



# The new US assurance standard SSAE 18

A practical update of the international ISAE 3402?

**Organizations continue to outsource parts of their business to realize potential cost benefits, to alleviate the need for hiring or retaining internal specialists and/or to create more flexibility to realize their business strategy. Outsourcing also impacts both user and service organizations, the audit of the financial statements and the auditors involved in financial and IT audits. It is important to remain in control of the outsourced part of the business and IT processes. Assurance reports play an important role as a management control. In the USA, the new SSAE 18 standard was introduced in 2016 and implemented in 2017. Although the impact is indirect, because outside the USA local or international standards apply, such as the ISAE 3000 and ISAE 3402 standards, it is still an important transition, as the USA usually leads the development of these assurance standards globally. In this article we will look at the various assurance standards and perform an analysis on the impact for international, Dutch and American standards.**



**Dr. J.J. van Beek RE RA**  
is an IT audit partner at KPMG IT Advisory.  
[vanbeek.jaap@kpmg.nl](mailto:vanbeek.jaap@kpmg.nl)



**Dr. H.G.Th. van Gils RE RA**  
is a senior manager at KPMG IT Advisory.  
[vangils.herman@kpmg.nl](mailto:vangils.herman@kpmg.nl)

## INTRODUCTION

In April 2016, the American Institute of Certified Public Accountants (AICPA) Auditing Standard Board (ASB) issued the Statement on Standards for Attestation Engagements (SSAE) No. 18, Attestation Standards: Clarification and Recodification. The effective implementation date is for service auditor's reports dated on or after 1 May 2017. If your organization is routinely involved in the process of issuing a SOC1 (Service Organization Control) report, or your organization is considering issuing such an assurance report, you may wonder what changes the new standard SSAE 18 will bring. This will also be relevant to the user organizations receiving these reports. In this article, we start by introducing the main assurance standards currently in use. We discuss the reasons why a new standard was deemed necessary and then consider the main changes and potential impact for auditors, user and service organizations. In the next section, the formal differences between SSAE 18 and ISAE 3402 are highlighted, and the impact on dual purpose reporting will then be discussed, followed by a brief conclusion.

## WHAT ARE THE APPLICABLE ASSURANCE STANDARDS AND HOW DID THEY DEVELOP OVER TIME?

For as long as organizations have relied on third party providers for the delivery of outsourced services, those organizations have had a need for information about the internal controls at third parties. Whether the information was specific to how the third party ensured the quality of the services provided, the accuracy and completeness of transactions processed, the security of the information, or the overall health of its controls environment, many of the basic drivers for reliable and timely reporting have not changed over the last decades. For many years, assurance reports used in the Netherlands have been mainly based on the publications from the Dutch Institute for Public Auditors (NBA, previously NIVRA) number 26 (1982) and 53 (1989), on reliability and continuity of Electronic Data Processing, which formed the standard for providing assurance reports. These reports were mostly called Third Party Statement Reports (abbreviated to TPM in the Netherlands).

In early 2002, the United States issued the Sarbanes-Oxley (SOx) Act and Regulation. This regulation mandated publicly listed companies to issue an internal control statement along with their financial statements. The internal controls statement had to be based on a structured and substantiated system of internal control, which was often based on the COSO standard. The financial auditor had to examine and report on the internal control statement of management. In SOx for outsourced processes and controls, the SAS 70 assurance standard was used, which therefore also became popular in Europe and the Netherlands. The primary reasons were that many of the US-listed companies leveraged service organizations from outside the USA or companies centered in Europe became SEC listed. Since obtaining an SAS 70 was mandatory, many companies considered this to be the standard. Later, the international ISAE 3402 standard was developed (2009) which each country could translate into local regulations, which became 'Standaard 3402' or 'Richtlijn 3402' in the Netherlands and SSAE 16 in the USA. Due to all these different standard numbers the American Institute of Chartered Public Accountants introduced the term Service Organization Control (SOC), and used SOC1 as equivalent for the SSAE 16. Also outside the USA the term SOC1 is now often used as equivalent for the ISAE 3402.

## WHY A NEW STANDARD IN THE USA?

As described above, since the early nineties, service organizations have been using public accountants service auditor reports to communicate the basic drivers for reliable and timely information to interested parties. The American Institute of CPAs (AICPA) has been and remains the industry leader in providing organizations with a reporting framework for obtaining information on the service organization services, as well as providing the service providers and auditors with guidance for producing and interpreting this assurance information.

