

SOC 2: What? Why? How?

As the use of cloud, data processing, data storage, and ‘everything-as-a-service’ organisations has proliferated, so too has the need for entities to address the risks associated with the use of service organisations.

What is a SOC 2?

Organisations providing these services need to demonstrate their principal service commitments and system requirements based on the trust services criteria of security and, if needed, availability, confidentiality, processing integrity and privacy.

They often do this by issuing a SOC 2 report. A SOC 2 report provides users with a description of the system, including the type of services provided, the entity’s principal service commitments and system requirements, and components of the system, such as infrastructure, procedures, and data used in providing the services.

The report also provides assurances as to whether the controls have been designed and operate effectively to achieve the entity’s service commitments and system requirements based on the applicable trust service criteria.

Why is SOC 2 the answer?

A SOC 2 report has become an essential tool to doing business, especially when targeting clients across multiple jurisdictions.

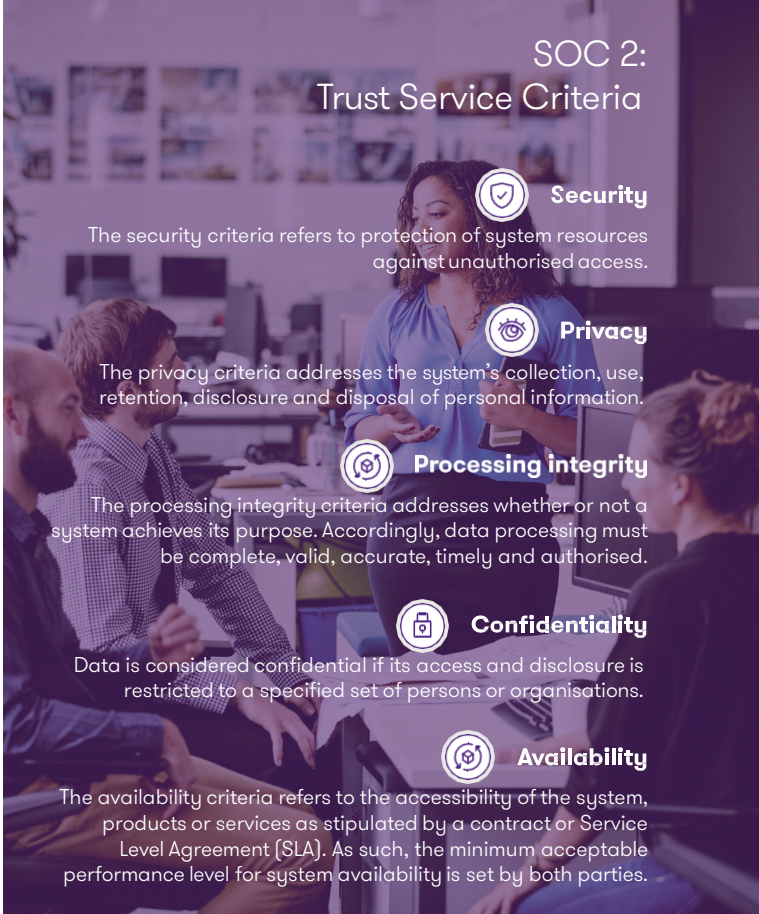
Users or customers of outsourced services regardless of their sector expect to have a means of gaining assurance on the security of the product/service they are using and the information systems that support the delivery of such solutions.

These reports also answer countless customer, vendor and third party enquiries on the security of information systems. They enable a strategic and business development agenda and they enhance business credibility and business profile in the marketplace.

Fundamentally a SOC 2 report has become a prerequisite to doing business and is often used as a screening mechanism in tendering and procurement processes.

How to achieve SOC 2 status?

A SOC 2 reporting solution is achieved on a phased basis, starting with a readiness assessment, before working towards preparation of a Type I SOC 2 report (control design only) and ultimately completing a Type II report (control design and operating effectiveness). The Type II report becomes the annual SOC 2 assurance solution that outsourced providers can distribute to their clients and other stakeholders as required.



**SOC 2:
Trust Service Criteria**

- Security**
The security criteria refers to protection of system resources against unauthorised access.
- Privacy**
The privacy criteria addresses the system’s collection, use, retention, disclosure and disposal of personal information.
- Processing integrity**
The processing integrity criteria addresses whether or not a system achieves its purpose. Accordingly, data processing must be complete, valid, accurate, timely and authorised.
- Confidentiality**
Data is considered confidential if its access and disclosure is restricted to a specified set of persons or organisations.
- Availability**
The availability criteria refers to the accessibility of the system, products or services as stipulated by a contract or Service Level Agreement (SLA). As such, the minimum acceptable performance level for system availability is set by both parties.

Types of SOC 2 reports:

- SOC 2 report provides reasonable assurance that the service organisation's service commitments and system requirements have been achieved based on the trust services criteria relevant to security, availability and processing integrity of the systems used to process users' data, and its confidentiality and privacy of the data.
- SOC 2+ report addresses compliance with SOC 2 trust services criteria '+' compliance with other regulations/standards including HIPAA, HITRUST, NIST, ISO, CSA Star or other specified subject matter. A SOC 2 + allows third-party service providers to take advantage of the synergies of overlapping control frameworks and satisfy their customers' evolving control requirements. This has the potential to reduce overall compliance costs and efforts as SOC 2+ reports create substantial efficiencies for many service organisations.

How can we help?

It goes without saying that being able to market your business as SOC 2 compliant enhances your credibility and attractiveness to both prospects and customers. With an ever expanding network of vendor-customer relationships in the technology sector and the importance of data security in these relationships, having a SOC 2 report is now essential.

Our SOC Centre of Excellence comprises IT security and SOC subject matter experts that have helped clients at every stage of their SOC 2 journey. We have a best in class offering that we provide to new and existing clients. We are accredited to provide SOC 2 assurance services globally.

Our proprietary software: SOC.x

SOC.x is a web-based application that features standardised reporting templates and supports a 'test once, report many' approach. SOC.x allows the firm's professionals to collaborate using integrated tools that includes standard interfaces, dashboards, comment threads and status reporting. SOC.x helps ensure consistent SOC reporting nationally and internationally.

Contact us

If you would like to learn more about SOC 2 compliance, please contact a member of our dedicated SOC 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

© 2022 Grant Thornton Ireland. All rights reserved. Authorised by Chartered Accountants Ireland ("CAI") to carry on investment business.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication.