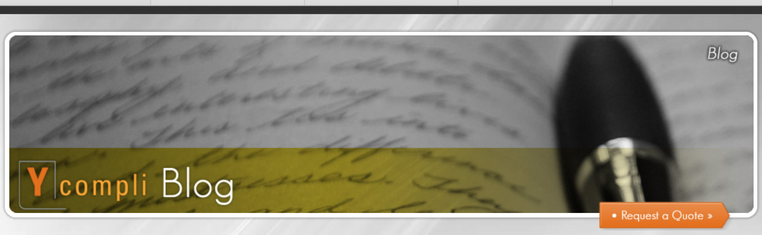

SOC Report Type 1 vs. Type 2 | SOC 1, 2, 3 Reporting Definitions

Posted by Ycompli Enthusiast on July 9, 2012

Organizations are confusing a TYPE 1 vs TYPE 2 report with the SOC 1 vs SOC 2 standards.

A SOC 1 report is for service organizations that impact or may impact their clients financial reporting.

A SOC 2 report is for service organizations that hold, store or process inforamtion of their clients, not financial reporting significant (e.g. would not affect their income statement or balance sheet)

Below explains more information on the TYPE 1 vs. Type 2 and provides some background on the different SOC reports. Contact us if you would like additional information.

There are a number of inquiries regarding the difference of a SOC Type 1 vs. Type 2 report. We wanted to take the time to explain the difference between the different types of reports and the difference SOC reporting versions. The short answer is that a Type 1 report just provides a report of procedures / controls an organization has put in place as of a point in time and a Type 2 report has an audit period and provides evidence of how an organization operated their controls over a period of time. It is important to understand there are not more stringent control requirements in a Type 2 SOC Report, but just describes how a company's control environment operated over their audit period (typically not less than 6 months). You can have the same controls in a Type 1 report as the Type 2, the only difference is that they are audited or examined over a period of time and testing results reported in a SOC 1 and SOC 2 report.

On June 15, 2011, the SAS 70 standard was effectively replaced by SSAE 16 (SOC 1). During this transition period, the AICPA decided to create a new brand for service organization control reports and they published the SOC reporting standards with 3 different SOC reports. It is important to understand that a SOC 1, SOC 2, SOC 3 are not the same reports with different levels. It is common for organizations to think that a SOC 3 report is a higher level for SOC 1, however that is just not the case.

Below is an explanation of the 3 different SOC reporting options. Hopefully you will find this explanation useful.

Organizations that were previously required to obtain a SAS 70 can undergo a SOC 1 audit to meet their client's requirements. SOC 1 is an engagement performed under SSAE 16 in which a service auditor reports on controls at a service organization that may be relevant to user entities' internal control over financial reporting. The scope of a SOC 1 report should cover the information systems that are utilized to deliver the services under review. There are two types of SOC 1 reporting options:

• SOC 1 Type 1: A design of controls report. This option evaluates and reports on the design of controls put into operation as of a point in time.
• SOC 1 Type 2: Includes the design and testing of controls to report on the operational effectiveness of controls over a period of time (typically six months).

A SOC 2 report is an engagement performed under the AT section 101 and is based on the existing SysTrust and WebTrust principles. This report will have the same options as the SSAE 16 report where a service organization can decide to go under a Type 1 or Type 2 audit. However, unlike the SSAE 16 audit that is based on internal controls over financial reporting the purpose of a SOC 2 report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality or privacy. The criteria for these engagements are contained in the Trust Services Principles Criteria and Illustrations. Organizations asked to provide an SSAE 16, but do not have an impact on their client's financial reporting should select this reporting option.

A SOC 3 report is an engagement performed under AT section 101 and is also based on the criteria contained in the Trust Services Principles Criteria and Illustrations. However, unlike the SOC 1 and 2 options, the SOC 3 report does not contain a description of the service auditor's test work and results. SOC 3 reports are general use reports and fall under the SysTrust and WebTrust seal programs. Clients that select a SOC 3 report can obtain a SysTrust or WebTrust seal to place on their website and marketing material as long as they maintain compliance (successfully complete a SOC 3 report every 12 months). Organizations whose primary goal is the marketing of their system/product against an industry approved standard should select this reporting option.

Assurance Concepts is a CPA firm that specializes in providing regulatory compliance and risk advisory services. Our expertise includes SSAE 16 (SAS 70) audits, SOX 404 compliance,SysTrust, WebTrust, HIPAA, ISO 27001 / 27002 and PCI DSS QSA services. Our service delivery model is designed to provide unparalleled client service to each one of our clients and help maximize the long-term value of their audit activities.

For more information contact:
Ben Osbrach
866.669.6561 Ext. 702
osbrach@assuranceconcepts.com

Post new comment

Subject:

Comment: *

CAPTCHA
This question is for testing whether you are a human visitor and to prevent automated spam submissions.

Math question: *
1 + 0 =

Solve this simple math problem and enter the result. E.g. for 1+3, enter 4.

Preview

Labels

blog
SAS 70 Audit
SSAE 16

More Information

Name

Company

Phone Number

Email Address

Request Information »

CAPTCHA
This question is for testing whether you are a human visitor and to prevent automated spam submissions.

1 + 15 =

Solve this simple math problem and enter the result. E.g. for 1+3, enter 4.