The AICPA's Auditing Standards Board (ASB) is the entity that maintains and develops the standards upon which service auditors reports are produced and relied on, and the underlying auditing procedures that produce these reports. In the summer of 2004, the AICPA's ASB embarked on a plan to improve the readability and understandability of its standards (including the service auditors reporting standards), as well as to increase the alignment of the US standards with similar standards managed by its international counterpart, the International Auditing and Assurance Standards Board (IASB). This clarity and convergence project has already resulted in significant changes in the service auditor reporting world, including the elimination of SAS 70 reports that were used for almost 20 years and the establishment of the service organization control or 'SOC'-branded reports SOC1, SOC2 and SOC3.

Perhaps more noteworthy is the identification, separation and codification of the various auditing and attestation standards themselves. Simply put, SSAE 18 is the standard that recodifies all the previous attestation standards. It is the culmination of the efforts to clarify the various standards for performing attestation engagements, which include combining, among many others, SOC1 (commonly referred to as SSAE 16) and SOC2 and SOC3 (sometimes referred to as AT section 101, which actually was a part of SSAE 16) into a single set of standards for auditors. Undoubtedly there will be report users, service providers and auditors, who will now be referring to SSAE 18 in much the same way that SAS 70, SSAE 16 and AT 101 are currently being used. However, for many parties these acronyms alone may be nothing more than general references to concepts or ideas about audits or assurance reports.

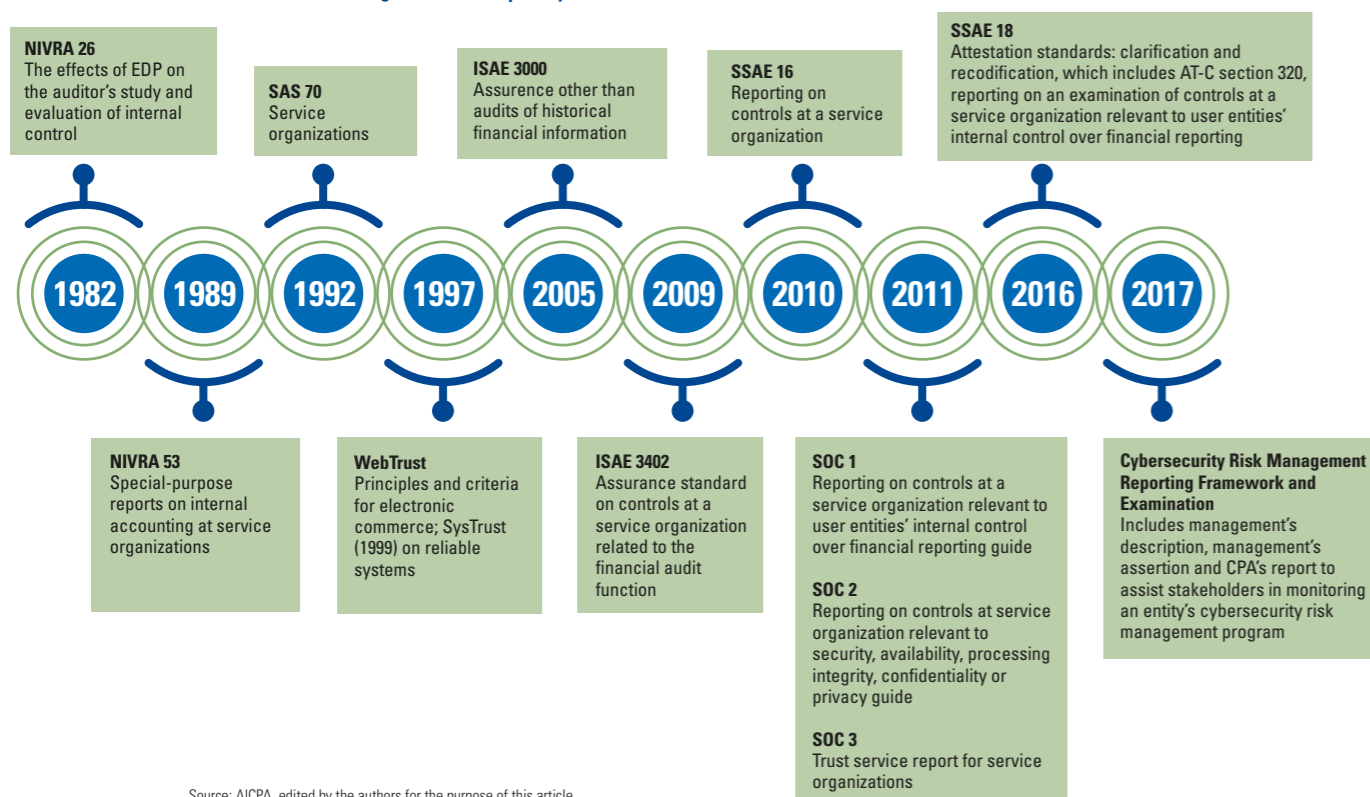
The scope of SSAE 18 will impact all attestation engagements in the USA, except for a limited number of exceptions. It will impact all Service Organization Control (SOC) reports like SOC1, SOC2 and SOC3. SSAE 18 is effective for Service Auditor's reports dated on or after 1 May 2017. Earlier adoption is permitted. Since the required implementation is based on the date

