NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA Guide

Guidance to Richtlijn (ISAE) 3000 Service Organization Control Reports for IT Service Organizations

Based on the AICPA SOC 2® report model and the Trust Services Principles and Criteria

March 2016

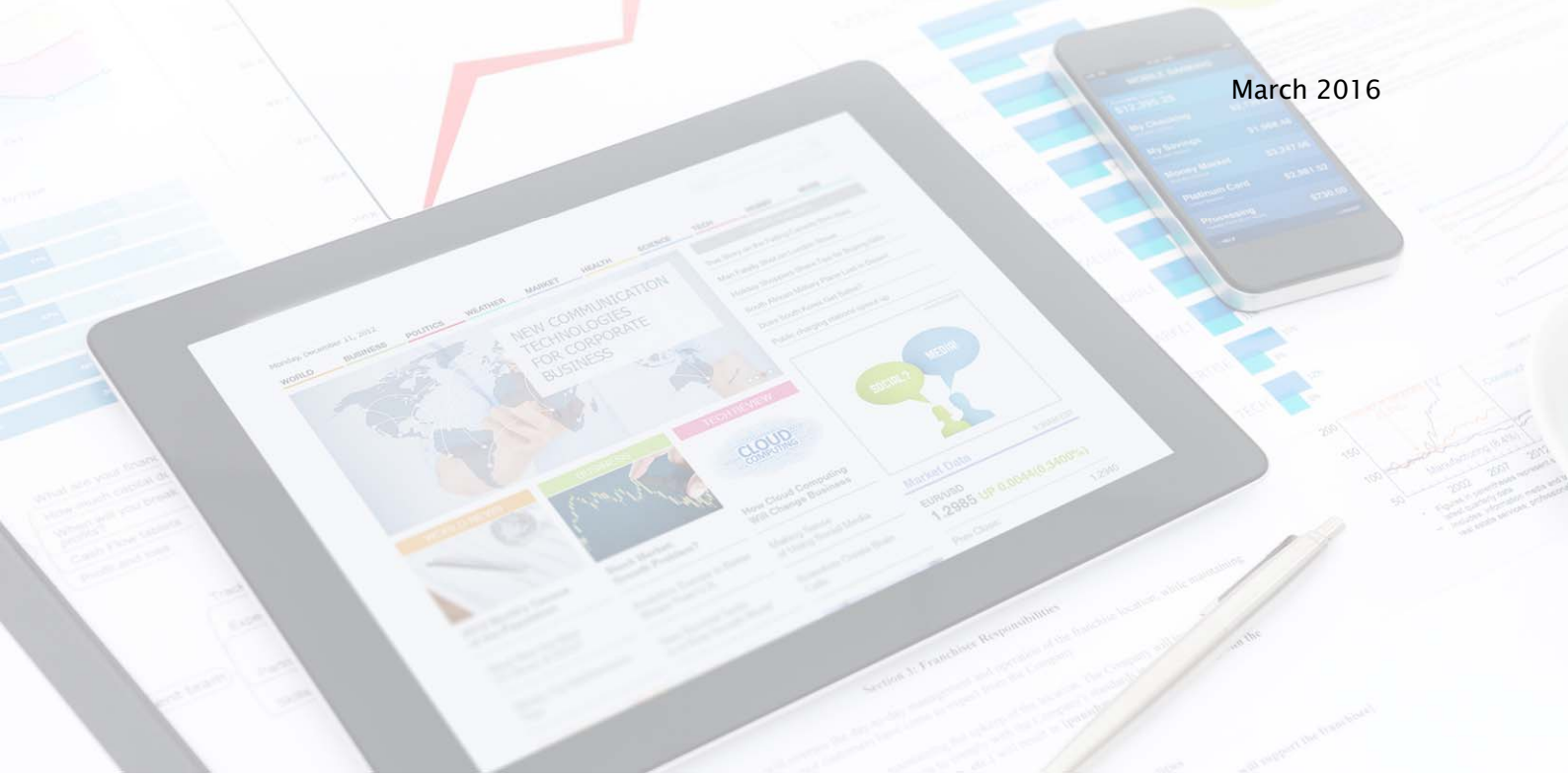


Table of Contents

Nederlandse vertaling (vanaf bladzijde 42)
Deze voor de Nederlandse auditors opgestelde handreiking is in de Engelse taal, dit om qua terminologie dicht bij de Amerikaanse SOC 2® guide te blijven. Ter vergroting van de toegankelijkheid is in het tweede deel van het document een Nederlandse vertaling opgenomen. De Nederlandse vertaling is een afgeleide, bij verschillen is de strekking van de Engelse tekst bepalend.

1 Introduction

1.1 Background

This guide (in Dutch: "handreiking") was developed for Dutch Register IT auditors (RE's) to guide them to issue reports in line with the American Institute of Certified Public Accountants (hereafter AICPA) Service Organization Control 2 (hereafter: SOC 2®) product under the International Standards on Assurance Engagements (hereafter: ISAE), 3000 or the local equivalent 'Richtlijn Assurance-opdrachten door IT-auditors' (3000)[1]. This publication is not a new standard but rather provides guidance for a specific ISAE 3000 assurance engagement. Although we realize that the guidance has a high level of professional expertise, the guidance 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.

This publication is in response to the increasing number of requests from IT service providers for SOC 2® 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 101[2]. This guide will provide guidance to produce the same kind of report based on the ISAE 3000 standard. This approach will avoid the requirement for the local Dutch practitioner to work under US regulations and standards. From a professional perspective, the practitioner will issue 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 structure of the specific ISAE 3000 / Service Organization Control report follows the format of ISAE 3402 (in the US SSAE 16 / AT section 801, referred to as SOC 1®) and the scope of the trust services principles and criteria. 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 the Dutch laws and regulations, including the NOREA regulations. These Dutch engagements cannot refer to any US laws or attestation standards including AT 101. To clarify that the report is made by using Dutch standards, laws and professional regulations the report is named for international use **ISAE 3000 / Service Organization Control Report** and for national use **Richtlijn 3000 / Service Organization Control Report**. We avoid references to SOC 2® as such refers to the US regulations and standards and may therefore misunderstood as such is used in a different context under international or local standards.

[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.

[2] In the course of 2016 the AICPA Attestation Standards are subject to a major revision, including changes in the naming of the standards.

1.2 Objective

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

- ISAE 3402 for service organizations who require assurance over the controls which may be relevant for the user entity's financial reporting
- ISAE 3000 / Service Organization Control Report for IT service organizations who require assurance on controls related to security, availability, process integrity, confidentiality, and privacy

In line with an ISAE 3402 report, an ISAE 3000 / Service Organization Control report focuses on the control environment and controls of a service organization and does not include assurance regarding the actual outcome of the process (e.g., the achievement of service level agreements (SLA) key performance indicators (KPIs)).

We decided to publish this guide in the English language 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. During the development of this guide, the taskforce has been in contact with the AICPA to help ensure that the Dutch guidelines on how to handle SOC 2® do not conflict with the US regulations and service mark regulations. However, we emphasize that the ISAE 3000 / Service Organization Control Report is a Dutch equivalent. A SOC 2® report under the AICPA service mark refers to the US standards (including AT 101) and an auditor's opinion issued by a CPA member of the AICPA.

1.3 Presumed level of knowledge

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

1.4 Constraints

One of the trust services principles is "privacy". The TSP privacy criteria are based on US and are recently renewed. For the Netherlands new EU privacy regulations are expected in due course. To prevent confusion we did not include the use of the Trust Services Principles and Criteria with respect to privacy. Nevertheless, we did mention in certain instances the relevant privacy elements for a full understanding of this guide in relation with the AICPA SOC 2® guide. Privacy

protection consists of IT related controls and compliance to specific procedures. However, the confidentiality principle could be useful to satisfy IT infrastructure related privacy controls.

Besides SOC 2®, the AICPA has also defined SOC 3® reports. A SOC 3® report can be considered if the service organization wishes to publish a public short form report (certificate) on the principles as mentioned under SOC 2®. SOC 3® is the rebranding of the old WebTrust, although WebTrust was not very popular over the years. With the introduction of the brand name SOC 3®, the guidance has not been updated yet.

Similar to SOC 2®, SOC 3® refers to a report published under US standards and regulation (including AT101) and is reserved for CPA's who are member of the AICPA. As illustrated in this guide, for the application of ISAE 3000 / Service Organization Control Report the practitioner may use the SOC 3® guidance to perform reviews and report under ISAE 3000. However, this is outside the scope of this ISAE 3000 / Service Organization Control guide.

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 guidance. For further details see chapter 2.5.

2 ISAE 3000 / Service Organization Control

2.1 Background

An ISAE 3000 / Service Organization Control report is a report that expresses assurance over the controls in scope of the service organization report. The AICPA distinguish three types of reports:

- A SOC 1® report: this is a report based on SSAE 16 / AT 801, the US implementation of the ISAE 3402 standard[3] and is restricted to use for financial reporting purposes;
- A SOC 2® report: this is a SOC report based on the AT101 standard, which is more or less the US equivalent of ISAE 3000 in the Netherlands. It reports on the trust services principles security, confidentiality, integrity, and availability (and privacy) criteria as defined by the standard itself.
- A SOC 3® report: this is a short form report based on the work supporting a SOC 2® report but made available for a more generic audience (not in scope of this guide please see chapter 1.4).

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

2.2 Key characteristics

As a NOREA Service Organization Control 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 ISAE 3000 / Service Organization Control 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 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);
- There are type I and type II reports (as there is in the ISAE 3402 standard);
- Unlike ISAE 3402, the minimum period is not specifically stated (however, a minimum reporting period of three months for a meaningful type II report is advised);

[3] 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).

- As is the case with an ISAE 3402 report, the report of the service organization must include a description of the system;
- 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:
  - management of the service organization,
  - 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 evaluating or reporting on controls at a user entity and
  - regulators.
- 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 use of a ISAE 3000 / Service Organization Control report).

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 likely to be 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 is based on Attestation Standards [AT] section 101. Such an engagement is known as a SOC 2® engagement, and a report on such an engagement is known as a SOC 2® report.

AT section 101 applies to engagements in which a practitioner is engaged to issue, or issues, an examination on subject matter, or a statement about the subject matter that is the responsibility of another party.

The international equivalent of AT section 101 is ISAE 3000. This standard deals with assurance engagements in which a practitioner aims to obtain sufficient 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).

An ISAE 3000 / Service Organization Control report exhibits all of 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 information will be available to 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))

A fully-fledged equivalent of SOC 2® assurance engagement can be based on one of the three implementations of standard 3000:

- ISAE 3000 or
- the Dutch equivalents
  - NBA Standard 3000 (HRA NV COS)
  - NOREA Richtlijn 3000

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

2.4 Structure of the ISAE 3000 / Service Organization Control report

As defined in ISAE 3000, the title page includes the identification of an ISAE 3000 / Service Organization Control report as follows:

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

ISAE 3000 / IT SERVICE ORGANIZATION CONTROL REPORT BASED ON THE SOC 2® REPORT MODEL AND THE TRUST SERVICES PRINCIPLES AND CRITERIA

RELEVANT TO [*followed by one or more principles:* SECURITY, AVAILABILITY, PROCESSING INTEGRITY, *and/or* CONFIDENTIALITY].

A typical table of content of an ISAE 3000 / Service Organization Control reports includes[4]:

Section I: Management statement[5]
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 that, in all material respects:

- 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 respectively type II), 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 trust services criteria as of a specific date or throughout the specified period (type I respectively type II);
- The controls stated in management's description of the service organization's system operated effectively throughout the specified period to meet the applicable trust services criteria (type II report)

Section II Independent service auditor's assurance report

The auditor's report in both the type I and II reports contains clearly, amongst others:

- 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)

[4] For an ISAE 3402 report the management statement is often placed after the Independent service auditor's assurance report. For an ISAE 3000 / Service Organization Control report the management assertion is placed in section 1 as management is responsible for the underlying subject matter and the assurance report is designed to enhance the degree of confidence of the intended users.

[5] The service organization's "statement" is equivalent to the service organization's "assertion" as defined under AICPA SOC 2® guidance

- That management is responsible for the description of the service organization's system;
- 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.

Examples of the opinion are included in the annex.

Section III Service organization's description of its system

The components of the system description as required in the ISAE 3000 / Service Organization Control report are as follows:

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

- 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.

Note: these aspects of the control environment will be included in the upcoming TSP update.

Section IV The principles, criteria, related controls and tests of controls

Section IV typically contains the principles, the 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 of the service organization, and the test approach and test results are those of 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

The content of this section is not pre-determined and is optional. Also, this section is not a part of the scope of work of the service auditor; however, its contents cannot be contradictory to the scope of the report or work performed by the 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 of approach to remediate any deficiencies noted in the report
- Responses from management for deviations 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, the 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 Logos

The AICPA has developed a logo[6] 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 Service Organization Control reports by using these print- and web-ready logos.

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

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

Please refer to section 4 of this guide for further considerations on marketing and promotion of an ISAE 3000 / Service Organization Control report.

3 Conducting an ISAE 3000 / Service Organization Control Engagement

An ISAE 3000 / Service Organization Control engagement is performed according to the professional standards as described in paragraph 2. In order to perform an ISAE 3000 / Service Organization Control engagement, the size and the maturity of the service organization should be on a sufficient level in order to be successful. Several key points to be addressed when performing an ISAE 3000 / Service Organization Control engagement are included in the following subsequent sections.

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

ISAE 3000 / Service Organization Control requires that: (1) "The practitioner accepts (or continue 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 so that it will be performed effectively." ISAE 3000 require the engagement personnel to have both a general knowledge and sufficient process, technical, industry, and reporting knowledge so as to be "assigned to tasks and supervised commensurate with their level of knowledge, skill, and ability so that they can evaluate the audit evidence they are examining."

