NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA Guide

Guide to performing SOC2 and SOC 3 based upon ISAE 3000/ Richtlijn 3000A

December 2021

Table of Contents

Table of Contents 2

1 Introduction 4

1.1 Background 4

1.2 Objective 5

1.3 Presumed level of knowledge 5

1.4 Constraints 6

2 System and Organization Control (SOC) Report 7

2.1 Background 7

2.2 Key characteristics of a SOC 2® report 7

2.3 Professional standards 8

2.4 Structure of the SOC 2® report 9

2.5 SOC 3* report 14

2.6 Structure of the SOC 3® Report 15

2.7 Logo 18

3 Conducting a SOC 2® and/or SOC 3® Engagement 19

3.1 Experience and knowledge of service auditor (engagement partner/team) 19

3.2 Independence 20

3.3 Inclusive / carve-out method 20

3.4 Materiality and evaluation of deviations (exceptions) 21

3.5 Types of procedures 24

3.6 Types of conclusions 25

4 Use of a SOC 2® and/or SOC 3® report 27

4.1 Marketing and communication by service organization 28

5 Categories and Criteria 29

5.1 Background 29

5.1.1 Introduction 29

5.1.2 Trust Services Principles 29

5.1.3 Criteria 30

5.2 Privacy 31

5.2.1 Privacy Criteria 32

5.2.2 mapping of the SOC 2® privacy criteria and the Privacy control framework (PCF) 33

5.2.3 Scope of the Privacy Criteria 34

5.2.4 Data Controller vs. Data Processor 35

5.3 Criteria for management statement and SOC 2® assurance report 35

5.3.1 Description Criteria 36

5.3.2 Design Criterion 36

5.3.3 Operating effectiveness Criterion 36

6 SOC 2® and SOC 3® versus other standards 37

6.1 Mapping criteria 37

6.2 SOC 2® and SOC 3® versus ISAE 3402 37

7 Annex 39

7.1 Management Statement 39

7.2 Assurance report SOC 2® 42

7.3 Trust Services Criteria 46

7.4 SOC 3® report – illustration 47

7.5 Key references to guidelines, professional standards, articles and brochures 51

7.6 List of contributors 52

7.7 Mapping Privacy Category – PCF 53

1 Introduction

1.1 Background

This guide (in Dutch: “handreiking”) was developed for Dutch Register IT auditors (REs) to guide them in issuing reports in line with the American Institute of Certified Public Accountants (AICPA) System and Organization Control 2 (SOC 2®) and System and Organization Control 3 (SOC3®) product under the International Standard on Assurance Engagements (ISAE) 3000 or the local equivalent ‘Richtlijn Assurance-opdrachten door IT-auditors’ (3000)[1]. This publication updates previously available guidance to provide further guidance for a specific type of ISAE 3000 engagements. Although we realize that to effectively use this guide requires a high level of professional expertise, the guide can also be useful for the users of service organization control reports or user entities who may consider asking the service organization for a SOC 2® report and a SOC3® report.

This guide is in response to the increasing number of requests from IT service providers for SOC 2® reports and SOC 3® reports and the expected adoption of these kinds of reports in the Netherlands. SOC 2® is not a standard, but it is a specific implementation of the US general attestation standard AT-C 205. This guide provides guidance on how to produce this type of report based on the ISAE 3000 standard. This approach avoids the requirement for the Dutch practitioners to work under US regulations and standards. From a professional perspective, the practitioner issues an ISAE 3000 report. For local use, instead of ISAE 3000, the practitioner can refer to the local equivalent of ISAE 3000: ‘Richtlijn Assurance-opdrachten door IT-auditors’ (3000)’. The SOC 3® report is a brief report describing the same engagement as the SOC 2,® but which has a wider distribution.

The structure of a SOC 2® report follows the format of ISAE 3402 (in the US SSAE 18 / AT-C section 320, referred to as SOC 1®) and the scope of the TSP Section 100. The format and scope are further elaborated in the AICPA guide Reporting on Controls at a Service Organization, relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®).

Engagements performed based upon this guide are subject only to Dutch law and regulations, including the NOREA regulations. These Dutch engagements cannot refer to any US laws or attestation standards including AT-C 205. To clarify that the report is produced under Dutch standards, laws and professional regulations the report is named for international use **ISAE 3000**

[1] Where in this guide reference is made to ISAE 3000 such may also be replaced with ‘Richtlijn Assurance-opdrachten door IT-auditors’ (3000)’. For the readability of this guide no double references have been used.

/ **Service Organization Control Report** and for national use **Richtlijn 3000 / Service Organization Control Report.** The name of the SOC 2® and SOC 3® terms are allowed to be included on the front page of the report.

1.2 Objective

The guide focuses on the support of Dutch practitioners in the implementation of reporting against the Trust Services Criteria in practice. The guide details the contents of SOC 2® and SOC 3® and how the requirements regarding the Trust Service Criteria may be implemented. Additionally, guidance is given for drafting the reports.

Although it is not the objective of this guide, it also provides guidance to determine which kind of assurance report best fits the service organization's or user entity's needs in a specific situation:

ISAE 3402 – report for service organizations who require assurance over the controls which may be relevant for the user entity's financial reporting

SOC 2® and SOC 3® – reports for IT service organizations who require assurance on controls related to some or all of Security, Availability, Processing Integrity, Confidentiality, and Privacy.

SOC 2® and SOC 3® reports focus – in line with an ISAE 3402 report – on the control environment and internal controls of a service organization and therefore do not provide assurance regarding the actual outcome of the process (e.g. the achievement of key performance indicators (KPIs) in service level agreements (SLAs)).

We decided to publish this guide in English to avoid any misunderstanding caused by translation from the original US documents. We emphasize that this publication is only intended for use by Dutch practitioners.

1.3 Presumed level of knowledge

Knowledge of the ISAE 3000 and ISAE 3402 frameworks for assurance engagements is required to understand and apply this guide. Reference to the assurance framework / standards has only been included if it is necessary to place the guide in the right context. The guide will not include the details of ISAE 3402, the AICPA SOC 2® guide or the Trust Services Criteria (referred to as TSP section 100). To deliver an ISAE 3000 / Service Organization Control Report, the guide assumes that the practitioner is familiar with the most recent versions of the publications mentioned.

1.4 Constraints

If a SOC 2® or SOC 3® report is published under US laws and regulations (including AT-C 205), the service auditor's opinion must be signed by a CPA who is a member of the AICPA or an individual who holds an equivalent professional certification.

The AICPA has developed logos that may be used in conjunction with a SOC 2® or SOC 3® report. The definition of a local equivalent of such a logo is also not part of this guide. For further details see chapter 2.7.

2 System and Organization Control (SOC) Report

2.1 Background

A SOC report provides assurance, through an independent service auditor's opinion, over the controls in scope of the service organization's report. The AICPA distinguishes three types of reports regarding service organizations:

- A SOC 1® report: a report based on SSAE 18 / AT-C 320, the US implementation of the ISAE 3402 standard[2] and is restricted to use only for financial reporting purposes;
- A SOC 2® report: a report based on the AT-C 205 standard, which is more or less the US equivalent of ISAE 3000 in the Netherlands. It reports on one or more of the trust services principles, being security, confidentiality, integrity, availability and privacy, using criteria defined in the standard.
- A SOC 3® report: a short form report based on the work supporting a SOC 2® report but made available for a more generic audience

This guide describes and concerns the Dutch equivalent of SOC 2® and SOC 3® under the standards and regulations applicable to the registry of IT auditors affiliated to NOREA.

2.2 Key characteristics of a SOC 2® report

As a NOREA System and Organization Controls report is based on ISAE 3000, it is important to realize and recognize the following key characteristics of the ISAE 3000 / Service Organization Control report, as a SOC report differs from ISAE 3402 or other ISAE 3000 reports:

- The structure of the report is similar to the ISAE 3402 reports (please also refer to 2.4);
- Only reasonable assurance can be provided in the opinion (contrary to ISAE 3000, which also allows for limited assurance);
- There are pre-defined principles and criteria (TSP section 100) to include in the report (each service provider can choose its own control activities to meet the criteria, however control matrix mappings with common control frameworks are available). In the TSP Section 100, 'Points of Focus' are included with the control objectives. The Points of

[2] For completeness purposes please note that a SOC 1® report under the rules and regulations of the AICPA is based on the Statement on Standards for Attestation Engagements no. 16 (SSAE 16) standard referring to AT 801 (which in itself is the US implementation of the ISAE 3402 standard).

Focus give examples of certain topics which may need to be implemented as internal controls at a service organization. The Points of Focus provide details regarding the important and minimal characteristics of each Trust Services Criteria and help the service organization and the auditor address important elements when identifying internal controls at the service organization, and to provide greater consistency between reports. The Points of Focus are not to be included in the report. The Points of Focus are explicitly not a checklist, do not need to be addressed completely and only serve as a guideline for the service organization and the auditor;

- There are type I and type II reports;
- Contrary to ISAE 3402, there is no minimum review period. However, a minimum reporting period of three months for a meaningful type II report is advised;
- As is the case with an ISAE 3402 report, the report of the service organization must include a description of the system, in line with the Description Criteria 200;
- The intended users of an ISAE 3000 / Service Organization Control report are users who can understand the report's content and its purpose. Report users who are most likely to have such knowledge include:
    - The management of the service organization,
    - The management of the user entities,
    - Prospective users that have gained such knowledge in performing due diligence who intend to use the information contained in the report as part of their vendor selection process or to comply with regulatory requirements for vendor acceptance,
    - Practitioners and accountants evaluating or reporting on controls at a user entity, and
    - Regulatory bodies.

