PRIVACY ATTESTATIONS

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 in the EU - the **General Data Protection Regulation (GDPR)** - which provides for new challenges on how personal data is exchanged with and processed within service organisations.

As of the 25th of May 2018 the GDPR has entered into force. In light of this regulation all organisations, including service providers, are confronted with additional requirements when processing personal data. Amongst others these include:

- Maintaining a register of processing activities
- Performing Data Protection Impact Assessments for most sensitive and high risk processing activities
- Assessing organisational and technical measures in place to adequately secure (personal) data
- Communicating transparently towards data subjects on the processing of personal information
- Supporting data subjects with the execution and exercising of their rights
- Putting in place processing agreements with (sub) processors where required
- Taking initiatives to increase privacy and information security awareness within the organisation

To demonstrate compliance with the GDPR, BDO has developed a **SOC2 attestation service offering** allowing you to reassure your customers and other interested parties that you have an adequate system and processes in place to comply with the applicable regulations and industry leading practices.

General Data Protection Regulation

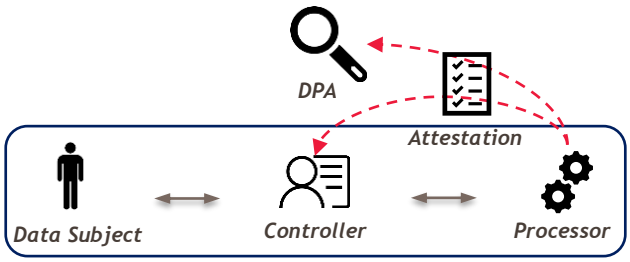
PRIVACY audit proof

BDO

ASSURANCE FOR YOUR CUSTOMERS

SOC2 Privacy Attestations

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 privacy regulations across the globe such as the GDPR is assured. System and Organisation Control (SOC) reports, also known as Third Party Assurance (TPA) attestations, are designed to provide this assurance and report on controls operating within your organisation. It is an efficient solution to meet your client's expectations with the key principle in mind: **assess once, assure many**.



The framework applied as the basis for this attestation is the **Privacy Control Framework** published by the NOREA. More details on the establishment and contents of the framework can be found on the following page.

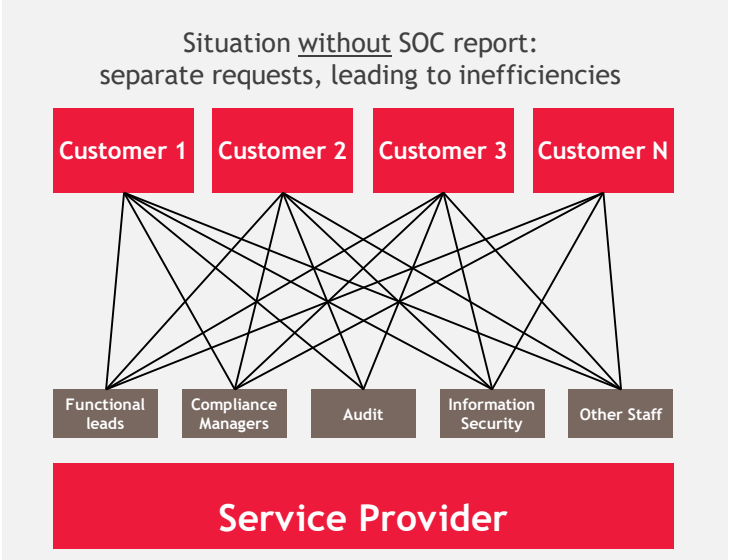
The value of a SOC report

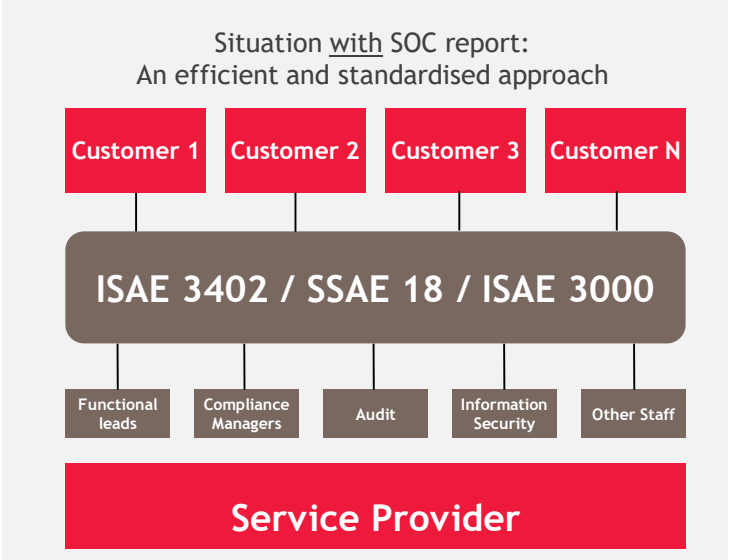
Working with a SOC report minimises the number of requested audits by different customers and their auditors. Less audits means less overhead for your organisation and more time for the business to focus on value generating activities.