In some instances when performing an ISAE 3000 / Service Organization Control engagement, the service auditor may determine that he or she does not possess sufficient knowledge or experience with certain aspects of the engagement. Also, 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. This knowledge requirement may be met, in part, 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[7] the chartered accountant and the IT auditor need to always maintain their professional knowledge and skills at the required level. For example when issuing an ISAE 3000 / Service Organization Control report for a data center, it is unlikely that a

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

chartered accountant (with no IT knowledge) would issue an ISAE 3000 / Service Organization Control 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 professional independence rules as prescribed by the applicable assurance standards. Such the "gedragscode" register IT auditors- of NOREA[8] or the VIO ('Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten') of NBA

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 trust services criteria. 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 ISAE 3000 / Service Organization Control 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 arguments as documented in the ISAE 3000 / Service Organization Control report

If the service organization uses the inclusive method to present the subservice organization, the description includes all of the elements identified in the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy[9] as they relate to the subservice organization. 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 organization related to the service delivered is part of the report.

[8] 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.

If the service organization uses the carve-out method to present the subservice organization, this should be sufficiently justified in the ISAE 3000 / Service Organization Control report (service auditor's opinion). The service auditor considers whether his engagement is rational (as defined by the Code of Ethics) with 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 trust services criteria, either alone or in combination with controls at the service organization.

The management statement as well as in the auditor's opinion mention the subservices organization and the way it is handled in the ISAE 3000 / Service Organization Control (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, there may not be a need to treat the vendor as subservice organization. Examples include technical engineers, but even in some instances, landlords of data centers.

3.4 Materiality and evaluation of deviations (exceptions)

When planning and performing an ISAE 3000 / Service Organization Control 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. Materiality relates to the system being reported on (qualitative materiality), not the financial statement materiality of user entities. In evaluating materiality, it should be considered 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 discrepancy.

The description of the system includes the significant aspects to process significant transactions, 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, qualitative and quantitative 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 deviation.
- Nature and cause of observed deviations.

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 our 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 deviations 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 principle 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 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 is necessary to reach a conclusion about whether the controls related to the criterion 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 addresses all exceptions. There is no materiality level, all exceptions are noted factual in the results for control measures. The service auditor has to determine if the control objective is met based on quantitative and qualitative materiality levels and the noted control exceptions.

Deviations 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.

It is important for the service auditor to include sufficient detail in the description of the deviations 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 deviation:

- 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 deviations.
- The cause of the deviation.

If deviations 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 deviations, the controls that mitigate the effect of the deviations, corrective actions taken, and other qualitative factors that would assist users in understanding the effect of the deviations. Such information may be presented in the optional section of the type 2 report titled "Other Information Provided by the Service Organization." Information in this section is not covered by the service auditor's report. If management's responses to deviations 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 control objective 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 deviations, such information is included in the section "Other Information Provided by the Service Organization".

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 are used.

Test procedure	Description
Inquiries	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

Please see the ISAE 3000 standard for more background on performing tests on the design of controls.

An ISAE 3000 / Service Organization Control 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 and should achieve a 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 2 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, or
- 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 deviations 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 deviations.
- The tolerable rate of deviations that the service auditor has established.
- The pervasiveness of the deviations (for example, whether more than one criterion would be affected).
- The likelihood that the deviations 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 deviations 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.

4 Use of ISAE 3000 / Service Organization Control Report

Unlike ISAE 3402 reports, the primary users of ISAE 3000 / Service Organization Control reports generally are not user entity auditors but management of the service organization and management of the user entities (and prospective users and regulators). ISAE 3000 / Service Organization Control reports are 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.

ISAE 3000 / Service Organization Control reports also may be useful to a user entity's auditor, as some controls included in the ISAE 3000 / Service Organization Control report may likely 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 an ISAE 3000 / Service Organization Control report is relevant and useful for his financial statement audit, as the primary purpose and scope for the ISAE 3000 / Service Organization Control report differs from an ISAE 3402 report.

ISAE 3000 / Service Organization Control reports have the potential to be misunderstood when taken out of the context in which they were 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 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 management of the service organization; management of the (prospective) user entities; practitioners evaluating or reporting on controls at a user entity and regulators.

The report is not intended to be used by anyone other than these specified parties.

4.1 Marketing and communication by service organization

As the ISAE 3000 / Service Organization Control report is for the intended users 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 –certificate is obtained, or other unsubstantiated claims like: "the service organization has an internal control system of high quality". Such is incorrect, could be misinterpreted and/or is misleading the intended users. It is the duty of the practitioner to address this towards the client.

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.

5 Principles 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 2014 version, which is effective for periods ending on or after 15 December 2014.

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, and confidentiality 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	28 common criteria
Availability	28 common + 3 additional criteria
Processing Integrity	28 common + 6 additional criteria
Confidentiality	28 common + 6 additional criteria
Privacy	Outside the scope of the guide

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

The common criteria are organized into seven categories:

- *Organization and management.* The criteria (4) relevant to how the organization 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.
- *Communications.* The criteria (6) relevant to how the organization 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 management and design and implementation of controls.* The criteria (3) 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 of controls.* The criteria (1) 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.
- *Logical and physical access controls.* The criteria (8) relevant to how the organization 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 organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.
- *Change management.* The criteria (4) relevant to how the organization 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.

For the trust service principle availability three additional criteria are applicable, while for both processing integrity and confidentiality six additional criteria are applicable. We refer to the AICPA bookshop[10] 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 Principles and Criteria are subject to regular updates it is recommended to make sure that you are using the most actual version.

5.2 Privacy

The privacy principle is no part of this guide, due to the following two main reasons:

- The criteria related to the privacy principle contained in the Generally Accepted Privacy Principles (GAPP) are being revised separately from the security, availability, processing integrity, and confidentiality criteria. GAPP is designed to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities. The GAPP are not applicable in the EU, the criteria should be modified based on the Dutch and EU regulation.
- The General Data Protection Regulation is subjected to several changes. A new Data Protection Regulation will replace the current laws that govern the use of personal data in the EU. Although there is no agreement on a final version yet and some more amendments are expected while the negotiations continue, a clear direction has been defined. The final approval was expected no later than 2015. The Regulation will come into effect within a period expected to be two years from the date of approval.

It is important to understand that privacy, processing integrity, confidentiality and security are strongly interconnected. It is not very rational if an opinion about security does not cover parts of the universal privacy criteria like responsibility, transparency, data limitation, data quality, privacy by design and privacy enhancing technology.

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

5.3 Criteria for management statement and assurance report

In an ISAE 3000 / Service Organization Control 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
- 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 these criteria for their statement and a service auditor will use these criteria to draft his opinion. Because those criteria may not be readily available to report users, management of the service organization should include in its statement all of the criteria.

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, the criterion a v) would not be pertinent to a service organization that does not prepare and deliver reports or other information to user entities or other parties, and the criterion in a vii) 2) 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 the reasons therefore. 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 following information:

   I. The types of services provided

   II. The components of the system used to provide the services, which are as follows:

      1. Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

2. Software. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
3. People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
4. Procedures. The automated and manual procedures.
5. Data. Transaction streams, files, databases, tables, and output used or processed by the system.

III. The boundaries or aspects of the system covered by the description

IV. For information provided to, or received from, subservice organizations and other parties

1. how the information is provided or received and the role of the subservice organizations and other parties
2. the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

V. The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

1. Complementary user entity controls contemplated in the design of the service organization's system
2. When the inclusive method is used to present a subservice organization, controls at the subservice organization

VI. If the service organization presents the subservice organization using the carve-out method

1. the nature of the services provided by the subservice organization
2. 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

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

VIII. 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

b. 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 report users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs

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 ISAE 3000 / Service Organization Control versus other standards

6.1 Mapping criteria

Assurance reports need benchmarks to come to a conclusion. For the ISAE 3000 / Service Organization Control 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, 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 3000 requirements, it is still a valid assurance report which could be useful to a user entity, but it cannot be titled an ISAE 3000 / Service Organization Control report.

In the situation that other frameworks are used instead of the trust service principles, the report structure as in ISAE 3402 report can be used (as indicated in paragraph 3 of ISAE 3402).

A suggestion is to publish an ISAE 3000 / Service Organization Control 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. Most of the professionals have mappings of the trust services principle and criteria to ISO 27002, CMM[11], PCI DDS, 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 ISAE 3000 / Service Organization Control report. Mappings with other frameworks are a professional interpretation and are outside the scope, this document.

6.2 ISAE 3000 / Service Organization Control versus ISAE 3402

ISAE 3000 / Service Organization Control report, as well ISAE 3402 assurance reports, 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”.

[11] 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 in a report of 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, an ISAE 3000 / Service Organization Control 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 ISAE 3000 / Service Organization Control

This ISAE 3000 / Service Organization Control Management Statement Template has the following restrictions:

- no Privacy principle in scope,
- 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, and 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 Assurance Services Executive Committee of the AICPA (applicable trust services criteria).

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

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

    f. how such information is provided or received; the role of the subservice organization and other parties.

    g. 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

    h. Complementary user entity controls contemplated in the design of the service organization's system.

    i. 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

    j. the nature of the services provided by the subservice organization;

    k. 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.

l. 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.

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

    m. 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 ISAE 3000 / Service Organization Control

ISAE 3000 / Service Organization Control Assurance Report illustrative examples text elements

The assurance report shall include at a minimum the following basic elements[12]:	Illustrative example
a) A title that clearly indicates the report is an independent assurance report.	Independent Service Auditors' Report
b) An addressee.	{ADDRESSEE}:
c) 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

[12] ISAE 3000 paragraph 69. Revised ISAE 3000 is effective for assurance engagements where the assurance report is dated on or after December 15, 2015. https://www.ifac.org/sites/default/files/publications/files/ISAE%203000%20Revised%20-%20for%20IAASB.pdf In the Netherlands the local equivalent of ISAE 3000 revised (issued by NBA or NOREA) will become effective for assurance engagements where the assurance report is dated on or after December 15, 2016.

	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.
d) Identification of the applicable criteria	The applicable criteria are identified in {Service Entity}'s statement in combination with the applicable trust services criteria
e) Where appropriate, a description of any significant inherent limitations associated with the measurement or evaluation of the underlying subject matter against the applicable criteria.	{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.
f) 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.
g) A statement to identify the responsible party and the measurer or evaluator if different, and to describe their responsibilities and	{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.
the practitioner's responsibilities. h) A statement that the engagement	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

was performed in accordance with this ISAE i) 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 j) A statement that the practitioner complies with the independence and other ethical requirements of the IESBA Code, or other professional requirements, k) An informative summary of the work performed as the basis for the practitioner's conclusion	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. 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. 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.
l) The practitioner's conclusion	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."

m)	The practitioner's signature	{Service auditor's signature}
n)	The date of the assurance report.	[Date of the service auditor's assurance report]
o)	The location in the jurisdiction where the practitioner practices.	[Service auditor's address]

7.3 Extract trust services principles and criteria

Published in 2014 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 2014.

- Criteria common to all [security availability processing integrity and confidentiality] principles,
  - CC1.0 common criteria related to organization and management,
  - CC2.0 common criteria related to communications
  - CC3.0 common criteria related to risk management and design and implementation of controls,
  - CC4.0 common criteria related to monitoring of controls,
  - CC5.0 common criteria related to logical and physical access controls,
  - CC6.0 common criteria related to system operation,
  - CC7.0 common criteria related to change management.

- A1. Additional criteria for availability.
- PI1. Additional criteria for processing integrity.
- C1. Additional criteria for confidentiality.
- Generally Accepted Privacy Principles (august 2009)

The detailed documentation of the trust services principles and criteria is available in the AICPA store (www.cpa2biz.com).

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

The AICPA SOC 2® guide and the Trust Services Principles and Criteria can be obtained from the AICPA bookshop at: http://www.cpa2biz.com/

The ISAE 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information can be obtained from at: https://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga

The NOREA richtlijn Assurance-opdrachten door IT-auditors (3000) can be obtained from: http://www.norea.nl/readfile.aspx?ContentID=36665&ObjectID=344023&Type=1&File=0000036319_Richtlijn%20assurrance-opdrachtenC2.pdf

