Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● *Who caused this incident?* ● *When did it occur?* ● *What device was used?* ***Who caused this incident?*** ● *We need to examine the access logs for the user account that initiated the unauthorized transfer. Specifically, look for the user ID or account name associated with the transaction.* ● *If the access log shows an IP address from an unusual location, that can help identify the*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ● *Should their account be active?* ***What level of access did the user have?*** ● *The user account involved had sufficient permissions to initiate bank transfers. This indicates an over-privileged account.* ● *It is possible that the user account had access to financial information that it should not have had*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* ***Implement the principle of least privilege:*** ● *Restrict user access to only the resources and permissions they absolutely need to perform their job functions. Regularly review and adjust permissions.* ***Implement Multi-Factor Authentication (MFA):***

	threat actor. ***When did it occur?*** ● *The access logs will provide timestamps for the login and transaction activity. This is crucial for establishing a timeline of events.* ***What device was used?*** ● *The access logs may contain information about the device used (e.g., IP address, user agent string). An unfamiliar device or IP address can be a red flag.* ●	*access to.* ***Should their account be active?*** ● *If the account was a former employee's, a dormant account, or an otherwise unnecessary account, it should have been deactivated.* ● *If the account was in use, it is possible that the principle of least privilege was violated.*	● *Require users to provide multiple forms of authentication (e.g., password, mobile app code) before accessing sensitive systems. This adds an extra layer of security.* ***Implement regular access reviews:*** ● *Conduct periodic reviews of user accounts and permissions to identify and remove unnecessary accounts or excessive privileges.* ***Monitor for unusual activity:*** ● *Implement security information and event management (SIEM) tools to monitor access logs for suspicious activity, such as unusual login times, locations, or transaction patterns.*

			Implement a change managment process for financial transactions: ● *Require multiple approvers for all financial transactions over a certain dollar amount.* ***Employee security awareness training:*** ● *Train employees on how to spot phishing attempts, social engineering tactics, and other cybersecurity threats.*