The reports are not intended to be available for the public and as such, may not be published on websites or other public means (please also refer to section 4).

2.3 Professional standards

The AICPA guide provides performance and reporting guidance for an examination of a service organization's description of its system and controls that are relevant to the security, availability, or processing integrity of a service organization's system or the confidentiality or privacy of the information processed by the system. Such an engagement is known as a SOC 2® engagement, and a report on such an engagement is known as a SOC 2® and/or SOC 3® report.

The SOC 2® and SOC 3® reports are based upon the AT-C 205. AT section 101 applies to engagements in which a practitioner is engaged to report on an examination on subject matter. The international equivalent of AT section 101 is ISAE 3000. This standard deals with assurance engagements in which a practitioner aims to obtain sufficient and appropriate evidence in order to express a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the subject matter information (that is, the outcome of the measurement or evaluation of an underlying subject matter against criteria). ISAE 3000 is an international equivalent of AT-C 205.

This guide is based upon the ISAE 3000 (and the Dutch Richtlijn 3000A), an assurance standard which contains the following characteristics:

- The underlying subject matter (i.e., the description of the service organization system and related internal controls) is appropriate;
- The criteria to be applied in the preparation of the subject matter information are suitable for the engagement circumstances;
- The criteria that the practitioner expects to be applied in the preparation of the subject matter will be available for the intended users;
- The practitioner expects to be able to obtain the evidence needed to support the practitioner's conclusion;
- The practitioner's conclusion, in the form of a reasonable assurance engagement, is to be contained in a written report;
- A rational purpose (i.e. it serves a purpose for the intended user organization(s))

The text in this guide refers to ISAE 3000 as it is the source for the Dutch NOREA Richtlijn and is recognized outside the Netherlands.

2.4 Structure of the SOC 2® report

To comply with ISAE 3000 and to classify as the equivalent of SOC 2® the title page contains the following:

[*Name of the service organization*]
[*Short description of the service*]
[*Date of the report in case of a type I report*]
[*The reporting period in case of a type II report*]

SOC 2® Report

Relevant to Security [followed by one or more principles: Availability, Processing Integrity, Confidentiality and/or Privacy].

The table of content generally includes the following elements:

Section I: Management statement[3]
Section II: Independent service auditor’s assurance report
Section III: Service organization’s description of its system
Section IV: The principles, criteria and tests performed by the independent service auditor including the outcome of the tests (this is optional in a type I report).
Section V: Other information provided by the service organization that is not covered by the service assurance report examination. This section is optional.

Below each of the sections is described in more detail.

Section I Management Statement

The written statement by management of the service organization includes the following aspects:

- Management’s description of the service organization’s system fairly presents the service organization’s system that was designed and implemented as of a specific date or throughout the specified period (type I and type II respectively), based on the criteria in [refer to the chapter, paragraphs or page numbers];
- The controls stated in management’s description of the service organization’s system were suitably designed to meet to the applicable criteria (TSP section 100) as at a specific date or throughout the specified reporting period (type I and type II respectively);

[3] The service organization’s “statement” is equivalent to the service organization’s “assertion” as defined under AICPA SOC 2® guidance

- The controls stated in management's description of the service organization's system operated effectively throughout the specified period to meet the applicable criteria (TSP section 100) (type II report).

An example is given in the Annex.

Section II Independent service auditor's assurance report

The service auditor's report in both the type I and II reports contains the following aspects:

- Use of the word 'independent' in the title of the section containing the assurance report
- Scope of the engagement (including subservice organizations, user entity control considerations and / or other information)
- The comment that management is responsible for the description of the service organization's system;
- The comment that the engagement is performed in agreement with **ISAE 3000**, and for Dutch use in agreement with **Richtlijn 3000A.**
- The opinion:
    - Fairness of the description
    - The suitability of the design of controls; and
    - In a type II report, the operating effectiveness of the controls.

An example of the report is included in the annex, which is based upon Appendix H of SOC 2® *Reporting on an Examinations of Controls at a service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy*.

Section III Service organization's description of its system

The components of the system description as required are as follows:

- The types of services provided;
- The main service commitments and system requirements;

- The components of the system necessary for the provision of the service, consisting of:
    - Infrastructure: The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunication networks);
    - Software: The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
    - People: The personnel involved in the governance, 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).
- In the case of identified incidents which are the consequence of (a) internal controls that were not appropriately designed or did not operate effectively or (b) which have led to a significant inability to achieve one or more of the service commitments, the following information must be reported:
    - A description of each incident;
    - The timing of the incident;
    - The scope (or the effect) of the incident.
- The applicable criteria and any related internal controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.
- If applicable, the necessary Complementary User Entity Controls (CUECs) to achieve service commitments and the system requirements;
- If the use of a sub-service organization and the internal objectives of the sub-service organization are necessary to achieve the objectives of the service organization, the following:
    - When the inclusive method is applied:
        - A description of the services provided by the service organization;
        - The necessary internal controls of the sub-service organization to achieve the objectives of the service organization;

        - Relevant aspects of the infrastructure, software, people, procedures and data of the sub-service organization;
        - Relevant parts of the systems that are the responsibility of the sub-service organization.
    - When the carve-out method is applied:
        - A description of the services provided by the sub-service organization.
        - Each of the trust service criteria which need to be achieved through the internal controls of the sub-service organizations.
        - The internal controls that need to be implemented by the sub-service organization achieve the objectives of the service-organizations.
- Any of the trust service criteria that is not relevant for the system and the reason why the criteria are indicated are not relevant.
- If the case of the Type II report, the relevant details of the significant changes to the system and the internal controls of the service organizations during the examination period.

In addition to these specific requirements that are unique for IT service organizations, the following relevant aspects of the control environment include:

- Control Environment (i.e., management philosophy, security management, security policies, personnel security, physical security and environmental controls, system monitoring, problem management, data back-up and recovery, system account management));
- Risk Assessment process;
- Information and Communication systems;
- Monitoring of controls.

Section IV The principles, criteria, related controls, tests of controls including conclusion

Section IV typically contains the principles and the associated criteria, the service organization control activity, the test approach, and the test results per criteria. The principles and criteria are defined by the trust service principles chosen by the service provider, the control activities supporting the criteria are those operated by the service organization, and the test approach and test results are those performed the service auditor. Note that including the description of tests of controls and the test results is part of a type II report. It is optional for type I reports to include the results of the evaluation of the suitability of the design.

Section V Other information provided by the service organization which is not assessed by the service auditor.

The content of this section does not have pre-determined characteristics and is optional. Also, this section is not a part of the scope of work of the service auditor; however, its contents cannot contradict to the scope of the report or work performed by the service auditor. It is the responsibility of the service auditor to confirm this. The service organization may wish to include this information if it is deemed appropriate. The following are examples of such information:

- Future plans for new systems applicable to the user entity or system;
- A plan to remediate any exceptions noted in the report;
- Responses from management to exceptions identified by the service auditor when such responses have not been subject to procedures by the service auditor;
- Other services provided by the service organization that are not included in the scope of the engagement, such as business continuity related controls.

However, section V may not contain material that denies any observations or conclusions of the auditor. In addition, the content needs to be related to the subject matter.

2.5 SOC 3® report

A SOC 3® report has the same scope as a SOC 2® report. However, to publish a SOC 3® report, it is explicitly required that this is a report without any relevant exceptions (unqualified opinion). A SOC 3® report is a brief report compared to the SOC 2® report. The objective of the report is broader publication compared to the SOC 2® report. The SOC 3® report is allowed to be publicly distributed, for example on the website of the service organization.

The NOREA System and Organization Control Report which applies SOC 3® will, similar to the SOC 2® report, be performed based on ISAE 3000. However, the report which contains SOC 3® has a different layout then the report which contains SOC 2®. Similarities are that the report contains a management statement, an independent service auditor's report and a description of the system. The most important characteristics and requirements of the report are mentioned below:

- The structure of the report is in line with the guideline as stated in 'SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.'
- Only an unqualified opinion based on reasonable assurance is possible for a SOC 3® report. This is contrary to Richtlijn 3000A, which also offers the option to provide an opinion based on limited assurance.
- The report is based on the TSP section 100 defined scope and criteria. The principles (categories) determine the criteria (objectives). The service organization can decide which internal controls are applicable to these principles. In the TSP Section 100 'Points of Focus' are included with the control objectives. The Points of Focus give examples of certain topics which may need to be implemented as internal controls at a service organization. The Points of Focus are explicitly not a requirement and only serve to provide details regarding the important and minimal characteristics of each Trust Services Criteria and support the service organization and the auditor to address important elements when identifying internal controls at the service organization, and to provide greater consistency between reports. The Points of Focus are not to be included in the report. The Points of Focus are explicitly not a checklist, do not need to be addressed completely and only serve for the purpose of a guideline for the service organization and the auditor;
- Only type II reports are allowed;
- Contrary to Richtlijn 3402 there is no minimum period of review. However, it is advised to cover at least 3 months.
- The report must contain a description of the system. The description is a brief version compared to the description of the SOC 2 report.
- Contrary to Richtlijn 3000A, where the report can only be distributed within a small circle, this report has no limitation to its distribution.

