Grant Thornton

Information Technology

Managing risk with Service Organisation Control

Grant Thornton | Malta

Contents

Managing risk with SOC

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 organisations 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, especially financial services, property management, technology, and healthcare.

One can outsource the process but cannot outsource the risk, therefore it is important for companies to be aware of all the risks that me be typically associated with outsourcing, including but not limited to reputational, control, compliance, privacy, and operational risks. Outsourcing any function, instilling confidence in outsourced business models equates to a need to assure oversight of outsourced services.

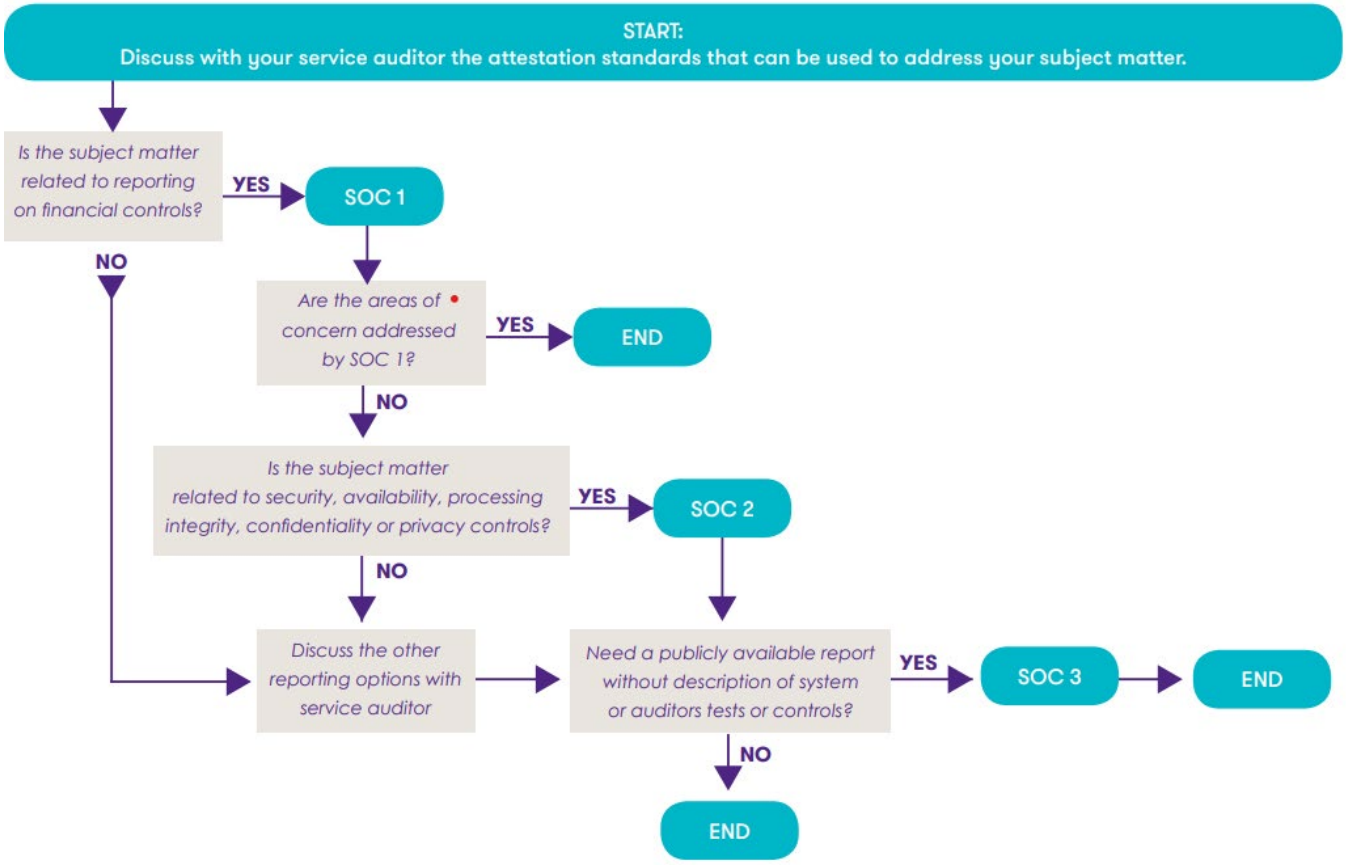
One of the most effective ways a service organisation can communicate information about its risk management and controls is through a service auditor report. By choosing the SOC route as your optimum assurance mechanism, it undoubtedly delivers several benefits, most notably:

- 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.

