Deloitte.

SOC 2 Assurance

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

A reference guide to SOC 2 and our methodology

Table of Contents

SOC 2 Overview

Deloitte's SOC 2 Services

SOC 2 comparison to other standards

SOC 2 in a nutshell

There is an ever-increasing demand for companies to provide SOC 2 reports to their customers and business partners. Many companies require a SOC 2 as part of a new contract or contract renewal process (especially U.S. based companies). Customers are requiring the formal documentation and independent assurance provided by a SOC 2 report and service organizations are seeing the commercial advantage of being able to state that they have a SOC 2 report.

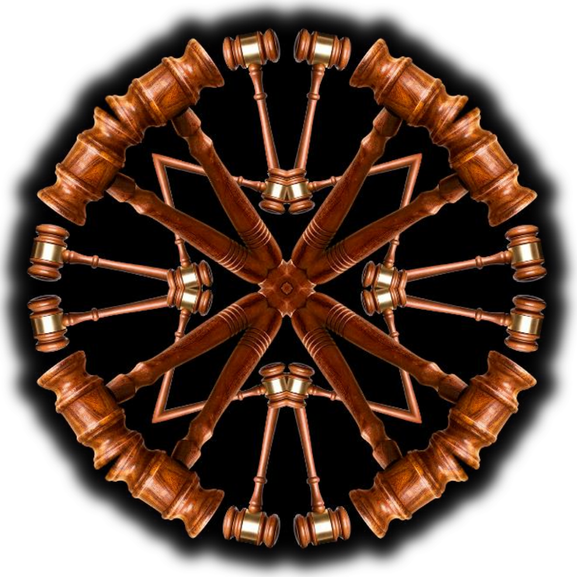
What is a SOC 2 Report?

A SOC 2 report is a type of audit report that assesses a company's controls related to security, availability, processing integrity, confidentiality, and privacy of a service organization's systems and services. The report is intended to provide assurance to customers and other interested parties that the service organization has effectively designed and implemented controls to meet the trust principles of security, availability, processing integrity, confidentiality, and/or privacy. SOC 2 reports are performed by independent auditing firms and are based on the AICPA's (American Institute of Certified Public Accountants) SOC 2 Trust Services Criteria.

Who needs a SOC 2 Report?

A SOC 2 report is typically needed by organizations that handle sensitive data and are subject to compliance requirements by their customers and regulators, such as:

- Managed IT service providers
- Software as a Service providers
- Cloud service providers
- Payment processors
- Healthcare providers
- Legal and accounting firms
- Government agencies



5 steps to SOC 2 Reporting

Step 1: Get the scope right

Getting the scope right ensures that you get the report that the recipients need and includes only the relevant entities, locations and criteria. You need to pick which Trust Criteria you want covered, when you need to issue the report, report type (1 or 2) and many other details that will have an effect on the report process. The scope should be set as clearly as possible from the start but may evolve over time.

Step 2: Gap analysis and remediation

We recommend starting off any SOC 2 engagement with a set of gap analysis workshops. We meet with key personnel at the service organization to walk through the requirements and identify potential gaps or weaknesses in controls that need to be remediated.

Step 3: Type 1 reporting

Starting with the ambition to issue a Type 1 report first is recommended to allow the service organization to get the control structure in place and to identify and remediate significant gaps or weaknesses while providing the recipient with a good ‘first step’. This will be the ‘baseline’ for which all future Type 2 reports can build and the controls in the Type 1 report whould be executed and documented to ensure compliance with Type 2 testing requirements.

Step 4: Type 2 reporting

A Type 2 report tests the operational effectiveness of the controls over a period of time (e.g., 1 year) and requires good audit evidence of the control having been executed. The auditor will include a separate section in the report detailing the tests performed and the results of the tests.

Step 5: Reevaluation and streamlining

The control regime, scope of the report and its contents and the methods and techniques used to test the controls should be reviewed at least annually to ensure ongoing relevance and efficiency.

Benefits of a SOC 2

Obtaining a SOC 2 report requires investment both in terms of time and cost for an organization. However, the advantages of getting a SOC 2 attestation are far more than the initial investment. Third party organizations 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 prioritize 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 organizations a competitive advantage and open up their market to new industries.

Benefits for Service Organization

- ✓ **Commercial advantage:** In sales situations, TPA reports can be one of the items which differentiate one service organization from its peers/competitors. It may also be seen as a disadvantage if the OSP does not have such a report, but their competitor does.

- ✓ **Cost savings:** Providing TPA reports, which require one audit team for a predictable period of time, is generally more cost effective than participating in customer audits. Customers receiving TPA reports are often required to pay for the reports, further reducing the cost burden of internal control testing.

- ✓ **Broad assurance:** Most TPA reports provide reasonable assurance to a broad range of clients with a single report.

- ✓ **Compliance requirements:** Demonstrates to regulatory bodies that controls are in place and operating effectively.

- ✓ **Improve overall control awareness:** The process of developing and issuing a TPA report at an OSP often generates increased internal control awareness within the organization.

- ✓ **Customer requirement:** Future customers / existing customers wishing to renew contracts may require such reports and having the report process in place may lead to increased ability to win new customers or keep existing relationships.

Benefits to SOC 2 report recipients

- ✓ **Confidence:** Increased confidence that the vendor is meeting the internal control expectations of their customers through independent and transparent reporting on operational effectiveness of controls at the supplier

- ✓ **Internal reporting requirements:** Ensuring that the company's multi-purpose reporting requirements — including operational and financial—are met

- ✓ **Valuable insight/monitoring:** Independent assessments of whether the controls of the OSP were in place, suitably designed and operating effectively, with a focus on continuous improvement when controls are found to be lacking

- ✓ **Cost savings:** OSPs may charge customers for TPA reports, or they may not. The cost of being required to pay for a TPA Attestation report should be weighed against the cost of the customer having to maintain their own staff or hiring staff to be able to perform regular audits of the supplier(s).