7.5 List of contributors

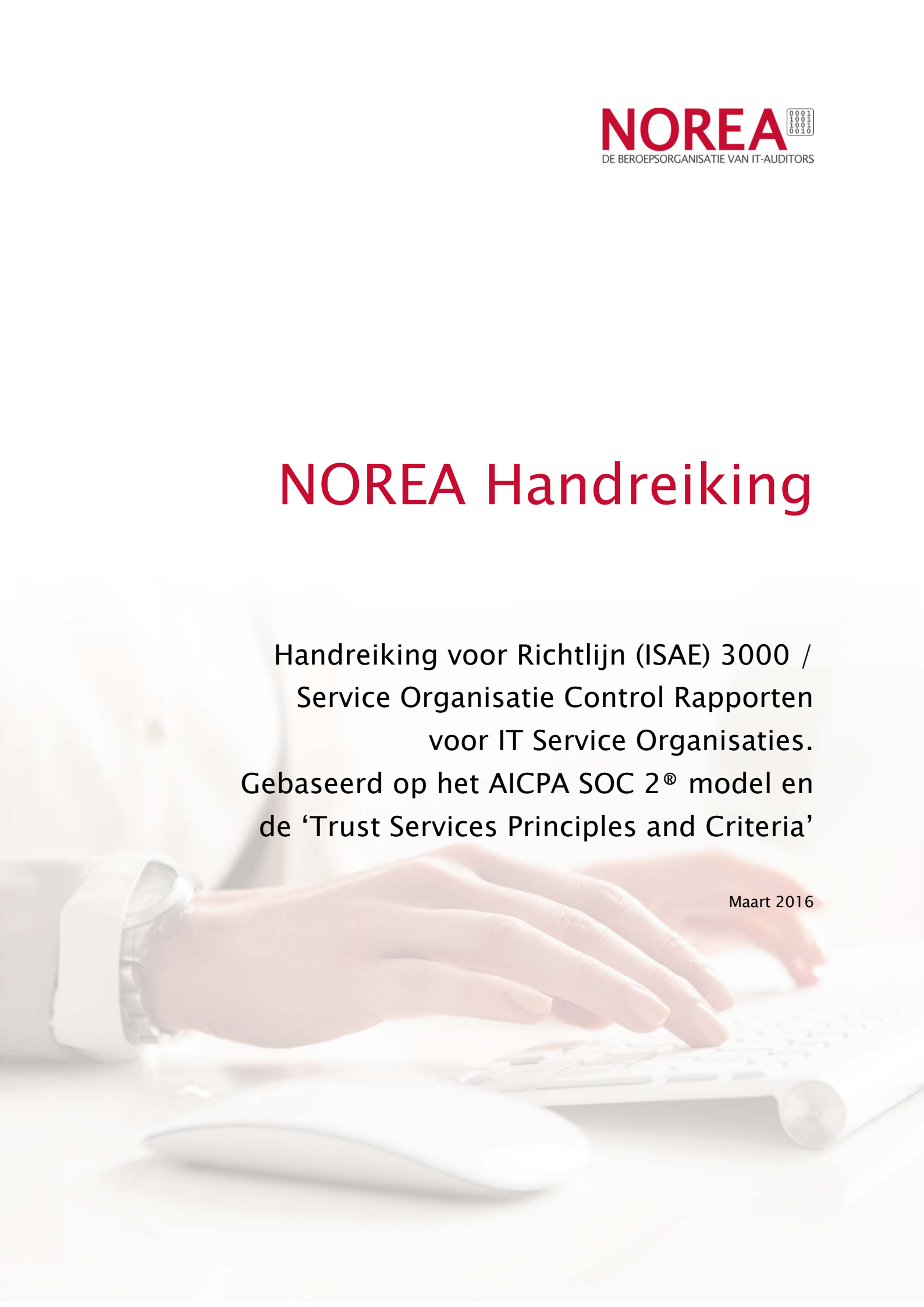
Chair	Han Boer	NOREA
Core team	René Ewals	ACS
Core team	Dennis Houtekamer	EY
Core team	Ronald van Langen	KPMG
Team member	Jan de Heer / René van de Hesseweg	KPN
Team member	Jan de Heer	KPN
Team member	Lars Hoogendijk / Marco Francken	BDO
Team member	Dave Klingens	Deloitte
Team member	Jan Matto	Mazars
Team member	Wilfried Olthof	NOREA
Team member	Tom Ooms / Dennis Stienen	PWC
Intermediate NBA	Jan Thijs Drupsteen	NBA
Advisor	Stacy Warmer	KPMG

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA Handreiking

Handreiking voor Richtlijn (ISAE) 3000 / Service Organisatie Control Rapporten voor IT Service Organisaties. Gebaseerd op het AICPA SOC 2® model en de 'Trust Services Principles and Criteria'

Maart 2016



Inhoudsopgave

1 Inleiding

1.1 Achtergrond

Deze handreiking is ontwikkeld voor Nederlandse IT auditors (RE's) om hen handvatten te geven voor het uitbrengen van Service Organisatie Control 2 rapporten (hierna: SOC 2®) onder ISAE 3000 of het equivalent de NOREA 'Richtlijn 3000 Assurance-opdrachten door IT-auditors'[13]. SOC 2® is een door het American Institute of Certified Public Accountants (AICPA) uitgebrachte guide. Deze Nederlandse publicatie is geen nieuwe richtlijn maar is een handreiking voor Register IT auditors (hierna: auditors) en kan ook nuttige achtergrond informatie geven aan de gebruikers van SOC 2® assurance-rapporten.

De publicatie van de handreiking speelt in op een groeiend aantal verzoeken vanuit IT serviceorganisaties voor de inzet van IT auditors bij het uitbrengen SOC 2® rapportages in Nederland. SOC 2® is geen standaard, maar een specifieke invulling van de Amerikaanse assurance standaard AT 101[14]. Deze handreiking geeft handvatten voor het uitbrengen van gelijksoortige rapporten gebaseerd op ISAE 3000. De auditor werkt hierbij niet onder Amerikaanse wet- en regelgeving. Professioneel gezien is er sprake van het opstellen van een ISAE 3000 rapport. IT Auditors verwijzen daarbij naar het lokale Nederlandse equivalent van ISAE 3000: 'Richtlijn Assurance-opdrachten door IT-auditors (3000)'.

De structuur van het specifieke ISAE 3000 / Service Organisatie Control Rapport volgt het formaat van ISAE 3402 (in de Verenigde Staten: SSAE 16 / AT section 801, met de service naam 'SOC 1®') met een reikwijdte als vastgelegd in de 'Trust Services Principles and Criteria'.

Opdrachten die worden uitgevoerd onder deze handreiking vallen uitsluitend onder Nederlandse wet- en regelgeving, waaronder de NOREA-reglementen en -richtlijnen. Deze Nederlandse opdrachten vallen niet onder de Amerikaanse wet- en regelgeving, waaronder AT 101. Om duidelijk te maken dat rapporten worden uitgevaardigd onder Nederlandse wet- en regelgeving, is het zaak om in de naamgeving gebruik te maken van de aanduiding **ISAE 3000 / Service Organization Control Report** en voor Nederlands gebruik van **Richtlijn 3000 / Service Organisatie Control Rapport**. Het is verder zaak om de aanduiding SOC 2® te vermijden om misverstanden kunnen te voorkomen over de vraag welke wet- en regelgeving de context van het rapport vormt.

[13] Referenties aan ISAE 3000 in deze publicatie mogen ook worden vervangen door 'Richtlijn Assurance-opdrachten door IT-auditors' (3000)'. Vanuit het oogpunt van leesbaarheid nemen we geen dubbele referenties op.

14 In de loop van 2016 zullen de AICPA assurance standaarden wijzigen, waaronder de namen van de standaarden.

1.2 Doelstelling

Hoewel het niet de doelstelling is van deze handreiking, geeft deze ook handvatten om te bepalen welk type assurance-rapport het beste past bij de behoeften van de gebruikers in specifieke situaties:

- ISAE 3402-rapport voor IT service organisaties die gebruikende entiteiten zekerheid willen bieden over de beheersingsmaatregelen die relevant zijn voor hun financiële rapportage processen.
- ISAE 3000 / Service Organisatie Control Rapport voor IT service organisaties die zekerheid willen bieden over de beheersingsmaatregelen op het vlak van Beveiliging, Beschikbaarheid, Integriteit van processen en Vertrouwelijkheid en Privacy.

Een ISAE 3000 / Service Organisatie Control Rapport richt zich – in lijn met ISAE 3402 – op de beheersingsomgeving en de beheersingsmaatregelen in een serviceorganisatie en verschaft geen zekerheid over de uitkomsten van processen (zoals bijvoorbeeld het voldoen aan Key Performance Indicators (KPI's) in Service Level Agreements (SLA))

De voor de Nederlandse auditors opgestelde handreiking is in de Engelse taal, dit om qua terminologie dicht bij de Amerikaanse SOC 2® guide te blijven. De voorliggende handreiking is een vertaling van deze Engelstalige handreiking. Beide zijn nadrukkelijk bedoeld voor gebruik door Nederlandse auditors. Tijdens de ontwikkeling van deze handreiking heeft de werkgroep contact onderhouden met de AICPA om te waarborgen dat de Nederlandse handreiking over het omgaan met SOC 2® niet conflicteert met Amerikaanse regelgeving. Wij benadrukken dat een ISAE 3000 / Service Organisatie Control Rapport een Nederlands equivalent is. Een SOC 2® rapport moet voldoen aan de Amerikaanse standaarden (waaronder AT 101) en vereist een oordeel van een auditor (CPA), lid van de AICPA.

1.3 Vereist kennisniveau

Om deze handreiking goed te begrijpen is kennis nodig van het raamwerk voor assurance-opdrachten en van de standaarden ISAE 3000 en ISAE 3402. We verwijzen alleen naar deze standaarden waar dat nodig is om de juiste context te verschaffen. De handreiking gaat er vanuit dat de auditors kennis hebben van inhoud van de meest recente versie van de AICPA SOC 2® guide en de Trust Services Principles and Criteria (TSP sectie 100, hierna 'TSP') Kennisname hiervan is noodzakelijk omdat niet alle details zijn overgenomen in deze Nederlandse handreiking. De lezer moet zich er bewust van zijn dat nieuwe versies van deze basis documenten invloed kunnen hebben op de invulling van de werkzaamheden en / of de rapportage.

1.4 Beperkingen

Een van de beginselen in de TSP sectie 100 is “privacy”. De recent vernieuwde TSP privacy criteria zijn opgesteld vanuit de Amerikaanse regelgeving. Voor het Nederlandse domein is nieuwe EU regelgeving op komst , Om niet op de zaken vooruit te lopen hebben we het privacy beginsel niet verder in deze handreiking uitgewerkt. Niettemin noemen we in een aantal gevallen de specifieke privacy elementen om goed de relatie tussen deze handreiking en AICPA SOC 2® te laten zien. De bescherming van privacy omvat IT gerelateerde beheersingsmaatregelen en vraagt om de naleving van specifieke procedures. Het beginsel Vertrouwelijkheid uit TSP sectie 100 kan zinvol zijn voor de beoordeling van beheersingsmaatregelen op het gebied van IT infrastructuur die gerelateerd zijn aan privacy.

De AICPA kent naast SOC 1® en SOC 2® ook SOC 3® rapporten. Een SOC 3® rapport past als een serviceorganisatie een beknopt openbaar rapport (een certificaat) wil publiceren binnen dezelfde scope als SOC 2®. SOC 3® geeft daarmee opnieuw vorm aan het oude WebTrust, een assurance-product dat nooit erg populair is geweest. De door de AICPA uitgegeven handreikingen zijn nog niet geactualiseerd voor deze “rebranding” van het WebTrust certificaat.

Evenals het geval is bij SOC 2® is er bij SOC 3® sprake van een rapport dat is gepubliceerd onder de Amerikaanse wet- en regelgeving (inclusief AT101) en dat wordt opgesteld door een CPA die aangesloten is bij de AICPA. Een auditor zou de SOC 3® handreikingen kunnen gebruiken voor het uitvoeren van reviews en het opstellen van vergelijkbare rapporten onder ISAE 3000. Dit valt echter buiten het bestek van deze handreiking.

De AICPA heeft logo’s ontwikkeld voor gebruik bij het uitvaardigen van een SOC 2®en SOC 3® rapport. Deze handreiking onderkent geen lokale equivalenten van deze logo’s. Verdere details zijn te vinden in hoofdstuk 2.5.

2 ISAE 3000 / Service Organisatie Control

2.1 Achtergrond

Een ISAE 3000 / Service Organisatie Control Rapport is een assurance-rapport dat zekerheid verschaft over de beheersingsmaatregelen die in dat rapport zijn geformuleerd. De AICPA onderscheidt drie geformaliseerde rapportages met betrekking tot service organisaties:

- SOC 1®: dit rapport is gebaseerd op SSAE 16 / AT 801, een Amerikaanse standaard afgeleid van de internationale ISAE 3402 standaard[15], en is alleen van toepassing voor assurance met betrekking tot processen die verbandhouden met financiële verantwoordingen.
- SOC 2®: dit rapport is gebaseerd op de Amerikaanse assurance standaard AT101, die min of meer het equivalent is van ISAE 3000. De rapportage heeft betrekking op de beginselen (in SOC 2® en TSP aangeduid met 'principle') van de TSP: Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en Privacy.
- SOC 3®: dit is een beknopt rapport voor een breed publiek gebaseerd op werkzaamheden gelijk aan SOC2®. Deze handreiking gaat niet verder op in, zoals toegelicht in paragraaf 1.4.

De voorliggende handreiking betreft de Nederlandse equivalent voor SOC 2® onder de standaarden en wet- en regelgeving zoals die van toepassing zijn voor bij de NOREA aangesloten register IT auditors.

2.2 Belangrijkste kenmerken

Het NOREA Service Organisatie Control Rapport is gebaseerd op ISAE 3000. De belangrijkste kenmerken van ISAE 3000 / Service Organisatie Control Rapport afgezet tegen ISAE 3402 of andere invullingen van ISAE 3000 zijn:

- De structuur van het rapport is vergelijkbaar met ISAE 3402 rapporten (zie ook paragraaf 2.4).
- Alleen een oordeel met een redelijke mate van zekerheid is mogelijk. Dit is een verschil met ISAE 3000, die ook de mogelijkheid biedt voor een oordeel met een beperkte mate van zekerheid.

[15] Voor de volledigheid merken we op dat een SOC 1® rapport onder de regelgeving van de AICPA is gebaseerd op de standaard 'Statement on Standards for Attestation Engagements no. 16' (SSAE 16). Deze verwijst naar AT 801, die op zichzelf de Amerikaanse implementatie is van de ISAE 3402 standaard).

- Het rapport is gebaseerd op de in de Trust Services Principles and Criteria (TSP) gedefinieerde reikwijdte en doelstellingen. De beginselen (principles) bepalen de criteria (beheersingsdoelstellingen). Een serviceorganisatie kan zelf bepalen welke beheersingsmaatregelen van toepassing zijn voor deze beginselen. In de TSP zijn onder de doelstellingen (criteria) voorbeelden van opgenomen.
- Er is – evenals in de ISAE 3402 standaard – sprake van type I en type II rapporten.
- Er is – in tegenstelling tot ISAE 3402 – geen sprake van een minimum review periode. Niettemin wordt geadviseerd dat een type II rapport minimaal betrekking heeft op een periode van drie maanden.
- Evenals bij ISAE 3402 moet het rapport een beschrijving omvatten van het systeem.
- Het rapport is bedoeld voor gebruikers die de inhoud en de doelstelling van het rapport kunnen begrijpen. De gebruikers van wie verwacht mag worden dat ze over deze kennis beschikken zijn:
    - het management van de serviceorganisatie;
    - het management van de gebruikende entiteit;
    - potentiële gebruikers die de informatie toepassen bij het selecteren van een serviceorganisatie of om vast te stellen of deze voldoet aan de eisen. Deze gebruikers verkrijgen de kennis daartoe tijdens het uitvoeren van de due diligence;
    - accountants en auditors die de beheersingsmaatregelen bij de gebruikende entiteit beoordelen;
    - Toezichthoudende autoriteiten.
- De rapporten zijn niet bestemd voor een breed publiek en mogen niet worden gepubliceerd op websites of andere publiek toegankelijke media. (zie ook hoofdstuk 4)

2.3 Professionele standaarden

De AICPA heeft voor Amerikaanse accountants een handreiking opgesteld voor het uitvoeren van onderzoeken van beheersingssystemen bij een IT serviceorganisatie met betrekking tot de beginselen Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en Privacy van de door het systeem verwerkte informatie. Een dergelijk onderzoek wordt aangeduid met de merknaam SOC 2® De rapportage over deze opdracht is een SOC 2® rapport.