2.6 Structure of the SOC 3® Report

To comply with ISAE 3000 and at the same time indicate that the report is an equivalent of SOC 3®, the title page includes:

[*Name of the service organization*]
[*Short description of the service*]
[*The reporting period*]

SOC 3® Report

Relevant to Security [Followed by one or more categories: Availability, Process Integrity, Confidentiality and Privacy].

A typical table of contents of a SOC 3® report includes:

Section I: Management statement
Section II: Independent service auditors’ assurance report
Section III: Service organization’s description of its system

Below, these sections are explained.

Section I Management statement

The written statement by management of the service organization includes the follow aspects:

- Management’s description of the service organization’s system fairly presents the service organization’s system that was designed and implemented throughout the specified period, based on the criteria in [refer to the chapter, paragraphs or page numbers].
- Management states, per category in scope (Security, Availability, Processing Integrity, Confidentiality and/or Privacy), that sufficient controls are in place to achieve the control objectives stated per category.
- The controls stated in management’s description of the service organization’s system were operated effectively to meet to the applicable trust services criteria (TSP section 100) throughout the specified reporting period;
- The management states that the internal controls have operated effectively if users implemented Complementary User Entity Control and these controls have operated effectively throughout the reporting period.

An example of the report is included in the annex.

Section II Independent service auditor’s assurance report

The section contains the following aspects:

- Use of the word ‘independent’ in the title of the section containing the assurance report;
- Scope of the engagement (including subservice organizations, user entity control considerations and / or other information);
- The comment that management is responsible for the description of the service organization’s system;
- The comment that the engagement is performed in compliance with **ISAE 3000**, and for Dutch use compliant with the **Richtlijn 3000A;**
- The opinion.

Examples of the report are included in the annex.

Section III Description of the boundaries of the system

The section contains at least the following components:

- Background of the system:
  - Service scope;
  - Boundaries of the system;
  - Subservice organizations
- An overview of the system which at least includes:
  - Infrastructure: The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunication networks);
  - Software: The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
  - People: The personnel involved in the governance, 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).

- Processes and procedures
- Internal control, this section at minimum includes:
    - Control Environment;
    - Risk Assessment;
    - Controls;
    - Information and Communication systems;
    - Monitoring of controls.
- Complementary user entity controls
- Complementary subservice organization controls

The section may not contain any information that may conflict with the observations or opinion of the auditor. Additionally, the content needs to be related to the subject matter of the report.

Contrary to the SOC 2® report, the SOC 3® report doesn't contain any information regarding the controls and the activities and the conclusion of the independent service auditor.

2.7 Logo

The AICPA has developed a logo[4] that may be used or displayed by a service organization provided it has had at least one of the three SOC reports issued by a licensed CPA and based on the AICPA standards. A service organization can promote its service organization's assurance through System and Organization Control reports by using these print- and web-ready logos.

A key requirement is that the System and Organization report is based on the AICPA standards. In the situation where a System and Organization Control report is based on ISAE 3000 (or the local equivalent), it will not comply with the requirements as determined by the AICPA. NBA and / or NOREA do not have a Dutch equivalent for such logos.

Please refer to chapter 4 of this guide for further considerations on marketing and promotion of a SOC 2® and/or SOC 3® report.

[4] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SOCLogosInfo.aspx

3 Conducting a SOC 2® and/or SOC 3® Engagement

A SOC 2® and/or SOC 3®engagement is performed according to the professional standards as described in paragraph 2. In order to perform a SOC 2® and/or SOC 3® engagement, the size and the maturity of the service organization should be at a sufficient level to be successful. Several key points to address when performing a SOC 2® and/or SOC 3® engagement are included in the following sections.

3.1 Experience and knowledge of service auditor (engagement partner/team)

There are two main requirements for accepting or continuing a SOC 2® and/or SOC 3® engagement by a service auditor: (1) “The practitioner accepts (or continues where applicable) an assurance engagement only if the practitioner is satisfied that those persons who are to perform the engagement collectively possess the necessary professional competencies.”; and (2) “The practitioner plans the engagement to execute the activities as efficiently as possible.”

ISAE 3000 requires the engagement personnel to have both a general knowledge and sufficient process, technical, industry, and reporting knowledge. Tasks are assigned to personnel based on their level of knowledge, skill, and ability so personnel can form a conclusion based on the audit evidence.

The practitioner should have adequate knowledge of the subject matter. A practitioner may obtain adequate knowledge of the subject matter through formal or continuing education, including self-study, or through practical experience. However, it is not necessary for a practitioner to personally acquire all of the necessary knowledge of the subject matter to be qualified to express a conclusion. In some instances, the service auditor may determine that he or she does not possess sufficient knowledge or experience with certain aspects of the engagement. This knowledge requirement may be met, partly, through the use of one or more specialists, if the practitioner has sufficient knowledge of the subject matter to communicate to the specialist the objectives of the work and to evaluate the specialist’s work to determine if the objectives were achieved.

The practitioner obtains a sufficient understanding of the field of expertise in order to determine the nature, scope, and objectives of the work of the auditor’s specialist for the auditor’s purposes, and to evaluate the adequacy of that work for the auditor’s purposes. Following the Code of Ethics[5] the chartered accountant and the IT auditor need to always maintain their

[5] Reglement gedragscode Register IT-auditors (NOREA) and Verordening gedrags- en beroepsregels accountants (NBA)

professional knowledge and skills at the required level. For example when issuing a SOC 2® and/or SOC 3® report for a data center, it is unlikely that a chartered accountant (with no IT knowledge) would issue a SOC 2® and/or SOC 3® report without the use of an IT auditor.

Furthermore, it is important for the service auditor to obtain an understanding of the services provided by organizations identified as subservice organizations by management of the service organization in order to determine whether controls at those organizations affect the service organization's ability to achieve the relevant trust services criteria and assess whether management has made an appropriate decision about whether these organizations are subservice organizations (refer to paragraph 3.3).

3.2 Independence

The practitioner follows the applicable professional independence rules. These are at minimum the gedragscode register IT auditors of NOREA[6]. For auditors contracted by accounting firms, the VIO ('Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten') of NBA may be applicable.

3.3 Inclusive / carve-out method

It is important for management of the service organization to determine whether controls over the functions performed by an organization from which it has contracted services are needed to meet one or more of the TSP section 100. If so, the contracted service organization is considered a subservice organization. It is important that all subservice organizations are identified as soon as possible during the planning phase of the examination in order to effectively plan the SOC 2® and SOC 3® engagement.

After identification of the subservice organizations the way to treat a subservice organization in a report needs to be defined. Either an inclusive or carve-out method can be used. The choice made is the responsibility of the service organization. It is the responsibility of the service auditor to review the suitability of the service organization's decision as documented in the SOC 2® and/or SOC 3® engagement.

If the service organization uses the inclusive method to present the subservice organization, the description includes all of the elements identified as they relate to the subservice organization

[6] Although the Code of Ethics of NOREA does not include detailed requirements for independence, one of the fundamental principles is Objectivity 'to not allow bias, conflict of interest or undue influence of others to override professional or business judgments' which is the fundamental principle for independence.

Security, Availability, Processing Integrity, Confidentiality, or Privacy[7]. Although these relevant aspects would be considered as a part of the service organization's system, only the portion of the system (including the related controls) that is attributable to the service organization is separately identified. Also, a management statement by the management of subservice organizations related to the service delivered is part of the report.

If the service organization uses the carve-out method to present the subservice organization, this should be sufficiently justified in the SOC 2® and/or SOC 3® report (service auditor's opinion). The service auditor considers whether this engagement is rational (as defined by the Code of Ethics) given this carved-out situation.

The description of the service organization's system identifies the following:

- The nature of the service provided by the subservice organization.
- Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, either alone or in combination with controls at the service organization.
- The types of controls expected to be implemented at carved-out subservice organizations that are necessary to meet the applicable TSP 100, either alone or in combination with controls at the service organization.

The management statement as well as the auditor's opinion mention the subservice organization and the way it is handled in the SOC 2® and/or SOC 3® report (inclusive or carved out).

Frequently, vendors are considered as a subservice organization. However, if the service organization covers the risk and controls in scope and is responsible for these there may not be a need to treat the vendor as subservice organization. Examples include technical engineers, and in some instances, landlords of data centers. When a subservice organization is relevant it is necessary to add monitoring controls that provide assurance about the operating effectiveness of the controls executed by the subservice organization during the report period.

3.4 Materiality and evaluation of deviations (exceptions)

An audit is performed with a certain tolerance level regarding exceptions, also known as materiality. The decisive factor is whether an exception is likely to influence decisions made by users of the report. Materiality in the context of procedure-based assurance reports applies to the system in scope of the report (qualitative materiality) and not to financial disclosure of user entities. When planning and performing a SOC 2® and/or SOC 3® engagement, the service auditor considers materiality with regard to: (1) the fair presentation of the description, (2) the suitability of the design of controls, and, in the case of a type 2 report (3) the operating effectiveness of controls. In evaluating materiality, the service auditor should remember that the intent of the report is to meet the common information needs of a broad range of user entities and their auditors who have an understanding of the manner in which the system is used. The basis for evaluating materiality is whether a typical user entity or their auditor would change their actions had they been made aware of the exception.