- ✓ **Compliance requirements:** Maintaining compliance with industry, governmental and other relevant regulatory requirements

What does it take to develop and issue a SOC 2?

Each of our SOC 2 engagements has roughly followed the same process. We have found that it is important to spend enough time up-front to get the scoping of the report right, develop a detailed plan of action, identify key stakeholders and make the practical arrangements. We have developed templates and, although each client's control environment is different, we have a good understanding of what types of controls to look for.

Planning, walkthroughs and gap analysis reporting

Phases 1 and 2 of any new SOC 2 project includes planning the engagement, getting to know the key stakeholders and getting them used to the SOC2 audit process and performing the initial process walkthroughs to identify control gaps or weaknesses. If we can get this analysis done early, the client is able to initiate remediation efforts to fill the control gaps and strengthen any weak controls early enough so that the rest of the SOC 2 testing process is as smooth as possible, and the resulting SOC 2 report is as free for 'findings' as possible.

Type 1 reporting

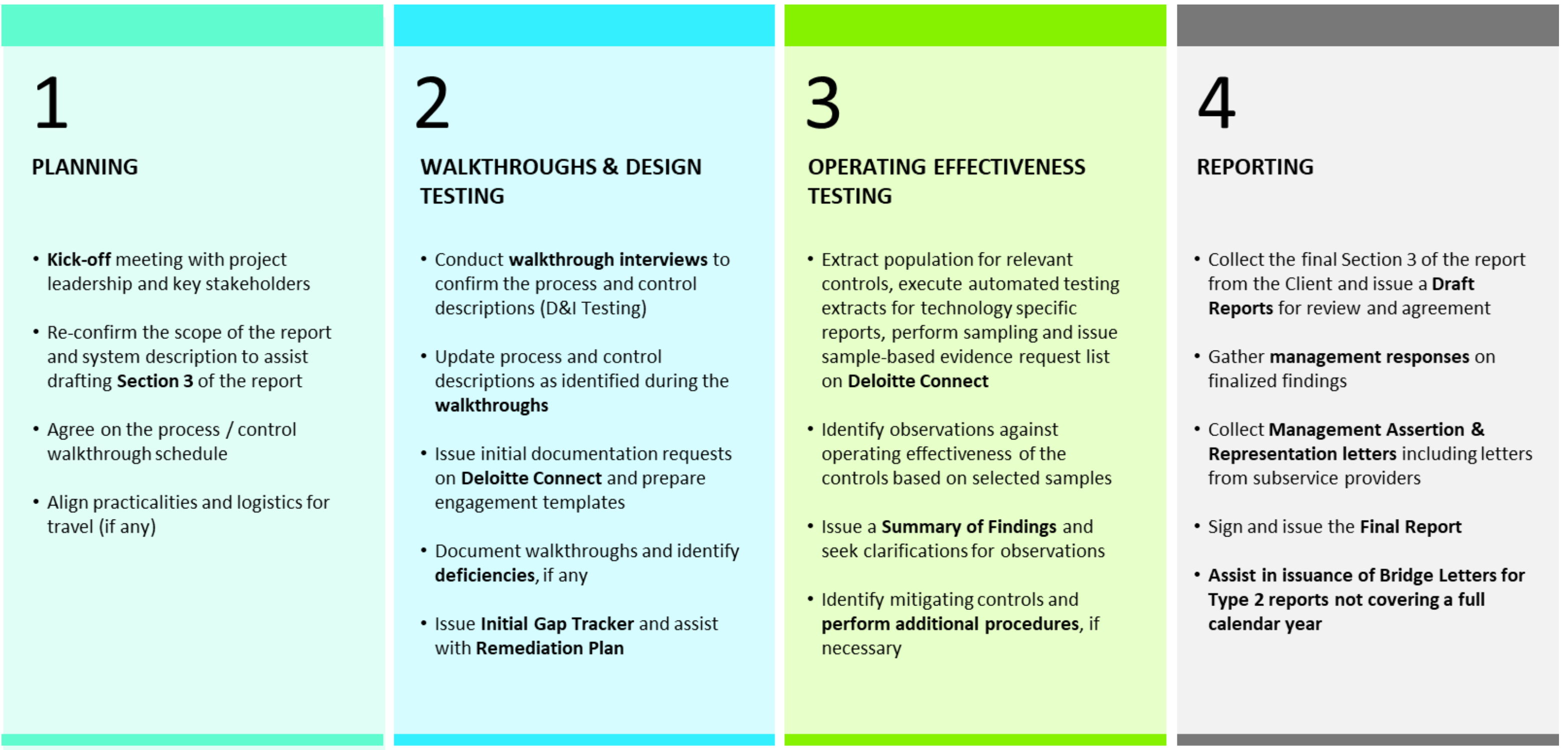
When the client is confident that any significant control gaps or weaknesses have been remediated, we perform the final control walkthroughs and assessment of the design and implementation of the controls necessary to produce the Type 1 version of the report. Most clients begin their SOC 2 process by issuing a Type 1 report with Type 2 reports for the future periods starting with the as-of date of the Type 1.

Type 2 reporting

When issuing a Type 2 report, we perform tests of the controls covering a period of time (at least 6 months), general from 01. January through to 31.December. These detailed tests are performed using internationally accepted audit sampling guidelines, which are designed to provide reasonable assurance that errors would be identified in the sample, if relevant.

Ongoing improvement

Discussing lessons learned with the client, tracking areas for future improvement with the report or our audit methods and regularly assessing the quality of our work ensures that our engagements and reports are of the highest quality.



