As easy as SOC 1, 2, 3

As a service organisation there are many ways to provide assurance to your customers and in turn other stakeholders over your control environment. One of the most effective and cost efficient ways is to issue a Service Organisation Control (SOC) Report.

Today, outsourcing has become the norm in many industries. Outsourced service providers play a vital role in contributing to an organisation's efficiency and profitability. Business processes are becoming more complex and organisation's are focusing on dynamic service delivery models as a way of managing increased technical complexity, scarcity of expertise and competitive pressures.

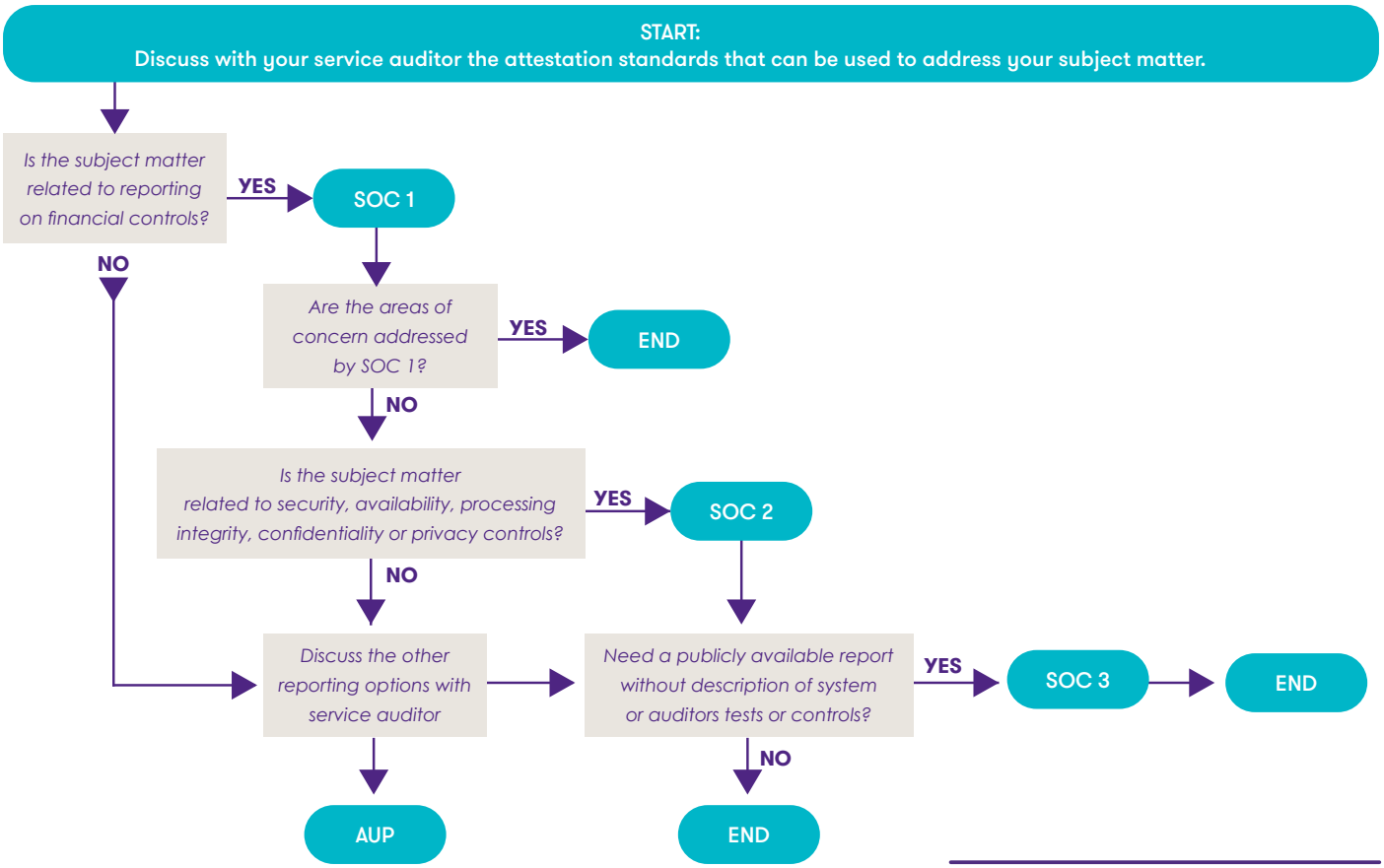
Cloud computing, IT managed services and data centre hosting are in many cases default business solutions for most sectors, most especially financial services, property management, technology and healthcare.

