:57 AM * The device that was being used is a computer “Up2-NoGud” with IP address “152.207.255.255” | **Objective:** Based on your notes, list 1-2 authorization issues:   * The access level is a Legal/Administrator " having access to payroll-related functions * Inactive user account: There is a possibility that the account of Legal/Administrator should have been inactive or closely monitored, especially the access to payroll function, to prevent unauthorized access | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * Role-Based Access Control or RBAC can be implemented to ensure users have minimum access or permission based on their job role. (authorization is determined by a user's role within an organization. ) * Account Review; Establish a regular review activity of the accounts. If the accounts are inactive or when they are not required anymore the accounts should be deactivated or review the account access to make sure every account has the right access based on the job's role. |