SOC 2 assurance becomes critical for cloud & IT service providers

Why SOC 2 fits in as future-proof business control model for cloud & IT service providers

Cloud and IT service providers that want to proof their performance in critical, non-functional areas such as Security, Availability, Processing Integrity and Confidentiality can leverage the SOC 2 Framework. This US/Canadian framework is becoming the de-facto international standard for providing assurance to client organizations. This article describes the SOC 2 components and benefits for service providers and user organizations, as well as the lessons learned when implementing and migrating to this framework.

Stefan Zwinkels
is a manager at KPMG IT Assurance & Advisory.
zwinkels.stefan@kpmg.nl

Ronald Koorn
is a partner at KPMG IT Assurance & Advisory.
koorn.ronald@kpmg.nl

INTRODUCTION

Major cyber security incidents, such as the hacks at Solarwinds, Uber, Equifax and Microsoft and ransomware at Maersk and Maastricht University, have increased the awareness at senior management that there is an urgent need for improving their security and availability – internally as well as at their business partners.

In addition to external and internal IT incidents, the Covid-19 pandemic also highlighted the third-party dependencies. Organizations expect their partners to be even better secured and prepared, especially those partners that are providing critical services, such as their cloud and IT service providers. These service providers are not only contractually required to implement and maintain strong controls but will also increasingly be requested to ensure and demonstrate compliance for the outsourced processes. Providing assurance by service providers to their clients is a means to this end.

MARKET TRENDS & (IT) ASSURANCE NEEDS

Traditionally, service providers have demonstrated their service quality – in ascending order – by:

- periodic service level reporting;
- annual testimonies such as an ISO 27001 or even an ISO 20000 certification;
- assurance over transaction processing through ISAE 3402 assurance.

The latter is related to the financial statement audit, has an emphasis on automated and manual process controls, supporting General IT Controls on related financial systems. For organizations that rely substantially on cloud and IT service providers, the three options above are insufficient for controlling their outsourced activities. These options partly or at a high level cover areas such as cyber security, business continuity, confidentiality, or processing integrity beyond the financial systems or beyond the implementation of controls. For example, the operational effectiveness of security controls across an organization is outside the scope of these options.

In recent years, the growing tendency of migrating to cloud platforms has given an impetus to service providers to broaden their scope for risk management and IT assurance. Public cloud solutions offer opportunities for standardized, scalable, highly available solutions that enable organizations to decrease the cost of control and increase flexibility, especially compared to housing and hosting solutions. All service providers were or are considering how cloud platforms would fit in their IT strategies.

Cloud services are offered in a wide variety: a public or a private cloud, or a hybrid solution. Many "as a Service" providers emerged leveraging cloud solutions. Well-known examples are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and/or Infrastructure-as-a-Service (IaaS), but there are also various intermediate solutions. Consequently, with such large variety on offer and new solutions tending towards cloud, IT landscapes of clients are becoming increasingly complex. Current IT landscapes are no longer based on a single hosted solution, but on a myriad of multi-vendor solutions. Service providers, in turn, also have contracted out specific services to other "subservice providers". This increased complexity affects the IT Supply Chain and Vendor Risk Management.

In such a complex IT landscape, it becomes more and more challenging for clients to maintain control over their data, and they will seek additional guarantees from their service providers. A number of universal criteria apply, and the following questions arise:

- Are my systems and data sufficiently secure from outside and inside threats?
- Are they available when I need them?
- Who can access confidential data?
- Is it processed correctly?
- How is privacy managed on a global scale?

To respond to these questions, the service provider needs to increase its transparency, which goes beyond whether agreed-on KPIs have been achieved and communicated via a service level report. Some service providers are wary of a higher degree of transparency, as it may lead to follow-up questions and maybe even too much (operational) involvement – if they were an internal IT department. Another factor that plays a role in the increased scrutiny of service providers is the external pressure of cyber threats, disruptions, specific legislation (e.g. privacy, critical infrastructures) and regulation (e.g. outsourcing in financial services) and specific supervisory requests.

For such situations, an independent third-party statement ("opinion") on whether all control objectives are achieved regarding the services provided, is an implementation of profound transparency. This addresses all key aspects based on which the providers deliver their services, notably: Infrastructure, Software, Hardware, People and Process.

