Access controls worksheet

	Note(s)	**Issue(s)**	**Recommendation(s)**
Authorization /authentication	**Objective:** Make 1-2 notes of information that can help identify the threat: ● ***Who caused this incident?*** The individual who caused this incident was Robert Taylor Jr. ● ***When did it occur?*** The incident occurred on 10/03/23 at 8:29:57 AM ● ***What device was used?*** The device that was used was a computer named “Up2-NoGud” with and IP address of “152.207.255.255”	**Objective:** Based on your notes, list 1-2 authorization issues: ● ***What level of access did the user have?*** The level of access the user had was Admin with a status of “Contractor (Legal Attorney) ● ***Should their account be active?*** The account shouldn’t not be active. The individuals account should have been terminated at the end of contracting which was 12/27/19 or 4 years ago prior to the date of the incident.	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* **Managerial Controls** need to be set in place to give restraints for temporary users who are not directly affiliated with the organization. As well as individuals who don’t meet the credentials to have Admin access. Individuals that only have temporary access for a specific period of time should have their access revoked once there work is done. This would require policies, standards, and procedures to be set in place to prevent this kind of incident

	Note(s)	Issue(s)	Recommendation(s)
			happening in the future. **Technical Controls** need to be set in place to ensure certain data is encrypted and not as accessible to all users that happen to have Admin access. As well as authentication systems ensuring the correct individual has access to the right data. **Direct Recommendations:** ● User accounts should expire after 30 days. ● Contractors should have limited access to business resources. ● Enable MFA