# Access controls worksheet

## Activity: Improve authentication, authorization, and accounting for a small business

---

## Scenario

Review the scenario below. Then complete the step-by-step instructions.

You’re the first cybersecurity professional hired by a growing business.

Recently, a deposit was made from the business to an unknown bank account. The finance manager says they didn’t make a mistake. Fortunately, they were able to stop the payment. The owner has asked you to investigate what happened to prevent any future incidents.

To do this, you’ll need to do some accounting on the incident to better understand what happened. First, you will review the access log of the incident. Next, you will take notes that can help you identify a possible threat actor. Then, you will spot issues with the access controls that were exploited by the user. Finally, you will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs.

| | Note(s) | Issue(s) | Recommendation(s) |
|---|---|---|---|
| **Authorization /authentication** | **The event took place:** 10/03/2023 8:29:57 AM;<br>**From:** Computer: Up2-NoGud IP: 152.207.255.255, User: Legal\Administrator; | Robert Taylor Jr. rt.jr@erems.net Contractor, but marked in system as an admin.<br>His contract ended in 2019, but he is still able to login to the payroll system in 2023. | • Contractor should have limited access to the system.<br>• Automatically expiration of accounts<br>• MFA |