For this purpose, professional associations in several countries have set up initiatives to develop a standard set of controls for the core IT processes. None of these national frameworks achieved international recognition. Almost 25 years ago, the American Institute of Certified Public Accountants (AICPA) along with the

Canadian Institute of Charted Accountants (CPA Canada) developed standard frameworks, such as WebTrust and SysTrust. Approximately 10 years ago, the AICPA and CPA Canada introduced the System and Organization Controls (SOC 2) standard for Service Organization Control Reporting based on the Trust Services Categories (see Figure 1). The last couple of years, this standard has been updated (2017) to align it more closely to the COSO model and moreover, the approach is getting traction in Europe.

For addressing the abovementioned questions, the SOC features the following so-called Trust Services Categories: Security, Availability, Processing Integrity, Confidentiality, and Privacy. They will be briefly outlined below.

Security

The weakest link of the "information chain" can be the primary attack surface for malicious parties. Therefore, despite the fragmentation in IT services, organizations need strong managed security services, which adhere to (inter)national security standards across the entire chain – without any blind spots. During the last revision, the AICPA has extended the SOC 2 Framework with Cyber Security as additional Trust Service Category ([AICP17]) to report on.

Availability

Dependency on multiple service providers can affect an organization's availability to provide services, especially if its requirements are not clearly defined and safeguarded. The scalability of cloud platforms opens a window of opportunity to increase and decrease processing capacity in a very flexible manner. An organization has to specify clear capacity requirements, especially when it comes to peak workloads in data processing. Especially for services where high availability is critical, outages can be costly and sometimes even disrupt a major part of business or even society.

Processing integrity

In case of complex data processing, organizations need to understand the controls that the service provider has in place to safeguard the integrity of data processing. This may include formalized validation controls regarding input, output and throughput. The service provider also needs to ensure the stability and integrity of stored procedures for automated processing as well as the parameters applied.

Confidentiality

For the confidentiality of its data, an organization may seek additional guarantees beyond the contract clauses.

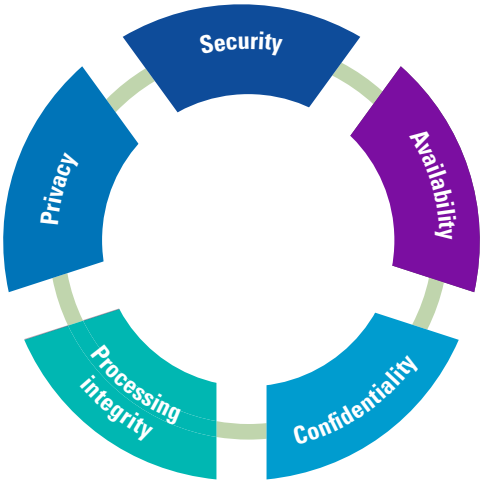


Figure 1. SOC 2 Trust Services categories.

Not only the IT Management of the organization that has outsourced, but also its Board, the Chief Data, Security and Privacy Officers, Internal Audit and even regulators may require transparency about the controls that the service provider has implemented for safeguarding data confidentiality. Confidentiality is addressing all types of sensitive data, such as about financials, mergers, intellectual property, etc. and not specifically personal data (see next).

Privacy

Privacy legislation, such as the European GDPR, requires organizations that are responsible for the personal data (as "controllers") to implement and maintain stringent personal data protection, especially if it concerns sensitive personal data. The more technical privacy requirements also extend to its service providers (as "processors") with whom standardized Data Processing Agreements have to be established and concluded. In certain cases, stakeholders may require an attestation of the implemented privacy controls. See the separate section on the relationship between SOC 2 Privacy with GDPR.

In each of the abovementioned categories, the relationship, responsibilities and a joint understanding of the precise services provided need to be clearly defined. The same is true for the control framework, as organizations and service providers predominantly use their internal, proprietary sets of controls. Aligning the services and controls definitions and overcoming conflicting interests can undermine the forecasted synergies outsourcing to cloud / IT service providers can bring.

THE BENEFITS OF SOC 2

The SOC 2 framework offers service providers a comprehensive, standardized baseline of controls for the services provided. By using SOC 2 report, organizations can manage its outsourcing risks and obtain insight in the effectiveness of the controls at their service providers. A SOC 2 report can also cater for the information needs of a broad range of (other) stakeholders.