Instilling confidence in outsourced business models equates to a need to assure oversight of outsourced services. By choosing the SOC route as your optimum assurance mechanism, it undoubtedly delivers a number of benefits most notably:

- time and cost savings in having a single solution to address multiple assurance requests;
- enhanced credibility in having a best practice assurance solution in place to retain and attract business; and
- evidenced oversight of your outsourced providers to appease regulators and other stakeholders.

Deciding on the configuration of your SOC reporting solution starts with deciding which SOC report or collection of SOC reports you require to meet your broad stakeholder needs.

We outline below a simple decision making diagram that can be used to determine your SOC 1, SOC 2 and SOC 3 reporting requirements. If none of the aforementioned options suit your needs, an 'Agreed Upon Procedures' (AUP) engagement may be the best assurance solution.



SOC types

SOC reports report under two primary best practice standards; SSAE 18, ISAE 3000 and ISAE3402.

SOC 1

SOC 1 reports 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 and are intended to be auditor to auditor communications.

At a high level the following are the basic elements of a SOC 1 report:

- 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 service 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 American Institute of Certified Public Accountants (AICPA) – Canadian Institute of Chartered Accountants (CICA) Trust Services Criteria (TSC). These TSC cover five categories - security, availability, processing integrity, confidentiality and privacy.

In a SOC 2 report, management identifies the mandatory common criteria (Security) and potentially other TSC criteria that it believes it has achieved and requires assurance on. While SOC 2 reports are intended for user organisation management, other stakeholders (eg, business partners, 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 but is more prescriptive than a SOC 1 when it comes to control scoping under the TSC regime.

SOC2+

SOC2+ reports are a great tool to incorporate various industry standards into a SOC2 report by combining the relevant standard with the mandatory common criteria (Security) and potentially other TSC's as set out by AICPA.

SOC2+ reports can be flexed to incorporate multiple frameworks such as ISO27001, NIST, GDPR etc. and can offer service organisations the opportunity to gain efficiencies.

SOC 3

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.

Unlike the other two types, SOC 3 reports are short-form, publicly available documents and tend to be aimed at the un-informed user. 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 market place has become much more informed in recent years when it comes to SOC reporting and the tangible benefits of such. It is seen as best practice to provide/obtain a SOC report as part of a risk management and oversight regime and in many cases is now a pre-requisite in securing and deploying client solutions.

SOC reports in effect provide a transparent and cost effective means for assuring internal control accountability and for addressing multiple stakeholder assurance demands.

We would recommend that service organisation's have an 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 organisation's and others.

Grant Thornton are happy to clarify these options for you. This will ensure that you have a full appreciation for the subject matter and in turn that you have chosen the best fit report/reports for your specific needs.

Understanding your third party 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

Contact us

If you would like to learn more about SOC compliance, please contact a member of our dedicated Risk Services team.

Sara McAllister
Partner
T +353 (0)1 680 5716
E sara.mcallister@ie.gt.com

Frankie Cronin
Partner
T +353 (0)1 646 9044
E frankie.cronin@ie.gt.com

Victoria Armitage
Director
T +353 (0)1 433 2525
E victoria.armitage@ie.gt.com

Onatkut Varis
Associate Director
T +353 (0)1 680 5905
E onatkut.varis@ie.gt.com

Richard Elwood
Manager
T +353 (0)1 500 8053
E richard.elwood@ie.gt.com

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

grantthornton.ie @GrantThorntonIE Grant Thornton Ireland

Grant Thornton