1

PLANNING

- **Kick-off** meeting with project leadership and key stakeholders
- Re-confirm the scope of the report and system description to assist drafting **Section 3** of the report
- Agree on the process / control walkthrough schedule
- Align practicalities and logistics for travel (if any)

2

WALKTHROUGHS & DESIGN TESTING

- Conduct **walkthrough interviews** to confirm the process and control descriptions (D&I Testing)
- Update process and control descriptions as identified during the **walkthroughs**
- Issue initial documentation requests on **Deloitte Connect** and prepare engagement templates
- Document walkthroughs and identify **deficiencies**, if any
- Issue **Initial Gap Tracker** and assist with **Remediation Plan**

3

OPERATING EFFECTIVENESS TESTING

- Extract population for relevant controls, execute automated testing extracts for technology specific reports, perform sampling and issue sample-based evidence request list on **Deloitte Connect**
- Identify observations against operating effectiveness of the controls based on selected samples
- Issue a **Summary of Findings** and seek clarifications for observations
- Identify mitigating controls and **perform additional procedures**, if necessary

4

REPORTING

- Collect the final Section 3 of the report from the Client and issue a **Draft Reports** for review and agreement
- Gather **management responses** on finalized findings
- Collect **Management Assertion & Representation letters** including letters from subservice providers
- Sign and issue the **Final Report**
- **Assist in issuance of Bridge Letters for Type 2 reports not covering a full calendar year**

Components of a SOC 2 report

Report section	Description
Section I: Independent service auditor's report (opinion)	**Section I of a type 2 SOC 2 report contains the service auditor's opinion about whether:** • Management's description of the service organization's system is fairly presented • The controls included in the description are suitably designed to meet the applicable trust services criteria stated in management's description and were operating effectively to meet the applicable trust services criteria • For SOC 2 reports that address the privacy principle, management complied with the commitments in its statement of privacy practices throughout the specified period
Section II: Management's assertion	**Management is required to provide a written assertion about whether, in all material respects and based on suitable criteria:** • Management's description of the service organization's system fairly presents the service organization's system that was designed and implemented as of a specified date • The controls stated in management's description of the service organization's system operated effectively throughout the specified period to meet the applicable trust services criteria • Management must have a reasonable basis for its assertion. Standards provide flexibility in the actual procedures performed by management. Management may not rely solely on the testing done by the service auditor.
Section III: Description of the system (provided by the service organization)	**Section III: System Description Overview (provided by the service organization)** • This information will be provided by the service organization • A system consists of five key components organized to achieve a specified objective. The five components are categorized as follows: ○ Infrastructure: The physical and hardware components of a system (facilities, equipment, and networks) ○ Software: The programs and operating software of a system (systems, applications, and utilities) ○ People: The personnel involved in the operation and use of a system (developers, operators, users, and managers) ○ Procedures: The automated and manual procedures involved in the operation of a system ○ Data: The information used and supported by a system (transaction streams, files, databases, and tables) • Applicability & Purpose of Report, System Overview, Entity level control information and Complementary User-Entity Controls will also be included in Section III
Section IV: Trust services criteria, related controls and tests of operating effectiveness	• Trust services criteria, related controls (provided by the service organization), and tests of operating effectiveness (provided by the service auditor), testing matrix with mapping to TSC • Topical Area System Descriptions (provided by the service organization), Testing and Results (provided by the service auditor)
Section V: Other information provided by the service organization	**Other Information Provided by the Service Organization (Optional)** • Section V will contain information that the service organization would like to provide to the users of the report, which is NOT covered by our opinion.

Section III: Trust Categories

A SOC2 report may include any of the trust services categories of security, availability, processing integrity, confidentiality, or privacy, either individually or in combination with one or more of the other trust services categories.

For each category addressed by the engagement, all the criteria for that category should usually be addressed. However, in limited circumstances, one or more criteria may not be applicable to the engagement. In such situations, the one or more criteria would not need to be addressed.

Further, the common criteria (included in the Security trust services category) should be applied regardless of which trust services category is included within the scope of the engagement.

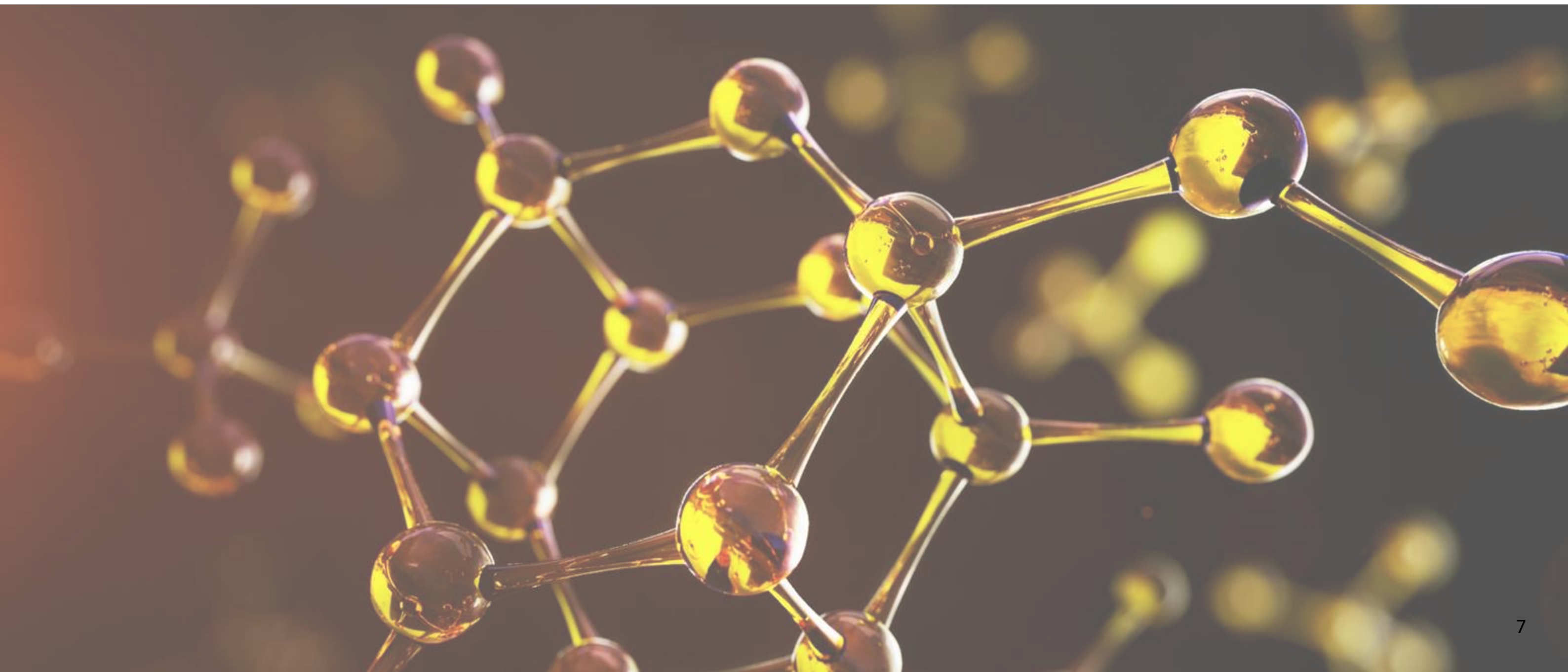
- **Security -** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