The description of the system includes the significant aspects of the processing of significant transactions, should not omit or distort relevant information, and only includes controls designed to provide reasonable assurance that the criteria would be achieved.

In establishing and concluding on materiality, the following factors are considered, including:

- The complexity of the process supported by the controls.
- The inherent risk of the process to fraud and error.
- Tolerable and observed rates of exceptions.
- Nature and cause of observed exceptions.

Initial consideration of materiality is documented by the service auditor and forms a base for a preliminary conclusion on the sufficiency of the criteria and the planned tests based on the understanding of the service organization’s system.

At the conclusion of the procedures performed, the materiality is re-evaluated based on the results of tests.

The service auditor evaluates the results of tests of controls. In evaluating the results of tests, the service auditor investigates the nature and cause of any identified exceptions and determines whether the testing performed provides an appropriate basis for concluding that the control did not operate effectively throughout the specified period.

Once the service auditor has analyzed the control exceptions, the service auditor determines its impact on the achievement of the criteria, individually and in aggregate. Exceptions will fall into the following four categories, and considerable judgment will often be required in determining the appropriate category:

- Exceptions that are clearly inconsequential and would be unlikely to affect the nature, timing, or extent of the criteria in scope. If so, the testing that has been performed provides an appropriate basis for concluding that the control operated effectively throughout the specified period.
- Exceptions that do not result in the evaluation of the control as ineffective but that may be considered relevant to a user; relevance is determined based on whether the service auditor believes that the exception could affect the nature, timing, or extent of the principle(s) in scope.
- Exceptions that require additional testing of the same control or other controls designed to meet the same criterion to reach a conclusion about whether the other controls related to the criterion in aggregate operated effectively throughout the specified period.
- Exceptions that result in the conclusion that the control did not operate effectively throughout the specified period, resulting in the evaluation of the control as ineffective.

Clearly inconsequential exceptions (not relevant) are those exceptions that would be unlikely to affect the user organization or user assessment of internal control. Often these result from the failure of a control to address a unique or minor difference in the environment or only result in a minimal increase in control risk due to other environmental factors. The service auditor discloses all exceptions. There is no materiality level: all exceptions are factually described in the results for tests of controls. The service auditor must determine if each criterion supported by the control(s) with exceptions is met. This is done based on quantitative and qualitative materiality levels and the noted control exceptions.

Exceptions noted by the service auditor, or a modified opinion in the service auditor's report, do not automatically mean that the service auditor's report will not be useful to the report user in assessing the risks of material misstatement. Rather, the user of the report uses that information to determine the effect of the service organization's controls that were not operating effectively, if any, on the user entity's financial statements as a basis for assessing risk.

NB: An engagement aimed at resulting in a SOC 3® report may only be completed in case no exceptions have been noted which are of such impact that criteria are not achieved. A SOC 3® report may only be published in case of an unqualified opinion.

It is important for the service auditor to include sufficient detail in the description of the exceptions identified in tests of controls to enable the user of the report to gain an understanding of what the deviation was and how it occurred. The user would gain such an understanding by having the following information about the exception:

- The control that was tested.
- Whether a sample of items or the total population was selected and tested.
- The nature of the test performed.
- The number of items tested.
- The number and nature of the exception.
- The cause of the exception.

If exceptions in tests of controls have been identified, it may be helpful to users of the report for management to disclose, to the extent known, the causative factors for the exceptions, the controls that mitigate the effect of the exceptions, corrective actions taken, and other qualitative factors that would assist users in understanding the effect of the exceptions. Such information may be presented in the optional section of the type 2 report titled "Other Information" Information in this section is not covered by the service auditor’s report.

If management’s responses to exceptions in tests of controls are included in the description of the service organization’s system (rather than in the section of the type 2 report containing information that is not covered by the service auditor’s report), the description of the applicable control and related criterion are usually included as well. In that case, the service auditor determines, through inquiries in combination with other procedures, whether there is evidence supporting the action described by management in its response. If the response includes forward-looking information, such as future plans to implement controls or to address exceptions, such information is included in the section "Other Information".

3.5 Types of procedures

Tests of the operating effectiveness of controls will be designed to cover each of the controls which are designed to achieve the specified criteria. Tests of the operating effectiveness include such tests as considered necessary in the circumstances to evaluate whether controls, and the extent of compliance with them, is sufficient to provide reasonable, but not absolute, assurance that the specified criteria were achieved during the audit period.

In selecting particular tests of the operating effectiveness of controls, the service auditor considers the nature of the controls being tested, available documentation, the criteria to be achieved, and the expected efficiency and effectiveness of the test. Such techniques will be used to evaluate the fairness of the description of controls and to evaluate the operating effectiveness of specified controls. The test procedures performed to determine the operating effectiveness of controls are described below. In evaluating the operating effectiveness of controls, often a combination of test procedures is used. In many cases a combination is made.

Test procedure	Description
Inquiry	Interview appropriate personnel regarding the relevant controls
Observation	View the application of specific controls
Inspection	Read documents and reports that contain an indication of performance of the control. This includes, among other things, reading of (management) reports to assess whether the specified control is properly monitored, controlled and resolved on a timely basis.
Re-performance	Re-perform the operation of a control to ascertain that it was performed correctly

ISAE 3000 provides more background on performing tests on the design of controls.

A SOC 2® and/or SOC 3® report is not intended to report on the output of controls or systems. However, the service auditor can decide to use tooling or data analysis techniques to test the output of controls. Please note that those procedures are always performed in relation to test procedures supporting the operating effectiveness of controls and should achieve sufficient coverage of testing performed.

3.6 Types of conclusions

An example of the assurance report has been included in the annex.

If the service auditor's conclusion is modified, the service auditor's report contains a clear description of all the reasons for the modification. If the service auditor concludes that:

- Management's description of the service organization's system is not fairly presented, in all material respects.
- The controls are not suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated as described.

- In the case of a type II report, the controls did not operate effectively throughout the specified period to meet the applicable trust services criteria stated in management's description of the service organization's system.
- A scope limitation exists, resulting in the service auditor's inability to obtain sufficient appropriate evidence.
- Management's written statement does not provide sufficient detail, fails to disclose deficiencies identified by the service auditor that resulted in a qualified opinion, or contains inaccuracies and management refuses to amend its statement to reflect the identified deficiencies. Please note that the management's written statement should be in line with the assurance-report.
- Other information that is not covered by the service auditor's report is attached to the description or included in a document containing the description and the service auditor's report, contains material inconsistencies, such as an apparent misstatement of fact, and management refuses to correct the information.

When determining whether to modify the service auditor's report, the service auditor considers the individual and aggregate effect of identified exceptions in management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls throughout the specified period. The service auditor considers quantitative and qualitative factors, such as the following:

- The nature and cause of the exceptions.
- The tolerable rate of exceptions that the service auditor has established.
- The pervasiveness of the exceptions (for example, whether more than one criterion would be affected).
- The likelihood that the exceptions are indicators of control deficiencies that will result in failure to meet the applicable trust services criteria.
- The magnitude of such failures that could occur as a result of control deficiencies.
- Whether users could be misled if the service auditor's opinion were not modified.

If the service auditor decides that his or her conclusion should be modified, the report should contain a clear description of all the reasons for the modification. The objective of that description is to enable report users to develop their own assessments of the effect of deficiencies and exceptions on users. If a modified opinion is appropriate, the service auditor determines whether to issue a qualified opinion, an adverse opinion, or a disclaimer of opinion.

In the case of a qualified, adverse or disclaimer of opinion, a SOC 3® report will not be valid and may not be published.

4 Use of a SOC 2® and/or SOC 3® report

Unlike ISAE 3402 reports, the primary users of SOC 2® and/or SOC 3® reports generally are not user entity auditors but management of the service organization and management of the user entities (and prospective users and regulators). A SOC 2® and/or SOC 3® report is intended to assist management of the user entities in carrying out their responsibility for monitoring the services provided by the service organization. For example, controls at a service organization that provides Internet-based storage of a user entity's back-up of proprietary information and trade secrets is unlikely to be of significance to the user entity's financial statement auditor. However, management of the user entity may be particularly concerned about the security, availability and confidentiality of their backed-up information.

The SOC 2® and/or SOC 3® reports also may be useful to a user entity's auditor, as some controls included in the SOC 2® and SOC 3® report may be relevant to user entities' internal control as it relates to financial reporting. It is the responsibility of the user entity's auditor to assess to what extent such SOC 2® and SOC 3® reports are relevant and useful for their financial statement audit, as the primary purpose and scope for the SOC 2® and SOC 3® differs from an ISAE 3402 report.

A SOC 2® report has the potential to be misunderstood when taken out of the context in which it was intended to be used. Accordingly, the service auditor's report is intended solely for the information and use of management of the service organization and other specified parties who have sufficient knowledge and understanding of the following, prospective users, regulators:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- The applicable criteria (Trust Services Criteria).

- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

Report users who are most likely to have such knowledge include:

- The management of the service organization
- The management of the user entity.
- The management of parties considering in the nearby future to use the services of the service organization.
- Practitioners whom form an opinion or report about the controls.
- Regulatory bodies.

The SOC 2® report is not intended to be used by anyone other than these specified parties. The SOC 3® report is a report with an unlimited distribution circle and is therefore, for example, allowed to be shared on the website of the service organizations.

