

Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	<p>Objective: List 1-2 pieces of information that can help identify the threat:</p> <ul style="list-style-type: none"> • <i>Who caused this incident?</i> • <i>When did it occur?</i> • <i>What device was used?</i> <p>Who caused this incident?</p> <ul style="list-style-type: none"> • <i>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.</i> • <i>If the access log shows an IP address from an unusual location, that can help identify the</i> 	<p>Objective: Based on your notes, list 1-2 authorization issues:</p> <ul style="list-style-type: none"> • <i>What level of access did the user have?</i> • <i>Should their account be active?</i> <p>What level of access did the user have?</p> <ul style="list-style-type: none"> • <i>The user account involved had sufficient permissions to initiate bank transfers. This indicates an over-privileged account.</i> • <i>It is possible that the user account had access to financial information that it should not have had</i> 	<p>Objective: Make at least 1 recommendation that could prevent this kind of incident:</p> <ul style="list-style-type: none"> • <i>Which technical, operational, or managerial controls could help?</i> <p>Implement the principle of least privilege:</p> <ul style="list-style-type: none"> • <i>Restrict user access to only the resources and permissions they absolutely need to perform their job functions. Regularly review and adjust permissions.</i> <p>Implement Multi-Factor Authentication (MFA):</p>

	<p><i>threat actor.</i></p> <p>When did it occur?</p> <ul style="list-style-type: none"> The access logs will provide timestamps for the login and transaction activity. This is crucial for establishing a timeline of events. <p>What device was used?</p> <ul style="list-style-type: none"> 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. 	<p><i>access to.</i></p> <p>Should their account be active?</p> <ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. <p>Implement regular access reviews:</p> <ul style="list-style-type: none"> Conduct periodic reviews of user accounts and permissions to identify and remove unnecessary accounts or excessive privileges. <p>Monitor for unusual activity:</p> <ul style="list-style-type: none"> Implement security information and event management (SIEM) tools to monitor access logs for suspicious activity, such as unusual login times, locations, or transaction patterns.
--	--	--	--

			<p><i>Implement a change management process for financial transactions:</i></p> <ul style="list-style-type: none">• <i>Require multiple approvers for all financial transactions over a certain dollar amount.</i> <p><i>Employee security awareness training:</i></p> <ul style="list-style-type: none">• <i>Train employees on how to spot phishing attempts, social engineering tactics, and other cybersecurity threats.</i>
--	--	--	--