SOC 2® is gebaseerd op AT sectie 101. Deze Amerikaanse attestation (assurance) standaard wordt gebruikt voor opdrachten waarin een auditor wordt ingeschakeld voor het onderzoeken van een specifiek onderwerp en het daarover afgeven van assurance-rapporten. De standaard gaat over assurance-opdrachten waarin een auditor zich ten doel stelt voldoende bewijsvoering te verzamelen om te komen tot een oordeel die het vertrouwen van de gebruiker – niet zijnde de verantwoordelijke partij – vergroot over het specifieke onderwerp. Het gaat hier om het meten

of evalueren van een specifiek onderwerp ten opzichte van criteria. ISAE 3000 is min of meer het internationale equivalent van AT sectie 101.

Deze handreiking is gebaseerd op ISAE 3000, een assurance standard met de volgende kenmerken:

- Het onderzoeksobject (de beschrijving van het systeem van de serviceorganisatie en de daarbij horende beheersingsmaatregelen) is afdoende beschreven.
- De uitgangspunten (criteria) die worden toegepast zijn geschikt gegeven de context van de opdracht.
- De normen waarvan de auditor verwacht dat ze zijn toegepast bij het opstellen van de informatie over het onderzoeksobject zijn beschikbaar voor de verwachte gebruikers van het rapport.
- De auditor verwacht voldoende bewijsvoering te kunnen verzamelen om tot een onderbouwd oordeel te komen.
- De conclusie van de auditor, in de vorm van een oordeel met redelijke zekerheid, wordt via een schriftelijk rapport uitgebracht.
- Het rapport dient een redelijk doel (met andere woorden: het heeft waarde voor de gebruikende entiteit).

Het in deze handreiking beschreven volwaardig equivalent van een SOC 2® assurance-opdracht onder de in Nederland van toepassing zijnde standaarden is gebaseerd op een van de drie volgende implementaties van standaard 3000:

- ISAE 3000.
- De Nederlandse equivalenten:
    - NBA Standaard 3000 (HRA NV COS);
    - NOREA Richtlijn 3000.

De tekst in deze handreiking verwijst naar ISAE 3000 aangezien dit de bron is van de Nederlandse NOREA richtlijn en de NBA standaard en deze aanduiding wordt herkend buiten Nederland.

2.4 Structuur van het ISAE 3000 / Service Organisatie Control rapport

Om aan ISAE 3000 te voldoen en tegelijkertijd duidelijk te maken dat het een volwaardig equivalent is van SOC 2® bevat de titelpagina:

[*Naam van de serviceorganisatie*]
[*Korte beschrijving van de service*]
[*Datum van waarneming in het geval van een type I rapport*]
[*De review periode in geval van een type II rapport*]

ISAE 3000 / IT SERVICE ORGANISATIE CONTROL RAPPORT GEBASEERD OP HET SOC 2® RAPPORT MODEL EN DE TRUST SERVICES PRINCIPLES AND CRITERIA

RELEVANT VOOR [Gevolgd door een of meer beginselen *:* BEVEILIGING, BESCHIKBAARHEID, INTEGRITEIT VAN PROCESSEN EN/OF VERTROUWELIJKHEID.].

De inhoudsopgave omvat doorgaans de volgende elementen:[16]

Sectie I: Vermelding van het management[17]
Sectie II: Assurance-rapport van de onafhankelijke auditor
Sectie III: Beschrijving van het systeem door de service organisatie
Sectie IV: De gehanteerde beginselen en criteria en de door de auditor uitgevoerde testwerkzaamheden inclusief de uitkomst daarvan (optioneel bij een type I rapport)
Sectie V: Overige informatie verschaft door de serviceorganisatie die niet is onderzocht door de auditor. Deze sectie is optioneel.

Hierna gaan we nader in op deze elementen.

Sectie I Vermelding van het management

De schriftelijke vermelding van het management van de serviceorganisatie omvat de volgende onderdelen:

- Het management stelt dat de beschrijving van het systeem van de serviceorganisatie een getrouw beeld geeft van het ontwerp en de implementatie op een bepaald moment of gedurende een bepaalde periode (respectievelijk type I en type II), gebaseerd op de criteria [met verwijzing naar hoofdstuk, paragraaf of paginanummers].
- Het management stelt dat de opzet van de beheersingsmaatregelen zoals geformuleerd in de beschrijving van het systeem voldoen aan de van toepassing zijnde criteria (TSP) per een bepaalde datum of gedurende een bepaalde periode (type I respectievelijk type II).

[16] In een ISAE 3402 rapport wordt de vermelding van het management vaak na het assurance-rapport van de auditor opgenomen. Voor een ISAE 3000 / Service Organization Control Rapport wordt de vermelding van het management in sectie 1 opgenomen aangezien het management verantwoordelijk is voor de onderliggende inhoud en het assurance-rapport ontworpen is om het vertrouwen bij de gebruikers daarover te vergroten.

[17] 'vermelding' is de vertaling overeenkomstig de vertaling van 'statement' in ISAE 3000; de AICPA gebruikt de term 'assertion'.

- Het management stelt dat de beheersingsmaatregelen zoals opgenomen in de beschrijving van het systeem effectief hebben gewerkt voor de van toepassing zijnde criteria (TSP) gedurende een bepaalde periode. (type II rapport).

In de bijlage is een voorbeeld opgenomen.

Sectie II Assurance-rapport van een onafhankelijke auditor

Deze sectie omvat (zowel bij een type I als II rapport) onder meer de volgende zaken:

- Gebruik van het woord 'onafhankelijk' in de titel van de paragraaf die het assurance-rapport bevat.
- De scope van de opdracht (inclusief sub-serviceorganisaties, verwachtingen ten aanzien van de beheersingsmaatregelen bij de gebruikende entiteit en/of andere informatie).
- De opmerking dat het management verantwoordelijk is voor de beschrijving van het systeem van de serviceorganisatie.
- Het oordeel:
    - In hoeverre de beschrijving een getrouw beeld geeft.
    - In hoeverre de opzet van de beheersingsmaatregelen afdoende is.
    - In een type II rapport: of er sprake is van een effectieve werking van de beheersingsmaatregelen

In de bijlage zijn voorbeelden opgenomen.

Sectie III Beschrijving van het systeem door de service organisatie

Deze sectie omvat de volgende componenten:

- Infrastructuur: de fysieke structuren van de gebruikte IT (zoals faciliteiten, computers, apparatuur, mobiele apparatuur, communicatienetwerken).
- Software: de applicatiesoftware en de systeemsoftware die deze applicatie software ondersteunt (zoals besturingssystemen, middleware, utilities).
- Mensen: de medewerkers die betrokken zijn bij de governance, het gebruik en het beheer van systemen (ontwikkelaars, operators, gebruikers en managers).
- Procedures: de geautomatiseerde en handmatige werkwijzen in en rondom het systeem.
- Data: de informatie die door het systeem wordt gebruikt en ondersteund (transacties, bestanden, databases, tabellen).

In aanvulling op deze eisen die specifiek zijn voor IT serviceorganisaties dient er verder nog aandacht te zijn voor de volgende aspecten:

- Beheersingsomgeving (zoals de filosofie van het management, beleid en management ten aanzien van beveiliging, fysieke beveiliging, beveiliging van medewerkers, beheersing van omgevingsfactoren, monitoring van systemen, problem management, back-up en herstel, systeem account management);
- Het proces van risicobeoordeling.
- Informatie- en communicatiesystemen.
- Monitoring van beheersingsmaatregelen.

NB deze aspecten met betrekking tot beheersingsomgeving worden in de eerst volgende TSP update opgenomen.

Sectie IV De gehanteerde beginselen en criteria en uitgevoerde testwerkzaamheden inclusief de uitkomst daarvan

Deze sectie omvat de gekozen beginselen, de criteria, de door de serviceorganisatie uitgevoerde beheersingsmaatregelen, de beschrijving van de testen door de auditor en de uitkomsten van de testen per criterium. De serviceorganisatie kiest het(de) van toepassing zijnde beginsel(en) en definieert de beheersingsmaatregelen die samenhangen met de bij de beginsel behorende criteria. De testaanpak en de uitkomsten van de test komen van de auditor. Bij een type II rapport is een omschrijving van de testen en de testuitkomsten uitkomsten een verplicht onderdeel van de rapportage. Voor een type I rapport is de beschrijving van de uitgevoerde testen op opzet en bestaan en de uitkomsten van deze tests optioneel.

Sectie V Overige informatie, verstrekt door de serviceorganisatie, die niet is onderzocht door de auditor.

Deze sectie is optioneel en kent geen vooraf gedefinieerde inhoudelijke elementen. De inhoud valt niet binnen de scope van het werk van de auditor. De inhoud mag echter niet tegenstrijdig zijn met de inhoud van het rapport of de werkzaamheden die zijn verricht door de auditor. Het is de verantwoordelijkheid van de auditor om dit vast te stellen. De serviceorganisatie kan in deze sectie informatie opnemen die zij van toegevoegde waarde acht voor de gebruiker van het rapport. Voorbeelden zijn:

- Het voornemen om nieuwe systemen te implementeren die relevant zijn voor de gebruikende entiteit of gebruikend systeem.
- Een plan van aanpak ter oplossing van onvolkomenheden die zijn opgenomen in het rapport.

- De reactie van het management op bevindingen die zijn geconstateerd door de auditor in geval deze reactie niet is beoordeeld door de auditor (bijvoorbeeld omdat de actie in de toekomst ligt).
- Andere diensten van de serviceorganisatie die niet binnen de scope van de opdracht vallen, zoals maatregelen gericht op het waarborgen van de continuïteit.

De sectie mag geen informatie bevatten die in tegenspraak is met observaties of oordelen van de auditor. Bovendien dient de inhoud een relatie te hebben met het onderwerp van het rapport.

2.5 Logo

De AICPA heeft een logo ontwikkeld[18] dat kan worden gebruikt door een serviceorganisatie als deze minstens over een van de genoemde SOC rapporten beschikt, verstrekt door een bij het AICPA aangesloten CPA die zich heeft gebaseerd op de AICPA-standaarden. Een service-organisatie kan bekendmaken dat assurance-rapporten beschikbaar zijn door deze logo's in drukwerk of online te gebruiken.

In de situatie waarin een Service Organisatie Control rapport is gebaseerd op ISAE 3000 (of het lokale equivalent) en afgeven door een Nederlandse IT auditor, wordt niet voldaan aan de eisen van het AICPA en kan het logo niet worden gebruikt. NOREA heeft geen Nederlands equivalent voor het logo.

Hoofdstuk 4 van deze handreiking gaat verder in op het onderwerp marketing en promotie van een ISAE 3000 / Service Organisatie Control rapport.

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

3 Uitvoering van een ISAE 3000 / Service Organisatie Control opdracht

De uitvoering van een ISAE 3000 / Service Organisatie Control opdracht verloopt conform de professionele standaarden zoals beschreven in hoofdstuk 2. Voor een succesvolle uitvoering is het nodig dat de inrichting van de serviceorganisatie voldoende ontwikkeld is en de organisatie een voldoende omvang heeft. Dit hoofdstuk bevat een aantal belangrijke aandachtspunten voor de verantwoordelijk auditor bij de uitvoering van de ISAE 3000 / Service Organisatie Control assurance-opdracht.

3.1 Ervaring en kennis auditor (engagement partner/team)

Er zijn twee hoofdvoorwaarden voor het accepteren of continueren van een ISAE 3000 / Service Organisatie Control opdracht door een auditor: (1) "De personen die de opdracht uitvoeren hebben samen de benodigde professionele competenties" en (2) "De auditor plant de uitvoering van de opdracht zodanig dat deze effectief kan worden uitgevoerd."

ISAE 3000 vereist dat de auditors naast een generiek kennisniveau ook specifieke kennis hebben van processen, technieken, bedrijfstak-specifieke aspecten en rapportering en dat teamleden alleen worden ingezet voor taken die overeenstemmen met hun kennisniveau en hun competenties zodat ze in staat zijn om tot bevindingen te komen en deze te beoordelen.

De auditor kan tijdens de opdracht tot de conclusie komen dat hij/zij op bepaalde onderdelen onvoldoende kennis of ervaring heeft op het vlak van vaktechniek, respectievelijk het onderwerp van de opdracht. De kennis wordt opgedaan door het volgen van onderwijs – waaronder zelfstudie – of door het opdoen van ervaring in de praktijk. Het is niet noodzakelijk dat de auditor persoonlijk alle benodigde kennis heeft om gekwalificeerd te zijn voor het afgeven aan een assurance-rapport. De kenniseisen kunnen deels worden ingevuld door specialisten in te zetten, mits de auditor voldoende kennis heeft om te communiceren met deze specialisten over de doelstellingen van het werk en in staat is om de uitkomsten van het werk van de specialisten te beoordelen om te zien of aan de doelstellingen is voldaan.