4.1 Marketing and communication by service organization

As the SOC 2® report is for the intended users only, it is not allowed to make a generic statement that the 'internal control system' has been audited and approved by an independent practitioner, that a Service Organization Control report or certificate is obtained, or other unsubstantiated claims like: "the service organization has an internal control system of high quality". Such statements are incorrect, could be misinterpreted and/or are misleading to intended users. It is the duty of the practitioner to address this with the service organization if such statements are made.

A service organization may explain on their website the nature of the service report that is available, for whom the report is available and how it can be obtained by intended users.

A SOC 3® report is intended for unlimited distribution so, for example, can be made available on the service organization's website.

5 Categories and Criteria

5.1 Background

5.1.1 Introduction

The AICPA Assurance Services Executive Committee (ASEC) has developed a set of principles and criteria (Trust Services Principles and Criteria) to be used in evaluating controls relevant to the security, availability, and processing integrity of a system, and the confidentiality and privacy of the information processed by the system. The trust services principles and criteria are updated from time to time. The description in this guide is based on the 2018 version, which is effective for periods ending on or after 15 December 2018

The starting point of the trust services principles and criteria is the system designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management specified requirements. System components can be classified into the following five categories: infrastructure, software, people, processes and data.

A principle has a set of criteria. The sets of criteria are for assessing the effectiveness of an entity’s controls relevant to the security, availability, processing integrity, confidentiality or privacy of the information processing by the system.

5.1.2 Trust Services Principles

The following are the Trust Services Principles (TSP):

- *Security:* The system is protected against unauthorized access, use, or modification.
- *Availability:* The system is available for operation and use as committed or agreed.
- *Processing integrity:* System processing is complete, valid, accurate, timely, and authorized.
- *Confidentiality:* Information designated as confidential is protected as committed or agreed.
- *Privacy:* Addresses the system’s collection, use, retention, disclosure, and disposal of personal information in conformity with the commitments in the entity’s privacy notice and with other criteria set forth.

5.1.3 Criteria

Many of the criteria used to evaluate a system are shared amongst all of the principles. The criteria for the security, availability, processing integrity, confidentiality and privacy principles are organized into the criteria that are applicable to all aforementioned four principles (common criteria) and criteria applicable only to a single principle.

Principle	Number of criteria
Security	33 common criteria
Availability	33 common + 3 additional criteria
Processing Integrity	33 common + 5 additional criteria
Confidentiality	33 common + 2 additional criteria
Privacy	33 common + 18 additional criteria

The common criteria constitute the complete set of criteria for the security principle. For the principles of availability, processing integrity, confidentiality and privacy, a complete set of criteria includes all of the common criteria and all of the criteria applicable to the principle(s) being reported on.

The common criteria are organized into nine categories:

- *Control environment.* The criteria (5) relevant to how the entity is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.
- *Communication and Information.* The criteria (3) relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
- *Risk assessment.* The criteria (4) relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

- *Monitoring activities.* The criteria (2) relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.
- *Control activities.* The criteria (3) relevant to which the entity identifies controls to addresses deficiencies and to mitigate risks.
- *Logical and physical access controls.* The criteria (8) relevant to how the entity restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.
- *System operations.* The criteria (2) relevant to how the entity manages the execution of system procedures and detects and mitigates processing exceptions, including logical and physical security exceptions, to meet the objective(s) of the principle(s) addressed in the engagement.
- *Change management.* The criteria (4) relevant to how the entity identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.
- *Risk mitigations.* The criteria (2) relevant to how an entity identifies risks, among which the subject and the implementation of the controls and other controls which lower the risks (iv) and constantly monitoring of the risks and the risk management – process.

For the trust service principle availability three additional criteria are applicable, while for processing integrity, confidentiality and privacy, 5, 2, and 18 additional criteria respectively are applicable. We refer to the AICPA bookshop[8] for both the common criteria and the criteria applicable to the principle(s) being reported on. An extract of the Trust Services Principles and Criteria are included in the appendix for illustration purposes. As TSP section 100 and Criteria are subject to regular updates to the practitioner should make sure they are using the most current version.

5.2 Privacy

The section describes the privacy principle of the Trust Services Criteria that may be included in a SOC 2® and/or SOC 3® report.

[8] https://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/Standards/PRDOVR~PC-TSPC13/PC-TSPC13.jsp

5.2.1 Privacy Criteria

The criteria from the Privacy category are divided into the following subjects:

1. Notice and communication of objectives
2. Choice and consent
3. Collection
4. Use, retention, and disposal
5. Access
6. Disclosure and notification
7. Quality
8. Monitoring and enforcement.

The SOC 2® privacy criteria, however, are not specifically aligned with the EU General Data Protection Regulation (GDPR). In the European Union the GDPR is applicable, which contains the following principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

A comparison with the GDPR privacy principles and the SOC 2® privacy criteria shows that there are many similarities between both frameworks. The use of the SOC 2® privacy criteria is therefore not excluded, as long as the underlying criteria and the points of focus do not conflict with any of the GDPR privacy principles.

To comply with the SOC 2® privacy criteria, the NOREA Privacy Control Framework (PCF) may be used. Analysis of the SOC 2® privacy criteria and 'points of focus' and the NOREA PCF shows:

- It is possible to include the SOC 2® privacy category in the scope of an engagement, because the SOC 2® privacy criteria and 'points of focus' are aligned with GDPR principles;
- The NOREA PCF may be used to implement internal controls can support compliance by the service organization with the SOC 2® privacy criteria, taking into account the objective of the (service) organization and the 'points of focus'. As such, the report is based on the criteria (control objectives) from SOC 2®, which have been given substance with controls from the PCF;
- To achieve the control objectives from the PCF and thus the SOC 2® privacy criteria, the illustrative controls from the 'NOREA Guide Privacy Control Framework' may be used as a basis. The specific privacy risks (that apply to the organization in scope of the SOC 2® engagement) that are mitigated by implementing internal controls need to be taken into account. Therefore, the service auditor needs to determine whether the internal controls are sufficient to achieve the control objective, taking into account the applicable privacy risks for the specific organization.
- Because not all topics covered by the PCF are included in the SOC 2® privacy criteria, the service auditor needs to determine whether additional internal controls related to privacy may be relevant to include under the other categories. Examples include the presence of a data protection officer, performing data protection impact assessments (DPIAs), and privacy by design and by default.

5.2.2 mapping of the SOC 2® privacy criteria and the Privacy control framework (PCF)

To be able to demonstrate an effective control environment with regard to privacy, the PCF was designed by NOREA; 'NOREA Guide Privacy Control Framework'. The primary objective of the PCF is to provide guidance to determine whether the control objectives of an entity regarding privacy are achieved. The PCF contains prescribed control objectives regarding different privacy subjects, is based on the articles of the GDPR and is built upon different 'good practices', among which is the GAPP framework (which the TSP section A-1, 2014 is based upon). The PCF is structured on the basis of the information lifecycle management model and therefore follows the structure of the TSP section 100 (2017) of the AICPA.

For the Privacy Criteria of the TSP Section 100 (2017) a direct mapping was made from the PCF. For each criteria from the TSP section 100 it was determined which control objective of the PCF is applicable. This method assures that each privacy criteria from the TSP section 100 is addressed on the basis of one of more control objectives in the PCF. The mapping shows that the PCF can be used to fulfill all of the privacy criteria from the TSP section 100 and it shows that the Privacy category does not conflict with the GDPR. Therefore, the control objectives of the PCF can be used to achieve the objectives of the SOC2® Privacy principle. Following this, the illustrative controls of the PCF can be used to fulfill the control objectives from the PCF and therefore also the SOC 2® Privacy Principle.

However, the use of the PCF (or parts of it) within the SOC 2® engagement does not mean that the organization, while achieving the SOC 2® Privacy Principle, is compliant with the GDPR. By performing the SOC 2® engagement, no assurance is given with regard to GDPR compliance, but only about the achievement of internal controls related to privacy. The mapping of the privacy Criteria and the PCF can be found in Annex 1 – Mapping Privacy category – PCF.

Some PCF control objectives cannot be matched directly with the SOC 2® Privacy Criteria. Therefore, when only privacy controls under the privacy criteria are included, fundamental privacy aspects of the GDPR will not be fulfilled. For example, the availability of the data officer, the execution of data protection impact assessments and privacy by design and default. If the subjects (referred to in the PCF as 'topics') and the underlying topics are not mapped with the SOC 2® criteria of the privacy category, generally speaking not all control objectives of the PCF are fulfilled. As a result, these aspects need to be included under the 'common criteria' of SOC 2® if the aim is that the SOC 2® should somehow provide assurance on the PCF control objectives. Within these criteria, even though these are the common criteria, privacy related objectives can be included by the service organization. These PCF subjects are also included in the mapping in Annex v1– Mapping Privacy Category – PCF, as part of the mapping of the PCF of the SOC 2® Common Criteria.

5.2.3 Scope of the Privacy Criteria

Within SOC 2® engagements, it is possible to scope out certain criteria if a certain type of risk is not applicable to the in-scope services. For example, if the organization is not responsible for the collected personal data of the involved parties, then privacy criteria P3.1 is not applicable.