The latest version of the SOC 2 Framework blends control over Technology, as well as control over the service provider entity – based on the well-known COSO model for Enterprise Risk Management (ERM). Hence, the control over services is extended to the entire system of Internal Control from which the services are delivered. This integration of system-level controls with entity-level controls provides a steering mechanism over key components and aspects that make up the service delivery. The Control Framework not only focuses on the service delivery processes and the generic (IT) management processes, but also on the quality system within which these are embedded. For example, control over required skills, education and training, and control over vendor and client relations and ethics, raise the bar for the execution of the service delivery processes. Control over information flows, Board involvement, risk management and monitoring, further strengthen the consistency and quality of service delivery at service providers.

The SOC 2 Control Framework allows the service provider to select the Trust Services Criteria that are of interest to its clients. One or more criteria can be selected; however, the common criteria that entail the COSO principals as well as the core controls over Security, are always included mandatorily (see Figure 2).

In the latest version of this SOC 2 Framework, a less prescriptive approach for controls has been taken in order to cater for a wider array of service organizations, not necessarily limited to IT service providers. A variant of the Framework also made it suitable for logistic processes (SOC 2 for Supply Chain) and for data integrity and software development.

The Framework sets a baseline through the requirement to fully implement Trust Services Criteria. Applying the Trust Services Criteria in actual situations at a service provider requires professional judgment. Therefore, the organization has the flexibility to shape its control environment based on its own risk assessment – using a set of pointers: so-called "points of focus". These points of focus represent important characteristics of the criteria and provide support for designing, implementing, and operating the controls. A well-defined control may serve multiple criteria (Control Objectives) in the Framework.

The mandatory element ensures that organizations know that what is presented to them is a complete set of controls to cover the attested Trust Service Criteria.

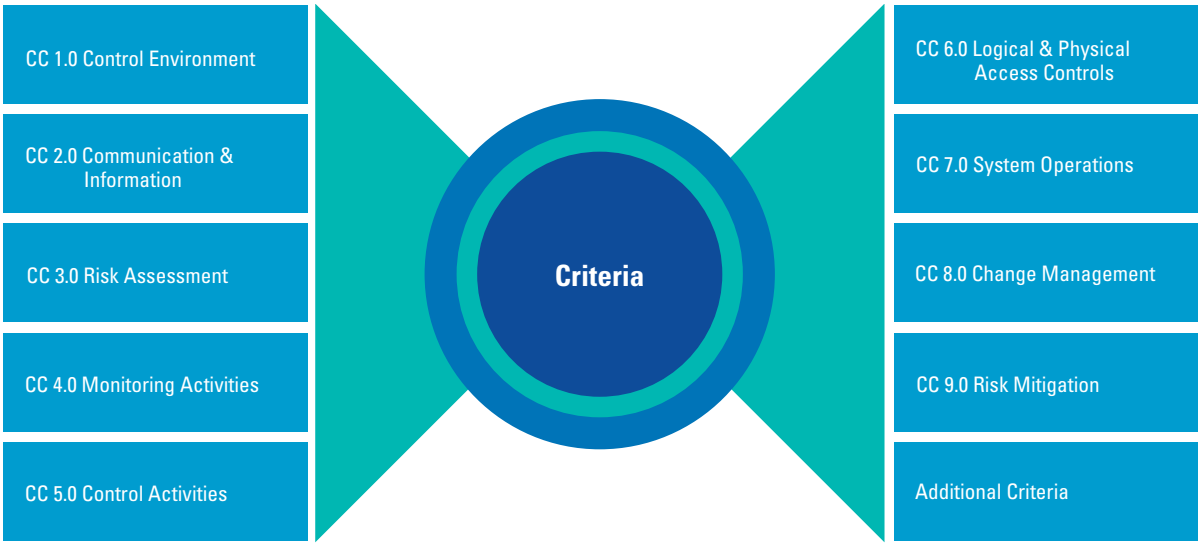
SOC 2 BENEFITS FOR SERVICE PROVIDERS

As SOC 2 is service-oriented, the standard has a number of clear benefits for cloud and IT service providers:

Transparency

For service providers, the SOC 2 Framework enables them to provide the transparency over the service delivery to their clients and other stakeholders over non-functional but critical IT subjects that are on the management

Figure 2. SOC 2 Trust Services criteria (including common COSO ERM criteria).



agenda or even Chefsache nowadays. Security is a Top-3 topics in Board rooms, and the control thereof a continuous challenge. By being transparent, service providers can demonstrate their control over processes related to their services. as the SOC 2 assurance can be of added value in the pricing of their services, this will open opportunities to distinguish operations and acquire new clients.