SOC types



SOC reports report under two primary best practice standards; ISAE3402, (SOC1) and ISAE 3000 (SOC2 and SOC3).

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 one or more TSC categories 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, other stakeholders (e.g., 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

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.

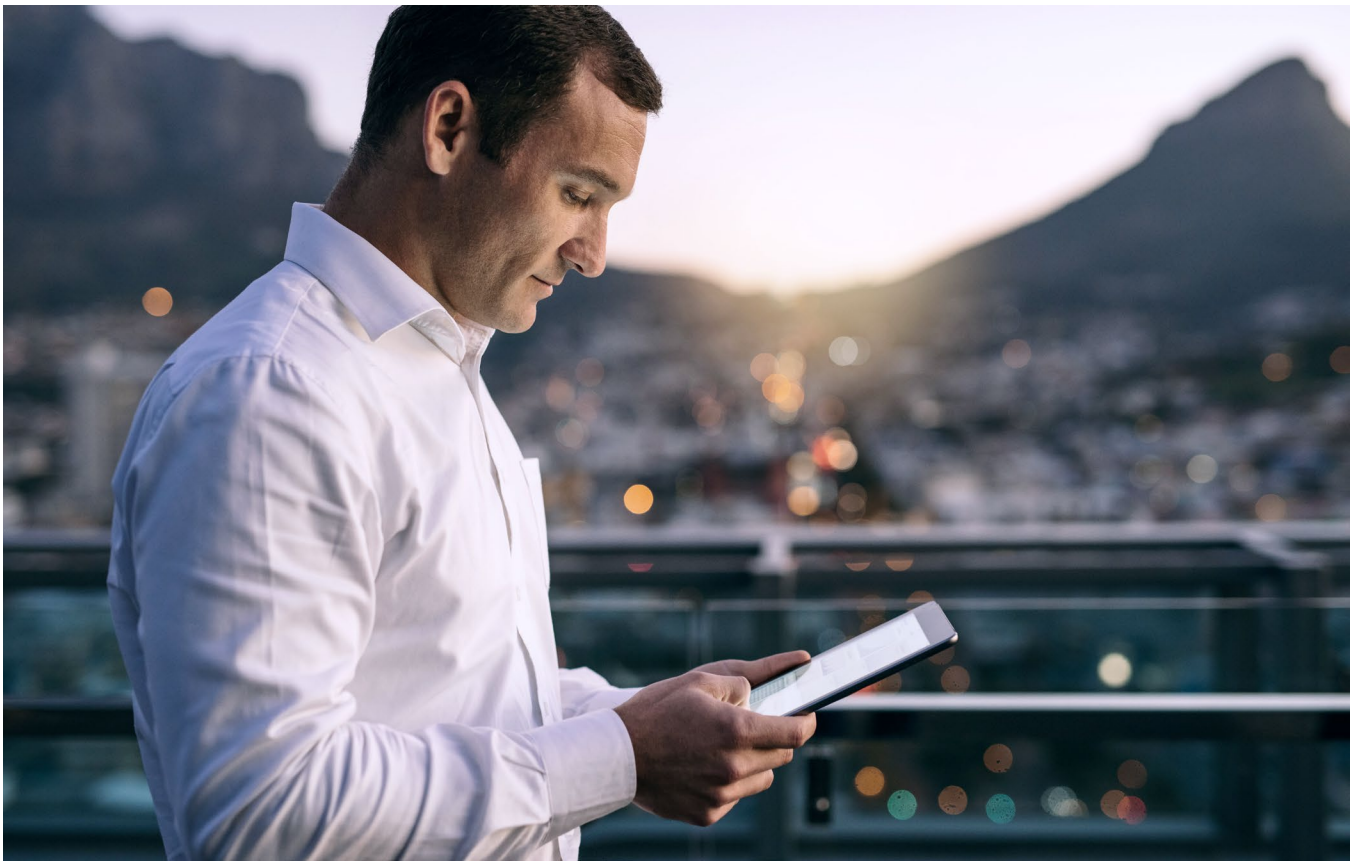
Which SOC report?