In this particular case, this needs to be included in the following sections of the report, where an explanation is given of which criteria will not be fulfilled by objectives and an explanation as to why this is the case (see point 7 on page 41 of the SOC 2® Guide):

- Management statement
- System description

In these sections a description needs to be given with regard to which criteria are out of scope of the assurance engagement because no controls have been included for this specific criteria, and an explanation provided as to why. The auditor must determine whether the privacy category as a whole is not applicable or only certain criteria are out of scope.

5.2.4 Data Controller vs. Data Processor

All of the fulfilled criteria and 'points of focus' are dependent on the nature of the organization. If the organization qualifies as data controller, it is possible that more criteria are applicable to the organization, compared to when the organization qualifies as data processor. Criteria or certain parts of the criteria may not be applicable to a data processor. If only a part of the criteria is applicable for the data processor, 'user entity controls' should be included to further determine the responsibility of the data controller.

5.3 Criteria for management statement and SOC 2® assurance report

In a SOC 2® report, the service auditor expresses an opinion on the following:

- Whether the description of the service organization's system is fairly presented, based on the description criteria (Description Criteria 200)
- Whether the controls are suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively
- In type 2 reports whether the controls were operating effectively to meet the applicable trust services criteria

The management of the service organization will use the criteria set out in paragraph 5.3.1 below (described in SOC 2® as 'criteria') for their statement and the service auditor will use these criteria to draft their opinion. Because those criteria may not be readily available to report users, management of the service organization should include all of the criteria in its statement. Although all of the criteria are included in management's statement, certain description criteria may not be pertinent to a particular service organization or system. For example, criterion a v) in paragraph 2.4 would not be relevant to a service organization that does not prepare and deliver reports or other information to user entities or other parties, and criterion a vii) 2) in paragraph 2.4 would not be applicable to a service organization that does not use a subservice organization. If certain description criteria are not pertinent to a service organization, report users generally find it useful if management presents all of the description criteria and indicates which criteria are not pertinent to the service organization and why they are not relevant. Management may do so either in its system description or in a note to the specific description criteria.

5.3.1 Description Criteria

The criteria for determining whether the description of the service organization's system is fairly presented are as follows:

a. The description contains the information as stated in paragraph 2.4;

b. The description gives a complete view of the system and is formed based on general information needed for a broad group of users. Therefore, the description should contain all aspects a user might find important.

5.3.2 Design Criterion

The criterion for determining whether controls are suitably designed is that the controls identified in the description would, if operating as described, provide reasonable assurance that the applicable trust services criteria would be met.

5.3.3 Operating effectiveness Criterion

The criterion for determining whether the controls identified in the description of the service organization's system operated effectively to meet the applicable trust services criterion is that the controls were consistently operated as designed throughout the specified period, including whether manual controls were applied by individuals who have the appropriate competence and authority.

6 SOC 2® and SOC 3® versus other standards

6.1 Mapping criteria

Auditors need criteria to form a conclusion in an assurance report. For the SOC 2® and SOC 3® report, the benchmarks are the criteria related to the trust service principle in scope. However, in practice a lot of other frameworks are in use at service organizations, such as ISO 27002 or PCI-DSS. Replacing the AICPA trust principles and criteria by another framework results in an assurance report that is not in line with the AICPA SOC 2® guidance. Assuming that the report meets the ISAE 3000A requirements, it is still a valid assurance report which could be useful to a user entity, but it is not a SOC 2® or SOC 3® report. If other frameworks are used instead of the trust service principles, the report structure in an ISAE 3000A / Richtlijn 3000A report can be used (as indicated in paragraph 3 of ISAE 3000A).

It is possible to publish an SOC 2® and SOC 3® report and include a mapping of the criteria of the principle(s) in scope and the required framework. This is the approach we see nowadays in the US and is referred to as a SOC 2®+ report. Most professionals have mappings of the trust services principle and criteria to ISO 27002, CMM[9], PCI-DSS, etc. available for their clients. Additionally, the Cloud Service Alliance published a SOC 2® mapping with the Cloud Control Matrix (CCM).

The focus of the guide is providing guidance on the application of SOC 2® and SOC 3® reports. Mappings with other frameworks are a professional interpretation and are outside the scope of this document.

6.2 SOC 2® and SOC 3® versus ISAE 3402

The SOC 2® and/or the SOC 3® report, as well ISAE 3402 assurance report, can help the financial auditor of a user organization to obtain assurance over the controls implemented and operated at a service organization. The difference is that an ISAE 3402 report always relates to controls supporting the financial reporting process. The main objective of an ISAE 3402 report is to cover business process controls relevant for the reliability of the financial report of user entities. ISAE 3402 fits with the requirements of ISA 402 "audit considerations relating to an entity using a service organization".

[9] CCM cloud control matrix, published by CSA cloud security alliance

IT supporting the information processing process could be part of an ISAE 3402 report or can be the scope of a report on an IT service bureau in the position of a subservice organization delivering services to a service organization running applications which may be relevant for the financial report of the users entities. However, a SOC 2® and/or SOC 3® report on security will probably better meet the needs of the user entities than an ISAE 3402 report.

7 Annex

In this annex, a template of the management statement is included, as well as illustrative example text for the elements of an assurance report of the practitioner. This guide does not include all relevant examples and more current ones may be available.

7.1 Management Statement

This SOC 2® Management Statement Template has the following restrictions:

- no user control considerations;
- no sub-service organizations;
- no qualification.

Management of {XYZ Service Organization}'s Statement

We have prepared the attached description titled "{Description of {Legal Service Entity Name}'s {name or title of system} System for the period {period start date} to {period-end date } " (the description), based on the criteria in items (a)(i)-(ii) below (the description criteria).

The description is intended to provide users with information about the {type or name of} System, particularly system controls intended to meet the criteria for the {security, availability, processing integrity, confidentiality and privacy} principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy issued by the Assurance Services Executive Committee of the AICPA (applicable trust services criteria).

We confirm, to the best of our knowledge and belief, that

a) the description fairly presents the {type or name of} system throughout the period {start date} to {end date} (the "specified period"), based on the following description criteria:

I. The description contains the following information:

   1. The types of services provided.
   2. The components of the system used to provide the services, which are the following:

    a. Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks).

    b. Software. The programs and operating software of a system (systems, applications, and utilities).

    c. People. The personnel involved in the operation and use of a system (developers, operators, users, and managers).

    d. Procedures. The automated and manual procedures involved in the operation of a system.

    e. Data. The information used and supported by a system (transaction streams, files, databases, and tables).

3. The boundaries or aspects of the system covered by the description.
4. If information is provided to, or received from, subservice organizations or other parties
    a. how such information is provided or received; the role of the subservice organization and other parties.

    b. the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
5. The applicable trust services criteria and related controls designed to meet those criteria, including, as applicable, the following
    a. Complementary user entity controls contemplated in the design of the service organization’s system.

    b. When the inclusive method is used to present a subservice organization, controls at the subservice organization
6. If the service organization present the subservice organizations using the carve-out method
    a. the nature of the services provided by the subservice organization;

    b. each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

7. Any applicable trust services criteria that are not addressed by a control and the reasons therefore.

8. In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

II. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

    a. the controls stated in the description were suitably designed throughout the period {start date} to {end date} to meet the applicable trust services criteria

    b. the controls stated in the description operated effectively throughout the period {start date} to {end date} to meet the applicable trust services criteria

{Service Organization Legal Name}

{Name}

{Title}

{Date}

7.2 Assurance report SOC 2®

Illustrative report.

The assurance report shall include at a minimum the following basic elements:	Illustrative example
a) A title that clearly indicates the report is an independent assurance report.	Independent Service Auditors' Report
b) An addressee.	{ADDRESSEE}:
c) The practitioner's conclusion d) Optional: in case of a qualified opinion, adverse opinion or disclaimer of conclusion, the basis for the opinion must be included	Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects, based on the criteria identified in {Service Entity}'s statement and the applicable trust services criteria a. The description fairly presents the [{type or name of} system that was designed and implemented throughout the period {Start Date}, to {End Date}. b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period {Start Date}, to {End Date}, and user entities applied the complementary user-entity controls contemplated in the design of {Service Entity}'s controls throughout the period {Start Date}, to {End Date}. c. The controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period {Start Date}, to {End Date}. The specific controls we tested and the nature, timing, and results of our tests are presented in the section of the report titled "Criteria, Controls, Test Procedures, and Results.
e) A statement that the engagement was performed in accordance with this guide. f) A notice that the auditor has been compliant with the Code of Ethics.	We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, 'Assurance Engagements other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion. We have complied with the independence and other ethical requirements of the Code of Ethics ('Reglement Gedragscode') issued by NOREA, the Dutch IT-Auditors

	institute, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.
g) An identification or description of the level of assurance obtained by the practitioner, the subject matter information and, when appropriate, the underlying subject matter.	We have been engaged to obtain reasonable assurance and report on the attached description titled "{Description of {Legal Service Entity Name}'s {name or title of system} System for the period {period start date} to {period-end date}} " (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the {security, availability, processing integrity, confidentiality} principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy issued by the American Institute of Certified Public Accountants and the Chartered Professional Accountants of Canada(applicable trust services criteria), throughout the period {Start Date}, to {End Date} . The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of {Legal Service Entity Name}'s ("{Service Entity}") controls are suitably designed and operating effectively , along with related controls at the service organization . We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls. [Service Entity} uses a service organization (subservice organization) {Legal Subservice Entity Name}'s ("{Subservice Entity}") to perform {Subservice Functions}. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description presents {Service Entity}'s system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. For its description [XYZ Service Organization] uses the carve-out method. The description of the system therefore does not include any of the controls implemented at the subservice organization. Our engagement did not extend to the controls provided by the subservice organization The information attached to the description titled "Other Information Provided by {Service Entity} That Is Not Covered by the Service Auditor's Report" describes the service organization's {type of} system. It is presented by the management of {Service Entity} to provide additional information and is not a part of the service organization's description of its {type of} system made available to user entities during the period from {Start Date}, to {End Date} . Information about {Service Entity}'s {type of} system has not been subjected to the procedures applied on the {Description Title} and the suitability of the design and operating effectiveness of controls to meet the related criteria stated in the {Description Title} and accordingly, we express no opinion on it.

