



What is SOC 2?


Service organisation controls (SOC) 2 is an internal controls offering that utilises the American Institute of Certified Public Accountants (AICPA) standards to provide an audit opinion on the security, availability, processing integrity, confidentiality and/or privacy of a service organisation's controls .


SOC 2 can be applied for regulatory or non-regulatory purposes to cover business areas outside of financial reporting. The report can be distributed to customers and other stakeholders to demonstrate a focus on system and processing controls to meet their requirements.


The need for assurance in these areas can be addressed through one or more of the five SOC 2 Trust Service Criteria (TSCs):

 **Security** - The system is protected against unauthorised access (both physical and logical).

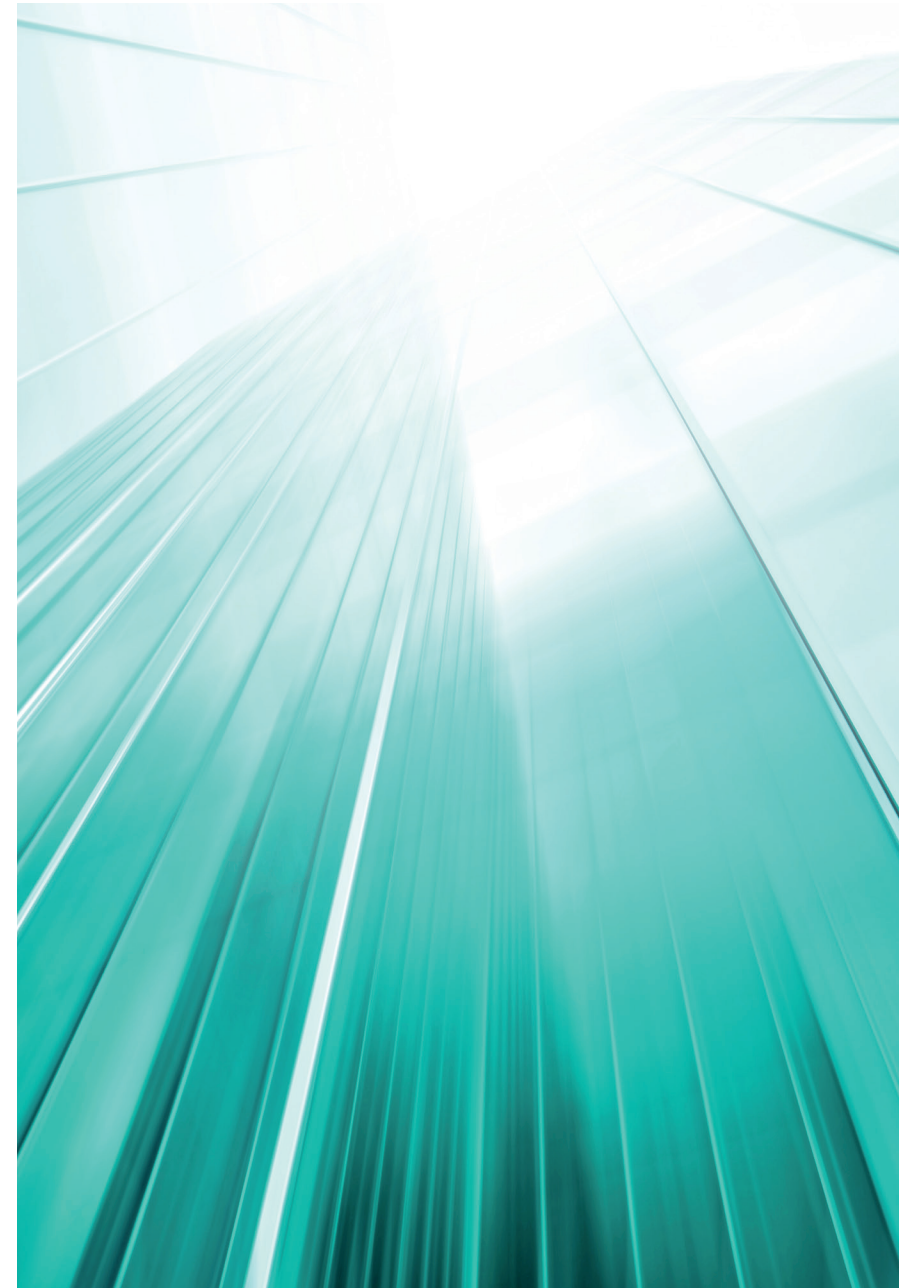
 **Availability** - The system is available for operation and use as committed or agreed.

 **Processing Integrity** - System processing is complete, accurate, timely, and authorised.

 **Confidentiality** - Information designated as confidential is protected as committed or agreed.

 **Privacy** - Personal information (e.g. Personally Identifiable Information) is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.

You may be more familiar with the SOC 1 report (also called ISAE 3402, SSAE 18, or formally SAS 70) which provides opinion on the financial controls performed by the service organisation. SOC 2 will be similar in structure which will provide opinion on the five TSCs and will have an option for a Type 1 or Type 2 report. A Type 1 only covers the design of controls, while a Type 2 covers design and operating effectiveness.