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.





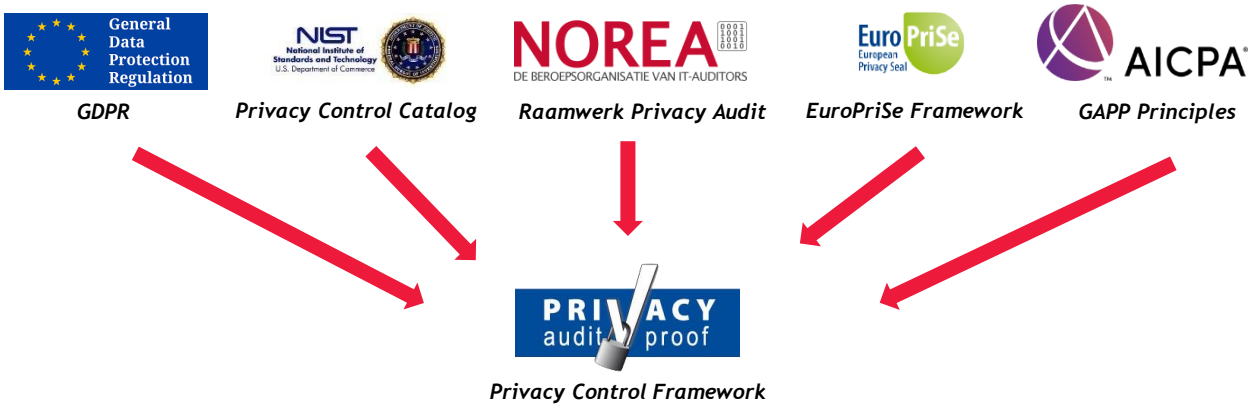
ASSURANCE FOR YOUR CUSTOMERS

Background of the PCF

The framework applied as the basis for this attestation is the Privacy Control Framework (PCF) 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 execution of **privacy audits** in the Netherlands. The recognition of the Dutch DPA, being a key contributor to the evolution of the regulation as a member of the Working Party 29, further accentuates and underlines the acceptance of this framework in Europe and beyond.

The PCF allows independant auditors to issue privacy control reports covering essential requirements in light of the GDPR and is in line with the International Standards on Assurance Engagements (ISAE) 3000. Several sources were considered when constructing the framework and multiple 'leading practice' framework have been integrated:



Contents

The framework contains 9 Lifecycle Management Phases, divided over 32 topics and a total of 104 controls spread over all topics.

Lifecycle phase	Related topics
Management	• Privacy policy; • Roles & Responsabilities; • Personal Data Identification and Classification; • Risk Management; • Data Protection Impact Assessments; • Privacy Incident and Breach Management; • Staff Competences; • Staff Awareness and Training; • Legal Review of Changes in the Environment.
Notice	• Privacy Statement.
Choice and Consent	• Consent Framework.
Collect	• Data Minimisation.
Use, Store and Dispose	• Use Limitation; • Privacy by Default and by Design; • Data Retention; • Disposal, Destruction and Anonymisation; • Use and Restriction.

Lifecycle phase	Related topics
Data Access and Data Quality	• Data Access Requests; • Data Correction Requests; • Data Deletion Requests; • Data Portability Requests; • Accuracy and Completeness of Data.
Disclose	• Third Party Disclosure and Registration; • Third Party Agreements; • Data Transfers.
Data Security	• Information Security Program; • Identity and Access Management; • Secure Transmission; • Encryption and End-point Protection; • Logging of Access.
Monitoring and Enforcement	• Review of Privacy Compliance • Periodic Monitoring on Privacy Controls

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