Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	***Who caused this incident?*** *Robert Taylor Jr.* ***When did it occur?*** *10/03/2023 at 8:29:57 AM* ***What device was used?*** *Up2-NoGud, IP: 152.207.255.255*	***What level of access did the user have?*** *The user had Admin access* ***Should their account be active?*** *The account should have been deactivated after the end date (12/27/2019)* ***Other issues:*** *- Over-privileged Accounts* *- Lack of Role-Based Access Control (RBAC)* *- No Automated Deprovisioning* *- No Activity Monitoring or Alerting*	***Technical Controls*** **1. Implement Role-Based Access Control (RBAC)** *Define roles (e.g., Office Manager, Designer, Legal) and assign permissions accordingly.* *Only system admins and IT staff should have Admin privileges* **2. Enforce Least Privilege Principle** *Users should have the minimum permissions necessary to perform their job functions.* **3. Deploy Multi-Factor Authentication (MFA)** *Especially for Admin and remote access accounts.* *Reduces the risk of credential theft or misuse.* **4. Enable Automated Account Deactivation** *Configure HR or identity systems to automatically disable user accounts once the end date is reached.*

		- Weak Authentication Controls	*Integrate with Active Directory or Identity Management Systems (e.g., Azure AD, Okta).* **5. Log and Alert on Anomalous Activity** *Set alerts for:* • *Logins from expired accounts* • *Out-of-hours access* • *New payroll entries or changes* *Use SIEM (Security Information and Event Management) tools for analysis and alerting.* ***Operational Controls*** **1. Conduct Regular Access Reviews** *Schedule quarterly reviews of all user accounts and access levels.* *Remove unnecessary or outdated privileges* **2. Maintain an Access Control Matrix** *Map each role to its required access level.* *Use it as a baseline for access audits.* **3. Improve Onboarding/Offboarding Processes** *HR and IT must coordinate closely:* • *Onboarding: Provision accounts with correct roles.*

			• *Offboarding: Immediately disable accounts upon termination.* **Managerial Controls** ***1. Create and Enforce an Access Control Policy*** *Define acceptable use, access request process, and consequences for violations.* **2. Security Awareness Training** *Train users on secure password practices, phishing awareness, and reporting suspicious activity.* **3. Assign Access Control Ownership** *Designate a system administrator or IT security officer to be accountable for access rights and audit logs.*