January 21, 2016

Standard SOC 2 Report Not Meeting Client Needs?

SOC

BY FRANK DEZORT

Upon distribution of your SOC 2 report, do you find that many clients are requesting additional subject matter related to your services or requesting that the standard report address criteria in addition to the applicable trust services criteria? Based upon the client inquiries, do you feel that your SOC 2 report is not sufficiently providing the scope of comfort and transparency that is most important to your clients?

Consider super-charging your standard SOC 2 report by enhancing the criteria into a SOC 2 +. The SOC 2 + reports provide the flexibility to report on subject matter in addition to management's description of a service organization's system or include regulatory requirements (or other control frameworks) in addition to the controls that are relevant to the trust services principles already included in the report. An example of additional subject matter would be reporting on historical availability data of computing resources at a service organization in addition to the controls relevant to the availability based on the trust services criteria for availability. Another example of additional subject matter would be reporting on customer service level compliance in addition to the controls relevant to the service-levels based upon the trust services criteria for security.

Examples of enhancing your SOC 2 for reporting on regulatory requirements would include reporting on privacy and/or security requirements under HIPAA (Health Insurance Portability and Accountability Act) in addition to reporting on controls at the service organization relevant to the privacy and/or security of the system based on the trust services criteria. The SOC 2 + provides the flexibility to evaluate and report on controls based upon criteria contained in frameworks such as ISO (International Standards Organization) 27001, NIST (National Institute of Standards and Technology) 800-53 or the HITRUST CSF (Health Information Trust Alliance Common Security Framework).

The SOC 2 + reports target a broader range of users who need to understand internal controls at a service organization that go beyond the criteria and controls contained in the Trust Services Principles relevant to security, availability, processing integrity, confidentiality and privacy. These reports are designed to address requests from service organizations based upon unique services or specific industry requirements.

If you are ready to super-charge your standard SOC 2 report, please contact a member of Schneider Downs team to determine an approach to increase the value and client comfort provided by your current report. Visit our SOC Reports services page to learn about the different types of SOC Reports, read case studies and FAQs.

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.

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.