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?* *The incident was likely caused by someone with access to the financial systems, potentially through a compromised account or an insider with the necessary permissions to initiate a transaction. Since the finance manager didn't make a mistake, it may indicate unauthorized access by another user or a potential compromise.*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* *It appears that the user had access to initiate financial transactions, which may be higher than necessary for their role, especially if they were not a finance team member or authorized personnel. This could indicate that over-privileged access was granted to accounts that didn't require such permissions.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* ***Implement Multi-Factor Authentication (MFA):*** ● ***Type:*** *Technical Control* ● ***Description:*** *Requiring MFA for all sensitive accounts, especially those with access to financial systems, would provide an extra layer of security. This way, even if a user's*

	• *When did it occur?* *The exact time of the incident was October 3, 2023 at 8:29:57 AM and the payment was successfully stopped before it was completed.* • *What device was used?* *The threat actor was using a company asset computer with an IP address of 152.207.255.255 and was using the named as Up2-NoGood with over privilege account*	• *Should their account be active?* *The account's activity status should be reviewed, especially if it belongs to someone who no longer needs access (e.g., a former employee or a user who changed roles). If the account should not be active, this indicates an issue with account deactivation processes and a need for routine access reviews.*	*credentials are compromised, an additional verification step would be required before any high-risk actions can be performed.*