Extend the service portfolio

The increased focus on security and business continuity can be a driver for extending the service portfolio, either by adding more depth to existing services or through providing additional services. For example, implementing state-of-the-art role-based access provisioning on its management platform by the service provider could be an interesting proposition for its client's (internal) IT environment.

Integrate control over technology with internal control

The most important benefit appears not to be related to its service delivery but to its control thereof. The combination of technology-driven controls and the common criteria as derived from the COSO ERM Framework, allows the service provider to take a systematic, integrated approach to its service delivery. The controls over technology, such as the management of firewalls, security baselines and authorizations are bolstered by additional controls that address risk management. Moreover, these technology controls can be linked to entity-level controls that govern the service provider, such as ensuring the appropriate flow of management information, having skillful and appropriately trained personnel and introducing tactical monitoring processes.

The Control Framework assists in operationalizing the management's risk assessment, ensuring an appropriate control environment, and that monitoring activities are in place. In this way, an effective Plan-Do-Check-Act cycle can be established, not only for continuously improving the control over the services but also for improving services.

HOW SOC 2 SERVES (USER) ORGANIZATIONS

For clients of service providers, a SOC 2 report provides valuable insights in the Service Organization's internal control. This has the following benefits:

Extending risk management to critical third parties / service provider

For clients of cloud/IT service providers, SOC 2 assurance allows them to obtain a comprehensive view on risks and controls, beyond the boundaries of their own organization. Through a SOC 2 report, the client organization receives significantly more information on how the service provider performs its services. Moreover, the organization will be in a better position to realistically assess its performance with internal "self-inflicted" standards and/or externally required standards.

The latter is increasingly the case, especially in the Financial Services sector where the Dutch Central Bank (De Nederlandse Bank, DNB) in its Assessment Framework wants to be informed about how service providers have organized their internal (IT) controls across the entire information supply chain. This goes beyond what is reported traditionally in service level reports or even ISAE 3402 reports.

Vendor / Third-Party Risk Management

DNB requires financial institutions to actively pursue third-party risk management. This type of risk management stipulates requirements on how organizations need to manage and monitor services by third parties. Third-party risk management consists of risks and controls for adhering to laws and regulations, ethical standards, industry standards, data classification – while taking into account the risk impact and risk tolerance. As the client organization is held accountable for all of its information, regardless of where it resides or who is processing it in their name, the client organization is expected to not only assess risk within its own organization but also to assess it beyond its own boundaries and across the entire supply chain.

Research performed by DNB (see [DNB19]), showed that the extent to which internal control at third parties was pursued scored a meagre rating of 1 out of 5. Few organizations actually had a clear view on third-party risks. Following these results and the wider implementation of Solvency II, third-party outsourcing has received significant additional scrutiny; insurance companies are expected to review their outsourcing relationships and report to the DNB as supervisory authority.

1 ISAE 3402 reports are also referred to as SOC 1 reports. For the sake of completeness, SOC 3 refers to the web seal for marketing reasons on the service providers website, only when an unqualified SOC 2 report has been issued.

Inspiration for continuous improvement

The SOC 2 report also emphasizes, more extensively than is the case in regular ISAE 3402 reports[1], the so-called "user entity control considerations" that are to be met by the client organization in order to rely on the report. This report section and the description of the services system may also serve as an inspiration and guideline as to how the organization could improve its own control environment and specific (boundary) controls. The SOC 2 standard provides a comprehensive, but also conclusive set of criteria to address in order to have an enterprise-wide span of risk management and control. Organizations may vary in size, scope and complexity and consequently will choose different controls; however, the principles remain the same and will also provide the client organizations with opportunities for continuous improvement.

Standardization and comparability

The SOC 2 methodology is prescriptive, all criteria of a selected Trust Service Category need to be addressed, including the common (ERM) criteria. This will ensure that service providers cannot cherry pick in terms of which well-performing controls are described in its system. Although the service provider is free to design its own controls, the obligation to include all criteria facilitates the completeness of the information provided over its internal controls. It allows for assessing the service provider's performance.