Since ISAE 3402 has scope limitations, because it only applies to internal controls that are relevant for the financial statements, there was also a need for assurance reports with a broader scope. In the ISAE 3402 standard, it is stated that the reporting and the assurance model can also be used with a broader scope, but that in that situation the ISAE 3000 standard has to be used. In the USA the SOC2 and SOC3 standards were developed for Security, Availability, Processing Integrity, Confidentiality and/or Privacy in 2011.

The most common assurance standards in the Netherlands nowadays are the Standaard/Richtlijn 3402 and Standaard/Richtlijn 3000, from both NBA and NOREA. Both standards are based on the international standards ISAE 3402 and ISAE 3000. Recently, both have been changed due to the Dutch clarification project, although with limited impact on either the service organization or the user organization. The main changes are using the term 'management statement' rather than 'management assertion' and referring more clearly to quality standards applicable for assurance engagements. Are these the only assurance standards in the Netherlands? No, there are others, such as for Sustainability the Standard 3410 and for Privacy the Standard 3600 by NOREA. However, as these standards will not be affected by the changes in SSAE 18, we will elaborate on other assurance standards in this article.

Figure 1. Timeline of assurance standards.

As shown in this timeline, auditors have been engaged to assess IT controls for decades. The new cybersecurity examination would be a continuation and outgrowth of this capability.



Source: AICPA, edited by the authors for the purpose of this article

**Table 1.** Organization of the clarified attestation standards.

AT-C section number	Title
n/a	Preface to the attestation standards
100	Common concepts
105	Concepts common to all attestation engagements
200	Level of service
205	Examination engagements
210	Review engagements
215	Agreed-upon procedures engagements
300	Subject matter
305	Prospective financial information
310	Reporting on pro forma financial information
315	Compliance attestation
320	Reporting on an examination of controls at a service organization relevant to user entities' internal control over financial reporting
395	Management's discussion and analysis

of the Service Auditor's Report, the new standards have the potential to impact a wide range of reporting periods.

For SOC reporting in the USA, the recodification of attestation standards (SSAE 18) is largely a simplified version of existing standards. The net effect is that an SSAE 16 SOC1 will look nearly identical to an SSAE 18 SOC1. The practitioners performing the attestation engagements will not notice many material changes in the standards; however, there are a few key aspects worth nothing for SOC1 reports, which we will discuss in the next section.

It is clear that the changes could be seen as a response to findings by the PCAOB in their reports on the quality of the financial audits. Re-emphasizing and clarifying standards can indeed help in the implementation of good practices in using the SOC reports as part of the financial statement audit. In that sense, the implemented changes could also help European practitioners to improve the quality of the assurance work performed.

Of course, the new SSAE 18 is still in line with the international (global) ISAE standards. In fact it is the Assurance Standard Board's strategy to converge its standards with those of the IASB. SSAE 18 is the container for all attestation engagements, including the global standards 3000, 3402 and 4400. So, SSAE 18 is more than solely the US equivalent of the ISAE 3402.

The equivalent of the ISAE 3000 is the AT-C 205 (plus the AT-C 105 which is always applicable). The equivalent of the ISAE 3402 is the AT-C 320 (plus the AT-C 205 and 105). This is the same structure as the ISAE framework, where in the ISAE 3402 it is stated that to comply with the ISAE 3402 the auditor must also comply with the ISAE 3000.

