



Reporting on Controls at Service Organizations

ADVISORY

Changes Ahead



For over 40 years, Statement on Auditing Standards No. 70 (SAS 70) and its predecessors have been the U.S. standard for reporting on controls at service organizations. In the post-Sarbanes-Oxley era, SAS 70 has evolved into a de facto global standard. The International Auditing and Assurance Standards Board (IAASB) and the Auditing Standards Board (ASB) in the United States have undertaken to develop new standards for reporting on controls at a service organization with a truly global constituency in mind.

Fundamentals of Change:

- SAS 70 to be superseded
- New auditing standard for user auditor
- New assurance standard for service auditor
- Assertion by management included in report – see page 6
- Suitable criteria – see page 7
- New service auditor’s report – see page 5

Type II opinions will cover a period of time for all three opinions.

Fundamentals of the Change

Under the approach adopted by the IAASB and the ASB, SAS 70 will be replaced by two standards: an auditing standard that will address the “user auditor’s” consideration of internal control when processing is performed by a service organization; and a new assurance standard that will guide service auditors in the conduct of an examination of, and the resultant reporting on, controls at a service organization.

As an assurance standard, the core framework for the service auditor will be based on ISAE 3000 (or as an attestation engagement under AT 101). The new assurance standard will require that management present an assertion regarding the subject matter of the report—in this case, the fairness of presentation of the controls, their suitability of design and the effectiveness of their operation. Likewise, the standard specifies the criteria that the service auditor must use to assess whether management’s assertion is fairly presented in all material respects. The new standard also includes a new service auditor’s report, based on the assurance standards, but significantly modified to reflect the history of SAS 70.

This paper provides an overview of the key provisions of the new standard and addresses some frequently asked questions.

Some Similarities and Differences Relative to the Existing SAS 70 Standard

Differences:

- The new standard will be an international assurance standard, not an audit standard. The service auditor's report will be significantly different.
- Management will be required to provide an assertion, which will be included in the report.
- In a Type II report, all three assertions/opinions will be for a period of time. (In a SAS 70 Type II report, the opinions on "fairness of presentation" and "suitability of design" are only as of the date at the end of the period.)

Similarities:

- Underlying work effort expected to be substantially the same.
- Two types of reports (Type I or Type II).
- Type II reports should cover a minimum of six months.
- Restriction on use—remains the same.
- Service auditor's tests included in report.
- Sample sizes disclosed only when exceptions are identified.



Suitable Criteria

A fundamental precept of the framework for assurance reporting is that the subject matter must be evaluated against "suitable criteria" as a basis for both management's assertion and the practitioner's examination opinion. Therefore, the new standard includes criteria that the IAASB/ASB have concluded are "suitable" in accordance with the guidance contained in the existing assurance literature (i.e., ISAE 3000/AT 101). Appendix A provides a summary of these criteria; however, we encourage everyone to read the relevant section of the final standards for a complete description.

Questions and Answers

I have heard that nothing is really changing—that is, that change embodied in the proposed new standard is form over substance. Is there any truth to this?

The sidebar on the right highlights some of the similarities to, and differences from, the existing SAS 70 standard.

However, this is an important effort to converge U.S. and international standards such that service auditors across jurisdictions can issue reports in accordance with locally developed standards, guidelines, and legal considerations. If a service auditor operates in a jurisdiction that adopts International Federation of Accountants (IFAC)/IAASB standards, then they may accept engagements in accordance with the related requirements of their jurisdiction (e.g., regarding independence, confidentiality).

What is the timetable/effective date for adoption of the new standards?

Timetable

The proposed effective date for the new standard is for reporting periods ending on or after June 15, 2011. Since service auditor reports may cover any period from six to twelve months, service auditors may be operating under the new standard as early as the 2nd quarter of 2010. The IAASB and the ASB are permitting early adoption of the new standard; thus, we may see reports issued under the new standard in the latter half of 2010.

PCAOB Auditing Standard No. 5 states that user organizations may rely on reports issued under AU324 (the existing SAS 70 standard). If service auditor reporting is no longer embraced by AU324, will the PCAOB standards permit registrants to rely on reports issued in accordance with the new attestation standard?

We believe that reports issued under both the new assurance and attestation standards will be acceptable under Auditing Standard No. 5, as well as the PCAOB's interim auditing standards.

If the report is to be based on an assertion by management that its controls are fairly presented, suitably designed, and operating effectively, is it anticipated that management will need to establish a "SOX-like" infrastructure to support its assertion—i.e., to document its controls and to assess their design and operating effectiveness?

