## Access controls worksheet

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| **Authorization /authentication** | The failed money transfer to an unknown bank called ‘Faux\_Bank’ was caused by user legal/administrator on March 10, 2023, at 8:29:57 AM, through a device named ‘Up2-NoGud’ with the following IP address: 152.207.255.255. | Turns out, the IP address is registered to the employee directory and, according to data, it belongs to ‘Robert Taylor Jr.’, a legal advisor contractor. The levels of access the user had was administrator, something that violates the principles of least privilege and separation of duties. Furthermore, the user account shouldn’t be active since his involvement with the company ended in December 12 2019. | To avoid any future incident like this one, it is highly recommended to enforce the principles of least privilege and separation of duties. To do this, a Role-based access control is recommended. Also, including MFA to verify a user’s identity in matters related to payments is recommended. |