Access controls worksheet

	Note(s)	**Issue(s)**	**Recommendation(s)**
Authorization /authentication	● ***Who caused this incident?*** *The incident was caused by the "Legal\Administrator" user.* ● ***When did it occur?*** *It occurred on October 3, 2023, at 8:29:57 AM.* ● ***What device was used?*** *The device used was named "Up2-NoGud" with the IP address 152.207.255.255.*	● ***Excessive Privileges:*** *The "Legal\Administrator" user seems to have access to add payroll events, which may be beyond the scope of their typical duties. This suggests a potential issue with excessive privileges or lack of proper segregation of duties.* ● ***Unauthorized Access:*** *The IP address suggests the access might have been from outside the company network. This raises concerns about potential unauthorized access or a*	● ***Review and Revoke Unnecessary Access:*** *Conduct a thorough review of user access privileges, especially for sensitive actions like payroll modifications. Revoke any unnecessary access and adhere to the principle of least privilege.* ● ***Implement Stronger Authentication:*** *Consider implementing multi-factor authentication (MFA) for all users, especially those with elevated privileges. This would add an extra layer of security and make it*

		compromised account.	*more difficult for unauthorized users to access the system.* ● ***Monitor and Alert on Suspicious Activity:*** *Deploy monitoring and alerting mechanisms to detect unusual activity, such as access from unfamiliar locations or outside of normal business hours. This allows for timely response and potential threat mitigation.* ● ***Regular Security Audits:*** *Conduct periodic security audits to identify and address potential vulnerabilities in access controls and user privileges.*