Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	• Event originated from the machine “Up2-NoGud” from the IP address “152.207.255.255” • This event user account was ‘Legal/Administrator’ • Event occurred on 10/02/2023 at 08:29:57 AM UST	**Objective:** Based on your notes, list 1-2 authorization issues: • *The suspicious users IP address points to the username “Robert Taylor Jr.” who had Admin privileges* • *According to the employee directory, Mr. Taylor’s account should’ve been locked over 4 years ago(End date is 12/27/19)*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: • *A policy should be in place where a user has their account deactivated after a certain period of time has passed with no activity, a 4-6 weeks is the best time range* • *A management policy in which users are only able to access what their job needs, since Robert Taylor Jr. was a legal contractor, they shouldn’t have had admin access.*