The common goal: building trust

Management and scientific publications refer to "trust" as a crucial pillar of any transactional relationship to work, which is no different in the relationship between service provider and its clients. SOC 2 reporting provides the opportunity to inspire trust, as the relationship moves from having faith in a service provider based on operational service level reporting to a much more standardized and informed way of placing reliance on the service provider. Especially when critical services are outsourced.

SOC 2 reporting will provide better understanding and transparency, allowing both parties to deepen their relationship and increase the predictability of activities in the relationship by controlling alignment and standardization. Other side effects can be the lowering of the transaction costs of outsourcing and achieving control over the entire supply chain, which can be supported by automation. The use of sophisticated (GRC) tooling is indispensable in managing security and availability in hybrid IT landscapes.

Finally, as service providers become more maturity with respect to security and controls, user organizations become more skilled in defining the scope and aligning the internal and provider's controls when requesting for SOC 2 assurance or receiving the SOC 2 result. See also the separate section on "What to request in and how to review a SOC 2 report".

> SOC 2 reporting can inspire trust in organizations that heavily rely on service providers

IMPLEMENTING SOC 2

For organizations that consider implementing SOC 2 assurance, there are a number of considerations.

Enterprise-wide impact

SOC 2 is definitely not adopted overnight, it will take considerably more effort than achieving ISO 27001 certification (see also the separate section on SOC 2 assurance vs. ISO 27001 certification). It involves aligning and assessing the entire system of internal control, and requires a structured, control-based approach at each level related to managerial to operational service delivery. All the way up to managerial level where points of focus such as "tone at the top", "board independence" and "skill diversity" need to be addressed. Without a well-structured, entity-wide approach, the implementation of a SOC 2 Control Framework that satisfies the ERM-type common criteria will be hardly possible.

Consider your maturity

The nature of the SOC 2 Framework more or less demands the service provider to function as an integrated unity. To implement such a framework, we recommend that the organization has experience and at least a basic maturity in internal (IT) control. The SOC 2 Framework is extensive and will only lead to benefits if controls can be demonstrably complied with in design, implementation (Type I) and operating effectiveness

(Type II). Therefore, staff awareness and experience in executing and documenting controls and controls execution is essential for success.

Performing an internal SOC 2 self-assessment and/or external gap analysis can show your controls readiness, but also your own maturity to embark on a formal SOC 2 attestation.

Scope is key

To design an effective system of internal control that covers the service delivery context, defining the services in scope is a key element. Once the provider has clearly defined its service commitment to its clients (based on contracts & SLAs), it can derive the "system requirements". The requirements consist of frequency and procedures for performing internal controls that satisfy the criteria in scope. The controls can then be designed based on these requirements along the axis of People, Process, Infrastructure, Hardware, Software and Data.

Redundancy with other frameworks

When implementing the SOC 2 Framework, a service provider may find redundancy with already applied standards, such as ISAE 3402. Both frameworks address General IT Controls on the processing of financial data, the overlap in this area can be as high as 95 percent. However, the service provider should carefully consider whether adopting SOC 2 could coincide with abandoning ISAE 3402 over time. The standards address different perspectives: ISAE 3402 of completeness and accuracy over financial reporting, while SOC 2 addresses internal control over the services provided. The scope and purpose may differ, but the controls may be similar. Even so, the audit object and the objective of the assurance reports are not (entirely) similar. The risk perception of control deficiencies in a financial 3402 context or in an SOC 2 IT Control context also varies.

Depending on the precise scope and assurance needs of user organizations, a SOC 2 report – with additional criteria (see Figure 2) – could eventually also succeed an ISAE 3402 report, preferably with only a single year overlap.

Phased approach

As the SOC 2 Framework allows for facultative adoption of the different criteria within a selected Trust Services Category, we recommend a phased approach when implementing SOC 2. The Common Criteria alone, mandatory in any SOC 2 report, involve 9 criteria classifications, which in total contain 33 criteria to be addressed and a total of 197 points of focus (directives for control design). Those Common Criteria are usually associated with the Security Trust Services Category. Any additionally selected Trust Services Category will result in an even higher number of criteria to be addressed and audited. However, not all points of focus need to be taken into account, only the relevant ones.

One can imagine that it not only requires significant effort and time to design and implement a framework that addresses all criteria; it is almost inevitable to prioritize and if needed, eventually delay inclusion of additional Trust Services Categories and criteria.

