Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● *Who caused this incident?* ● *When did it occur?* ● *What device was used?* *Company has been notified that there has been a deposit from the business to an unknown business account. From the information we have, we can understand that it was from the user -Legal\Administrator and from the computer Up2-No-Gud which occurred at 8:29:57 AM. This was all done from a computer with the IP address 152.207.255.255. When we look further into the employee directory, it is evident that Robert Taylor Jr. a former legal attorney is responsible for the incident.*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ● *Should their account be active?* *Robert Taylor Jr. had admin authorizations when he should have not. He should not even have an active account as he is a former employee and in the legal department as they have nothing to do with finances.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* *Technical-Implement Multi-Factor Authentication (MFA): Reduce the risk of unauthorized access by requiring multiple forms of verification. Add principle of least privilege* *Operational-perform audits* *Managerial- Risk Assessment and Management: Periodically evaluate risks to assets and implement mitigations accordingly.*