onelogin

SOLUTION BRIEF

SOX Compliance Solution

www.onelogin.com | **twitter.com/onelogin**

OneLogin, Inc. | 150 Spear Street, Suite 1400, San Francisco, CA 94015

855.426.7227

OneLogin supports your Sarbanes Oxley compliance efforts by providing your IT system administrators the functionality needed to centrally manage some of the most deficiency prone IT control areas.

ACCESS MANAGEMENT

Granting and removing access to applications can be done either through the OneLogin portal, or if you set up directory integration, through your existing LDAP directory. By establishing or mapping your existing roles and groups to OneLogin, you can quickly grant, modify, or remove access based on role based privileges that are as granular as you want to make them. With real time LDAP to OneLogin updates, changes you make in your local directory system are immediately pushed to OneLogin, thus removing the need for you to have to update several access lists or having to wait for a batch program to start and complete in a timely and complete manner. E.g., all finance personnel get "Finance" role and two of them also get the "Equity Accountant" role so they can access the stock options application. If you disable the LDAP account for one of those two Equity Accountants, the update is made immediately in OneLogin, which secures the access to all the applications managed through the portal.

SEGREGATION OF DUTIES

Roles and groups in OneLogin also help you plan your segregation of duties strategy by allowing you to map out pre-defined access levels and document any authorized exceptions based on your own organizational structure and resource pool. E.g., one developer needs access to the ERP in production for troubleshooting on a case by case basis and the admins can quickly grant and remove the "Dev Troubleshooting" role accordingly, without the need of having to go into the ERP itself to grant him access. In addition, OneLogin creates a login audit trail to correlate the troubleshooting request to when the developer accessed the ERP.

AUTHENTICATION

Not all applications support the same, or robust enough, password requirements. This requires you to keep track of the various password requirements and in extreme cases, having to explain to your auditors how you compensate for weak password requirements. OneLogin allows you to centrally manage one or more password policies in addition to providing you with a multi-factor authentication (MFA) option. This allows you to create a more robust authentication scheme for remote users or for users of higher risk applications. E.g., you use a SaaS solution to securely store your draft SEC filings documentation and require the strong password requirements and MFA to access.

MONITORING

In addition to having preventive controls in place, detective controls provide you the ability to compensate for any exceptions in the performance of preventive controls. In addition, for higher risk applications, monitoring controls have become a de facto requirement. OneLogin provides you with various reports that can help you actively or periodically monitor what your users are doing in the OneLogin portal, and by extension the apps being managed by the same. E.g., your quarterly OneLogin roles report review helps you identify a user with access to an additional application that should have been removed the previous month. After updating their access, you review the logs to validate that they did not access the application during that time.

AUDIT EVIDENCE

Your auditors will request a lot of documentation, including several access control lists and evidence that access was granted appropriately for those in scope. Instead of chasing down several access lists or trying to evidence that the list of new users is complete and accurate, if you are using OneLogin as your central point of access management and authentication, you will greatly reduce the SOX audit level of effort and documentation needed. E.g., you provide auditors with a OneLogin portal log showing users added to it during the audit period for their access testing population and provide the list of active and disabled users from OneLogin for their testing evidence.

ABOUT THE AUTHOR

Alvaro Hoyos is the Director, Risk and Compliance for OneLogin, Inc. He has over 8 years of compliance experience working for PwC and Grant Thornton, two of the largest global public accounting firms. During that time he provided local and national leadership in the areas of SSAE 16, SOC 2, FedRAMP, FISMA, and SOX 404. He also has extensive experience working with Cloud Service Providers in the Bay Area and has been in the IT field for over 16 years.