For Europe (and other countries) the impact remains to be seen. The differences between the old SSAE 16 and ISAE 3402 are very limited. It was therefore relatively easy in some countries to provide so-called dual reporting reports, which provide assurance according to both national and international standards. With the introduction of SSAE 18, these differences appear to widen. This effect has to be considered in case of dual reporting. The old and the new standards have appendices (Exhibit B in SSAE 16 and Appendix F in SSAE 18) to highlight substantive differences between SSAE 16 respectively 18 and ISAE 3402, and to explain the rationale for these differences. The same nine substantive differences are highlighted with minor textual changes.

One can also argue that SSAE 18 re-emphasizes certain aspects which are already part of ISAE 3402, but some formal new rules must be taken into considerations and can probably also be followed when issuing an ISAE 3402. In this way the ISAE 3402 and SSAE 18 are still close and dual reporting is possible. We will discuss this in more detail at the end of this article.

## CHANGES OR A FORMALIZED GOOD PRACTICE?

As the SSAE 18 is more recent than the ISAE 3402, some new rules were introduced, although they should not really be new to service organizations and service auditors that already adhere to the common good practices in audit standards. The changes or revisions are mainly based on convergence with ISAE 3000 (revised version) and with certain changes made to reflect professional standards. Table 2 outlines the 'new' elements in the SSAE 18 that are most important.

### 1. Information produced by the service organization (IPE)

In financial audits, especially for controls testing, the auditor is required to evaluate evidence around the completeness and accuracy of the so-called Information Produced by the Entity (IPE) (e.g. lists of data that have specific characteristics, exception documents, transaction reconciliations, documentation that provides evidence of the operating effectiveness of controls, such as user access lists and system generated reports), and the ability to include the procedures performed in the description of the tests of the controls. The audit technique for controls testing for financial audit and for SOC1 purposes should, of course, be similar. It is therefore clearly stated in the SSAE 18 that the service auditor is required to evaluate whether the information is sufficiently reliable and precise, and obtain evidence around completeness and accuracy.

The practical impact on the service organization could be high, as the service organization has to provide the service auditor with a thorough understanding of how information is produced and provide additional documentation as needed. The SSAE 18 standard does not impose a requirement on management to include the procedures in the description, but recommends inclusion in the description of the service auditor's test of controls. Although not explicitly stated in the ISAE 3402, the service auditor should also review the IPE on completeness and accuracy. This difference is therefore not very big, only making requirements that were already there more explicit. Outside the context of internal control for financial reporting we see that not all parties involved were aware of these requirements. In that case it is good to have this clarification, which will lead to more robust internal control frameworks.

### 2. Complementary User Entity Controls

From the beginning, the definition of the relevant 'Complementary User Entity Controls' (CUEC) was a challenging section and many service organizations had problems

**Table 2.** Most important 'new' elements in the SSAE.

New rules in SSAE 18	Related to ISAE 3402
• Information produced by the service organization (IPE)	• Should be common practice
• Complementary User Entity Controls	• Should be common practice
• Complementary subservice organization controls	• Will need more attention, as it is often not as extended as SSAE 18
• Obtaining evidence regarding design of controls	• Should be common practice
• Risk management and review of internal audit reports and regulatory examinations	• Should be common practice, although this could have more attention.
• Management assertion	• Also applicable for ISAE 3402, makes things more explicit

to write this section in the system description. As a consequence, a listing of user responsibilities or controls that were not necessary to achieve the control objectives were listed as well. The new standard now reinforces the fact that CUECs should only include controls that are *necessary* to achieve the control objectives stated in the management's description. The service auditor should evaluate the CUECs to determine if these are necessary to achieve the control objectives. If they are not, then they should be removed.

As with the previous aspect, this is not explicitly stated in the ISAE 3402, but was certainly intended as it now is in the SSAE 18, and should be common practice. For a more detailed analysis and practical solutions we refer to [Beek17].

## SSAE 18 formalizes what should already be common practice

### 3. Complementary subservice organization controls

In the USA, this revision is seen as the biggest change from the old standard. SSAE 18 requires that controls are implemented at the service organization that monitors the effectiveness of their controls over the subservice organization. The following monitoring activities are given as examples:

- reviewing and reconciling output reports;
- holding periodic discussions with the subservice organization;
- making regular site visits to the subservice organization;
- testing controls at the subservice organization by members of the service organization's internal audit function;
- reviewing Type 1 or Type 2 reports on the subservice organization's system;
- monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization.

