March 18, 2019

Service Organization Control Report

SOC
BY TIMOTHY WOLFGANG

The SOC reporting process can start with an organization's desire to communicate to customers and potential customers that the organization's internal control processes are being implemented effectively. Or it can be prompted when an organization's customers start to request to review the organization's SOC report.

Organizations are responsible for defining the scope of a SOC report engagement.

If a SOC report's scope is too narrow, then it might not be useful to the intended users of the report, since key information is omitted. If a report's scope is too broad, organizational resources and time could be wasted implementing unnecessary control processes.

We recognize that SOC reports are a significant investment and recommend the following five guideline questions be considered when defining the scope of your SOC report.

1.) What are the core services your organization provides?

Is your company completing processes that are relevant to a customer's internal control over financial reporting, such as processing payroll or taxes?If so, a SOC 1 report should be considered.

If your company is providing services to other organizations, and those services are not significant to internal control over financial reporting, such as IT infrastructure hosting or support, data processing or network security, then a SOC 2 report should be considered.

2.) What are the key service commitments your organization makes with customers?

Contractual agreements between your organization and customers are a good starting point for answering this question.For a SOC 1 examination, identify the classes of transactions processed or functions performed for clients.The internal controls that your company maintains over these processes and functions will be relevant to report users and should be included in the report.

For a SOC 2 examination, identify the commitments or service level agreements your organization has made.All SOC 2 reports will include the Security (Common Criteria) category, but the inclusion of one or more additional categories (Availability, Confidentiality, Privacy, Processing Integrity) should be considered for inclusion based on these commitments.For example, if your organization has specified a system uptime metric, then the Availability category should be considered for inclusion in the report.

3.) What systems are used to deliver your organization's services?

In a SOC 2 examination, a system is defined as: the infrastructure, software, procedures and data that are designed, implemented and operated by people to achieve one or more of the organization's business objectives. This SOC 2 definition can also be applied to SOC 1 report systems.Answer the following questions to assist with identifying in-scope systems:

- What software or applications are used to perform our services?
- What infrastructure supports the software? This includes servers, firewalls, and monitoring systems. Where is the infrastructure hosted?
- What types of data are used by the system? What are the sources and outputs?
- What automated or manual procedures are completed to provide our organization's services?
- Who is carrying out the procedures noted above and who is responsible for maintaining the software/infrastructure?

4.) What third parties does your organization utilize to deliver its services?

Any third parties used to deliver your organization's services should be presented in in your organization's report. To guide an organization's determination regarding which third parties to present in a SOC report, Schneider Down's SOC specialists have published full articles on how to define Vendors or Subservice Organizations and on the Inclusive and Carve-Out Methods .

5.) Does your organization need to comply with regulatory requirements?

If your organization is subject to regulatory oversight, then controls around your organization's compliance should be considered for inclusion in the SOC report. Regulatory topics can be included as individual controls, and the control can be phrased such as: "HIPAA compliance audits are conducted on an annual basis." Or the regulatory topic can be addressed by incorporating an additional reporting framework such as the HITRUST CSF or ISO-27001 using the SOC 2 Plus reporting format.

Service Auditors can help to clarify the scope for your SOC Report.

The factors discussed above provide a base for defining SOC report scope. While an organization's management is ultimately responsible for defining scope, service auditors can provide clarification as needed for management.

For example, we are often asked to help determine whether a third party is a vendor or subservice organization or if the timeframe for completing a report is appropriate. If you have questions about scoping your SOC report, we welcome the opportunity to discuss it with you. Ask your Schneider Downs representative or our **SOC Report practice professionals.**

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.