Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	Based on the event log, the incident was caused by the user "Legal\Administrator". Date: 10/03/2023 Device: Up2-NoGud It is essential to investigate and interview the legal administrator to determine if the unauthorized access occurred due to malicious action or if there was a possible exploitation of their account. According to the event log, the user "Legal\Administrator" had administrator privileges. This indicates a high level of access that could have been exploited to make the deposit to the unknown bank account. It is important to review	Administrator privileges	Implement the principle of least privilege, which means granting users only the privileges necessary to perform their tasks and functions. Conduct regular reviews of access permissions and update them based on changes in users' roles and responsibilities. Disable or revoke unnecessary privileges from user accounts to reduce the attack surface. Perform audits and regular monitoring of activities on privileged accounts to detect and prevent

	Note(s)	Issue(s)	Recommendation(s)
	and adjust user privileges to ensure that they only have the necessary access to perform their functions.		suspicious or unauthorized behavior. Implement multi-factor authentication for privileged accounts to add an additional layer of security and reduce the risk of unauthorized access. Establish intrusion detection systems and security monitoring tools to identify and alert potential malicious or anomalous activities in real-time.