- **Availability -** Information and systems are available for operation and use to meet the entity's objectives.

- **Processing Integrity -** System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

- **Confidentiality -** Information designated as confidential is protected to meet the entity's objectives.

- **Privacy -** Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.



SOC 2 for supply chain

SOC 2 for supply chain

Manufacturers, producers, and distribution companies (referred to herein as “organizations”) must manage a complex network of plants, service providers, and suppliers to operate efficiently and meet commitments to customers. At the same time, the threats to and vulnerabilities of each supplier in the chain have increased significantly. When a supply chain is disrupted, the organization is at risk of failing to meet production or delivery commitments it has made to its customers.

Disruption to supply chains

Causes of disruption to supply chains include the following:

- Weather and other natural disasters (such as hurricanes or tornadoes) in a geographic area that is home to a supplier’s facility
- Threat of war or military action in a geographic area that is home to a supplier’s plant
- The lack of financial well-being of a key supplier or shipper
- Wide-spread diseases (such as SARS, MERS, or the COVID-19 coronavirus) that can affect the entire supply chain

For these reasons, an organization’s ability to achieve its objectives is increasingly dependent on events, processes, and controls that are not visible to the organization and are often beyond its control, such as controls at the suppliers.

Failure to manage risks

Manufacturers, producers, and distribution companies are looking for visibility across their complex supply chain networks to better understand the risks of doing business with suppliers and the controls the suppliers have in place to mitigate those risks. The failure to manage these risks appropriately can result in:

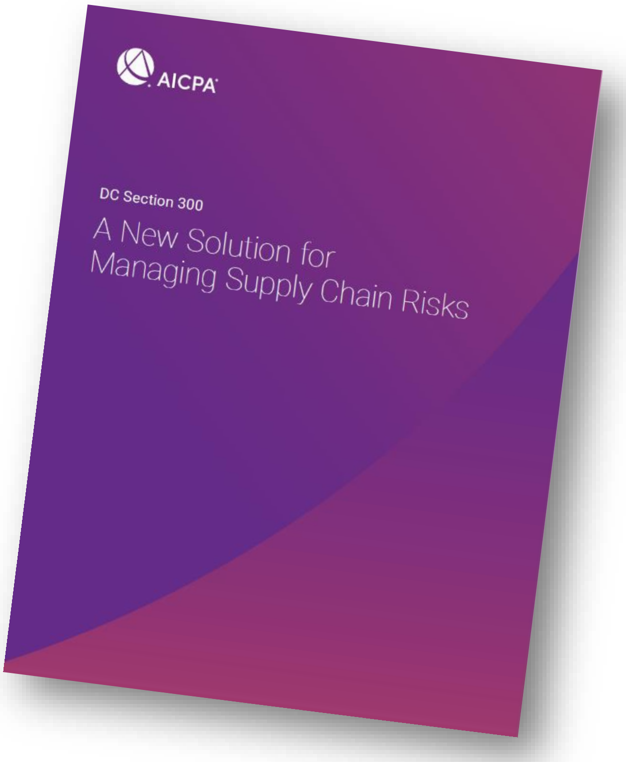
- reputational damage,
- loss of intellectual property,
- disruption of key business operations,
- fines and penalties,
- litigation and remediation costs, and
- exclusion from strategic markets.

This is why supply chain risk management has become such a significant issue to many organizations and their stakeholders. Suppliers are also increasingly interested in communicating how they manage the production and distribution risks in their own systems as a way of reassuring the organizations with whom they do business.

SOC 2 for supply chain

In recognition of the needs of commercial customers and business partners of manufacturers, producers, and distribution companies, the AICPA has developed a framework for reporting on the controls over a manufacturing, production, or distribution system. Organizations can use the reporting framework to communicate to stakeholders relevant information about their supply chain risk management efforts and the processes and controls they have in place to detect, prevent, and respond to supply chain risks.

The reporting framework also enables an attestation provider to examine and report on management-prepared system information and on the effectiveness of controls within the system, thereby increasing the confidence that stakeholders may place in such information. A report that results from an examination of a manufacturing, production, or distribution system and its controls is referred to as a SOC for Supply Chain report.



