Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	The incident was caused by the user Legal\Administrator. It occurred at 8:29:57 AM and was carried out from the device identified as Up2-NoGud, using the IP address 152.207.255.255.	Robert Taylor Jr. had administrator access, giving him full control over the system. However, his account shouldn't be active, as his departure date from the company is recorded as December 27, 2019. Despite this, activity was detected on his account just five days ago, at 8:29:57 a.m., indicating a flaw in the process for deactivating former employee accounts and posing a significant security risk.	It is essential to implement technical, operational, and administrative controls that strengthen system security. It is recommended to conduct periodic audits to verify compliance with the principle of least privilege and proper separation of roles. In the case analyzed, these principles were not properly applied, as all users had administrator access, giving them full control over the system regardless of their specific functions. This creates a significant risk, as any employee can make critical changes, diluting responsibility. Furthermore, it is essential to

			establish a rigorous account management process, which includes the immediate revocation of permissions from former employees, as in the case of Robert Taylor Jr., who retained access to the system after leaving the company.