THIRD PARTY ASSURANCE REPORTING

System and Organisation Controls (SOC) reports

Putting your customers' minds at rest

Across the globe, organisations are confronted with an increased focus on risks and how they are managed. Not only from an internal - corporate governance - perspective, but also from third-party stakeholders and regulators. Privacy regulations for example have been receiving a lot of (media) attention around the world and more recently there was the introduction of a new **privacy regulation (GDPR)** in the EU which provides for new challenges on how personal data is exchanged with and processed within service organisations.

For their outsourced activities, your customers and other stakeholders want to be reassured that their business and (personal) data is in safe hands and that compliance with applicable regulations (e.g. GDPR) is assured. System and Organisation Control (SOC) reports, also known as Third Party Assurance (TPA) reports, are designed to provide the assurance your customers are seeking. They can address specific concerns such as compliance with privacy regulations, for which a specific SOC2 offering was developed, but also cover a wider context of outsourced processes and activities. It is an efficient solution to meet your client's expectations with the key principle in mind: **assess once, assure many**.

Customer expectations

- *Customers want to be reassured that their business is taken care of and they are not running additional risks, trusting part of their business and data to your organisation.*
- *Providing a SOC report to your customers will significantly **increase customer reliance** and the perceived service professionalism.*

Competitive pressure

- *A SOC report can be used as a commercial argument to complement the service offering to existing and potential customers.*
- *In competitive markets it is a clear strength to be able to **demonstrate the trustworthiness of your services**. Similar to quality certificates, a SOC report is more and more a must-have.*

Compliance with Standards & Regulation

- *Whether you are operating locally or internationally, there are always rules to be complied with (e.g. GDPR) - and **compliance is not optional**.*
- *Our deliverables are in line with the existing standards ISAE 3402 and SSAE 18 (SOC1 - SOC2 - SOC3)*

Fair price and value for money

- *Our assurance reports are affordable, also for smaller organisations. We can realise this through strong organisation, not over-complicating things and a fair pricing of our services.*
- *Benefits include the ability to provide **clear answers to your customers** regarding their assurance needs and on top of that a continuous improvement opportunity for your processes.*

BDO

ASSURANCE FOR YOUR CUSTOMERS

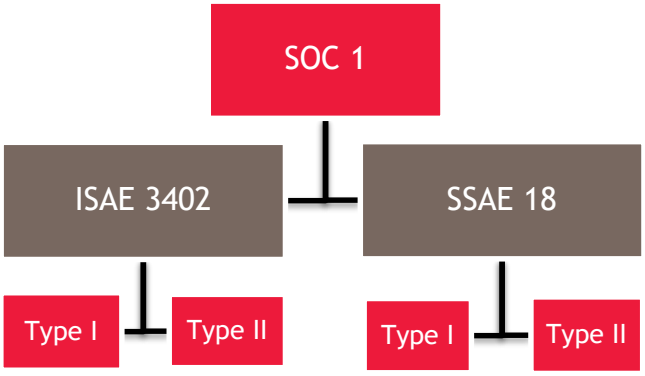
What types of SOC reports exist?

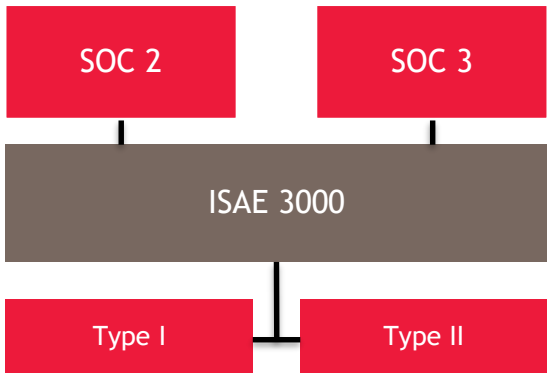
Service Organisation Control reports certify that a service provider has been subject to a profound audit of the services offered by the organisation. These reports are issued by an independent audit organisation (such as BDO), to guarantee the objectivity of the conclusions.

SOC reports can be divided into two major categories

- SOC 1 – these reports are focussed on providing assurance over systems involved with the processing of **financial information**. Our SOC 1 reports are in line with the applicable international standard ISAE 3402 and the US-equivalent SSAE 18.
- SOC 2 and SOC 3 – these reports are focussed on providing assurance over **internal controls related to Information Technology** and typically report on the globally recognised Trust Service Principles (Security, Availability, Confidentiality, Processing Integrity and Privacy) or allow for specific reporting on the Privacy Control Framework published by the NOREA (Privacy Attestation) and on other published frameworks across the globe. Our SOC 2/3 reports are in line with the international reporting standard ISAE 3000.

Schematical overview SOC reports





Assurance over financial information

- ISAE 3402 and SSAE 18 standards are very similar and both can be provided by BDO.
- Type 1 reports are referred to as “point-in-time” assessments covering control design whereas Type II reports cover a “period-of-time” including design and operating effectiveness of controls.
- The scope of the report is determined by the service organisation and varies depending on the type of service provided. Naturally the scope includes processes and controls related to the processing of financial transactions.
- The reports focus on the Accuracy, Completeness, Existance and Valuation of the financial transactions processed by the system.
- In addition relevant ITGCs may be included.