SOC 2 for supply chain (continued)

Managing supply chain risk of suppliers

Because of their dependence on suppliers, organizations are responsible for understanding the risks of doing business with suppliers and for designing, implementing, and operating controls to mitigate those risks. For that reason, organizations are interested in, among other things,

- obtaining an understanding about the risks identified by a supplier that affect the supplier's
- production, manufacturing, or distributions of goods.
- comparing the supplier's objectives for the production, manufacturing, or distribution of goods with customers' needs.
- obtaining an understanding of the production, manufacturing, or distribution process of a
- supplier to better understand the risks to the customer of doing business with the supplier and the controls that the supplier has implemented to mitigate those risks.
- when establishing IT connectivity with a supplier or business partner, understanding the information security controls implemented by the supplier or business partner in order to more effectively integrate the security controls of the two entities.

Currently, organizations interested in the systems and controls of their suppliers have to assemble desired information from many different sources, including the following:

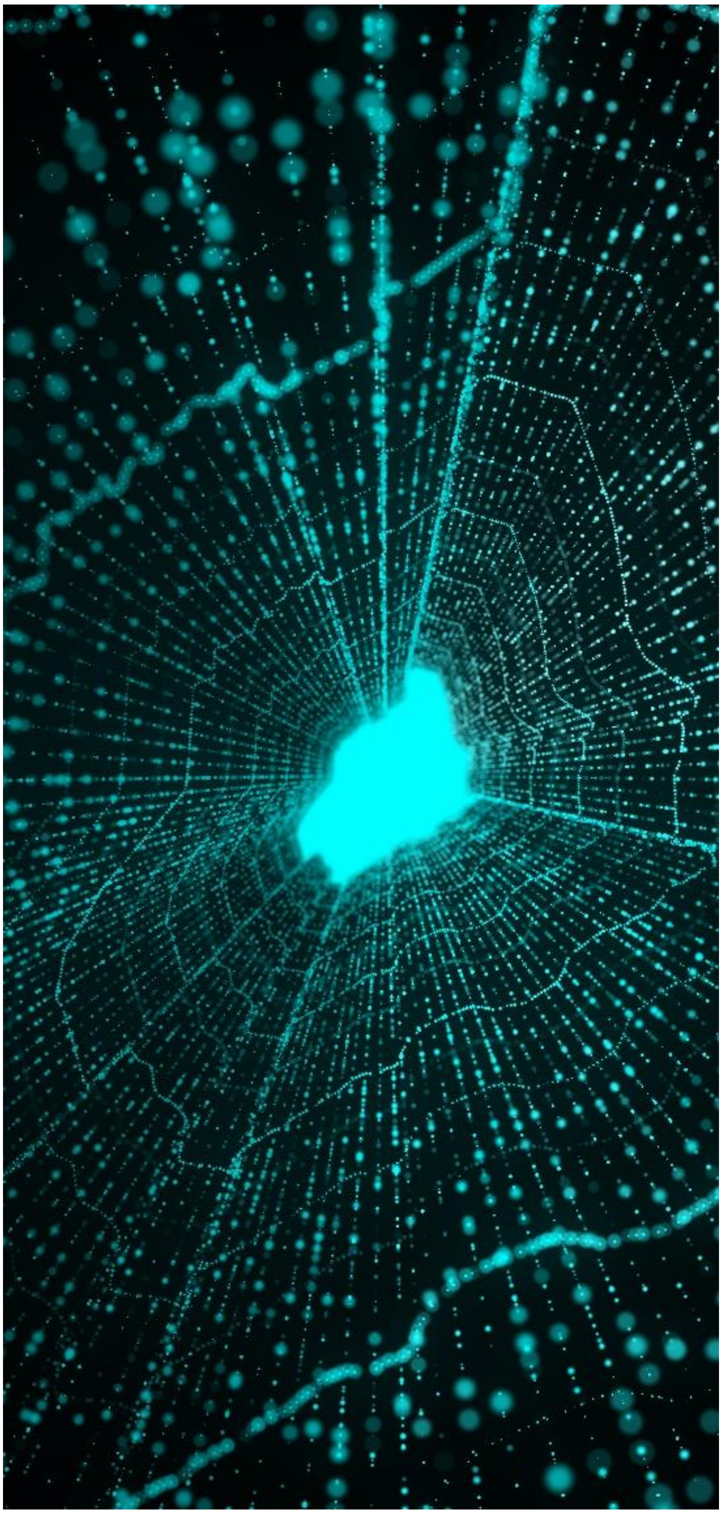
- Supplier-provided information
- Site visits, inspections, and other procedures performed by the supplier's internal audit functions
- Assurance programs (such as International organization for Standardization [ISO] certifications) performed by third-party assessors

A more efficient way to building supplier trust

With the introduction of a SOC for Supply Chain framework, however, organizations may find that obtaining a SOC for Supply Chain report from their suppliers is the most efficient way to get the information they need to understand the risks of doing business with suppliers.

Objective of the SOC for Supply Chain reporting framework

The objective of the SOC for Supply Chain reporting framework is to provide a means by which manufacturers, producers, and distribution companies can communicate useful information about their systems and the controls within the systems to customers and business partners. CPAs can examine and report on such information, thereby increasing the confidence that customers and business partners can place in the information.



SOC 2 for supply chain (continued)

What does the SOC 2 for supply chain report do?