When using the carve-out method to report on subservice organizations, the management will be required to identify controls that they assume will be implemented by these subservice organizations, and that are necessary to achieve the control objectives stated in the management's description. Of course, this is exactly the same as

**Box 1.** Example of changes in the management assertion due to control over subservice organizations (bold text).

#### Illustrative example of changes to management's assertion (excerpt)

- b.** The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period [date] to [date] to achieve those control objectives **if subservice organizations and user entities applied the complementary controls assumed in the design of XYZ service organization's controls throughout the period [date] to [date].** The criteria we used in making this assertion were that:
- i.** The risks that threaten the achievement of the control objectives stated in the description have been identified by the management of the service organization.
  - ii.** The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
  - iii.** The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

when user organizations and their auditors who obtain a SOC1 report are expected to evaluate their own controls, as stated in the Complementary User Entity Controls in the system description. Therefore, if a service organization obtains a SOC1 report from a subservice organization, it is important that the management and the service auditor evaluate the Complementary User Entity Controls in the SOC1 report of the subservice organization.

The impact on the service organization could be substantial, as the existing set of subservice organizations presented in the report needs to be evaluated and the impacted control objectives identified. The controls at each carved-out subservice organization to achieve the control objectives need to be linked and included in the description. A common example is when a service organization outsources data center operations to a co-location facility or its platform hosting services to a cloud services provider. In both instances, the service organization normally assumes that the co-location provider or cloud service provider has implemented controls regarding physical and/or logical safeguarding of their operating environment. As a result, those safeguards and controls would complement the additional controls to be performed by the service organization itself. In these instances, a description of such assumed complementary control should be included in the service organization's system description. As a result of this revision, the Service Auditor's report and the management assertion also need to be amended to reflect these changes.

### 4. Obtaining evidence regarding design of controls

This SSAE 18 revision changes the requirements for the service auditor with respect to obtaining evidence regarding the design of the control. The service auditor is to assess whether the controls identified by the management were suitably designed to achieve the control objectives by:

- obtaining an understanding of the management's process for identifying and evaluating the risk that threatens achieving the control objectives and assessing the completeness and accuracy of the management's identification of those risks;
- evaluating the link of the controls with these risks;
- determining that the controls have been implemented.

The management was already responsible for the design of controls under SSAE 16 and ISAE 3402; however, under the SSAE 18, the auditor will focus on management assessment rather than performing an independent assessment. As a result, the management should ensure that it is prepared to provide and discuss its assessment with the service auditor.

### 5 Review of internal audit reports and regulatory examinations

Whether or not the service auditor will make use of the work of Internal Audit, in the new standard the service auditor is required to review internal audit reports and regulatory examinations relating to the services provided to user entities and to the scope of the report. This requirement to review internal audit and regulatory examination reports is relevant for taking the findings into consideration as part of the risk assessment and in the nature, timing, and extent of the testing. The service organization needs to provide these reports to the service auditor completely and on time.

### 6 Management assertion

Several aspects are reinforced and explained more clearly in the SSAE 18:

- *Evaluation of criteria.* In the management assertion, the management is required to assess the suitability of the criteria in the system description. The standard defines information that must be included as a minimum. In practice, information was sometimes left out on the assumption that it was irrelevant. An example is: 'The types of services provided, including, as appropriate, the classes of transactions processed.', while a common hosting provider may argue that no transactions are processed, and thus will want to leave it out. Now, the management and the service auditor should ensure that the assertion contains all the criteria and that the management has included an explanation of how particular criteria are not relevant in their description.
- *Materiality language.* SSAE 18 deletes the phrase 'in all material respect', as it relates to the management assertion. A service organization will not be permitted to limit its assertion using the phrase 'in all material respects'.
- *Management assertion versus description.* SSAE 18 reinforces that the management assertion is not part of the management's description. If the assertion and description are included in the same section, they need to be clearly distinguished.

### WHAT ARE THE MORE FORMAL DIFFERENCES BETWEEN SSAE 18 AND ISAE 3402?

Many of the paragraphs in SSAE 18 have been converged with the related paragraphs in ISAE 3000 (revised). An important exception is that in the USA, a practitioner is not permitted to issue an assurance report if there is no written management assertion about the subject matter in scope, in relation to the criteria. In the ISAE 3000, this is not required, but seen as a good practice.