De auditor moet voldoende inzicht hebben in het expertisedomein van de specialist om de aard, scope en doelstelling van diens werk te kunnen definiëren en om vast te kunnen stellen of het werk van de specialist in het licht van de doelstellingen adequaat is. De Code of Ethics[19] bepaalt dat een auditor altijd voldoende professionele kennis en competenties moet bezitten. Dit betekent bijvoorbeeld dat het onwaarschijnlijk is dat een registeraccountant met weinig kennis van IT in staat is om een ISAE 3000 / Service Organisatie Control rapport uit te brengen zonder de hulp van een gespecialiseerde auditor.

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

Verder is het belangrijk dat de auditor begrip heeft van de diensten die door de serviceorganisatie worden ondergebracht bij sub-serviceorganisaties om vast te kunnen stellen of dit invloed heeft op het kunnen voldoen aan de trust services criteria door de service organisatie. Daarbij hoort ook het kunnen beoordelen of het management de juiste afwegingen heeft gemaakt over de vraag of een organisatie moet worden gekwalificeerd als een sub-serviceorganisatie (zie ook paragraaf 3.3)

3.2 Onafhankelijkheid

De auditor volgt de van toepassing zijnde standaarden ten aanzien van de professionele onafhankelijkheid. Het gaat hierbij om de gedragscode register IT auditors van NOREA[20] of voor de auditors die werken voor accountantskantoren de VIO ('Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten') van de NBA.

3.3 Opname methode / uitsluitingsmethode

Voor het management van een serviceorganisatie is het belangrijk om vast te stellen of de beheersingsmaatregelen behorende bij activiteiten die zij heeft uitbesteed aan een leverancier nodig zijn om te voldoen aan een of meer van de gedefinieerde criteria (TSP). Als dat het geval is, is er sprake van een sub-serviceorganisatie. Het is belangrijk dat al deze sub-service-organisaties tijdens de planning van een ISAE 3000 / Service Organisatie Control opdracht zo vroeg mogelijk worden geïdentificeerd.

Er zijn twee opties voor het omgaan met een sub-serviceorganisatie: de opname methode (inclusive method) en de uitsluitingsmethode (carve-out method). De keuze is een verantwoor-delijkheid van de serviceorganisatie. De auditor heeft de verantwoordelijkheid om de argumenten van het management te toetsen.

De opname methode gaat ervanuit dat de werkzaamheden van de auditor ook gericht zijn op de relevante beheersingsmaatregelen bij de sub-serviceorganisatie. De omschrijving van het systeem door de serviceorganisatie omvat dan ook, zover van toepassing alle elementen ten aanzien van de beginselen Beveiliging, Beschikbaarheid, Integriteit van processen en Vertrouwelijkheid (en privacy), waar deze liggen bij de sub-serviceorganisatie.

Bij de uitsluitingsmethode is het bovenstaande niet het geval. De betreffende activiteiten van de sub-serviceorganisatie worden niet opgenomen in de beschrijving van het systeem. Als de serviceorganisatie deze methode gebruikt dient dit te worden gemotiveerd door het management. Deze motivatie wordt opgenomen in het rapport, en wel in de paragraaf met het

[20] Hoewel de gedragscode van NOREA niet specifiek ingaat op het aspect onafhankelijkheid is er wel sprake van een fundamenteel beginsel 'Objectiviteit' als cruciale voorwaarde voor onafhankelijkheid. Dit beginsel stelt dat er geen sprake mag zijn van vooringenomenheid, conflicterende belangen of ongewenste invloeden die het oordeel kunnen beïnvloeden.

oordeel van de auditor. De auditor stelt vast of er – gegeven de uitsluiting – sprake is van een rationele opdracht die hij kan accepteren volgens de voorwaarden van de Code of Ethics.

De beschrijving van het systeem dient in het geval van sub-serviceorganisaties het volgende te omvatten:

- De aard van de services die door de sub-serviceorganisatie worden verleend
- Waar van toepassing aangeven dat beheersingsmaatregelen (mede) bij de sub-serviceorganisatie liggen.
- De beheersingsmaatregelen die nodig zijn bij een uitgesloten sub-serviceorganisatie om te voldoen aan de beginselen en criteria (TSP), al dan niet in combinatie met maatregelen bij de serviceorganisatie zelf.

De sub-serviceorganisatie – evenals de keuze voor een opname of uitsluitingsmethode – moet worden genoemd in de vermelding van het management en in het oordeel van de auditor.

Leveranciers worden vaak gezien als sub-serviceorganisaties. Echter, als de serviceorganisatie zelf de verantwoordelijkheid neemt voor de risico's en de noodzakelijke beheersings-maatregelen hoeft er geen aanleiding te zijn om deze leverancier te kwalificeren als een sub-serviceorganisatie. Voorbeelden daarvan zijn installatiebedrijven, verhuurders van datacenter-locaties.

3.4 Materialiteit en de beoordeling van bevindingen (uitzonderingen)

Een audit wordt uitgevoerd met een bepaald tolerantieniveau ten aanzien van bevindingen, ook wel materialiteit genoemd. Beslissend hierbij is de vraag of een bevinding bepalend is voor door de gebruiker van het rapport te maken afwegingen. Materialiteit heeft in de context van procedure gerichte assurance-rapporten betrekking op het systeem waarover wordt gerapporteerd (kwalitatieve materialiteit) en niet op financiële verantwoording van de gebruikende entiteiten. In de planning en uitvoering hanteert de auditor een materialiteit ten aanzien van drie gebieden: (1) de getrouwe presentatie van de beschrijving van het systeem (2) de opzet van de beheersingsmaatregelen en (3) in geval van een type II rapport de effectieve werking van beheersingsmaatregelen. Bij het bepalen van de materialiteit is het zaak om uit te gaan van de gebruikelijke verwachtingen en wensen van een brede groep gebruikers en hun auditors die begrip hebben van de wijze waarop het systeem van de serviceorganisatie wordt gebruikt.

De beschrijving van het systeem omvat de aspecten die nodig zijn om, met een redelijke mate van zekerheid, te kunnen komen tot inzicht in de uitvoering van transacties, zonder dat belangrijke aspecten ontbreken of zijn vertekend.

Bij het bepalen van de materialiteit spelen onder meer de volgende factoren een rol:

- De complexiteit van het proces dat wordt ondersteund door de beheersingsmaatregelen.
- Het inherente risico op fraude of fouten.
- Acceptabele en waargenomen niveaus van bevindingen.
- De aard en oorzaak van gedane bevindingen.

De initiële vaststelling van de materialiteit wordt door de auditor gedocumenteerd. Het is de basis voor een voorlopig oordeel over de toepasbaarheid van de criteria en voor de geplande testwerkzaamheden, gebaseerd op zijn begrip van het systeem van de service organisatie.

Nadat de werkzaamheden zijn uitgevoerd vindt een her- beoordeling plaats van de materialiteit op basis van de uitkomsten.

De auditor evalueert de bevindingen uit de testwerkzaamheden en onderzoekt de aard en oorzaak van de geconstateerde bevindingen. Op basis daarvan stelt hij vast of de uitkomsten reden zijn om te concluderen dat de beheersingsmaatregel niet voldoende effectief heeft gefunctioneerd in de betreffende periode.

Na het analyseren van de bevindingen en de invloed op de effectiviteit van de beheersings-maatregel stelt de auditor vast wat de impact is op het bereiken van de gedefinieerde beheersingsdoestellingen (criteria) – zowel de afzonderlijke doelstellingen als het geheel van de doelstellingen. De bevindingen kunnen in de volgende vier categorieën vallen. In veel gevallen is er een gedegen professionele afweging nodig om de categorie te bepalen.

- Bevindingen die duidelijk onbelangrijk zijn en waarschijnlijk geen impact hebben op het beginsel / de beginselen waar het assurance-rapport betrekking op heeft. In dit geval zijn de testwerkzaamheden voldoende basis voor de conclusie dat de beheersingsmaatregelen effectief hebben gewerkt gedurende de gespecificeerde periode.
- Bevindingen die niet tot gevolg hebben dat een beheersingsmaatregel als ineffectief wordt beoordeeld maar die wel relevant kunnen zijn voor een gebruikende entiteit. De relevantie wordt bepaald door de vraag of de auditor van mening is dat de uitzondering impact heeft op het beginsel / de beginselen waar het assurance-rapport betrekking op heeft.
- Bevindingen die aanleiding geven tot meer testwerk om vast te kunnen stellen of de betreffende beheersingsmaatregelen of andere beheersingsmaatregelen adequaat inspelen op het criterium en daarmee afdoende basis vormen voor een conclusie over de effectieve werking van de beheersingsmaatregelen gedurende de gespecificeerde periode.

- Bevindingen die tot de conclusie leiden dat de beheersingsmaatregel niet afdoende heeft gewerkt gedurende de gespecificeerde periode. De beheersingsmaatregel wordt dan beoordeeld als niet effectief.

Duidelijk onbelangrijke bevindingen zijn bevindingen die waarschijnlijk geen effect hebben op de organisatie van de gebruiker en de beoordeling van de interne beheersing door de accountant van de gebruiker. Het gaat dan om unieke of kleine zaken die niet door beheersingsmaatregelen worden afgedekt en slechts in een kleine toename van het controlerisico resulteren. De auditor adresseert alle bevindingen in het rapport. Er is geen materialiteitsniveau: alle bevindingen worden feitelijk genoteerd in de testresultaten om (werking van) de beheersingsmaatregelen te meten. De auditor stelt op basis van de analyse van de bevindingen vast of de doelstellingen van de beheersingsmaatregel(en) zijn gerealiseerd op basis van kwantitatieve en kwalitatieve materialiteit.

Indien er sprake is van bevindingen of als er naar aanleiding van bevindingen sprake is van een oordeel met beperkingen van de auditor betekent dit niet dat het rapport geen waarde meer heeft voor de gebruikende entiteit bij het beoordelen van de risico's op materiële onjuistheden. De gebruiker van het rapport gebruikt de informatie uit het rapport immers voor de eigen risico-inschatting.

Het is belangrijk dat de auditor in voldoende detail rapporteert over de bevindingen die voortkomen uit het testwerk, zodat de gebruiker goed inzicht krijgt in deze bevindingen en wat de oorzaak van de bevinding is. Daartoe is de volgende informatie nodig:

- De beheersingsmaatregel die is getest.
- Of het gaat om een test met betrekking tot een deelwaarneming of een test van de gehele populatie.
- De aard van de test.
- Het aantal geteste eenheden per test.
- Het aantal en de aard van de bevindingen.
- De oorzaak van de bevindingen.

Wanneer bij het testwerk bevindingen zijn geïdentificeerd kan het voor de gebruikers van het rapport zinvol zijn als het management, voor zover mogelijk, inzicht verschaft in de oorzaken van de bevindingen, de beheersingsmaatregelen die het effect van de bevinding compenseren, corrigerende acties en andere kwalitatieve factoren die gebruikers helpen om goed te begrijpen wat het effect is van de bevinding.

Deze informatie kan door de serviceorganisatie worden gepresenteerd in de optionele sectie van een type II-rapport getiteld 'Overige Informatie'. Deze sectie valt zoals beschreven in hoofdstuk 2 niet onder de verantwoordelijkheid van de auditor.

Een andere optie is dat het management in de sectie met de beschrijving van het systeem een reactie op de bevinding van de auditor opneemt. In dat geval dient de auditor vast te stellen of er voldoende onderbouwing is voor de reactie van het management door nadere inlichtingen in te winnen in combinatie met andere werkwijzen. Als er daarbij sprake is van toekomst-gerichte informatie vanuit het management – zoals het voornemen om beheersings-maatregelen te implementeren of bevindingen te adresseren – dient deze informatie te worden opgenomen in de sectie 'Overige Informatie'.

3.5 Types procedures

Het testen of beheersingsmaatregelen effectief zijn heeft als doel om vast te stellen of de verschillende gedefinieerde criteria worden behaald. Het testwerk moet zijn afgestemd op de omstandigheden en richt zich op het verkrijgen van een redelijke mate van zekerheid over het voldoen aan de criteria gedurende de gespecificeerde periode.

Bij het bepalen van het uit te voeren testwerk voor het vaststellen van de werking van de maatregelen beoordeelt de auditor de aard van de beheersingsmaatregelen, de beschikbare documentatie, de te behalen doelstellingen (criteria) en de verwachte efficiency en effectiviteit van de beschikbare test procedures en technieken. Het geheel van het testwerk wordt gebruikt om vast te stellen of de beschrijving van de beheersingsmaatregelen getrouw is en of de maatregelen effectief werken. Er zijn verschillende soorten test procedures, zoals hieronder opgenomen. In veel gevallen zal er sprake zijn van een combinatie.

Test procedure	Omschrijving
Inwinnen inlichtingen	Interviews met relevante medewerkers over de relevante beheersingsmaatregelen.
Observatie	Vaststellen dat specifieke beheersingsmaatregelen worden toegepast
Inspectie	Het lezen van documenten en rapporten die een indicatie geven over het functioneren van de beheersingsmaatregel. Dit omvat ook het lezen van (management) rapporten om te beoordelen of beheersingsmaatregelen adequaat worden gemonitord en of management tijdig actie onderneemt indien dat nodig is.
Herhaalde uitvoering	Het opnieuw uitvoeren van een beheersingsmaatregel om na te gaan of deze correct is uitgevoerd.

De ISAE 3000 standaard geeft meer achtergrond over het uitvoeren van deze test procedures.

Een ISAE 3000 / Service Organisatie Control rapport geeft geen oordeel in de uitkomsten van beheersingsmaatregelen of systemen. De auditor kan niettemin data analyse technieken of ander tooling inzetten om middels de output van het proces de effectiviteit van beheersingsmaatregelen te testen. Dergelijke testprocedures worden ingezet om de effectiviteit van de beheersingsmaatregelen te testen en dienen ter waarborging dat voldoende testwerk is uitgevoerd.

3.6 Types conclusies

In de bijlage is een voorbeeld opgenomen van een assurance-rapport.