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 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 organisations 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 and commercial reward for your business

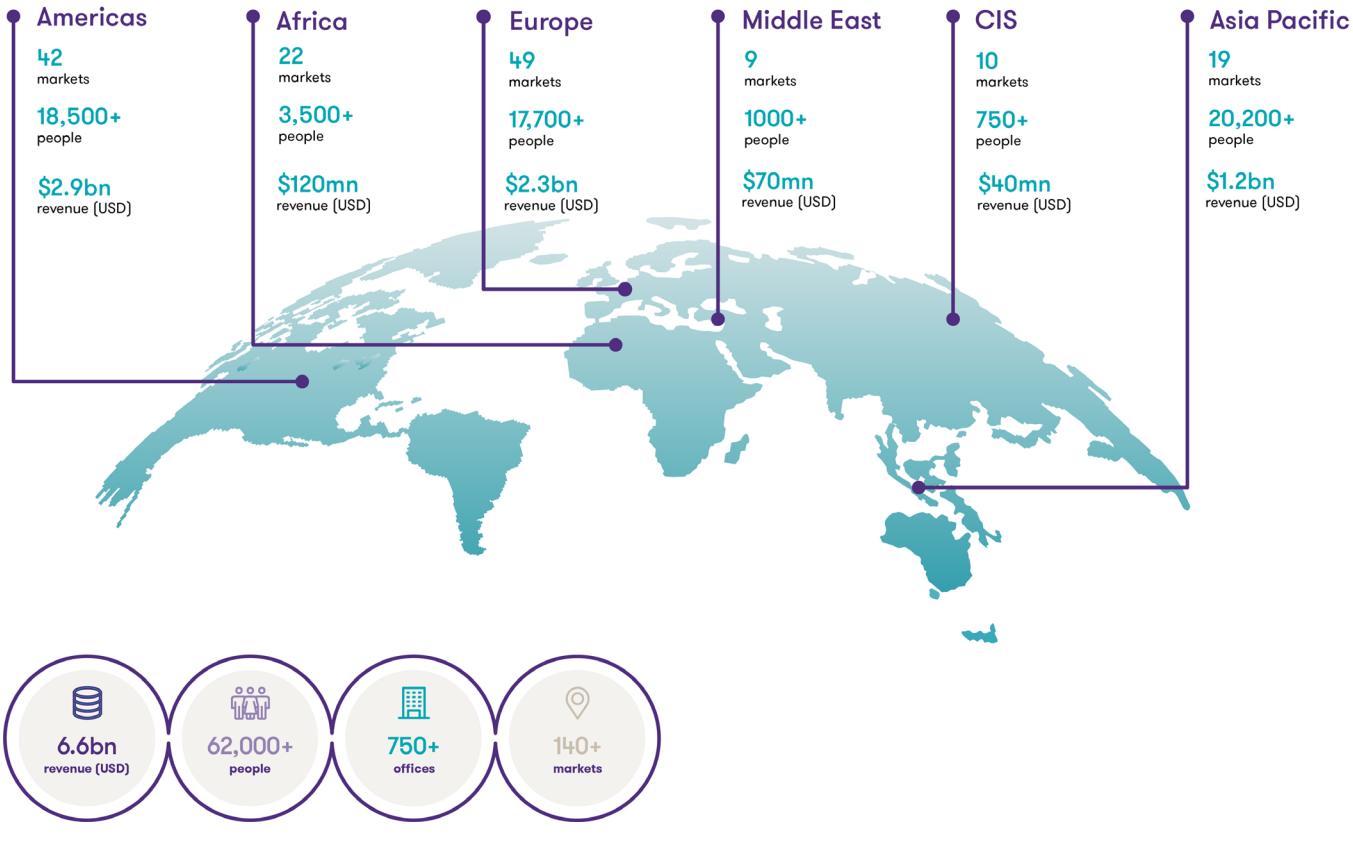
Grant Thornton International

Grant Thornton Malta is a member firm of Grant Thornton International

Grant Thornton International Ltd is a not-for-profit, non-practicing, international umbrella membership entity. It is organised as a private company limited by guarantee, not having a share capital, incorporated in England and Wales and does not provide services to clients. Services are delivered independently by the Grant Thornton firms.

