January 24, 2019

SOC 2 Reports: Common Control Exceptions and How to Avoid Them

RISK ADVISORY/INTERNAL AUDIT, SOC
BY SCHNEIDER DOWNS PROFESSIONAL

In performing SOC 2 examinations, we often come across the same types of control exceptions. To assist organizations with avoiding these exceptions, we've compiled a list, in no particular order, of the most common ones we typically identify.

- **All employees did not complete security awareness training.** Service organizations typically utilize an online training platform that enables employees to complete security awareness training at their convenience. The training platform makes it easy to track those employees who have not completed the training and will send automated emails reminding them of their requirements.

- **The risk assessment is incomplete and did not include all relevant threat events.** Service organizations should follow NIST's guidance by referencing NIST SP800-30 rev1. Risk assessments need to list all relevant threat events, the likelihood of the threat event occurring, the impact to the organization if the threat event were to occur and the overall risk of the threat event. Organizations should create a template based on NIST's guidance and executive leadership needs to review results of the risk assessment, which should be updated annually.

- **Independent assessments of internal controls were not performed.** Service organizations should engage independent third parties to perform penetration tests, including web application penetration tests for any cloud-based products that are included in the scope of the SOC 2 report. In addition, service organizations need to run vulnerability scans on a quarterly basis to identify misconfigurations and missing patches.

- **Multifactor authentication is not used for remote access.** Service organizations should require employees to enter a second factor of authentication in addition to passwords when accessing the network remotely. Typical second factors of authentication are soft tokens, sent via SMS or mobile applications, or hardware tokens that must be plugged into employee's machine.

- **Super user access is not restricted to appropriate personnel.** Service organizations need to follow the "principle of least privilege" when determining which users require super user access to the network and critical applications. For those who do not require such access, specific roles should be created that limit access to only the functions necessary to perform one's job responsibilities.

- **Terminated user access was not removed in a timely manner.** Service organizations

should mandate that a notice of termination needs to be communicated to HR and IT prior to the departing employee's last day. Upon receiving such notice, IT should remove access immediately or set the employee's account to expire on his or her last day.

- **Developers have access to make changes to production systems.** Service organizations like software-as-a-service (SaaS) providers that develop custom cloud-based applications should restrict developers from having access to make changes to production code files. In the event that's not feasible, the service organization should implement a monitoring control, such as file integrity monitoring software that automatically alerts management when production code files are changed. If an unexpected change is detected, management can investigate to determine if the change was unauthorized or malicious.

For more information on SOC Reports and how Schneider Downs can help with meeting your customers' SOC reporting requirements, please contact our SOC experts.

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.