Benefits of SOC 2

Obtaining a SOC 2 report requires investment both in terms of time and cost for an organisation. However, the advantages of getting a SOC 2 attestation are far more than the initial investment.

Third party organisations that successfully complete a SOC 2 audit can offer their clients reasonable assurance that an independent reviewer has assessed their controls that relate to operations and compliance; and they meet the criteria prescribed by AICPA for the five TSCs. The report helps to prioritise risks in order to ensure that high quality services are being delivered to the clients.

Essentially, a SOC 2 report is a tool that can give organisations a competitive advantage and open up their market to new billion dollar industries.

Benefits for Service Organisation



The service organisation can undergo one audit and distribute the report to multiple customers, reducing the time spent with individual auditors.



The Trust Criteria relate directly to the core service obligations and commitments of IT, Cloud and Hosting providers.



The ability to integrate with other frameworks over IT controls and governance such as COBIT and ISO/IEC 27001



Staff throughout the service organisation gain improved insight over risk, governance and internal control.

Benefits to users of the SOC 2 report



Independent Assurance over the controls operated by the Service Organisation to which you have outsourced an element of your business.



A comprehensive report of the process and controls in place at the Service Organisation.



Clearly articulated controls that need to be performed by your organisation when working with the Service Organisation.

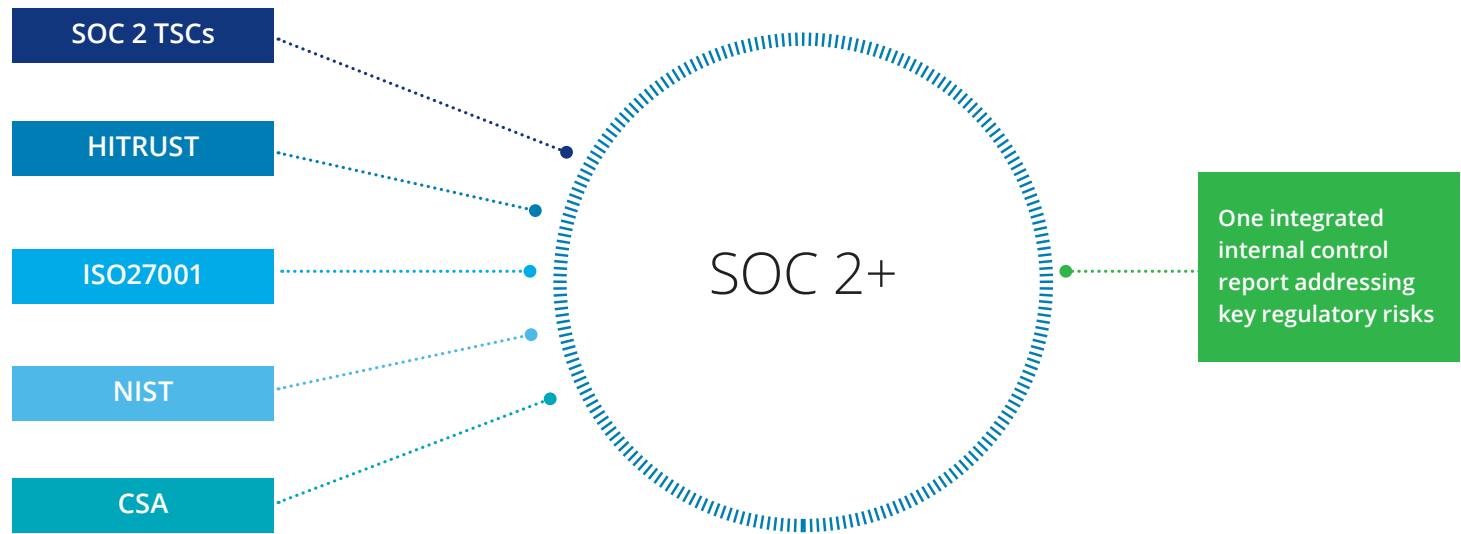


Insight into control gaps highlighted in the report.

Third-party reporting proficiency with SOC 2+

SOC 2 can be further enhanced by incorporating multiple frameworks, also called SOC 2+.

Providing assurance with regard to the AICPA TSCs may be sufficient for some outsourced service providers' (OSPs) customers. But others may require greater detail. For this reason, the AICPA has created SOC 2+. This extensible framework allows OSPs' auditors (also known as service auditors) to incorporate various industry standards, such as the National Institute of Standards and Technology (NIST) and the International Standardisation Organisation (ISO), into one SOC 2 report. This can also provide assurance to service organisations on their General Data Protection Regulation (GDPR) obligations and Cloud Computing processes and controls.



