Access controls worksheet

Scenario

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.

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	Objective: A report was raised from an account owner claiming that a deposit was made to an unknown bank account. Based on the logs, it was found that on Oct. 3, 2023, 8:29:57 AM, on Up2-NoGud machine with IP 152.207.255.255, that an event was logged called	Objective: It was found that the level of access the user, Robert Taylor Jr., has was an administrator. He was a contractor that ended his contract on 12/27/2019.	Objective: With this kind of issue, an operational control should be implemented. One or more of the following should be applied: 1. Role-based Access Control 2. Proper offboarding procedure

	FAUX_BANK. It was performed by a user from the legal department.		3. Continuous logging and monitoring 4. MFA for all users 5. Least privilege principle 6. Separation of duties These recommendation should mitigate incidents like this in the future.