Grant Thornton

An instinct for growth™

As easy as SOC 1, 2, 3

Up until June 2011, the Statement on Auditing Standards No. 70 (SAS 70) was used by service auditors to report on service organisations' involvement with the financial reporting controls of their clients. While the SAS 70 report was always intended to be an auditor to auditor communication, over time service organisations realised that SAS 70 reports were also useful to user organisation management, stakeholders, regulators and non-user entities.

With the release of the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) in 2010 the American Institute of Certified Public Accountants (AICPA) replaced SAS 70. SSAE 16 provided the AICPA with the opportunity to create new terminology, clarify the various System and Organisation Controls (SOC) engagements and their applicable standards. The AICPA applied the SOC 1℠ name to what had previously been referred to as SAS 70. Furthermore by introducing SOC 2℠ and SOC 3℠ reports, the AICPA offered guidance on the standards that should be used for reports covering operational and technological business risks exclusive of any financial reporting risks.

SOC types

Up to 1 May 2017 SSAE 16 provided a framework for the three categories of SOC reports. This framework has now been revised by SSAE18 (the update to SSAE16) and carries with it an **effective date of 1 May 2017**.

SOC1

SOC 1 reports retain the original purpose of SAS 70 reports, in that, they provide a vehicle for reporting on a service organisation's systems of internal controls that are relevant to a user organisation's internal controls over financial reporting. SOC 1 reports are intended to be auditor to auditor communications, just as the SAS 70 reports had been.

SOC 1 reports have nearly all of the same elements as SAS 70 reports, but specific content will depend on the service auditor and the service organisation's system. The following are the basic elements outlined in a SOC 1:

- an independent service auditor's report;
- management's assertion letter;
- a description of the system; and
- a section containing the service auditor's tests of the operating effectiveness of controls and the related test results (Type II report only).

Additional information provided by the service organisation but not covered by the service auditor's opinion may also be included within a SOC 1 report.

SOC 2

SOC 2 reports offer service auditors and organisations a reporting option they can use when the subject matter is not relevant to controls over financial reporting. The SOC 2 report addresses controls at a service organisation that are pertinent to the joint AICPA and Canadian Institute of Chartered Accountants (CICA) Trust Services Principles and Criteria. These Trust Services Principles include security, availability, processing integrity, confidentiality and privacy. In a SOC 2 report, as with a SOC 1 report, management identifies one or more Trust Services Principles that it believes it has achieved and the criteria upon which it will base its assertion of achievement. While SOC 2 reports are intended for user organisation management and other stakeholders (eg business partners and customers) along with regulators, may also benefit from the information contained within a SOC 2 report. The structure of the report includes many of the same elements as a SOC 1 report.

SOC 3

In the past, the AICPA has used the terms SysTrust® or WebTrust® to denote a service organisation control report that was focused on the Trust Services Principles and Criteria and was made available to a reader through a link on a service organisation's website. These reports are now more commonly known as SOC 3 reports. Like SOC 2 reports, SOC 3 reports allow service organisations to provide user organisations and other stakeholders with a report on controls that are relevant to security, availability, processing integrity, confidentiality and privacy. Unlike SOC 1 and SOC 2 reports, SOC 3 reports do not include a description of the system or

the detailed description of the tests of controls and related test results. Moreover, unlike the other two types, SOC 3 reports are short-form, publicly available documents that state whether the service organisation's system for providing its services to user entities is suitable to meet the applicable criteria outlined in Trust Services Principles, Criteria and Illustrations. SOC 3 reports can be freely distributed or posted on service organisations' websites with a seal.

What SOC report?

Deciding how the three types of SOC reports will best meet the varying needs of different audiences and cover different subject matter can be challenging. As your service auditor, Grant Thornton, can assist you with all your SOC requirements. For instance determining which SOC report or reports are appropriate may mean for some organisations that the answer is contrary to the type of report the organisation obtained in the past.

Additionally, in instances where obtaining multiple reports might satisfy the organisation's various needs, the level of effort needed to obtain more than one report will vary based on the specific scope and coverage of the report. If controls overlap, we can leverage the work from one audit for another and the necessary work will only be incremental.

Not covered by SOC?

If your organisation needs to address subject matter that does not appear to be satisfied by the description of SOC reports, a customised attestation report using another AICPA attestation standard may be the answer. Our dedicated team can discuss with you the alternative standards to find the one that will best address your unique needs.

The SOC decision

The marketplace is still getting to grips with SOC reporting choices and we hope that businesses will continue to embrace the diversity of options presented by the AICPA. We would recommend that service organisations should have open discussions with their user organisations in order to understand exactly why a certain SOC report is being requested. This information will inform the question as to which SOC report or reports are appropriate to the needs of user organisations and others.

As a service organisation, you may be trying to navigate your third party reporting needs. Grant Thornton will be happy to clarify these options for you. This will ensure that you have a full appreciation for the subject matter and in turn you have chosen the best fit report for your specific needs. Understanding your SSAE 18 reporting options will go a long way toward providing your clients and their auditors with the information they require, instilling confidence in the services that you provide and delivering brand enhancing and commercial rewards for your business.

Contact

Please contact a member of our team below for further information and discussion.

Sara McAllister
Director, Business Risk Services
T +353 (0)1 680 5716
E sara.mcallister@ie.gt.com

Paul Carroll
Associate Director, Business Risk Services
T +353 (0)1 433 2563
E paul.carroll@ie.gt.com

Kai Song
Assistant Manager, Business Risk Services
T +353 (0)1 436 6546
E kai.song@ie.gt.com

Usha Selvaraju
Assistant Manager, Business Risk Services
T +353 (0)1 500 8105
E usha.selvaraju@ie.gt.com

Offices in Dublin, Belfast, Cork, Galway, Kildare, Limerick and Longford.

www.grantthornton.ie

#GTgrowth

Grant Thornton Ireland

Grant Thornton

An instinct for growth™

grantthornton.ie