h)	Identification of the applicable criteria	The applicable criteria are identified in {Service Entity}'s statement in combination with the applicable trust services criteria.
i)	Where appropriate, a description of any significant inherent limitations associated with the measurement or evaluation of the underlying subject matter against the	[Service Entity}'s description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.
j)	When the applicable criteria are designed for a specific purpose, a statement alerting readers to this fact and that, as a result, the subject matter information may not be suitable for another purpose.	This report and the description of tests of controls and results thereof are intended solely for the information and use of {Service Entity}; user entities of {Service Entity's System Name} during some or all of the period {Start Date}, to {End Date} ; and independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following: • The nature of the service provided by the service organization • How the service organization's system interacts with user entities, subservice organizations, and other parties • Internal control and its limitations • Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria • The applicable trust services criteria • The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks. This report is not intended to be and should not be used by anyone other than these specified parties.
k)	A statement to identify the responsible party and the measurer or evaluator if different, and to describe their responsibilities and the practitioner's responsibilities.	{Service Entity} has provided the attached statement titled "{Statement Title}" which is based on the criteria identified in management's statement. {Service Entity} is responsible for (1) preparing the description and statement; (2) the completeness, accuracy, and method of presentation of both the description and statement; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.
l)	The responsibility of the auditor	Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in {Service Entity}'s statement and on the suitability of the design and operating effectiveness of the controls to meet

	the applicable trust services criteria, based on our procedures to obtain reasonable assurance. We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, ‘Assurance Engagements other than Audits or Reviews of Historical Financial Information’ established by The International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion.
m) A statement that the firm of which the practitioner is a member applies ISQC 1, or other professional requirements, or requirements in law or regulation	The firm applies the NOREA Standard on Quality Control (Reglement Kwaliteitsbeheersing NOREA – RKBN), and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.
n) An informative summary of the work performed as the basis for the practitioner’s conclusion	Our assurance engagement involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures depend on the service auditor’s judgment and included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our procedures also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.
o) The practitioner’s signature	{Service auditor’s signature}
p) The date of the assurance report.	[Date of the service auditor’s assurance report]
q) The location in the jurisdiction where the practitioner practices.	[Service auditor’s address]

7.3 Trust Services Criteria

Published in 2017 by the American Institute of Certified Public Accountants and Chartered Professional Accountants of Canada. The set is effective for periods ending on or after 15 December 2018.

- Criteria common to all categories [security availability processing integrity, confidentiality and privacy]:
    - Common criteria related to 'control environment',
    - Common criteria related to 'communication and information'.
    - Common criteria related to 'risk assessment',
    - Common criteria related to 'monitoring activities',
    - Common criteria related to 'controls activities'
    - Common criteria related to 'logical and physical access controls',
    - Common criteria related to 'system operation',
    - Common criteria related to 'change management'.
    - Common criteria related to 'risk mitigation'.
- A1. Additional criteria for availability.
- PI1. Additional criteria for processing integrity.
- C1. Additional criteria for confidentiality.
- P1. Additional criteria for privacy

The documentation of the trust services principles and criteria is available in the AICPA website (https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf).

7.4 SOC 3® report – illustration

A SOC 3® report contains the following elements	Example
a. A title page which clearly states that the report is a SOC 3 report	SOC 3® report Report about <system/service> relevant for <applicable criteria> <start review period> until <end review period>.
b. Management statement	We are responsible for designing, implementing, operating, and maintaining effective controls within <client>'s <system or type of service> (system) throughout the period <start review period> to <end review period>, to provide reasonable assurance that <client>'s service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in <attachment A> and identifies the aspects of the system covered by our assertion. We have performed an evaluation of the effectiveness of the controls within the system throughout the period <start review period> to <end review period>, to provide reasonable assurance that <client>'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). <client>'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in <attachment B>. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved. We use subservice organization(s) <subservice organization(s)> to perform <service>. The description of the boundaries of the system (<attachment A> of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system of <system or type of service> also indicates the complementary subservice organization controls assumed in the design of <client>'s controls. The description does not disclose the actual controls at the subservice organization.

	The description of the boundaries of the system (<attachment A> of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of <client>'s controls are suitably designed and operating effectively, along with related controls at the service organization. The description presents <client>'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of <client>'s controls. We assert that the controls within the system were effective throughout the period <start review period> to <end review period>, to provide reasonable assurance that <client>'s service commitments and system requirements were achieved based on the applicable trust services criteria. <signature Service Organization>
c. Assurance report of the independent auditor	1. Scope We have examined <client>'s accompanying assertion titled "<Client's Assertion>" (assertion) that the controls within <client>'s <system or type of service> (system) were effective throughout the period <start review period> to <end review period>, to provide reasonable assurance that <client>'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). 2. Sub-service organizations <Client> uses subservice organization(s) <subservice organization(s)> to perform <service>. The description of the boundaries of the system (<attachment A> of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system of <system or type of service> also indicates the complementary subservice organization controls assumed in the design of <client>'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls. 3. Objectives at the user entity (Complementary User Entity Controls). The description of the boundaries of the system (<attachment A> of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of <client>'s controls are suitably designed and operating effectively, along with related controls at the service organization. The description presents <client>'s controls, the applicable trust services criteria, and the complementary user entity controls

assumed in the design of <client>'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

4. Service organization's responsibilities

<Client> is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that <client>'s service commitments and system requirements were achieved. <client> has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, <client> is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

5. Responsibility of the service auditor.

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, 'Assurance Engagements other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion.

We have complied with the independence and other ethical requirements of the Code of Ethics ('Reglement Gedragscode') issued by NOREA, the Dutch IT-Auditors institute, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies the NOREA Standard on Quality Control (Reglement Kwaliteitsbeheersing NOREA - RKBN), and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve <client>'s service commitments and system requirements based on the applicable

	trust services criteria. • Performing procedures to obtain evidence about whether controls within the system were effective to achieve <client>'s service commitments and system requirements based the applicable trust services criteria. Our examination also included performing such other procedures as we considered necessary in the circumstances. 6. Inherent limitations There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate. 7. Opinion In our opinion, management's assertion that the controls within <client>'s <system or type of service> were effective throughout the period <start review period> to <end review period>, to provide reasonable assurance that <client>'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects. [Date] [Signature of IT auditor]
d. Attachment A <Clients> descriptions of the scope of the system	*The description is a brief version of the description of the SOC 2* Report. The description needs to contain at least the following aspects:* • *Background (general information)* • *System overview (including the paragraphs infrastructure, software, people, procedures and data)* • *Internal control (including the paragraphs control environment, risk assessment, control activities, information & communication, monitoring activities)* • *Scope of the service / boundaries of the system / sub-service organizations* • *Complementary user entity controls.* • *Complementary subservice organization controls.*
e. Attachment B <Client>'s principal service commitments and system requirements	*Attachment B provides an overview of the principal service commitments and system requirements. These can, for example, be based on requirements or responsibilities included in internal processes and procedures, service level agreements or relevant laws and regulations.*

7.5 Key references to guidelines, professional standards, articles and brochures

The DC-Section 200 - Description Criteria for a Description of a Service Organization's System in a SOC 2* Report (Description Criteria 200) can be obtained from : https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/dc-200.pdf

The 'TSP Section 100 - 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy' can be obtained op AICPA website: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

The ISAE 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information can be obtained from at: https://www.ifac.org/system/files/publications/files/ISAE%203000%20Revised%20-%20for%20IAASB.pdf

The NOREA richtlijn Assurance-opdrachten door IT-auditors (3000) can be obtained from: https://www.norea.nl/download/?id=5640

The NOREA Richtlijn 3402 - Assurance report regarding internal objectives at a service organization: https://www.norea.nl/download/?id=474

The NOREA Privacy Control Framework can be obtained from: https://www.norea.nl/download/?id=6313

7.6 List of contributors

Chair	Rene Ewals	ACS
Core team	Jeroen Francot	BDO
Core team	Carlijn Frins	BDO
Core team	Dennis Houtekamer	EY
Core team	Milan van Helden	EY
Team member	Mark Russel	EY
Team member	Jan Matto	Mazars
Team member	Robert Boon	Deloitte
Team member	Jeroen Meulendijks	VanderBeecken

7.7 Mapping Privacy Category – PCF

This annex includes the mapping between the Privacy Criteria (TSP section of 2017) and the PCF control objectives (‘NOREA Guide Privacy Control Framework’), which can support the design and implementation of controls under the SOC 2® privacy criteria. For a complete overview of the SOC 2 privacy criteria refer to the Trust Services Criteria 2017 (TSP section 100) of the AICPA Assurance Services Executive Committee (ASEC). The PCF controls objectives are included as a whole. Since the mapping with the PCF is only there as supporting information, it is not necessary to include the mapping in the report. To comply with SOC 2® guidelines, the criteria in TSP section 100 must be included in the report.

