

## Access controls worksheet

|  | Note(s)   | Issue(s)  | Recommendation(s)   |
|--|---|---|---|
| <b>Authorization<br/>/authentication</b> | The user account was the Legal/Admin account. The associated IP address also corresponds with the legal attorney, Robert Taylor Jr. The incident occurred 5 days ago at 8:29:57 AM. A computer with the host-name Up2-NoGud, was the device used in the incident. | The user had administrative access, which is a vulnerability. Legal advisors should not have admin privileges. In addition, their user account should not be active any longer. The end date for their employment was 12/27/2019. | <p>In order to prevent an incident such as this from happening in the future, periodical auditing is highly recommended. Out of the three approaches, the privilege audit would have been the most useful in this scenario. All three approaches are suggested. User accounts should also automatically expire after 30 days. Additionally, contractors such as this one should have very limited access to business resources. This helps prevent any unwanted access.</p> <p>Lastly, implementing file encryption, or an MFA system is highly recommended in order to enhance security posture.</p> |