Next, we will outline the most important differences between the SSAE 18 and ISAE 3402 standards. This excludes terminology differences, such as the management's *statement* under ISAE 3402 that is called the management's *assertion* under US standards.

### Fraud by service organization personnel

If the service auditor notifies a deficiency, the auditor has to investigate the nature and cause of the deficiency. That is the same in both standards. In the new US standard, an additional requirement is included that if the service auditor becomes aware of fraud by the service organization personnel, the service auditor has to evaluate the risk that the system description is not fairly presented, controls are not suitably designed, and – in a Type 2 engagement – the controls are not operating effectively. Although this is not explicitly mentioned in the ISAE 3402, the discovery of fraud would normally have the same effect. Information about fraud effects the nature, timing, and extent of the service auditor's procedures.

### Anomalies

ISAE 3402 contains a requirement that enables a service auditor to conclude that a deviation identified during controls testing, with regard to sampling, is not representative for the entire population. SSAE 18 has not replicated this requirement, as it uses terms such as 'in extremely rare circumstances' and 'a high degree of certainty' that are not used in US professional standards.

### Direct assistance

SSAE 18 allows the use of the service provider's internal audit staff. ISAE 3402 does not address it, but does not prohibit it either. However, we note that in the Netherlands direct assistance is not allowed as part of the financial statement audit.

### Documentation completion

The requirement for completing the administrative process of assembling the final engagement file on a timely basis, is worded slightly different in both standards. The SSAE 18 indicates that a timely basis is no later than sixty days following the service auditors report release date.

### Subsequent events and subsequently discovered facts

These refer to events that occur between the end of the audit period and the issuing of the report, and that could have a significant effect on the subject matter or assertion. The ISAE 3402 does not require the service auditor to apply procedures other than making an inquiry. SSAE

18 requires auditors to also apply other appropriate procedures, like the review of documentation to obtain evidence regarding such events.

### Reading reports of the internal audit function and regulatory examinations

In the SSAE 18, the service auditor is explicitly required to read the relevant reports of the internal audit function and regulatory examinations. These findings are considered part of the risk assessment and for determining the nature, timing and extent of the tests. Although not explicitly in the ISAE 3402, this should be common practice for the auditor, regardless of which standard is used.

### Required written representations

SSAE 18 requires the service auditor to request specific written representations from the management. Some are not required by ISAE 3000 or ISAE 3402. In addition, there are differences with respect to the actions the service auditor is required to take when the management refuses to provide written representations.

### Elements of the service auditor's report required by SSAE 18, but not by ISAE 3402

SSAE 18 has certain additional requirements regarding the content of the service auditor's report. These requirements are very similar to the 'old' standard SSAE 16. These additional requirements are that the report for example includes a statement:

- that controls and control objectives included in the description are those that the management believes are likely to be relevant to user entities internal control over financial reporting, and that the description does not include those aspects that are not likely to be relevant to user entities internal control over financial reporting;
- that if the work of the internal audit function has been used to obtain evidence, then the report must include a description of the internal auditor's work and of the service auditor's procedures with respect to that work;
- that if the application of a complementary subservice organization's controls is necessary to achieve the related control objectives stated in the management's description of the service organization's system, then a statement to that effect is required;
- that the report is not intended to be and should not be used by anyone other than the specified parties.

We listed some of the new text elements to get an understanding. For the complete set we refer to the standard.

### Elements of the report required by ISAE 3402, but not by SSAE 18

ISAE 3000 requires the inclusion of a statement that the firm of which the practitioner is a member applies the International Standard on Quality Control (ISQC)1 or requirements, which are at least as stringent as the SSAE 18. Moreover, ISAE 3000 requires that the practitioner complies with the independence and other ethical requirements of the Code of Ethics for Professional Accountants or requirements that are at least as demanding. SSAE 18 does not contain these requirements.

Overall, when comparing SSAE 18 with SSAE 16, we note that slight changes have taken place, but that most of the differences with IASE 3402 have remained the same.

