SCHNEIDER DOWNS
Big Thinking. Personal Focus.

OUR THOUGHTS ON

Third Party Risk Management Insights

The Top Ten Most Common SOC 2 Exceptions

What are some of the most common SOC 2 audit exceptions the our teams have encountered?

SOC 2 (Type 2) report exceptions are when a service organization fails to effectively operate its control as designed. From my experience, the top ten most common exceptions I have seen in the field are:

- Failure to remove/disable access to terminated user account(s) in a timely manner
- Failure to complete or retain evidence of policy (InfoSec, code of conduct, etc.) acknowledgment/sign off
- Failure of user(s) to complete security awareness training upon hire and/or annually thereafter
- Failure to retain evidence of or document a system change for approval or testing
- Failure to complete or retain evidence of annual performance review of employees with responsibilities related to security, availability, and confidentiality
- Failure to complete a background check for new hire user(s) in a timely manner
- Failure to perform an annual third party risk review of subservice organizations and/or third parties
- Failure to design action plans or remediate moderate/high-risk vulnerabilities identified in scans
- Failure to complete or retain evidence for regular password or key rotation
- Failure to deploy anti-virus software or endpoint management solution on all in-scope devices

Both our Third Party Risk Management and SOC practices see these exceptions most often when service organizations are going for their first SOC report, switching audit firms, or migrating to new systems/infrastructure.

Are these exceptions similar to your experiences, or are there others you are running into not on the list?

How Can Schneider Downs Help?

Schneider Downs is a registered assessment firm with the Shared Assessments Group, the clear leader in third-party risk management guidance. Our personnel are experienced in all facets of vendor risk management, and have the credentials necessary (CTPRP, CISA, CISSP, etc.) to achieve meaningful results to help your organization effectively achieve new vendor risk management heights.

For more information, please visit www.schneiderdowns.com/tprm or contact us at contactsd@schneiderdowns.com

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

Pittsburgh
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

Columbus
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

Washington, D.C.
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003