Access Controls Investigation

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: - The user is Legal\Administrator. - The incident occurred on October 3rd, 2023 at 8:29:57 AM local time. - The device used was a computer named: Up2-NoGud (likely out of network) on IP: 152.207.255.255	**Objective:** Based on your notes, list 1-2 authorization issues: - The user has administrator access - This account should not be active because Robert's contract ended prior to the incident.	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: - Separation of Duties would help by using different individuals to create an order and approve the order. - Include regular security audits across all users to revoke any unnecessary access. - Restrict access to information and resources to contractors. - Multi-Factor Authentication to

			prevent login attempts by unauthorized users.