The reporting framework and the report resulting from its use do the following:

- **Provide a set of common criteria for disclosures** about a manufacturing, production, or distribution company's system — Through the use of a common set of description criteria that set forth disclosures about the system, the SOC for Supply Chain report reduces the information burden on organizations by providing customers and business partners with useful information about the system and its controls to help users better understand the associated risks and make better decisions.
- **Provide a set of common criteria for assessing control effectiveness** —The SOC for Supply Chain report provides an independent assessment of the effectiveness of a manufacturer, producer, or distribution company's controls using the AICPA's 2017 trust services criteria for one or more of the following categories: security, availability, processing integrity, confidentiality, or privacy.
- **Reduce the communication and compliance burden on organizations** — The SOC for Supply Chain report reduces the number of information requests from customers and the amount of information sought if such requests are made.
- **Provide useful information to customers and business partners** while minimizing the risk of creating vulnerabilities to the organization— Information provided in the SOC for Supply Chain report is designed to meet the needs of customers and business partners without disclosing critical defenses that might be targeted by malicious actors.
- **Provide comparability** — The SOC for Supply Chain report would provide customers and business partners with information that could be used to track the progress of the organization's supply chain efforts across time and to benchmark those efforts against other organizations.
- **Provide scalability and flexibility** — The SOC for Supply Chain framework is useful to manufacturers, producers, and distribution companies of varying sizes and across all industries.
- **Evolve to meet changes** — The SOC for Supply Chain framework will be updated and modified over time based on experience, changes to the environment, and organization and stakeholder needs.

The SOC for Supply Chain framework leverages the core competencies of attestation providers as providers of examination services, applying them to an organization's supply chain efforts in accordance with the AICPA's Code of Professional Conduct and attestation standards.

Transparent information to stakeholders to build trust

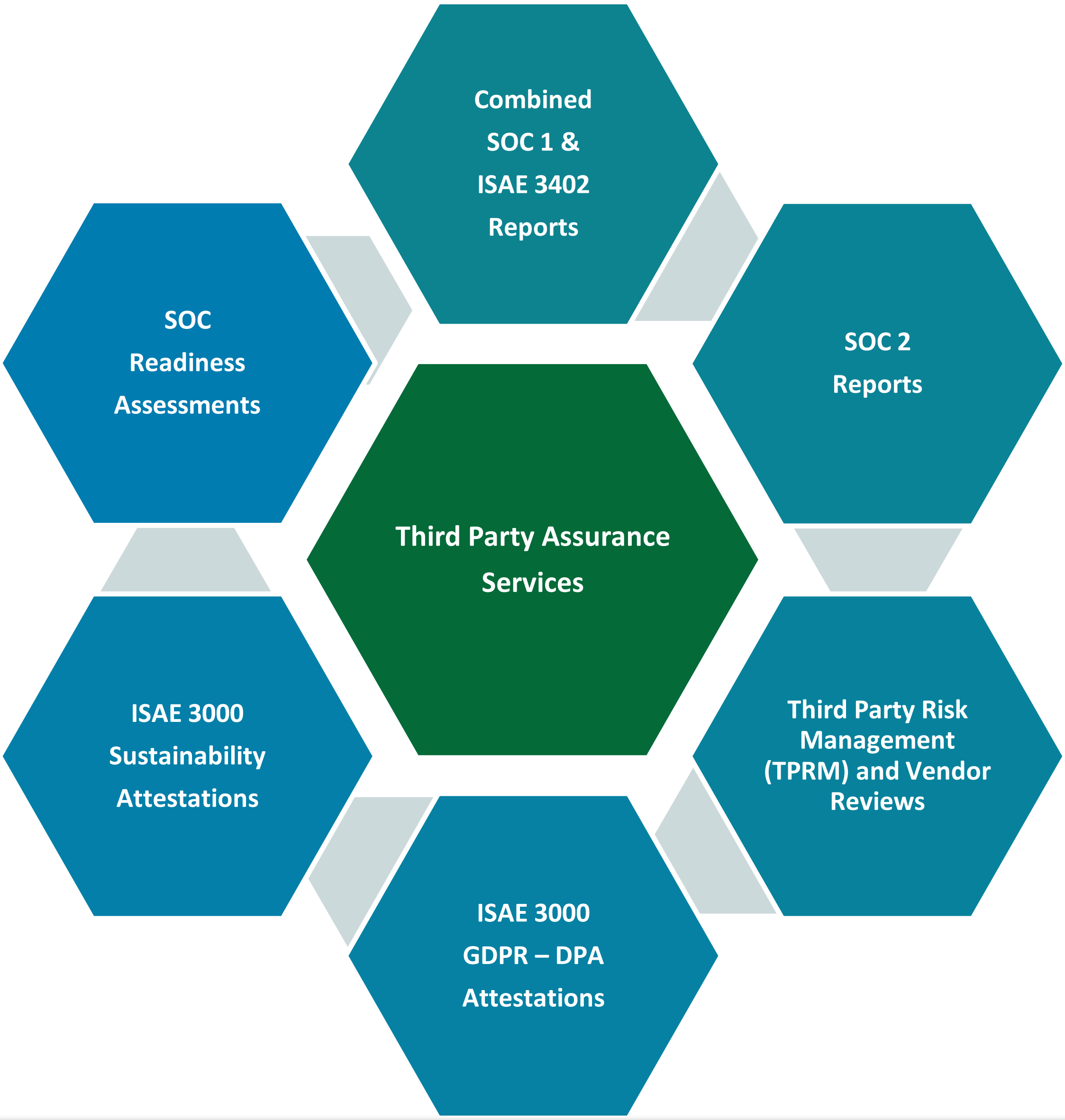
A manufacturer, producer, or distributor and its customers and business partners will be best served if there is a defined set of information intended to enhance understanding of controls over manufacturing, production, and distribution systems. The information in the SOC for Supply Chain report is intended to provide useful information to stakeholders while also being:

- transparent,
- consistent across time,
- comparable between entities,
- reasonably complete,
- scalable, and
- flexible.

The SOC for Supply Chain examination could go far in meeting the information needs of customers and business partners of manufacturers, producers, or distributors.