Als de auditor in zijn conclusie beperkingen aanbrengt, dan geeft hij in het auditor's report een duidelijke omschrijving van de redenen daarvoor. Het gaat daarbij onder meer om de volgende gevallen:

- De beschrijving van het systeem door het management geeft in alle materiële opzichten geen getrouw beeld.
- De opzet van de beheersingsmaatregelen is onvoldoende om door onderzoek naar de werking te kunnen komen tot een redelijke mate van zekerheid dat de van toepassing zijnde beheersingsdoelstellingen (criteria) worden gehaald.
- Bij een type II rapport: de beheersingsmaatregelen hebben niet effectief gewerkt gedurende de gespecificeerde periode om de van toepassing zijnde beheersingsdoelstellingen (criteria) te halen.
- Er is sprake van een beperking in de scope die ervoor zorgt dat de auditor onvoldoende bewijs kan verkrijgen.
- De schriftelijke vermelding van het management geeft onvoldoende detail, gaat niet in op bevindingen van de auditor die leiden tot een oordeel met beperkte zekerheid of bevatten onvolkomenheden die het management niet bereid is aan te passen. Hierbij moet de vermelding van het management in lijn zijn met het assurance-report.
- Materiele inconsistentie tussen de overige informatie (sectie IV), en de inhoud van het rapport, zoals een verkeerde voorstelling van zaken, waarbij het management weigert om de informatie te corrigeren.

In de afweging over het aanpassen van het auditor's rapport houdt de auditor rekening met de gevolgen van individuele bevindingen ten aanzien van de vermelding van het management en het totaal van die bevindingen. Ook houdt de auditor rekening met de opzet en werking van de beheersingsmaatregelen gedurende de beoordeelde periode. De auditor weegt onder meer de volgende kwalitatieve en kwantitatieve factoren:

- De aard en oorzaak van de bevinding.
- De tolerantie die de auditor heeft gehanteerd ten aanzien van het aantal bevindingen.
- De alomtegenwoordigheid van de bevinding (bijvoorbeeld of de bevinding meer dan een criterium raakt).
- De waarschijnlijkheid dat de bevinding een indicator is dat er sprake is van tekortkoming die ertoe leiden dat criteria niet worden gehaald.

- De omvang van de fouten die kunnen ontstaan als gevolg van ontoereikende beheersingsmaatregelen.
- De vraag of gebruikers mogelijk misleid worden als het oordeel van de auditor geen beperking bevat.

Als de auditor geen goedkeurend oordeel afgeeft, dan neemt hij in het auditor's report een duidelijke omschrijving van de redenen op. Het doel is dat gebruikers van het rapport zelf kunnen beoordelen wat het effect is. Als geen goedkeurend oordeel mogelijk is kan de auditor kiezen voor een oordeel met beperking, een oordeelonthouding of een afkeurend oordeel,

4 Het gebruik van een ISAE 3000 / Service Organisatie Control Rapport

Een verschil met ISAE 3402 rapporten is dat de primaire gebruiker van een ISAE 3000 / Service Organisatie Control rapport veelal *niet* de accountant van gebruikende entiteit is, maar het management van de serviceorganisatie en het management van de gebruikende entiteiten (en toekomstige gebruikers en de toezichthouders). Een ISAE 3000 / Service Organisatie Control Rapport helpt het management om de uitbestede diensten te monitoren. Als een organisatie bijvoorbeeld back-up services bij een serviceorganisatie inkoopt zonder dat daarbij sprake is van bedrijfsgeheimen, zal dit niet relevant zijn voor de accountant en diens controle van de financiële verantwoording. Maar het management zal wel geïnteresseerd zijn in de beveiliging, beschikbaarheid en vertrouwelijkheid van deze service.

Niettemin kan een ISAE 3000 / Service Organisatie Control Rapport nuttig zijn voor de accountant van de entiteit die gebruik maakt van een service organisatie. Sommige beheersingsmaatregelen uit het rapport kunnen gerelateerd zijn aan processen die invloed hebben op de financiële verantwoording. De accountant heeft de verantwoordelijkheid om te beoordelen in hoeverre dit het geval is, aangezien het primaire doel en de scope verschilt van die van een ISAE 3402 rapport.

Het is mogelijk dat er misverstanden ontstaan over een ISAE 3000 / Service Organisatie Control Rapport als dit buiten de context wordt gebruikt waarvoor het is bedoeld. Het rapport is dan ook alleen bestemd ter informatie van en voor gebruik door het management van de serviceorganisatie en andere gespecificeerde partijen die voldoende kennis en begrip hebben van:

- De aard van de door de serviceorganisatie verleende diensten.
- Hoe het systeem van de serviceorganisatie samenhangt met de gebruikende entiteit, sub-serviceorganisaties en andere partijen.
- Interne beheersing en de beperkingen daarvan.
- Aanvullende beheersingsmaatregelen bij de gebruikende entiteit en hoe deze samenhangen met de beheersingsmaatregelen bij de serviceorganisatie om aan de van toepassing zijnde criteria te voldoen.
- De van toepassing zijnde criteria (Trust Services Principles and Criteria).
- De risico's die van invloed zijn op het voldoen aan deze criteria en hoe beheersingsmaatregelen deze risico's adresseren.

Gebruikers van het rapport die geacht worden over deze kennis te beschikken zijn:

- het management van de serviceorganisatie
- het management van de gebruikende entiteit
- het management van partijen die overwegen in de toekomst diensten te gaan afnemen van de serviceorganisatie
- auditors die beheersingsmaatregelen beoordelen of erover rapporteren
- toezichthouders.

Het rapport is niet bestemd voor gebruik door andere partijen dan de hiervoor genoemde.

4.1 Marketing en communicatie door de serviceorganisatie

Het rapport is alleen bestemd voor gespecificeerde gebruikers en het is niet toegestaan om generieke kwaliteitsuitingen te doen die inhouden dat het systeem van interne beheersing aan een audit is onderworpen en goedgekeurd door een onafhankelijke auditor. Ook andere claims (bijvoorbeeld dat een Service Organisatie Control certificaat is verkregen, of dat de serviceorganisatie beschikt over een systeem van interne beheersing van hoge kwaliteit) zijn niet toegestaan. Deze claims zijn niet correct, kunnen verkeerd worden geïnterpreteerd en zijn misleidend. De auditor dient dit bij zijn cliënt onder de aandacht te brengen.

Wat wel kan is dat een serviceorganisatie op haar website toelicht wat de aard is van het rapport, voor wie het rapport beschikbaar is en hoe die organisaties het rapport kunnen verkrijgen.

5 Beginselen en Criteria

5.1 Achtergrond

5.1.1 Introductie

De AICPA Assurance Services Executive Committee (ASEC) heeft een set beginselen en criteria ontwikkeld (Trust Services Principles and Criteria, kortweg TSP) voor het beoordelen van beheersingsmaatregelen op het gebied van Beveiliging, Beschikbaarheid, Integriteit van processen van systemen, Vertrouwelijkheid en Privacy. Deze beginselen en criteria worden van tijd tot tijd herzien. De beschrijving in deze handreiking gaat uit van de versie van 2014, die van toepassing is voor periodes die eindigen op of na 15 december 2014.

Het uitgangspunt van deze beginselen en criteria is de opzet, implementatie en operatie van het systeem van de serviceorganisatie dat bedoeld is om bepaalde zakelijke doelen te bereiken (zoals het verlenen van diensten of de productie van goederen) en dat is ingericht in

overeenstemming is met door het management gedefinieerde eisen. Er zijn vijf categorieën van systeem componenten: infrastructuur, software, mensen, processen en data.

Elk beginsel heeft een set criteria (in het Nederlands ook wel aangeduid met 'beheersings-doelstellingen'). Deze sets zijn er voor het beoordelen van de effectiviteit van beheersings-maatregelen voor zover deze relevant zijn voor de Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en Privacy van de informatie die door het systeem wordt verwerkt.

5.1.2 Trust Services Principles (TSP)

De Trust Services beginselen zijn de volgende:

- *Beveiliging:* Het systeem is beveiligd tegen ongeautoriseerde toegang, gebruik of aanpassing.
- *Beschikbaarheid:* Het systeem is beschikbaar voor gebruik zoals aangegeven door de serviceorganisatie of zoals overeengekomen.
- *Integriteit van processen:* De processen in het systeem zijn volledig, valide, accuraat, tijdig en geautoriseerd.
- *Vertrouwelijkheid:* De informatie is vertrouwelijk zoals overeengekomen.
- *Privacy:* Het verzamelen, gebruiken, opslaan en verstrekken en vernietigen van persoonlijke informatie is in overeenstemming met het privacybeleid van de gebruikende entiteit en met andere criteria.

5.1.3 Criteria (beheersingsdoelstelingen)

Een groot aantal van de criteria die worden gebruikt om een systeem te beoordelen zijn van toepassing op alle beginselen. De criteria zijn georganiseerd in algemene criteria die van toepassing zijn op alle vier de beginselen en in aanvullende criteria die specifiek gelden voor één beginsel:

Beginsel	Aantal criteria
Beveiliging	28 algemene criteria
Beschikbaarheid	28 algemene + 3 aanvullende criteria
Integriteit van processen	28 algemene + 6 aanvullende criteria
Vertrouwelijkheid	28 algemene + 6 aanvullende criteria
Privacy	Buiten de scope van deze handreiking

De algemene criteria vormen een complete set voor het beginsel Beveiliging. Voor de andere drie beginselen is sprake van een combinatie van algemene en aanvullende criteria.

De algemene criteria zijn gegroepeerd in zeven categorieën:

- *Organisatie en management.* Deze criteria (4) gaan over hoe de organisatie is gestructureerd en welke processen er zijn voor het managen en ondersteunen van medewerkers in afdelingen. De criteria gaan onder meer over verantwoordelijkheden, integriteit, ethiek, en de kwalificaties van de medewerkers en hun werkomgeving.
- *Communicatie.* Deze criteria (6) gaan over hoe de organisatie communiceert over beleid, processen, procedures, afspraken en eisen aan geautoriseerde gebruikers en andere partijen en de verplichtingen die deze gebruikers en partijen hebben ten aanzien van een effectief gebruik van het systeem.
- *Risicomanagement en het ontwerp en de implementatie van beheersingsmaatregelen.* Deze criteria (3) gaan over hoe de organisatie (i) potentiële risico's identificeert die van invloed kunnen zijn op het bereiken van de doelstellingen; (ii) deze risico's analyseert; (iii) reageert op deze risico's, waaronder het ontwerp en de implementatie van beheersingsmaatregelen en andere maatregelen die het risico verlagen en (iv) voortdurend monitort hoe risico's en het risicomanagement-proces zich ontwikkelen.
- *Monitoring van beheersingsmaatregelen.* Dit criterium (1) gaat over hoe de organisatie het systeem monitort, onder meer op geschiktheid, opzet en operationele effectiviteit van de beheersingsmaatregelen en over hoe de organisatie maatregelen neemt om onvolkomenheden te adresseren.
- *Logische en fysieke toegangsbeveiliging.* Deze criteria (8) gaan over hoe de organisatie voorziet in logische en fysieke toegangsbeveiliging tot het systeem en hoe ongeautoriseerde toegang wordt voorkomen om te voldoen aan de criteria in de assurance-opdracht.
- *Systeem operatie.* Deze criteria (2) gaan over hoe de organisatie het systeem uitvoert en daarbij detecteert waar er sprake is van bevindingen, waaronder inbreuken op logische en fysieke beveiliging, en daarmee voldoet aan de criteria in de overeenkomst.
- *Change management.* Deze criteria (4) gaan over hoe de organisatie nagaat of er veranderingen in het systeem nodig zijn, hoe deze veranderingen volgens een beheerst change management-proces worden doorgevoerd en hoe ongeautoriseerde veranderingen in het systeem worden voorkomen om te voldoen aan de criteria waar de assurance-opdracht op gericht is.

Voor het beginsel Beschikbaarheid gelden drie aanvullende criteria, voor de beginselen Integriteit van processen en Vertrouwelijkheid gaat het om zes aanvullende criteria. Meer informatie over de algemene en aanvullende criteria is te vinden in de AICPA bookshop[21]. In de bijlage is een overzicht opgenomen van de TSP, met uitzondering van privacy. TSP is onderhavig aan updates en het is dan ook aanbevolen om vast te stellen dat gebruik wordt gemaakt van de actuele versie.

5.2 Privacy

Het beginsel privacy vormt geen onderdeel van deze handreiking. Hiervoor zijn twee hoofdredenen:

- De criteria die gelden voor het principe Privacy zijn gebaseerd op de 'Generally Accepted Privacy Principles' (GAPP) die worden herzien. Het privacy principe is anders opgebouwd en staat hierdoor los van de overige principles.
- Ze staan in de TSP separaat van de beginselen Beveiliging, Beschikbaarheid, Integriteit van processen en Vertrouwelijkheid. GAPP ondersteunt het management bij het opzetten van een effectief programma dat de verplichtingen, risico's en kansen van privacy adresseert. GAPP is echter niet van toepassing in de EU en de criteria zouden moeten worden aangepast naar Nederlandse en Europese regelgeving.
- De Europese regelgeving rondom persoonsgegevens wordt herzien. Hoewel er op het moment van het schrijven van deze handreiking nog geen overeenstemming is over de finale versie en er sprake is van amendementen in de onderhandelingen, is er wel een duidelijke richting vastgesteld. De inwerkingtreding zal niet lang op zich laten wachten.

Het is belangrijk om te begrijpen dat het principe Privacy en de principes Integriteit van processen, Vertrouwelijkheid en Beveiliging sterk met elkaar samenhangen. Het is niet rationeel als een oordeel over veiligheid geen rekening houdt met universele elementen van privacy, zoals verantwoordelijkheid, transparantie, exclusiviteit, data kwaliteit, 'privacy by design' en 'privacy enhancing technologies'.

