Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	- The incident occurred at 8:29:57 AM on 10/03/2023. - The user involved was "Legal\Administrator" from the computer named "Up2-NoGud" with IP address 152.207.255.255.	- The user had administrator-level access, which allowed them to make changes to the payroll. - The "Administrator" account should not be used for daily operations and should be strictly controlled.	***Implement Role-Based Access Control (RBAC):*** *Limit administrator privileges to only those who need them to perform their duties. Regular employees should have restricted access based on their roles.* ***Establish Regular Audits and Enforce MFA:*** *Regularly audit the activities of all administrator accounts and enforce multi-factor authentication (MFA) for high-level accounts to add an extra layer of security.*