No. It is not necessary that management put in place a function to document and assess its controls. However, the service auditor must be able to conclude that management has a reasonable basis to support its assertion. The application guid-

ance contained in the proposed standard states: "Management of the service organization is responsible for documenting the service organization's system. No one particular form of documentation is prescribed and the extent of documentation may vary depending upon the size and complexity of the service organization and its monitoring activities."

As such, management must have more than a passive interest in forming its assertion on the fairness of presentation of the system, the suitability of design of the controls, and the effectiveness of the operation of the controls to meet the specified control objectives.

Given that many of today's service organizations have processing facilities in multiple countries around the world, which standard must the service auditor follow—U.S. or International?

For those reports issued in the United States, the service auditor must issue the report in accordance with AICPA standards. Reports issued outside the United States would be issued in accordance with the applicable international standard. However, it is anticipated that these standards will be substantially the same. While certain differences between the two standards will exist in their final versions to accommodate the manner in which standards are framed and promulgated in each jurisdiction, it is anticipated that these will be minor and will not impact the intent or substance of the respective standards.

Are all countries obligated to follow the international standard? If not, what countries have indicated they will adopt the standard?

ISAE 3402 is proposed by the IAASB, which has the authority to establish auditing and assurance standards within IFAC. IFAC is the global organization for the accountancy profession. One hundred twenty-two countries' national professional accountancy bodies are represented in its membership, including the AICPA in the United States. Each of these countries will

adopt IAASB standards in accordance with its established protocols, similar to what the ASB is undertaking in the United States. It is expected that each member country will adopt ISAE 3402 in substantially equivalent form, if not verbatim. You can view the membership of IFAC at www.ifac.org.

Is there expected to be a transition period, during which both SAS 70 reports and reports under the new standard are acceptable?

It is the intent of both Boards (the IAASB and the ASB in the United States) that both versions of the standard be adopted with the same effective date. However, early adoption will be permitted under the new standards. As a result, there may be instances, prior to mandatory adoption, where SAS 70 reports, as well as the new reports may be issued. Thus, we may begin to see reports issued under the new standard in the latter half of 2010.

Will there be an impact on the degree of time and effort expended by the service auditor in the year of adoption of the new standard? Will there be any ongoing impact?

Based on the exposure drafts, we anticipate that the underlying effort to perform an assurance engagement will affect the service organization to varying degrees depending upon their particular environment. For example, if sub-service organizations are utilized and will be addressed using the inclusive method, a greater degree of effort may be required by the service auditor to address the requirements of the new standard.

I have heard that the new assurance and attestation standards permit reporting on nonfinancial systems; i.e., systems that are not part of the user organization's information systems relevant to financial reporting. Is this true?

The proposed standard does not directly permit reporting on nonfinancial systems.

A report issued under either standard may not be combined with a report on controls that are not likely to be relevant to user entities' internal control over financial reporting.

The guidance in the standards may be helpful to a practitioner performing an engagement under ISAE 3000/AT 101 to report on controls not relevant to internal controls over financial reporting. When the guidance in the new standards is used in the performance of such an engagement, the practitioner may encounter issues that differ significantly from those associated with engagements to report under the new standards. These issues include, for example, identification of suitable and available criteria, appropriateness of control objectives, identification of intended users and intended use, application of the concept of materiality, and development of the language to be used in the practitioner's report.

I understand that user auditor considerations are addressed within a separate standard. Do the proposed assurance and attestation standards present any significant changes to the way user auditors will use a service auditor's report?

No, they will not. ISA 402, Audit Considerations Related to an Entity Using a Service Organization, outlines user auditor responsibilities for obtaining sufficient appropriate evidence in an audit of the financial statements of an entity that uses one or more service organizations. User auditor requirements related to obtaining an understanding of the services provided by service organizations, assessing the risk of material misstatement in the financial statement audit, and using the service auditor's report remain largely unchanged from requirements outlined in existing guidance. ISA 402 does include new/updated guidance that aligns it to corresponding elements of the proposed



assurance and attestation standards and provides for additional user auditor responsibilities; however, such changes will not significantly impact the way user auditors use a service auditor's report.

Will the AICPA Audit Guide be updated? When?

We understand that such an update is planned by the AICPA. Given the required time lines for ASB review and approval, it is likely this will not be complete until the third or fourth quarter of 2010.

The IAASB will not issue an Audit Guide, and due to the fact that the IAASB and ASB standards are intended to be the same (for the most part), the AICPA Audit Guide may be useful for engagements performed under ISAE 3402.

What should we (the service organization) do?

1. Understand the change—particularly that you, and any sub-service organizations included in your report(s), will be required to provide an assertion that will be part of the report(s).