Managing expectations

Besides the lead time for implementation, it is important to manage expectations of client organizations. Laying the foundations for an effective SOC 2 Framework requires a team project, even when client perception and patience for the implementation is limited. Even with an orchestrated effort, it may take at least 6 to 9 months before the full set of controls has been implemented. If clients require results earlier, an intermediate step could be worthwhile, such as providing assurance over a small set of controls under the 3000A Directive / ISAE 3000 Standard.

Strong 2nd line

The extent and required effort of the service provider to achieve a successful SOC 2 Framework deployment makes a strong 2nd line function that can monitor, facilitate and report on the control performance almost indispensable. Even in mature organizations such a 2nd line is critical to ensure that all tactical risk management, compliance and control processes are executed. All levels need to be involved for such an enterprise-wide system of internal control.

Tooling for efficiency and (meta) control

Service providers can deploy tooling in support of managing their system of internal controls. Tools can contribute to detailing the responsibilities, linking the SOC 2 Control Framework to services and processes, planning and monitoring certain tasks, and to documenting controls testing. Furthermore, a tool facilitates the aggregation and reporting to management and supports the 2nd line functions in their roles.

Strong Governance, Risk & Compliance (GRC) tooling is offered by multiple software vendors, several also integrate with Service Desk activities (see [Lamb17]). The advantage of this integration is that it prevents duplicated efforts and can act as a "single source of truth" with real-time information on the state of controls and control performance.

An alternative approach

Assurance on internal controls over the cloud services provided with a SOC 2 assurance report has clear benefits that ultimately facilitates the focus on the quality of services. Applying the Trust Services Criteria can have a lasting impact and provide service providers with the capability to prove its reliability as a business partner, while achieving internal harmonization of processes and control information.

However, full implementation of the SOC 2 Framework is challenging due to its standard form and size. Not all organizations have the capacity or financial strength to afford this type of assurance over such a control framework. In these circumstances, service providers may choose to adopt specific criteria to incorporate in their own custom control frameworks which can be audited according to the 3000A Standard/Directive. The downside is the lack of completeness and comparability.

Service providers that cannot afford or have no strong demand for IT assurance were for long dependent on various stand-alone ISO certifications, usually in domains such as security (ISO 27001 and 27002), IT Management (ISO 20000) or cloud security (ISO 27017). For those service providers, the initiative CSPCert of the EU agency for Cyber Security (ENISA) can be interesting (see [ENIS20]). CSPCert will introduce a new cyber security baseline certification for cloud security which is based on six existing cloud and security standards and can be attested at several certification levels. This new cloud certification may have less focus on internal controls and provide less assurance in comparison to SOC 2 assurance (esp. the SOC 2 for Cybersecurity) but can provide the opportunity and flexibility to obtain comfort about cloud security for a broad target group.

CONCLUSION

With the increasing complexity in IT landscapes and outsourcing relations, there is a growing need for assurance over cloud services, especially concerning critical elements such as Security, Availability and Confidentiality. ISO certification is insufficient to provide organizations with reasonable assurance. The SOC 2 standard, introduced in Northern America, satisfied this need in a standardized manner. Just like with SAS 70 in the past, we expect that this US/Canadian-based assurance standard will eventually become a global standard.

When applying the SOC 2 Control Framework, a structured implementation scope and strategy is crucial. We recommend service providers to identify and harmonize the assurance needs of user organizations in order to avoid the obligation to provide overlapping assurance reports (ISAE 3000/3402 & SOC 2) for multiple years, as well as ending up with a qualified opinion. We expect that cloud and IT service providers that offer critical services and/or in regulated sectors can anticipate for a SOC 2 future.

References

[AICP17] AICPA (2017). SOC 2 for Cybersecurity. Retrieved from: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html

[Beek13] Beek, J.J. van & Gils, H. van (2012). Nieuwe ontwikkelingen IT-gerelateerde Service Organisation Control-rapportages, SOC 2 en SOC 3. *Compact* 2013/2. Retrieved from: https://www.compact.nl/articles/nieuwe-ontwikkelingen-it-gerelateerde-service-organisation-control-rapportages/ (in Dutch)

[DNB19] DNB (2019). *Beoordelingskader Informatiebeveiliging.* Retrieved from: https://docplayer.nl/126014097-Beoordelingskader-informatiebeveiliging-dnb.html (in Dutch)