Illustrative Examples for SOC 2

All Industries	SOC 2 for Service Organisation	The application for SOC 2 is very broad and can be applied to every industry and business sector. SOC 2 will allow service organisations to provide assurance to customers and other stakeholders that effective internal controls are in place. This also offers a standardised format for meeting a broad range of regulatory and non-regulatory control requirements. Companies which are required to comply with data privacy and data protection regulations (e.g. GDPR) can obtain a SOC 2 report to demonstrate to customers that effective controls are in place to comply with these regulations.
	Deloitte's Capabilities	Deloitte is recognised as one of the market leaders in SOC reports and internal control services. We have a dedicated practice of risk and control specialists with deep industry focus and experience to reduce ramp up time. We also have subject matter experts (SMEs) with in-depth knowledge of specific regulations.
Cloud Computing	SOC 2 for Cloud Service Providers	Cloud service providers need to provide their customers assurance of effective controls across all the SOC 2. Trust Criteria in order for those customers to comfortably entrust the cloud provider with their sensitive data and critical computing needs. SOC 2 reports provide a way to build trust with customers and demonstrate compliance in controls with various industry regulations and standards (e.g. Cloud Security Alliance).
	Deloitte's Capabilities	Deloitte has considerable cloud computing capabilities with experience serving the largest cloud providers and the most demanding cloud customers. We are leaders in security, privacy, and internal control services. Our strong brand in assurance makes us a first choice provider for SOC 2 services to cloud providers.
Data Centre	SOC 2 for Data Centre Hosting Companies	Data centres and co-locations should provide a reliable infrastructure in hosting critical systems for their customers to ensure business continuity. A secure environment is also a top priority to provide assurance over the integrity of data hosted within their environment. SOC 2 will provide a high level of assurance to customers that the data centre is secure, highly available, and operating with high standards of integrity.
	Deloitte's Capabilities	Deloitte has significant qualifications and experienced staff reviewing controls over data centres or co-location companies, as well as proficiency in best practices for this industry and other relevant standards (e.g. ISO 27001).
Other IT Managed Services	SOC 2 for Other IT Managed Service Companies	Companies providing other IT Managed Services to customers including application management, job processing, network monitoring, and other IT outsourced activities can leverage to SOC 2 reports demonstrating to their customers that IT managed services provided are within their service level agreements. This report can provide assurance that you have effective controls in place aligned with other various control frameworks (e.g. PCI-DSS, ISO 27001, COBIT).
	Deloitte's Capabilities	Deloitte is one of the leading firm in the attest space for IT Managed Service companies with deep business experience. We also have significant qualifications around relevant standards which positions us as a leader in the marketplace for this service.

Why work with us?



Clear, easy-to-use report

While meeting the AICPA's reporting guidelines, we customise your report, including an executive summary that highlights critical information that is most important to your customers. The remainder of the report is organised by topical areas so that stakeholders can easily find details when needed.



Proven methodology

With our flexible work plans and structured walkthrough processes, we tailor our approach that works for you - reducing the effort needed to gather required information while also helping you and your staff gain a clearer understanding of the SOC 2 requirements. We also have our proprietary processes, templates, and deliverables which allow us to accelerate every phase of the audit and reporting process while keeping you up-to-date in all phases of the engagement.



Certification by a recognised leader

Deloitte is recognised as one of the market leaders in security, privacy, and internal control services. We have a dedicated practice of risk and control specialists with deep industry focus and experience. A Deloitte opinion stating that your operating controls meet SOC 2 standards is likely to reinforce customer confidence in your company.



Experienced professionals

You'll work with a carefully selected project team with in-depth industry knowledge and experience, as well as experienced service auditor professionals. Deloitte Ireland is also part of the Deloitte North West Europe (NWE) member firms which allow us to make greater impact on your business by combining capabilities across the region, with a greater capacity to deliver more innovative, high-quality services.

Contacts

**Colm McDonnell**

Partner, Risk Advisory

L: Dublin

T: +353 1 417 2348

M: + 353 87 813 8198

E: cmcdonnell@deloitte.ie

**Paul Hare**

Senior Manager, Risk Advisory

L: Dublin

T: +353 1 417 5704

M: +353 87 149 0125

E: phare@deloitte.ie

Deloitte.

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with approximately 263,900 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has nearly 3,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients so they can move forward with confidence.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte Ireland LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication. Deloitte Ireland LLP is a limited liability partnership registered in Northern Ireland with registered number NC1499 and its registered office at 19 Bedford Street, Belfast BT2 7EJ, Northern Ireland.

Deloitte Ireland LLP is the Ireland affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2018 Deloitte Ireland LLP. All rights reserved.

Dublin

Deloitte & Touche House

Earlsfort Terrace

Dublin 2

T: +353 1 417 2200

F: +353 1 417 2300

Cork

No.6 Lapp's Quay

Cork

T: +353 21 490 7000

F: +353 21 490 7001

Limerick

Deloitte & Touche House

Charlotte Quay

Limerick

T: +353 61 435500

F: +353 61 418310

Galway

Galway Financial Services

Centre

Moneenageisha Road

Galway

T: +353 91 706000

F: +353 91 706099

Belfast

19 Bedford Street

BT2 7EJ

Belfast, Northern Ireland

T: +44 (0)28 9032 2861

F: +44 (0)28 9023 4786

deloitte.ie