Which SOC Report is Right for You?

As we move away from the era of the SAS 70 and even the term SSAE 16, organizations are asking themselves which report they should be obtaining from their service providers. The basic intentions of the reports are as follows:

SOC 1 – Related to Internal Control over Financial Reporting
SOC 2 – Related to testing over the Trust Services Principles of Security, Availability, Processing Integrity, Confidentiality and Privacy
SOC 3 - A simplified report on the same principles in a SOC 2 and available for public use. We will not cover the SOC 3 report in detail here, as the majority of questions we receive relate to SOC 1 and SOC 2 reports.

One of the first questions to ask when deciding on a report is – Who is the intended user?

SOC 1 – Intended for the auditor or internal auditor of a user organization
SOC 2 – Intended for security, compliance and operations departments at user organizations

An example of a situation requiring a SOC 1 would be ABC Inc., a publicly traded company who outsources its payroll processing to a vendor. ABC's financial auditor and internal audit department will need to obtain a SOC 1 Type 2 report in order to gain comfort over the controls at the payroll processing vendor in terms of internal control over financial reporting. In this case, both management (typically through their internal audit department) and external auditors are the intended users of the report for their purposes and goals. They need comfort over internal control over financial reporting to properly support their related certifications and opinions.

An example of a situation involving a SOC 2 would be BCD Bank who outsources its data center function to an external data center company. The security, compliance, operations and other functions at BCD Bank would want to gain comfort over one or all of the five trust principles of Security, Availability, Processing Integrity, Confidentiality and Privacy at the data center provider depending on the scope of services provided. A report focused on internal control over financial reporting may touch on those principles, but would not provide the comfort in those areas that a SOC 2 report does. The SOC 2 shows whether the controls at the service organization address the Trust

Services Principles. It will evidence if the service organization's controls operating as committed or agreed.

A question that often follows these descriptions is – Are there companies that should issue both a SOC 1 and SOC 2? More and more the answer is becoming yes. In our second example of BCD Bank, let's add that BCD is a publicly traded entity or one that has a strong need related to internal control over financial reporting. BCD's financial auditors and internal auditors would want to see a SOC 1 report related to the data center in addition to the other department's needs for the detail and rigor of the SOC 2 surrounding the Trust Services Principles. With that fact pattern, both a SOC 1 and SOC 2 apply.

Another consideration is whether to obtain a Type 1 or Type 2 SOC report. A Type 1 report is centered on the description of a service organization's system and the design of the service organization's controls. The reports are issued as of a specific date. A Type 2 report encompasses the same information as a Type 1 report adding an opinion on the operating effectiveness of the controls at the service organization. Type 2 reports are issued over a specific time period, usually from six to twelve months. A Type 2 report includes detailed descriptions of the service auditor's tests of controls and results of those tests, noting whether testing passed or exceptions were noted. A Type 1 report can provide great detail into a service organization's purpose and controls. When more rigor and due diligence is needed, a Type 2 tests those controls to assess their operating effectiveness.

In this entry we have provided some high-level facts in regards to a detailed and complicated process. If you have any further questions regarding the reports or would like to hear more about The Mako Group's process for performing SOC engagements, please reach out. We are here to be your trusted advisor and partner.

For parties reviewing these reports, please review our related Mako Bytes entry titled "How to Properly Review a SOC Report".

Shane M. O'Donnell, CISA, CPA, MSA
Chief Audit Executive
March, 2014