Grant Thornton International is an organisation of independently owned and managed accounting and consulting firms. Each member firm within Grant Thornton International is a separate national firm. These firms are not members of one international partnership or otherwise legal partners with each other, nor does membership within Grant Thornton International thereby make any firm responsible for the services or activities of any other. Each firm governs itself and handles its administrative matters on a local basis. Most of the member firms carry the Grant Thornton name, either exclusively or in their national practice names, facilitated by a name use agreement.

At 31 December 2021 Grant Thornton had more than 62,000 people in its member firms represented in over 140 countries. Global revenues amounted to US$ 6.6 billion.



Grant Thornton Malta

Global team, local feel

Founded in 1975, the Malta firm became a Grant Thornton member in 1991. We truly believe that the service we offer is personal and of top quality, one that will make a significant contribution to your business. We have an instinct to help people achieve their ambitions.

From new start-ups or small businesses to large enterprises and public institutions, our clients look to us for objective and impartial support on how their business is performing and how they can achieve their business goals.

When you choose Grant Thornton as your partner and service provider, you will discover what so many companies and organisations have already discovered - the power of enthusiasm and certainty.

We are successful because of our people and because we bring to bear for our clients all that our global firm has to offer. We are a leader in the global marketplace and among the top audit and advisory firms in Malta. Our continued rapid growth is a testament to the assurance our clients experience every day.

Building on more than 40 years of experience, Grant Thornton combines the international reach, depth and expertise of the global brand with the personal attention, value for money, focus and relationship approach of the local team. It is how we keep you moving forward. Initiative you can rely on and knowledge you can trust.

We know that by applying our professional, yet personal business philosophy we will retain the trust and loyalty of our clients, our staff and the wider community. In an increasingly complex and rapidly changing world, it's time to take the lead with Grant Thornton and unleash your potential for growth.

Related Experts

Joseph Pullicino
Partner | Head of Information Technology
T +356 9949 9660
E joe.pullicino@mt.gt.com

Joseph (Joe) joined the firm in 1988, after many years at the Central Bank of Malta where he gained extensive experience in banking, foreign exchange and information technology, and was admitted partner at Grant Thornton in 1993.

Joseph's expertise centres around computer security and audit procedures. As partner responsible for the Business Risk and Outsourcing Services Division of Grant Thornton, Joseph is heavily involved in computer systems consultancy for Government and other major clients of the firm and also internal and online-gaming audits.

He has accumulated extensive experience in the analysis, design and implementation of integrated accounting systems for corporate customers of varying size, including the Departmental Accounting System (DAS) for the Government of Malta, and for a number of Government entities, manufacturing concerns and service companies.

Chris Farrugia
Partner | Information technology
T +356 9982 9636
E chris.farrugia@mt.gt.com

Chris Farrugia is an IT Consultant and Information System Auditor within the Business Risk Services and Outsourcing division of Grant Thornton Malta.

He has been associated with Grant Thornton Malta for the past 20 years and has extensive experience in business requirements analysis, software implementation and project management for information systems for corporate customers in varying business sectors.

During his time as Director with Grant Thornton's associate company, Information Technology Services Limited, Chris was in charge of Operations, including day-to-day running of the business. Also, during his time as Director at Information Technology Services Limited, Chris had established and nourished the necessary contacts with the Unit4 Group, authors of Business World ERP software, with whom Grant Thornton Malta partnered to provide a Corporate Financial Management Solution (CFMS) for the Government of Malta.

Grant Thornton
Fort Business Centre, Level 2
Triq l-Intornjatur, Zone 1
Central Business District
Birkirkara CBD1050,
Malta

T +356 2093 1000
E grantthornton@gt.mt.com