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

5.3 Aanwijzingen voor de vermelding van het management en het assurance-rapport

Een ISAE 3000 / Service Organisatie Control rapport geeft een oordeel over:

- De vraag of de beschrijving van het systeem van de organisatie getrouw is en gebaseerd is op de scope van de criteria (TSP).
- De vraag of de beheersingsmaatregelen in opzet een redelijke mate van zekerheid geven dat wordt voldaan aan de van toepassing zijnde criteria (TSP) als de beschreven maatregelen effectief werken.
- In type II rapporten: de vraag of de beheersingsmaatregelen effectief hebben gewerkt om te voldoen aan de van toepassing zijnde criteria (TSP).

Het management van de serviceorganisatie hanteert de aanwijzingen in paragraaf 5.3.1 (in SOC 2® aangeduid met 'criteria') bij het opstellen van hun vermelding (in SOC 2® aangeduid met 'assertion', ISAE 3000 – revised – aangeduid met 'statement') over het systeem en de auditor verwijst ernaar in zijn oordeel. Deze aanwijzingen zijn niet direct beschikbaar voor de gebruikers en om die reden dient het management alle aanwijzingen op te nemen in haar vermelding. Het is mogelijk dat niet alle aanwijzingen van toepassing zijn voor een specifiek geval. De aanwijzing v) is bijvoorbeeld niet van toepassing op een serviceorganisatie die geen rapportages of andere informatie verstrekt aan een gebruikende entiteit of andere partijen. De aanwijzing in vii) (2) is niet van toepassing bij een serviceorganisatie die geen gebruik maakt van een sub-serviceorganisatie. In dergelijke gevallen vinden gebruikers het doorgaans zinvol dat alle elementen waar de aanwijzingen betrekking op hebben in het rapport worden opgenomen en dat het management aangeeft welke normen om welke redenen niet van toepassing zijn. Dat kan zij doen in de beschrijving van het systeem of in een separate notitie over de uitwerking van de aanwijzingen voor de omschrijving.

5.3.1 Aanwijzingen voor de omschrijving

De aanwijzingen voor een getrouw beeld van de beschrijving van het systeem vereisen dat de volgende informatie in het rapport is opgenomen:

a. Beschrijving omvat:

I. De types dienstverlening.

II. De componenten van het systeem die worden gebruikt voor de diensten:

1. Infrastructuur. De fysieke structuren van IT en andere hardware (zoals faciliteiten, apparatuur, communicatie netwerken).
2. Software. De toepassingen en de systeemsoftware die deze toepassingen ondersteunt (zoals besturingssystemen, middleware, utilities).

3. Mensen. De medewerkers die betrokken zijn bij de governance, het gebruik en het beheer van systemen (ontwikkelaars, operators, gebruikers en managers).
4. Procedures. De handmatige en geautomatiseerde procedures in en rondom het systeem.
5. Data. De informatie die door het systeem wordt gebruikt en ondersteund (bestanden, databases, tabellen, transacties).

III. Afbakening van het object van de systeembeschrijving en de aspecten die aan de orde komen.

IV. Voor het verstrekken of ontvangen van informatie aan of van sub-serviceorganisaties en andere partijen,
1. hoe dit gebeurt, wat de rol van de sub-serviceorganisatie of andere partij is en
2. volgens welke procedures de serviceorganisatie vaststelt dat die informatie en de verwerking, onderhoud en opslag daarvan onderworpen zijn aan adequate beheersingsmaatregelen.

V. Voor elk principe waarover wordt gerapporteerd: de daaraan gerelateerde trust services criteria en de daarmee samenhangende beheersingsmaatregelen om te voldoen aan de criteria, waaronder:
1. Aanvullende beheersingsmaatregelen bij de gebruikende entiteit die zijn verondersteld bij het ontwerpen van het systeem van de serviceorganisatie.
2. In geval van toepassing van de opname methode: de beheersingsmaatregelen bij de sub-serviceorganisatie.

VI. Als gebruik wordt gemaakt van de uitsluitingsmethode voor de sub-serviceorganisatie,
1. de aard van de diensten die worden verleend door de sub-serviceorganisatie,
2. de van toepassing zijnde trust services criteria die moeten worden afgedekt door beheersingsmaatregelen bij de sub-serviceorganisatie, zelfstandig of in combinatie met beheersingsmaatregelen bij de service organisatie, en de typen beheersingsmaatregelen die naar geacht worden aanwezig te zijn bij de sub-serviceorganisatie om te voldoen aan deze criteria.

VII. Alle van toepassing zijnde trust services criteria die niet worden afgedekt door beheersingsmaatregelen en de redenen daarvoor.

VIII. In geval van een type 2 rapport de relevante veranderingen in het systeem van de serviceorganisatie gedurende de betreffende periode.

b. De beschrijving laat geen relevante zaken weg of geeft geen verkeerde voorstelling van zaken over het systeem en is opgesteld voor de algemene informatiebehoefte van een brede groep gebruikers. De beschrijving hoeft dekt daarom niet alle aspecten af te dekken die een individuele gebruiker belangrijk acht.

5.3.2 Aanwijzingen voor de opzet

De aanwijzing om vast te stellen of de opzet van de beheersingsmaatregelen voldoet betreft de vraag of de maatregelen, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat aan de van toepassing zijnde criteria wordt voldaan.

5.3.3 Aanwijzingen voor effectieve werking

De aanwijzing om vast te stellen of de beheersingsmaatregelen van het systeem effectief hebben gewerkt om te voldoen aan de van toepassing zijnde criteria (TSP) betreft de vraag of deze gedurende de specifieke periode consistent hebben gewerkt overeenkomstig de opzet, waaronder de vraag of de handmatige beheersingsmaatregelen zijn uitgevoerd door competente en bevoegde personen.

6 ISAE 3000 / Service Organisatie Control versus andere standaarden

6.1 Het 'mappen' van criteria

Een auditor heeft een norm nodig om in een assurance-rapport te komen tot een conclusie. Er zijn in de praktijk echter meerdere normen zoals ISO 27002 en PCI-DSS. In het geval van een ISAE 3000 / Service Organisatie Control rapport gaat het om de criteria van TSP. Indien TSP niet wordt gehanteerd is er sprake van een rapport dat niet in lijn is met de aanwijzingen van AICPA SOC 2® handreikingen. Ervan uitgaande dat het rapport voldoet aan de eisen van ISAE 3000 is er nog steeds sprake van een valide assurance-rapport wat waarde kan hebben voor een gebruiker. Het is echter geen ISAE 3000 / Service Organisatie Control rapport.

Bij het toepassen van andere raamwerken dan TSP kan het rapport de structuur van een ISAE 3402 rapport volgen, zoals aangegeven in paragraaf 3 van ISAE 3402.

Indien er tevens behoefte is aan een referentie naar een ander normen stelsel dan de TSP is een suggestie om het ISAE 3000 / Service Organisatie Control Rapport af te zetten tegen andere raamwerken, een praktijk die in de Verenigde Staten bij SOC 2® populair is. Veel professionals hebben 'mappings' beschikbaar voor hun cliënten van de TSP met ISO 27002, CMM[22], PCI-DDS, etc. De Cloud Service Alliance heeft een SOC 2® mapping gepubliceerd met de Cloud Control Matrix (CCM).

Deze handreiking gaat over de toepassing een ISAE 3000 / Service Organisatie Control Rapport. Mappings vallen buiten het bestek van dit document.

6.2 ISAE 3000 / Service Organisatie Control versus ISAE 3402

Zowel een ISAE 3000 / Service Organisatie Control Rapport als een ISAE 3402 assurance-rapport kan zekerheid verschaffen aan de accountant van een gebruikende entiteit. Het verschil is dat een ISAE 3402 altijd is gerelateerd aan processen die verbandhouden met de financiële verslaglegging en waarbij de beheersingsmaatregelen als hoofddoel hebben het bijdragen aan de betrouwbaarheid (juistheid, volledigheid, tijdigheid) van een financiële verantwoording. ISAE 3402 sluit aan op de eisen uit ISA 402 "audit considerations relating to an entity using a service organization".

Informatie technologie die ondersteunend is aan de administratieve processen kan onderdeel uitmaken van een ISAE 3402 rapport. Het kan ook de scope zijn van een ISAE 3402 rapport van IT service bureau waar applicaties worden uitgevoerd die een verband houden met de financiële verslaglegging. Echter een ISAE 3000 / Service Organisatie Control Rapport over beveiliging zal veelal beter inspelen op de behoefte van de gebruikende entiteit dan een ISAE 3402 rapport.

[22] CCM cloud control matrix, gepubliceerd door de CSA cloud security alliance

7 Bijlage

Deze bijlage bevat een template voor de vermelding van het management en geeft ter illustratie een voorbeeldtekst voor een assurance-rapport van een auditor. Deze bijlage omvat niet alle relevante voorbeelden en er kunnen actuelere versies beschikbaar zijn.

7.1 Vermelding van het management

Deze template voor de vermelding van het management in een ISAE 3000 / Service Organisatie Control rapport heeft de volgende beperkingen:

- Het beginsel Privacy valt niet binnen de scope.
- Er is geen invulling gegeven aan eventuele overwegingen betreffende beheersingsmaatregelen bij de gebruikende entiteit.
- Er is geen invulling gegeven aan eventuele sub-serviceorganisaties.
- Er is geen invulling gegeven aan een eventueel niet goedkeurend oordeel.

Vermelding van het management van {XYZ Service Organisatie}

Wij hebben de bijgevoegde beschrijving gemaakt met de titel "{Beschrijving van {juridische naam van organisatie}'s {naam of titel van systeem} Systeem over de periode {start datum} tot {eind datum}" (de beschrijving) gebaseerd op de criteria zoals genoemd onder de punten (a)(i)-(ii) hieronder (de criteria voor de beschrijving).

De beschrijving is bedoeld om gebruikers informatie te verschaffen over {type of naam van} systeem, en in het bijzonder beheersingsmaatregelen in het systeem om te voldoen aan de criteria voor {Beveiliging, Beschikbaarheid, Integriteit van processen en Vertrouwelijkheid} beginselen zoals uiteengezet in TSP section 100, "Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy", uitgegeven door het Assurance Services Executive Committee van de AICPA (van toepassing zijnde trust services criteria).

We bevestigen naar eer en geweten dat:

a) de beschrijving een getrouw beeld geeft van {type of name van} systeem gedurende de periode van {start datum} tot {eind datum} (de "gespecificeerde periode"), gebaseerd op de volgende normen voor de beschrijving:

   i. De beschrijving bevat de volgende informatie:

      1. De types dienstverlening.

      2. De componenten van het systeem die worden gebruikt voor de diensten:

a. Infrastructuur. De fysieke structuren van IT en andere hardware (zoals computers, apparatuur, mobiele telefoons, communicatie netwerken)

b. Software. De toepassingen en de systeemsoftware die deze toepassingen ondersteunt (zoals besturingssystemen, middleware, utilities).

c. Mensen. De medewerkers die betrokken zijn bij de governance, het gebruik en het beheer van systemen (ontwikkelaars, operators, gebruikers en managers)

d. Procedures. De handmatige en geautomatiseerde procedures in en rondom het systeem.

e. Data. De informatie die door het systeem wordt gebruikt en ondersteund (bestanden, databases, tabellen, transacties)

3. De grenzen die in de beschrijving aan het systeem worden gesteld en de aspecten die aan de orde komen.

4. Voor het verschaffen of ontvangen van informatie aan of van sub-serviceorganisaties en andere partijen,

   a. hoe dit gebeurt, wat de rol van de sub-serviceorganisatie of andere partij is

   b. welke procedures er zijn om vast te stellen dat die informatie en de verwerking, onderhoud en opslag daarvan onderworpen zijn aan adequate beheersingsmaatregelen.

5. De van toepassing zijnde trust services criteria en de daarmee samenhangende beheersingsmaatregelen om te voldoen aan de criteria, waaronder:

   a. Aanvullende beheersingsmaatregelen bij de gebruikende entiteit die dienen te worden overwogen in de opzet van het systeem.

   b. In geval van toepassing van de opname methode: de beheersingsmaatregelen bij de sub-serviceorganisatie.

6. Als gebruik wordt gemaakt van de uitsluitingsmethode voor de sub-serviceorganisatie,

   a. de aard van de diensten die worden verleend door de sub-serviceorganisatie;

   b. de van toepassing zijnde trust services criteria die moeten worden afgedekt door beheersingsmaatregelen bij de sub-serviceorganisatie, zelfstandig of in combinatie met beheersingsmaatregelen bij de service organisatie, en de typen beheersingsmaatregelen die naar verwachting nodig zijn bij de sub-serviceorganisatie om te voldoen aan deze criteria.

7. Alle van toepassing zijnde trust services criteria die niet worden afgedekt door een beheersingsmaatregel en de reden daarvan.
8. In de situatie van een type 2 rapport de relevante veranderingen in het systeem van de organisaties gedurende de betreffende periode.

ii. De beschrijving laat geen relevante zaken weg of geeft geen verkeerde voorstelling van zaken over het systeem en is opgesteld voor de gebruikelijke informatiebehoefte van een brede groep gebruikers. De beschrijving dekt daarom niet alle aspecten af die een individuele gebruiker belangrijk acht.

   a. De beheersingsmaatregelen die in de beschrijving zijn opgenomen zijn toereikend in opzet en bestaan gedurende de periode {start datum} toto {eind datum} om te voldoen aan de van toepassing zijnde trust services criteria
   b. De beheersingsmaatregelen die in de beschrijving zijn opgenomen zijn toereikend in opzet en bestaan en werking gedurende de periode {start datum} toto {eind datum} om te voldoen aan de van toepassing zijnde trust services criteria

{Officiële naam Service Organisatie}

{Naam}

{Titel}

{Datum}

7.2 Assurance-rapport ISAE 3000 / Service Organisatie Control

Ter illustratie.