Deloitte’s Services and Reference Engagements

Deloitte’s Third-Party Assurance Services


Combined SOC 1 & ISAE 3402 Reports
SOC 2 Reports
SOC Readiness Assessments
Third Party Assurance Services
ISAE 3000 Sustainability Attestations
Third Party Risk Management (TPRM) and Vendor Reviews
ISAE 3000 GDPR – DPA Attestations

We have experience in providing the following Third-Party Assurance services:

- **SOC1 & ISAE 3402 attestation –** We deliver numerous ISAE3402 reports for customers each year and even have clients where we issue a combined ISAE3402 and SOC1 report, increasing the useability of the report for their US customer base.

- **SOC2 attestation** – performed in accordance with AICPA issued Trust Service Criteria for Confidentiality, Availability, Security, Processing Integrity and Privacy, we issue more than 10 SOC2 reports for Norwegian companies annually.

- **ISAE 3000 Data Processing Agreement Attestation (GDPR Compliance)** – we provide attestations to customers which are used to evidence compliance with the terms outlined in their Data Processing Agreements.

- **Third Party Risk Management (TPRM)**– assisting clients in formalizing their third-party risk evaluation and mitigation efforts, including methods to inventory third-party relations, classify the risk of each existing and any future third-party relations, developing self-assessment questionnaires for covering varying risk themes (e.g., cyber, financial, climate and sustainability), methods for reviewing responses and defining and executing audit procedures necessary resulting from the assessments.

- **Vendor Reviews** – using our vast experience in both auditing and assisting vendors with their internal control needs, we can perform reviews of your vendors for you to provide you with assurance for specific risks you have identified or just follow one of our specific vendor audit programs for specific topics.

- **Sustainability Reporting attestation** – we provide attestation reports on companies’ sustainability reporting as well as other Climate and Sustainability related topics.

- **SOC Readiness Assessments** – We perform gap analyses and readiness assessments for all of the above topics.

Note: *The names of our references are made anonymous for this brochure.*

Deloitte engagement references

Our core team of Third-Party Assurance experts each has significant experience in providing attestation services.

Our client experience

Our team of more than 90+ TPA resources in the Nordic region, supported by subject matter experts from our IT audit, Cyber Security, Financial Audit, Legal and Consulting departments, deliver more than 200 attestation reports to more than 100 clients in the region. We work on some of Nordic's most challenging and exciting attestation engagements.

The following is a list of some of the engagements our Norwegian Team has worked on or are currently delivering. We support engagements across the Nordic region, as indicated (NO, SE, DK).

- **Payroll processing** (ISAE3402 Type 2 - Payroll)
- **SaaS provider** (SOC 2 Type 2 – SaaS))
- **SaaS provider** (ISAE3000 GDPR – SaaS) (DK)
- **Telecom** (ISAE3402 – Transaction processing)
- **SaaS provider** (ISAE3000 Type 1 – SaaS) (DK)
- **SaaS provider** (ISAE3000 GDPR – SaaS) (DK)
- **IT services provider** (SOC2 Type 2 – IT)
- **SaaS provider** (ISAE3402 Type 2 – SaaS) (DK)
- **Transportation services** (ISAE3402 Type 2 – Ticket income distribution)
- **IT services** (SOC2 Type 2 – IT) (DK)
- **Financial services** (ISAE3402 Type 2 – IT) (DK)
- **Educational Institution** (ISAE3402 Type 2 and ISAE3000 GDPR (DK)
- **SaaS provider** (SOC2 Type 2 - SaaS)
- **Financial services** (ISAE3402 and multiple SOC2 reports – Financial services) (SE)
- **IT services provider** (ISAE3402 Type 2 – Managed IT)
- **SaaS provider** (ISAE3402 Type 2 – SaaS)
- **IT security services** (SOC2 Type 2 – IT Services)
- **Airline** (ISAE3000 Type 1 – Process integrity)
- **SaaS provider** (SOC2 Type 2 – SaaS)
- **SaaS provider** (SOC2 Type 2 – SaaS)
- **IT services** (SOC2 Type 2, ISAE3402 Type 2 and ISAE3000 GDPR – Managed IT))
- **Financial services** (SOC2+ with CSA CCM – Financial services) (DK)
- **SaaS provider** (ISAE3402 Type 1 – SaaS) (DK)
- **SaaS provider** (SOC2 Type 2, ISAE3000 GDPR and ISAE3000 for MitID and NSIS - SaaS)
- **IT services provider** (ISAE3402 / SOC1 combined and SOC2 Type 2 – Data center services)
- **SaaS provider** (ISAE3402 Type 2 and 3 ISAE3000 GCPR – SaaS) (DK)
- **IT services** (Multiple ISAE3000 reports – Managed IT Services)
- **SaaS provider** (ISAE3402 Type 2)

Our customers will vouch for us

Considering using our services but uncertain? We can provide you with multiple client references that you can feel free to contact to discuss our team, our services and our quality. These references can be provided as part of a request for proposal discussion.

SOC 2 Comparison
to
other standards

SOC 2 and ISAE 3402

SOC 2 and ISAE3402 (SOC 1)

SOC 2 and ISAE3402 reports are two widely used frameworks for assessing and reporting on the control objectives and activities of an organization, with regards to information security and data protection. However, there are several differences between the two that determine their focus, scope, use, and target audience.

Focus

SOC 2 focuses on the overall security and privacy of an organization's information systems, including their infrastructure, network, data, and applications.

ISAE3402 focuses on the manual and IT-based controls put in place by a service organization that are relevant to the processing of financial transactions on behalf of their customers. It also takes into account the management of risks that may impact the services they provide.

Scope

The scope of a SOC 2 report is broad and covers all customer-facing information systems and activities related to security, availability, processing integrity, confidentiality, and privacy, with the main focus of the report being security.

