AT Section 101 – SOC 2 Reports

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

ABOUT SOC 2 REPORTS

In the past, SAS 70 reports encompassed financial reporting controls, operational controls, and compliance controls. SSAE 16 SOC 1 Reports, which have effectively replaced SAS 70 reports, will be prepared in accordance with *Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization*. SSAE 16 SOC 1 reports can no longer be used for any other purpose except for reporting on the system of internal control for purposes of complying with internal control over financial reporting. For reports that are not specifically focused on internal controls over financial reporting, the AICPA has issued an Interpretation under AT Section 101 permitting service auditors to issue reports. These reports will now be considered SOC 2 or SOC 3 reports and focus on controls at a service organization relevant to the following principles:

- ***Security:*** *The system is protected against unauthorized access (both physical and logical).*
- ***Availability:*** *The system is available for operation and use as committed or agreed.*
- ***Processing Integrity:*** *System processing is complete, accurate, timely, and authorized.*
- ***Confidentiality*****:** *Information designated as confidential is protected as committed or agreed.*
- ***Privacy:*** *Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CICA.*

This means, many companies which have used SAS 70's in the past, will now need a SOC 2 report (e.g. managed service providers, Software as a Service (SaaS), cloud computing, etc.). SOC 2 reports are restricted use reports, which means the use of the reports are restricted to:

- Management of the service organization (the company who has the SOC 1 performed),
- User entities of the service organization (customers, regulators, business partners, suppliers, etc.)

As with SSAE 16 reports, both SOC 2 Type I and SOC 2 Type II reports can be issued:

- Type I – a Type I is a report on policies and procedures placed in operation as of a specified point in time. SOC 2 Type I Reports evaluate the design effectiveness of a service provider's controls and then confirms that these controls have been placed in operation as of a specific date.

- Type II – a Type II is a report on policies and procedures placed in operation and tests of operating effectiveness for a period of time. SOC 2 Type II Reports include the examination and confirmation steps involved in a Type I examination plus include an evaluation of the operating effectiveness of the controls for a period of at least six calendar months. Most user organizations require their service provider to undergo the Type II level examination for the greater level of assurance it provides.

The AICPA has outlined the following essential elements that must be incorporated in the SOC 2 report:

- Service auditor's opinion
- Management's assertion letter
- Management's description of the service organization's system
- Service auditor's tests of controls and results of tests (Type II report only)
- Other supplemental information not covered in other sections

ABOUT US

SSAE 16 Professionals, LLP is one of the nation's leading firms focusing solely on SSAE 16 reports, SOC 2 reports, SOC 3 reports, and SSAE 16 Readiness Assessments. Each of our professionals has over 10 years of relevant experience at "Big 4" and other large international or regional accounting firms. Unlike many larger audit firms, with SSAE 16 Professionals, you are guaranteed to receive one-on-one attention from one of our partners. Each professional is certified as a CPA (Certified Public Accountant), CISA (Certified Information Systems Auditor), CIA (Certified Internal Auditor), CISSP (Certified Information Systems Security Professional), CRISC (Certified in Risk and Information Systems Control), and/or MBA (Master of Business Administration).

For additional information regarding AT 101 SOC 2 reports, please contact:

Tim Roncevich, CISA | SSAE 16 Professionals, LLP
Practice Leader - SSAE 16
T/ 866.480.9485 Ext. 215 | **D**/ 714.318.2458
E/ Tim.Roncevich@ssae16professionals.com
W/ www.ssae16professionals.com