[ENIS20] ENISA (2020, December). *European Cybersecurity Certification Scheme for Cloud Services.* Retrieved on 22 March 2021 from: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/

[Koor13] Koorn, R.F. & Stoof, S. (2013). IT-assurance vs. IT-certificering: wat biedt mij (voldoende) zekerheid? *Compact* 2013/2. Retrieved from: https://www.compact.nl/articles/it-assurance-versus-it-certificering/ (in Dutch)

[Lamb17] Lamberiks, G.J.L., Wit, I.S. de & Wouterse, S.J. (2017). Trending topics in GRC tooling. *Compact* 2017/3. Retrieved from: https://www.compact.nl/articles/trending-topics-in-grc-tooling/

About the authors

Stefan Zwinkels is a manager at KPMG IT Assurance & Advisory experienced in Risk Management, IT Audit and Internal (IT) Controls. He has performed various types of IT audits and IT assurance engagements (SOC 2, ISAE 3402, ISAE 3000) for several IT service providers.

Ronald Koorn is a partner at KPMG IT Assurance & Advisory. His focus areas are IT Governance, Information supply chains, Privacy and emerging technologies, especially in the public, education and IT sectors. He also spent two years at KPMG US and is editor-in-chief of Compact Magazine.

What to request in and how to review a SOC 2 report?

Obtaining a SOC 2 report is not a tick in the box, it needs to be carefully aligned and reviewed with respect to your assurance needs. If you are in the driver seat to make your cloud service provider provide a SOC 2 report, you need to consider more than just the Trust Services categories that need to be included – as discussed in this article. If you are the recipient of a SOC 2 report, you can specifically focus on:

- **Reporting period**: The reporting period should fit your fiscal year. However, if there is a gap between your fiscal year and the reporting period, for instance the 4th quarter of a calendar year, you probably need to obtain information on the relevant controls for the missing 1 to 3 months without assurance. In most instances, a "bridge letter" provided by the service provider will suffice. However, this bridge letter is a self-declaration and sometimes misses the critical December month with many year-end changes. Although additional independent testing is a less viable option, this approach may deemed to be required in case of a qualified opinion or major migrations outside the SOC 2 reporting period.
- **Scope**: the scope of SOC 2 reports can include all or a specific set of generic services that a cloud service provider can offer, although you may not have contracted services such as data archiving, etc. Likewise, you may use specific services, such as SOC/SIEM monitoring, or locations/environments that are actually outside the SOC 2 report.
- **Other service providers**: when your service provider has contracted other (sub) service providers for its offering, which in turn may also have engaged other parties, you need to scrutinize whether either the SOC 2 assurance includes the most critical parties ("inclusive") or obtain assurance reports of those parties as well (in case of "carve-out"). In both instances, the reader should be informed by the report how all parties cooperate for the joint service offering. And be aware (see also the section with SOC 2 – ISO 27001 comparison), SOC 2 assurance cannot rely on an ISO 27001 certification for sub-service providers in scope!
- **System description**: not the auditor but the service provider itself is responsible for the description of its organization, governance, processes, risk management, monitoring, etc. However, it is not meant to be a marketing brochure with hyperbolic statements as the auditor will have to ascertain that this situation is fairly described and actually in place.
- **Key changes**: as part of the system description, it should be crystal clear whether or not changes to the services, environment or control framework has taken place during the audit period.
- **Your own controls**: the SOC 2 report usually contains a listing of so-called "complementary user entity control considerations", in other words, what is expected from your organization to have in place to properly living up to your end of the sourcing agreement and be eligible to rely on the SOC 2 results. A weakly organized or loosely controlled client organization cannot expect the cloud service provider to compensate for you. So, if your organization is not up to par, your control weaknesses may be worse than any exceptions in a SOC 2 report. Moreover, it is important to match the SOC 2 controls to these "control considerations" and you own control framework to validate that they are aligned.
- **Opinion and exceptions**: of course, most readers immediately search for a (positive) opinion and any exceptions. This selective perspective may prove its value for the speed-reading C-level executive but may not cater for assessing the impact of any exceptions on their own systems and controls. In some cases, the auditor may report compensating controls, which in place may reduce your risks sufficiently.
- **Audit firm & auditor**: you may want to verify whether the auditor is sufficiently trained, experienced, and adhering to professional standards and guidelines in cloud environments and SOC 2 assurance?
- **Management response**: the service provider may comment on any exceptions, not to downplay them, but to provide more context and remediation activities. In addition, this separate section in the report may be used for indicating other upcoming initiatives. These are "forward-looking statements" and not scrutinized or validated by the auditor, so be cautious that this text is not overly positive wishful thinking!

