## Access controls worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | **Objective:** Make 1-2 notes of information that can help identify the threat:   * *Who caused this incident?* * *When did it occur?* * *What device was used?* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?* * *Should their account be active?* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?* |

### Event Log Overview

The Event Log contains structured information regarding a specific incident, identified by its Event ID (1227), which occurred on 10/03/2023 at 8:29:57 AM. The log entries provide a timestamp and potentially the source of the event, indicative of the moment an unauthorized transaction was attempted or processed.

### Employee Directory Overview

The Employee Directory lists various employees with their roles, email addresses, IP addresses, status (Full-time, Part-time, Seasonal), authorization levels (Admin), last access times, and employment start and end dates. It's notable that multiple employees have admin access, which is a significant observation concerning access control issues.

Given this information, we proceed with the analysis to identify the possible threat actor and access control issues that may have led to the incident, and subsequently, develop recommendations for mitigating future risks.

### 1-2 Notes about the User

To pinpoint the potential threat actor, a comparison between the event timestamp and the "Last access" times of employees would be crucial. Given that the event occurred on 10/03/2023 at 8:29:57 AM, identifying which employee(s) accessed the system around this time could shed light on who might have initiated the transaction. We see it was Robert Taylor jr., with access that make the transaction. As a contractor he should not have full admin permissions.

### 1-2 Access Control Issues

The primary access control issue identifiable from the provided data is the indiscriminate granting of admin access to multiple employees, regardless of their role or necessity for such elevated privileges. This broad access could easily lead to abuse or unintentional misuse of sensitive functionalities, including financial transactions. They need to limit Admins to few people as possible, and given everyone is, not everyone should be.

### 2 Recommendations for Access Control Mitigations

1. **Principle of Least Privilege:** Implement a policy where employees are granted the minimum level of access necessary to perform their job functions. Admin access should be restricted to a select few who absolutely need it for their roles, reducing the risk of unauthorized transactions.
2. **Regular Access Reviews:** Establish a routine review process of user access levels, particularly for those with elevated privileges. This process should ensure that only current employees have access and that their access levels are appropriate for their roles. In case of role changes or termination, access rights should be promptly adjusted or revoked.

By addressing these issues and implementing the recommended mitigations, the business can significantly enhance its security posture and reduce the likelihood of similar incidents occurring in the future