### WHAT ABOUT DUAL REPORTING?

User organizations sometimes lack understanding of the specific content of the standards (behind the acronyms). When a US user organization requested a SSAE 16 report from a service organization that is located in the Netherlands, the service organization auditor has to explain that they will provide an assurance report under the Dutch 'Standaard 3402'. In fact, that is the translated Dutch equivalent of the ISAE 3402 standard. The service auditor could consider to perform dual reporting, so that he provides an assurance report based on both the Dutch and international standards. This would be allowed for auditors in most countries. As SSAE 16 was the most used acronym for the US translation of the ISAE 3402 standard, this should be sufficient in most cases. As the differences between ISAE 3402 and SSAE 16 are very limited, the auditor could, in case of any issues, highlight these differences in a mapping table in (an appendix to) the report, so that the US-based user auditor can evaluate if this would be sufficient for his assurance needs.

In some instances, we noted that in the contract a requirement for a SSAE 16 (or 18) report is included. When the user organization does not understand the assurance context, sometimes the local service auditor is required to provide a dual report based on the SSAE 18 standard. We do not favor this solution. Based on this article, it should be clear that SSAE 18 is more than only the US equivalent. Therefore, we are very hesitant to refer to foreign auditing standards like SSAE 18. Most European auditors are not trained as a US CPA, and have no further guidance about how to overcome the differences between the standards (and references in standard 18 to other US standards and guidelines). Furthermore, an ISAE 3402 report should even be sufficient for US customers, therefore there is no need to refer to foreign standards. With the introduction of the new SSAE 18

standard, the situation is much the same, but as mentioned above, potentially more differences may be present. If dual purpose reporting takes place as an exception, it would be wise to use a checklist (as discussed in the previous section), based on the changes which SSAE 18 brings (in comparison to the SSAE 16) and the formal differences between SSAE 18 and ISAE 3402. Based on such a checklist, the service auditor can show the user auditor how he has considered the relevant issues. Based on the checklist, the user auditor can evaluate whether additional work is needed, or that he can rely on the work performed in the context of SSAE 18. In our opinion, using that solution would make dual reporting no longer necessary at all.

### CONCLUSION

Although the changes as a result of the new assurance standard SSAE 18 could be considered as limited, the impact could be significant in the ISAE 3402 or a local standard context. If the service organization and the practitioner have not followed the development of international professional audit standards, there will be a bigger impact. We would expect this especially in situations where assurance reports are used outside the context of internal control for financial reporting. It could then create a good evaluation moment if another assurance standard like ISAE 3000 would not be more appropriate. Most changes relate to improving the quality of assurance reports in the context of financial statement audits, which is beneficial for all parties involved. We consider it to be common sense to also implement changes resulting from the SSAE 18 in assurance engagements, in the case of ISAE 3402 or local standards.

### References

- [Beek12] J. van Beek, *Praktijkids 4; Service Organisatie Control-rapport, ISAE3402*, KPMG, 2012.
- [Beek17] J. van Beek and R. van Vught, *User control considerations voor ISAE3402-assurancerapportages*, Compact 2017/3.
- [Boerr13] H. Boer and J. van Beek, *Nieuwe ontwikkelingen IT-gerelateerde SOC-rapportages*, Compact 2013/2.
- [Bruck16] R. Bruckner, *Recodifying SOC reports: What SSAE 18 means for SOC1*, [www.accountingtoday.com](http://www.accountingtoday.com), December 2016.
- [Gils13] H. van Gils and J. van Beek, *Assurance in the Cloud*, Compact 2013/2.
- [Mell16] M. Mellor and N. Drury, *Moving from SSAE 16 to SSAE 18*, *Compass IT Compliance blog*, August 2016.
- [Palmer16] D. Palmer, *Clarified attestation standards-SSAE 18*, KPMG, September 2016.

### About the authors

**Drs. J.J. van Beek RE RA** is an IT audit partner at KPMG IT Advisory. He has more than 30 years of experience with all aspects of IT assurance and advisory engagements, with a focus on clients within Financial Services. Within EMA and the Netherlands he is the leader of the KPMG service line IT attestation and responsible for the development and deployment of the services in this domain. He published several articles and practice guides on assurance engagements.

**Drs. H.G.Th. van Gils RE RA** has been working as a senior manager at KPMG IT Advisory for more than 35 years. He focuses on IT attestation and advisory engagements (ISAE 3402/3000) and Privacy. His main clients are within the Financial Services sector. He is also active as a teacher at the University of Amsterdam.