Based on this listing, it would be beneficial to let the SOC 2 report be reviewed by the responsible (senior) management, the Service Level Manager as well as your internal and external IT auditors.

How do SOC 2 assurance vs. ISO 27001 certification align or differ?

The similarities and differences between IT Assurance and ISO certification are still cause for confusion. Without spending an article on this comparison, we have summarized the main aspects of both in the table below, where we used Security and ISO 27001 as most closely aligned.

Aspects	Regular IT Assurance (ISAE 3000)	SOC 2 Assurance	ISO 27001 Certification
Specific target audience (closed user group)	☑	☑	☒
Standard set of criteria	☒	☑	☑
Additional criteria specific to your organization, sector or cloud services	☑	☑ (SOC 2+ allows additional criteria)	☒
System description	☒ (optional)	☑	☒ (only Statement of Applicability, SoA)
Test of (Information Security) Management System ("Plan-do-check-act" cycle)	☒	☑	☑
Test of Design (Type I) ("Documentation audit")	☑ (all controls each year)	☑ (all controls each year)	☑ (all controls in 3-year cycle)
Test of Operational Effectiveness (Type II) ("Implementation audit")	☑	☑	☒
Standard reporting	☒	☒	☑ (1-pager)
Future-oriented statement	☒ (past ½ - 1 year)	☒ (past ½ - 1 year)	☑ (1 year ahead)
External reporting of exceptions / non-conformities	☑	☑	☒
Amount of (Audit) effort	☒ (high)	☒ (high)	☑ (low)
Providing (reasonable) assurance	☑	☑	☒

The above evaluation matrix is based on [Koor13], which elaborates on the similarities and differences between IT assurance and ISO certification.

In addition to the above comparison, cloud service providers may want to use SOC 2 assurance in addition to ISO 27001 certification to fulfil the requirements of all its clients and prospects. Cloud service providers also have the option to be certified against the ISO 27017 or ISO 27018 standards, an addendum to the ISO 27001.

The ISO 27017:2015 is the "Code of Practice for Information Security Controls" for cloud service providers, the ISO 27018:2014 is the "Code of Practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors".

Similarly, the ISO 27701 standard ("Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management") can be used on top of an ISO 27001 certification for all other environments. The ISO 27701:2019 outlines the Privacy Information Management System (PIMS), which includes controller- and processor-specific controls.

See further the text box on SOC 2 Privacy for details on GDPR assurance.

Can we leverage SOC 2 Privacy for GDPR assurance?

One of the Trust Services Categories focuses on privacy; however, would it suffice for a cloud service provider to prove its GDPR compliance? In short, the answer is "No" for multiple reasons:

- The SOC 2 Privacy category is not (fully) aligned to the GDPR, which is understandable as it was developed some 10 years ago and originated in North America. It also needs to be universally applicable, not specifically tied to any specific legislation. Just like the ISO 27701 (see text box on ISO certification), it contains an appendix in which the privacy controls are mapped against the GDPR principles.
- So far, neither any of the national Data Protection Authorities nor the European Data Protection Board has approved any form of GDPR certification or assurance as stipulated in Articles 42 and 43 of the GDPR. The German Europrise privacy certification is potentially the first eligible to obtain formal European approval.
- Technically speaking, GDPR compliance is by definition impossible to attest to as this European regulation is based on open norms. An SOC 2 Privacy engagement can provide assurance on the privacy controls as designed, implemented and operating, but never state that a process or entire organization is compliant with legislation.

However, you can expand the scope of a SOC 2 Privacy report with an "Additional Subject Matter" to let this so-called SOC 2+ report also include coverage of the delta of missing GDPR-based privacy controls.

A related misunderstanding is that Privacy and Confidentiality categories are overlapping: Confidentiality is distinguished from Privacy in that the latter applies only to personal information, whereas Confidentiality applies to various types of sensitive information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property. While both categories cover the information life cycle of collection, use, retention, disclosure, and disposal, the Privacy category is significantly more extensive, and only addresses personal data. Conversely, the Confidentiality category addresses the cloud service provider's ability to protect information that they designate as confidential, which could include personal data.