A. Mapping Privacy Criteria – PCF Controls objectives

Privacy Criteria – TSP section 100 (2017)	PCF Tag	PCF Topic	PCF Control objective
P1.1	PPO (01.1)	Privacy policy	The entity has established and communicated a policy that states its objectives and responsibilities regarding privacy and is in line with accepted privacy principles and applicable laws and regulations.
	PST (02.1)	Privacy statement	The entity transparently informs data subjects of the entity’s policy, requirements, and practices regarding the collection, use, retention, disclosure and disposal of personal data.
P2.1	CFR (03.1)	Consent framework	The entity obtains data subject’s consent for processing personal data where required or necessary.
P3.1	PDI (01.3)	Personal data identification and classification	The entity understands and documents which personal data is stored and processed and identifies and treats personal data appropriately. Measures to safeguard personal data take into account the differences in sensitivity in personal data, leading to identification of risks and compliance with laws and regulations.
	DMI (04.1)	Data minimization	Personal data is adequate, relevant, and limited to what is necessary in relation to the legitimate purposes for which it is processed.

Privacy Criteria – TSP section 100 (2017)	PCF Tag	PCF Topic	PCF Control objective
P3.2	CFR (03.1)	Consent framework	The entity obtains data subject's consent for processing personal data where required or necessary.
P4.1	ULI (05.1)	Use limitation	Personal data is not disclosed, made available or otherwise used for other purposes than those specified in the entity's privacy statement except: a. with the consent of the data subject; or b. by the authority of law.
P4.2	DRE (05.3)	Data retention	Personal data is retained no longer than the minimum time needed, as required by applicable laws and regulations, or for the purposes for which it was collected.
P4.3	DDA (05.4)	Disposal, destruction and anonymization	Personal data is anonymized and/or disposed of within the entity where required. Identities should not be identifiable and personal data should not be available once it is past its retention date.
	DDR (06.3)	Data deletion requests	Data deletion requests are responded to adequately and data subjects are able to have their personal data deleted if applicable criteria are met.
P5.1	DAR (06.1)	Data access requests	Data subject access requests are responded to adequately, and data subjects are able to determine which personal data relating to her/him is processed and in what way.
	DPR (06.3)	Data portability requests	Data portability requests are responded to adequately and data subjects are able to have their personal data transferred to another entity if applicable criteria are met.
P5.2	DCR (06.2)	Data correction requests	Data subject correction requests are responded to adequately, and data subjects are able to determine whether their personal data is correct/up-to-date, and are able to correct their personal data.
	ACD (09.1)	Accuracy and completeness of data	Documented procedures for validation, editing and update of personal data assure accurate and complete personal data processing and the ability to access it when needed.

Privacy Criteria – TSP section 100 (2017)	PCF Tag	PCF Topic	PCF Control objective
P6.1	TPD (07.1)	Third party disclosure and registration	Personal data is not disclosed to third parties, or further processed for purposes for which the individual has not consented to.
	DTR (07.3)	Data transfers	Personal data is not transferred (i.e. movement, viewing, or printing of data in another location) internationally to countries that have an inadequate legal privacy regime.
	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.
P6.2	TPD (07.1)	Third party disclosure and registration	Personal data is not disclosed to third parties, or further processed for purposes for which the individual has not consented to.
P6.3	PIB (01.6)	Privacy incident and breach manageme nt	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
P6.4	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.
P6.5	PIB (01.6)	Privacy incident and breach manageme nt	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.

Privacy Criteria – TSP section 100 (2017)	PCF Tag	PCF Topic	PCF Control objective
P6.6	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
P6.7	DAR (06.1)	Data access requests	Data subject access requests are responded to adequately, and data subjects are able to determine which personal data relating to her/him is processed and in what way.
	PDI (01.4)	Personal data identification and classification	The entity understands and documents which personal data is stored and processed and identifies and treats personal data appropriately. Measures to safeguard personal data take into account the differences in sensitivity in personal data, leading to identification of risks and compliance with laws and regulations.
P7.1	ACD (09.1) DMI (04.1)	Accuracy and completeness of data Data minimization	Documented procedures for validation, editing and update of personal data assure accurate and complete personal data processing and the ability to access it when needed. Personal data is adequate, relevant, and limited to what is necessary in relation to the legitimate purposes for which it is processed.
P8.1	REV (10.1)	Review of privacy compliance	Adequate oversight of the internal organization and third parties ensures compliance with applicable privacy laws and regulatory requirements and decreases the risk of data breaches or loss of personal data.
	MON (10.2)	Periodic monitoring on privacy controls	The entity systematically and periodically assesses privacy processes and controls, as to establish that they operate as designed, resulting in ongoing compliance with applicable laws and regulatory requirements.
	URE (05.5)	Use and restriction	Personal data is not used in case of the restriction of the data subject or in case of specific legal restrictions by local government. Objections to processing by data subject will be handled adequately.

B. Mapping privacy points of focus under Common Criteria – PCF control objectives

In addition to the SOC 2® privacy criteria, there are some common criteria where privacy controls should be included, if the privacy category is included in the SOC 2® report. These are the following Common Criteria:

Common Criteria – TSP sectie 100 (2017)	TSP Topic	PCF Tag	PCF Topic	PCF Control objective
CC2.3	Communication of objectives related to privacy	PST (02.1)	Privacy statement	The entity transparently informs data subjects of the entity's policy, requirements, and practices regarding the collection, use, retention, disclosure and disposal of personal data.
CC7.3	Assessment of impact of security events on personal information	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
CC7.3	Identification of affected information after unauthorized use or disclosure of personal information	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.

CC7.4	Communication of affected information after unauthorized use or disclosure of personal information	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
CC7.4	Evaluation and, if appropriate, sanctioning of individuals involved in the unauthorized use or disclosure of personal information	PIB (01.6)	Privacy incident and breach management	The entity adequately detects and handles privacy-related incidents; privacy-related incidents are responded to appropriately as to limit the consequences and to take measures to prevent future breaches.
CC8.1	Protection of personal information during the change processes	PBD (05.2)	Privacy architecture (Privacy by Design and Privacy by Default)	The entity takes into account solid privacy policies, principles, and/or applicable laws and regulations when designing or changing products, services, business systems or processes.
CC9.2	Obtaining privacy commitments from vendors and business partners with access to personal information	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.

CC9.2	Assessing compliance by vendors and business partners with the entity's privacy commitments and requirements	TPA (07.2)	Third party agreements	Privacy considerations and requirements are adequately covered when procuring (personal data related) solutions or services from third parties resulting in appropriate handling or protection of personal data.

C. Mapping missing PCF Control objectives – Common criteria

The subjects (topics) of the PCF which cannot be directly mapped to the SOC 2® criteria of the privacy category, need to be included within the common criteria of SOC 2®. Related to these criteria, even though these are 'common' criteria, privacy related controls may be included. This mapping is as follows:

PCF Tag	PCF Topic	PCF Control objective	Common Criteria SOC 2
DRR	Definition of roles and responsibilities	The entity has established and implemented clear roles and responsibilities regarding the safeguarding of personal data and the achievement of privacy objectives.	CC1.3
RMA	Risk management	The entity systematically and periodically identifies, assesses, and mitigates factors that endanger the achievement of privacy objectives.	CC3.1 CC3.2
PIA	Data Protection Impact Assessments	The privacy-related impact of new products and services and their use within the entity is systematically identified, assessed and addressed.	CC3.4
SCO	Staff competences	Staff in positions with access to or control over personal data and personal data processes have the necessary privacy competences to adequately perform their duties.	CC1.4
SAT	Staff awareness and training	Staff is sufficiently aware of privacy laws, regulations and organizational privacy policies and guidelines, and their individual responsibilities with regard to privacy, and the entity engages in programs to establish and maintain awareness.	CC1.4 CC2.2

PCF Tag	PCF Topic	PCF Control objective	Common Criteria SOC 2
LRC	Legal review of changes in regulatory or business requirements	Privacy risks associated with changes to the entity (structure and strategy) and to regulatory requirements are adequately considered.	CC3.4
ISP	Information security program	Personal data is adequately secured from accidental errors or loss, or from malicious acts such as hacking or deliberate theft, disclosure or loss.	CC5.1
IAM	Identity and access management	Assignment of appropriate access rights, appropriate changes to access rights and timely removal of access rights decreases the likelihood of unauthorized access to, or inappropriate handling of personal data, or data breaches by internal employees, third parties or hackers.	CC6.1 CC6.2 CC6.3 CC6.6
STR	Secure transmission	Restricted access to personal data during transmission adequately prevents unauthorized disclosure, breach, altering or destruction of personal data.	CC6.7
ENC	Encryption and end-point security	Encryption assures the prevention of a breach of personal data (accidental loss of personal data, or malicious acts such as deliberate theft, disclosure or loss).	CC6.1 CC6.7
LOG	Logging of access	The entity detects and investigates access or access attempts to personal data by staff, third parties or hackers that could result in a breach, sabotage of systems, insertion of malicious code, theft of personal data, etc.	CC7.2