Assurance over controls related to IT

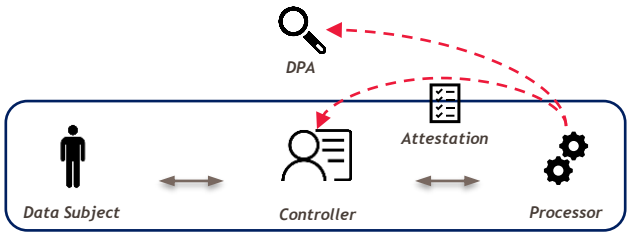
- Similar to ISAE 3402 and SSAE 18 a distinction is made between Type I and Type II reports.
- SOC 2 reports are more detailed compared to the summary level reporting of SOC 3.
- The scope is not limited to systems involved with the processing of financial transactions and is focussed on the Trust Service Principles (covering one or more Principles depending on the needs).
- GDPR compliance can also be demonstrated in the SOC 2 format by reporting over the Privacy Control Framework published by the NOREA.

ASSURANCE FOR YOUR CUSTOMERS

Privacy Attestations

As of the 25th of May 2018 the General Data Protection Regulation (GDPR) has entered into force. In light of this regulation all organisations, including service providers, are confronted with additional requirements when processing personal data.

To **demonstrate compliance with the GDPR**, BDO has developed a SOC2 attestation service offering so that you can reassure your customers and other interested parties that you have an adequate system and processes in place to comply with the regulation.



The framework used as the basis for this attestation was published by the NOREA, the professional association of IT auditors in the Netherlands. The NOREA has been recognised by the Dutch Data Protection Authority (DPA) "De Autoriteit Persoonsgegevens" for their efforts in providing guidance towards the performance of privacy audits in the Netherlands. The recognition of the Dutch DPA, being a key contributor to the evolution of the regulation through the Working Party 29, further accentuates and underlines the acceptance of this framework in the EU.

The value of a SOC report

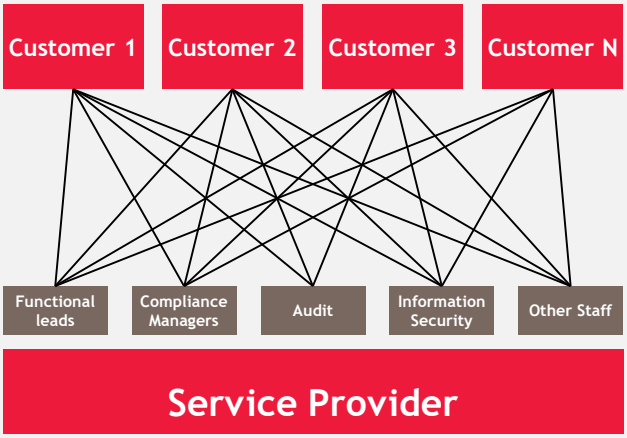
Working with a SOC report minimises the number of requested audits by different customers and their auditors. Less audits means less overhead for your organisation and more time for the business to focus on value generating activities.

Working with BDO, you will find the process to issue a SOC report well controlled and allowing for proper planning.

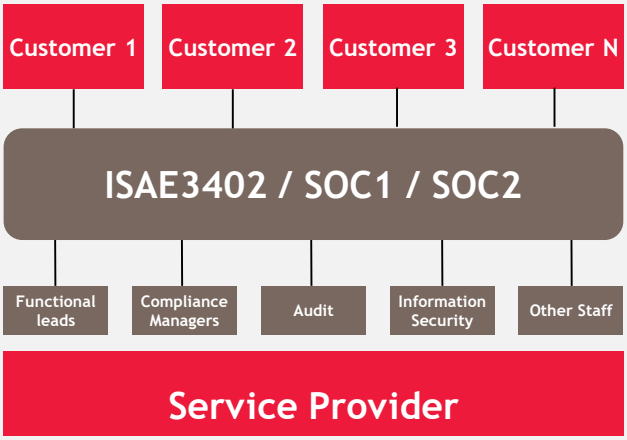
Auditing your services once and using the results to satisfy the needs of many customers, guarantees also a standardisation of the assessment, the representation and communication of the results. Customers will have access to the same information and this will lower the risk of misunderstandings and the need for additional clarifications.

A SOC report puts your organisation in full control and also offers a clear competitive advantage for your organisation.

Situation without SOC report:
separate requests, leading to inefficiencies



Situation with SOC report:
An efficient and standardised approach



ASSURANCE FOR YOUR CUSTOMERS

Our expertise in assurance attestations

Below we provide some examples of organisations for which we already deliver assurance report services.

«Last year BDO took over our ISAE 3402 certification. All work is executed by an experienced team, respecting high quality standards and delivering at a fair price.»

Risk & Compliance Manager

«When BDO took over the ISAE 3402 in 2016 they invested significantly in rationalizing and aligning the report with our organization improving the quality and coverage of the report. All whilst offering a significant fee reduction compared to the previous service auditor»

Chief Operating Officer

«BDO provided us with a clear roadmap and timing of the engagement. Through regular feedback and communication we were able to reach a very efficient collaboration and minimize the overhead on our internal organization.»

Head of Internal Audit

Please contact us for more information

Koen Claessens, Partner
T: +32 497 51 53 83
E: koen.claessens@bdo.be

Steven Cauwenberghs, Partner
T: +32 497 05 12 23
E: steven.cauwenberghs@bdo.be

Christophe Daems, Senior Manager
T: +32 474 90 78 51
E: christophe.daems@bdo.be