The scope of an ISAE3402 report is more focused on the risks and internal controls related to the business processes and controls and general IT controls in place to ensure the complete and accurate processing of financial transactions for their clients.

Use

The ISAE 3402 report is typically used by organizations that provide services to customers, such as data centers, cloud services, and software-as-a-service providers. The report is used to demonstrate their commitment to security and data protection and to provide assurance to customers that their information is being handled appropriately. On the other hand, SOC 2 reports are used by organizations to demonstrate their overall security posture and to provide assurance to stakeholders and customers that their information systems are secure and their data is protected.

Target Audience

The ISAE 3402 report is intended for customers, stakeholders, and auditors who require assurance on the security and data protection measures put in place by the service organization. The report provides information on the service organization's internal controls and the measures they have taken to manage risks. On the other hand, the SOC 2 report is intended for customers, stakeholders, and auditors who require assurance on the overall security and data protection of an organization.

These two report types serve different purposes and have different focuses, scopes, uses, and target audiences. Choosing the correct framework that best fits the needs of your customers, stakeholders and their auditors is important. We have extensive experience in making the right choice.

SOC 2 and PCI DSS

While both PCI DSS and SOC 2 audits are designed to ensure that organizations protect sensitive data, they have different scoping, testing strategies and levels of assurance. PCI DSS is geared towards compliance with specific requirements for credit card data handling, while SOC 2 is focused on the overall control environment of the organization, including security, availability, processing integrity, confidentiality, and privacy.

Main differences

PCI DSS (Payment Card Industry Data Security Standards) and SOC 2 (Service Organization Control 2) are two different types of audits that organizations can undergo to ensure compliance with security and data protection standards. The main differences between the two audits lie in their scoping and testing strategies, as well as the level of assurance they provide.

PCI DSS

PCI DSS is a set of standards developed by major credit card companies to ensure that merchants and service providers who process, store, or transmit credit car<d information maintain a secure environment. The audit for PCI DSS is typically more focused on the specific systems and processes that handle credit card data, such as point-of-sale terminals and online payment portals. The scope of the audit is typically limited to the parts of the organization that handle credit card data, and the testing is geared towards identifying vulnerabilities and non-compliance with the PCI DSS requirements.

SOC 2

SOC 2, on the other hand, is a broader audit that looks at an organization's overall control environment, including security, availability, processing integrity, confidentiality, and privacy.

Scope

The scope of the SOC 2 audit is typically much wider, covering all aspects of the organization's operations and systems, including those that do not handle sensitive data.

Testing

The testing for SOC 2 is geared towards assessing the design and effectiveness of the organization's controls, rather than identifying specific vulnerabilities.

Level of assurance

In terms of the level of assurance provided, PCI DSS is typically considered to be more specific and prescriptive, while SOC 2 is considered to be more general and principles-based. PCI DSS is focused on compliance with a specific set of requirements, while SOC 2 is focused on the overall control environment of the organization.

Target audiences

A PCI DSS audit is focused on organizations that process credit card transactions and The target audience for this type of audit would typically include companies in the retail, hospitality, and financial services industries.

A SOC 2 audit is focused on organizations that handle sensitive data and provide services, such as cloud providers and managed service providers. The target audience for this type of audit would typically include technology and service companies.

SOC 2 and ISO27001

Isn’t my ISO 27001 certification enough?

We get this question a lot. The answer is, ‘*enough for what purpose?*’

ISO 27000 and SOC 2 are two distinct standards for information security and data protection. Both are widely recognized and respected in their respective fields, but they serve different purposes and have different requirements.

ISO 27000

ISO 27000 is a series of international standards for information security management. The standard provides a framework for managing sensitive information and includes guidelines for risk management, incident management, and compliance. To achieve ISO 27000 certification, an organization must demonstrate that it has implemented the necessary controls and processes to protect sensitive information.

SOC 2

SOC 2, on the other hand, is an attestation standard for service providers. It is designed to provide assurance to customers that the service provider has implemented appropriate controls to protect their sensitive information. SOC 2 focuses on five trust principles: security, availability, processing integrity, confidentiality, and privacy. To achieve SOC 2 compliance, a service provider must undergo an independent audit and provide a report to its customers.

What’s the difference?

Purpose:
ISO 27000 is focused on information security management within an organization, while SOC 2 is focused on providing assurance to customers that a service provider has implemented appropriate controls to protect their sensitive information.

Audience:
ISO 27000 certification is intended for organizations of all sizes and types, while SOC 2 is primarily intended for service providers.

Scope:
ISO 27000 covers a wide range of information security management topics, while SOC 2 is focused specifically on security, availability, processing integrity, confidentiality, and privacy.

Compliance:
ISO 27000 certification is based on self-assessment and internal audit with controls tested on a rotation basis over 3 years, while SOC 2 compliance provides a higher level of audit assurance with all controls tested annually, is based on independent testing and the production of a comprehensive report to share with customers.

Contact Information

Contact information

Kevin F. McCloskey
Associate Partner, Third-Party Assurance Services
CISA, CIA, CIPP/e, CRMA
Mobile: +47 913 68 848
Email: kmccloskey@deloitte.no

Lasse Vangstein
Partner, State Authorized Auditor
Mobile: +47 975 84 086
Email: lvangstein@deloitte.no

Jouni Viljanen
Partner, Risk Advisory
Mobile: +35 820 755 5312
Email: Jouni.Viljanen@deloitte.fi

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.no for a more detailed description of DTTL and its member firms.

Deloitte Norway conducts business through two legally separate and independent limited liability companies; Deloitte AS, providing audit, consulting, financial advisory and risk management services, and Deloitte Advokatfirma AS, providing tax and legal services.