

## Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
<b>Authorization /authentication</b>	<p><b>Objective:</b> List 1-2 pieces of information that can help identify the threat:</p> <ul style="list-style-type: none"> <li>• <i>Who caused this incident?</i></li> <li>• <i>When did it occur?</i></li> <li>• <i>What device was used?</i></li> </ul> <p><i>The payroll event was added by the Legal/Administrator at 8:29:57 AM on 10/03/2023.</i></p>	<p><b>Objective:</b> Based on your notes, list 1-2 authorization issues:</p> <ul style="list-style-type: none"> <li>• <i>What level of access did the user have?</i></li> <li>• <i>Should their account be active?</i></li> </ul> <p><i>The event log shows that the Administrator account initiated the action. This is concerning because Robert Taylor Jr contract ended in 2019 and his account was utilized to access payroll systems in 2023.</i></p>	<p><b>Objective:</b> Make at least 1 recommendation that could prevent this kind of incident:</p> <ul style="list-style-type: none"> <li>• <i>Which technical, operational, or managerial controls could help?</i></li> </ul> <p><i>1. Implement role-based access control (RBAC) to ensure that only authorized personnel have access to sensitive operations like payroll.</i></p> <p><i>2. Enable Multi Factor authentication (MFA).</i></p> <p><i>3. User accounts should expire after a certain amount of days.</i></p>