Het assurance-rapport omvat minimaal de volgende elementen[23]	Voorbeeld
p) Een titel die duidelijk aangeeft dat het een onafhankelijk assurance-rapport betreft.	Onafhankelijk Service Auditor Rapport
q) De geadresseerde.	{Geadresseerde}:
r) Een aanduiding of beschrijving van het niveau van zekerheid dat door de auditor is verkregen, de informatie over het onderzoeksobject en, wanneer van toepassing het onderzoeksobject zelf.	We hebben de opdracht gekregen assurance te geven met een redelijke mate van zekerheid over de bijgaande beschrijving getiteld “Beschrijving van {juridische naam van serviceorganisatie}’s {naam of titel van systeem} Systeem” over de periode {start datum} tot {eind datum} (de beschrijving) en de geschiktheid van de opzet en effectieve werking van beheersingsmaatregelen om te voldoen aan de criteria {Beveiliging, Beschikbaarheid, Integriteit van processen en Vertrouwelijkheid} beginselen zoals uiteengezet in TSP section 100, “Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy”, uitgegeven door het Assurance Services Executive Committee van de AICPA (van toepassing zijnde trust services criteria) gedurende de periode van {Start Datum}, tot {Eind Datum} . De beschrijving geeft aan dat aan bepaalde van toepassing zijnde trust services criteria alleen kan worden voldaan als de in het ontwerp van het systeem van {juridische naam van serviceorganisatie} veronderstelde aanvullende beheersingsmaatregelen bij {officiële naam gebruikende entiteit} in opzet adequaat zijn en gedurende de gespecificeerde periode effectief hebben gewerkt, in samenhang met gerelateerde beheersingsmaatregelen bij {juridische naam van serviceorganisatie}. We hebben de opzet en werking van deze aanvullende beheersingsmaatregelen niet onderzocht. {Service Organisatie} gebruikt een serviceorganisatie (sub-serviceorganisatie) {Juridische naam van sub-serviceorganisatie} voor de {Sub-service Functies}. De beschrijving geeft aan dat aan bepaalde trust services criteria alleen kan worden voldaan als de beheersingsmaatregelen bij de sub-serviceorganisatie adequaat zijn in opzet en werking. De beschrijving gaat in op het systeem van {Service Entity}, de beheersingsmaatregelen die relevant zijn voor de van toepassing zijnde trust services criteria en de types beheersingsmaatregelen die de serviceorganisatie verwacht van de sub-serviceorganisatie (opzet en effectieve werking) om te voldoen aan de van toepassing zijnde trust services criteria. [Naam Service Organisatie] gebruikt voor de beschrijving de uitsluitingsmethode. De beschrijving van het systeem gaat dan ook niet in op de beheersingsmaatregelen die zijn getroffen bij de sub-serviceorganisatie. Onze

[23] ISAE 3000 paragraaf 69. Revised ISAE 3000 is van toepassing op assurance-opdrachten als het rapport is gedateerd op of na december 15, 2015. https://www.ifac.org/sites/default/files/publications/files/ISAE%203000%20Revised%20-%20for%20IAASB.pdf In Nederland zal een lokaal equivalent beschikbaar komen van de herziene ISAE3000 (vanuit NBA of NOREA) die van kracht zal worden voor rapporten gedateerd op of na 15 december 2016.

		opdracht strekt zich niet uit tot de beheersingsmaatregelen bij de sub-serviceorganisatie. De informatie met de titel "Overige Informatie verstrekt door {naam Service Organisatie} die niet valt onder het Service Auditor's Rapport" is opgenomen door <Name Entity NL> om additionele informatie te verschaffen en vormt geen onderdeel van de beschrijving van het {type} systeem dat ter beschikking is gesteld aan gebruikende entiteiten. Deze informatie is geen onderdeel van ons onderzoek naar de beschrijving en wij brengen daarover geen oordeel tot uitdrukking.
s)	De beschrijving van de van toepassing zijnde criteria.	De van toepassing zijnde criteria worden aangeduid in de vermelding van de {Service Organisatie}'s in combinatie met de van toepassing zijnde trust services criteria.
t)	Waar van toepassing, een beschrijving van de significante inherente beperkingen die verband houden met de meting of evaluatie van het onderzoeksobject ten opzicht van de van toepassing zijnde criteria.	De beschrijving van de {Service Organisatie} is opgesteld voor de algemene informatiebehoefte van een brede groep gebruikers en hun auditors. De beschrijving dekt daarom niet alle aspecten af die een individuele gebruiker belangrijk acht. Verder is het mogelijk dat beheersingsmaatregelen, vanwege hun aard en inherente beperkingen, niet altijd effectief werkten om te voldoen aan de van toepassing zijnde trust services criteria. Bovendien is de projectie van een eventuele beoordeling van de getrouwheid van de presentatie van de beschrijving of de conclusies omtrent de geschiktheid van de opzet of de effectieve werking naar toekomstige periodes onderhevig aan het risico dat het systeem wordt gewijzigd of dat interne beheersingsmaatregelen bij een serviceorganisatie inadequaat worden of tekortschieten.
u)	Wanneer de van toepassing zijnde criteria voor een bepaald doel zijn gekozen, een vermelding die lezers hierop attent maakt en op het feit dat, als gevolg hiervan, de informatie over het onderzoeksobject mogelijk niet geschikt is voor een ander doel.	Dit rapport en de beschrijving van de testwerkzaamheden en de resultaten daarvan is alleen gericht op gebruik door organisaties die gebruik maken van {Service Entity's Systeem Name} van {Service Organisatie} gedurende de gehele of gedeeltelijke periode van {Start Datum}, tot {Eind Datum} en onafhankelijke auditors die diensten verleen aan deze organisaties voldoende kennis en begrip hebben van: • De aard van de door de serviceorganisatie verleende diensten. • Hoe het systeem van de serviceorganisatie samenhangt met de gebruikende entiteiten, sub-serviceorganisaties en andere partijen. • Interne beheersing en de beperkingen daarvan. • Aanvullende beheersingsmaatregelen bij de gebruikende entiteit en hoe deze samenhangen met de beheersingsmaatregelen bij de serviceorganisatie om de van toepassing zijnde criteria in te vullen. • De van toepassing zijnde criteria (Trust Services Criteria). • De risico's die van invloed zijn op het voldoen aan deze criteria en hoe beheersingsmaatregelen deze risico's adresseren. Dit rapport is niet bedoeld voor gebruik door andere dan de hiervoor genoemde partijen en dergelijk gebruik is niet toegestaan.
v)	Een vermelding van de verantwoordelijke partij en van de evalueerder indien dit	{Service Organisatie} heeft de bijgevoegde {Titel Management vermelding} verstrekt, gebaseerd op de daarin geïdentificeerde criteria. {Service Organisatie} is verantwoordelijk voor (1) het opstellen van de beschrijving en de vermelding; (2) de volledigheid, accuratesse en de presentatie van zowel de beschrijving als

een andere partij betreft alsmede een omschrijving van hun verantwoordelijkheden.	de vermelding; (3) het verlenen van de diensten zoals in de beschrijving weergegeven; (4) het specificeren van de beheersingsmaatregelen die voldoen aan de van toepassing zijnde trust services criteria en de opname daarvan in de beschrijving; en (5) het opzetten, implementeren en documenteren van de beheersingsmaatregelen om te voldoen aan de van toepassing zijnde trust services criteria.
De verantwoordelijk-heid van de auditor. w) Een vermelding dat de opdracht is uitgevoerd conform deze handreiking. x) Een vermelding dat de auditeenheid waar de auditor werkzaam is of aan verbonden is en dat het Reglement Kwaliteitsbeheersing NOREA (RKBN) of regelgeving die ten minste gelijkwaardig is, toepast. y) Een vermelding dat de auditor het Reglement Gedragscode ('Code of Ethics') heeft nageleefd. z) Een informatieve samenvatting van de uitgevoerde werkzaamheden als basis voor de conclusie van de auditor.	Onze verantwoordelijkheid is het uitspreken van een oordeel over de getrouwheid van de presentatie van de beschrijving, gebaseerd op de criteria zoals uiteengezet in de vermelding van {Service Organisatie} en over hoe de opzet en werking van de beheersingsmaatregelen leiden tot het voldoen aan de van toepassing zijnde trust services criteria op basis van procedures die wij hebben gevolgd om een redelijke mate van zekerheid te verschaffen. We hebben onze assurance-opdracht uitgevoerd conform Nederlandse wetgeving en de NOREA Richtlijn Assurance-opdrachten door IT-Auditors (3000). Deze richtlijn vereist dat we de planning en uitvoering van onze opdracht zo inrichten dat er sprake is van een redelijke mate van zekerheid in ons oordeel. Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag. De auditeenheid past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhoudt het een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en procedures voor de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving. Onze assurance-opdracht omvat het uitvoeren van procedures die assurance-informatie over de vraag of de presentatie van de beschrijving getrouw is en dat opzet en werking van de beheersingsmaatregelen voldoen aan de van toepassing zijnde trust services criteria. Deze procedures hangen af van beoordelingen door de auditor en de inschatting van het risico dat de beschrijving niet getrouw is en dat de opzet en werking van de beheersingsmaatregelen niet voldoen aan de van toepassing zijnde trust services criteria. De procedures omvatten ook het testen van de effectieve werking van die beheersingsmaatregelen die we noodzakelijk achten om te komen tot een redelijke mate van zekerheid dat wordt voldaan aan de van toepassing zijnde criteria. Onze procedures omvatten ook de beoordeling van de overall-presentatie van de beschrijving. Naar onze mening hebben we voldoende assurance-informatie verkregen om te komen tot een oordeel met een redelijke mate van zekerheid.
aa) De conclusie van de auditor.	We hebben onze conclusie gevormd op basis van de zaken die in dit rapport uiteen zijn gezet. Ons oordeel, gebaseerd op de criteria uiteengezet in de vermelding van {Service Organisatie} en de van toepassing zijnde trust services criteria luidt dat: a. De beschrijving een getrouw beeld geeft van ontwerp en implementatie van [{type of naam} gedurende de periode van {Start Datum}, tot {Eind Datum}.

	b. De beheersingsmaatregelen zoals opgenomen in de beschrijving zijn geschikt om met een redelijke mate van zekerheid te voldoen aan de van toepassing zijnde trust services criteria als deze maatregelen effectief hebben gewerkt gedurende de periode van {Start Datum}, tot {Eind Datum}, en als de gebruikende entiteit de aanvullende beheersingsmaatregelen heeft getroffen zoals verondersteld in het ontwerp van het systeem van {Service Organisatie} gedurende de periode {Start Datum}, tot {Eind Datum}. c. De geteste beheersingsmaatregelen, die samen met de aanvullende beheersingsmaatregelen bij de gebruikende entiteiten, zoals beschreven in de scope-paragraaf van dit rapport, indien deze effectief werken, waren de maatregelen die nodig zijn om een redelijke mate van zekerheid te verschaffen dat de van toepassing zijnde trust services criteria worden behaald. Deze maatregelen werkten effectief gedurende de periode {Start Datum}, tot {Eind Datum}. De specifieke testwerkzaamheden op beheersingsmaatregelen en de aard, timing en resultaten daarvan zijn opgenomen in de sectie van dit rapport met de naam "Criteria, Beheersingsmaatregelen, Test Procedures, en Resultaten."
bb) Handtekening auditor.	{Handtekening auditor}
cc) Datum van het assurance-rapport.	{Datum van het assurance-rapport}
dd) De locatie in het rechtsgebied waar de auditor werkzaam is.	{Adres van auditor}

7.3 Trust Services Principles and Criteria

Gepubliceerd in 2014 door het American Institute of Certified Public Accountants and Chartered Professional Accountants of Canada. Deze set is van toepassing voor periodes die op of na 15 december 2014 eindigen.

- Criteria voor alle beginselen [security availability processing integrity and confidentiality] principles:
    - CC1.0 algemene criteria gerelateerd aan organisatie en management.
    - CC2.0 algemene criteria gerelateerd aan communicatie.
    - CC3.0 algemene criteria gerelateerd aan risk management en de opzet en implementatie van beheersingsmaatregelen.
    - CC4.0 algemene criteria gerelateerd aan monitoring van beheersingsmaatregelen.
    - CC5.0 algemene criteria gerelateerd aan logische en fysieke toegangscontrole.
    - CC6.0 algemene criteria gerelateerd aan systeem operaties.
    - CC7.0 algemene criteria gerelateerd aan change management.

- A1. Aanvullende criteria voor Beschikbaarheid.
- PI1. Aanvullende criteria voor Integriteit van processen.
- C1. Aanvullende criteria voor Vertrouwelijkheid.
- Generally Accepted Privacy Principles (august 2009).

Gedetailleerde documentatie is beschikbaar in de AICPA store (www.cpa2biz.com).

7.4 Belangrijkste verwijzingen naar handreikingen, professionele standaarden, artikelen en brochures

De handreiking AICPA SOC 2® en de Trust Services Principles and Criteria zijn te vinden in de AICPA bookshop: http://www.cpa2biz.com/.

De standard ISAE 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information is te vinden op: https://www.ifac.org/publications-resources/international-standaard-assurance-opdrachten-isae-3000-revised-assurance-enga.

De NOREA richtlijn Assurance-opdrachten door IT-auditors (3000) is te vinden op: http://www.norea.nl/readfile.aspx?ContentID=36665&ObjectID=344023&Type=1&File=0000036319_Richtlijn%20assurrance-opdrachtenC2.pdf.

7.5 Auteurs

Voorzitter	Han Boer	NOREA
Kernteam	René Ewals	ACS
Kernteam	Dennis Houtekamer	EY
Kernteam	Ronald van Langen	KPMG
Teamlid	Jan de Heer / René van de Hesseweg	KPN
Teamlid	Jan de Heer	KPN
Teamlid	Lars Hoogendijk / Marco Francken	BDO
Teamlid	Dave Klingens	Deloitte
Teamlid	Jan Matto	Mazars
Teamlid	Wilfried Olthof	NOREA
Teamlid	Tom Ooms / Dennis Stienen	PWC
Contactpersoon NBA	Jan Thijs Drupsteen	NBA
Adviseur	Stacy Warmer	KPMG