KirkpatrickPrice
Innovation. Integrity. Delivered.

Frequently Asked Questions (FAQ's) about SOC Audits

What is a SOC report?

Developed for third-party service providers, SOC reports are issued by Certified Public Accountants (CPAs) and report on a service organization's internal controls, meaning policies and procedures, which impact their client's sensitive data. SOC reports meet the needs of a Service Organization's clients (called user entities) who need to comply with regulatory and/or contractual requirements. These reports allow user entities to obtain an objective evaluation of the effectiveness of controls that address the compliance, operations, and financial reporting of a service organization. The AICPA has developed three Service Organization Control (SOC) reporting options (SOC 1, SOC 2, SOC 3).

What is an SSAE 16 (SOC 1) audit report?

SOC 1 engagements, also known as SSAE 16 engagements, are performed in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16), which was formerly known as SAS 70. SOC 1 reports are designed to report on the controls of a Service Organization that could ultimately impact their client's financial statements. An SSAE 16 engagement is not a review of the service organization's financial statements.

What is the difference between SSAE 16 and SAS 70?

The SSAE 16 uses much of the same groundwork as the SAS 70, however, broadening the use of the Service Auditor's Report. The main differences between the two are the extent of information you will now be required to provide. Management at the Service Organization must now provide a formal attestation of controls as well as evidence of a risk assessment methodology employed in selecting the control objectives. Finally, controls related to disaster recovery and business continuity are now available for review under SSAE 16, which were previously out of scope under SAS 70.

Do I need an SSAE 16?

Many organizations are legally required to verify the adequacy of internal controls at a service provider prior to providing access to certain data. Generally speaking, publically traded companies looking to comply with Sarbanes Oxley (SOX), financial institutions looking to comply with the Gramm–Leach–Bliley Act (GLBA), as well as state and local government, have all standardized on SOC reports to meet these requirements. If your clients outsource any aspect of their information system to your organization, then their auditors may request from you an SSAE 16 report to gain a better understanding of the controls at your organization and how they meet the requirements.

What are the benefits of undergoing an SSAE 16 audit?

SOX and GLBA legislation, among others, require a user entities' service provider to have adequate internal controls. By being able to produce an SSAE 16 report to your clients, you gain a competitive advantage and client trust by demonstrating that you have the proper controls in place that have been verified by a valid third party.

16057 W. Tampa Palms Blvd. | #134 | Tampa, FL 33647 | kirkpatrickprice.com | 800.770.2701

Who can perform a SOC audit?

A SOC audit can only be performed by an independent Certified Public Accountant (CPA). CPAs must adhere to the specific standards that have been established by the American Institute of Certified Public Accountants (AICPA) and have the technical expertise to perform such engagements.

How are SOC reports used?

Generally speaking, your SOC report will be requested and read by your client's auditor. SOC Reports are considered an "auditor to auditor report" allowing the auditor to avoid having to audit the service provider directly. SOC reports will be used by the Service Organization with current and potential clients and their independent auditors. While the existence of a SOC report is generally marketed, the SOC reports themselves are restricted from being used for general marketing purposes.

What are the contents of a SOC report?

Depending on the needs of the service organization, a CPA can issue either a Type I or a Type II report. Each type of report is described in the following:

Contents	Type I	Type II
Independent Service Auditor's Report	•	•
Service Organization's description of controls	•	•
Offers opinion on management's presentation of the Service Organization's current controls	•	•
Evaluates the suitability of design of managements description of the Service Organization's system	•	•
Evaluates the Service Organization's control systems		•
Offers a description of the Service Auditor's tests of the operating effectiveness of controls and the results of each test	•	•

How does the audit process work?

We utilize our Online Audit Manager tool to ask a series of custom questions regarding your current controls to prepare you for your specific requirements. Our process will efficiently document where you are today, provide specific guidance on identified areas of weakness, and allow you to work through as much of the audit process as possible prior to conducting the onsite portion of the audit. Our approach minimizes the cost and disruption associated with extended onsite visits. Our senior level auditors will assess, guide, monitor, test, and help mature your organization's information security program and internal controls.

16057 W. Tampa Palms Blvd. | #134 | Tampa, FL 33647 | kirkpatrickprice.com | 800.770.2701