2. Engage your service auditor—the following topics should be discussed with your service auditor:

- Anticipated impact on their report and their work
- Their approach for performing an assessment of your management assertion
- Whether you are considering early adoption and implications to testing. Consider your customers' appetite for early adoption and the costs and benefits of early adoption
- The impact of sub-service organizations that are or may be within the scope of your current SAS 70 examination and how they will be treated within your report(s).

3. Plan for the transition—if planning activities are identified and scheduled for completion early in the process, a smoother and more efficient transition to the new standard may be achieved. Develop a transition time line that considers key implementation activities such as:

- **Conducting internal training** and awareness activities to help ensure that key members of the organization understand, and can fulfill, potentially new and changed responsibilities under the proposed standard. Such activities should include briefings with sales, support, and other customer-facing personnel so that they can effectively articulate changes to and answer questions from your customers.
- **Coordinating with your legal department** to review contracts with customers and, as necessary, sub-service organizations to identify required modifications resulting from the new standard.
- **Developing a customer communication plan** to help alleviate unnecessary customer anxiety over the transition to the new standard and be responsive to customer inquiries.
- **Reviewing your internal processes and current report(s)** to determine whether the criteria outlined in the new standard have been satisfied. Notably, you should identify the basis on which you will form your management assertion. Activities to form this basis may include periodic internal audits, management reports and related monitoring activities, quality assurance testing, service level agreement monitoring and reporting, and management's testing in support of Sarbanes-Oxley compliance.

Example: Service Auditor's Assurance Report

Following is an example of a service auditor's Type II report.
This is subject to change and further modifications by the firm.



Legal Member Firm Name
Street and/or postal address
City and code

Telephone 123 456 1234
Fax 123 456 1235
Internet www.memberfirm.kpmg.com

Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Effective Operation

To: XYZ Service Organization

Scope

We have been engaged to report on XYZ Service Organization's description at pages [bb-cc] of its [type or name of] system for processing customers' transactions throughout the period [date] to [date] (the description), and on the design and operation of controls related to the control objectives stated in the description.¹

XYZ Service Organization's Responsibilities

XYZ Service Organization is responsible for: preparing the description and accompanying assertion at page [aa], including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on XYZ Service Organization's description and on the design and operation of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization" issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organization and described at page [aa].

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

Limitations of Controls at a Service Organization

XYZ Service Organization'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, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described at page [aa]. In our opinion, in all material respects:

- The description fairly presents the [the type or name of] system as designed and implemented throughout the period from [date] to [date];
- The controls related to the control objectives stated in the description were suitably designed throughout the period from [date] to [date]; and
- The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from [date] to [date].

Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed on pages [yy-zz].

Intended Users and Purpose

This report and the description of tests of controls on pages [yy-zz] are intended only for customers who have used XYZ Service Organization's [type or name of] system, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

[Service auditor's signature]

[Date of the service auditor's assurance report]

[Service auditor's address]

¹ If some elements of the description are not included in the scope of the engagement, this is made clear in the assurance report.

Example: Service Organization's Assertion

Following is an example of a service organization's management assertion for a Type II report.
This is subject to change and further modifications by the firm.

Month, Day, Year

Telephone 123 456 1234
Fax 123 456 1235
Internet www.xyzorganization.com

XYZ Service Organization
Street and/or postal address
City, State, Zip Code

Type 2 Service Organization's Assertion

Assertion by the Service Organization

The accompanying description has been prepared for customers who have used [the type or name of] system and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements. [Entity's name] confirms that:

- (a) The accompanying description at pages [bb-cc] fairly presents [the type or name of] system for processing customers' transactions throughout the period [date] to [date]. The criteria used in making this assertion were that the accompanying description:
 - (i) Presents how the system was designed and implemented, including:
 - The types of services provided, including, as appropriate, classes of transactions processed.
 - The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
 - The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for customers.
 - How the system dealt with significant events and conditions, other than transactions.
 - The process used to prepare reports for customers.
 - Relevant control objectives and controls designed to achieve those objectives.
 - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
 - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions.
 - (ii) Includes relevant details of changes to the service organization's system during the period [date] to [date].
 - (iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the 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.
- (b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period [date] to [date]. The criteria used in making this assertion were that:
 - (i) The risks that threatened achievement of the control objectives stated in the description were identified;
 - (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
 - (iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period [date] to [date].

Name
Title

Appendix – Suitable Criteria

The table below provides a summary of the criteria that the IAASB/ASB have concluded are “suitable” in accordance with the guidance contained in the existing assurance and attestation literature (i.e., ISAE 3000/AT 101); however, we encourage everyone to read the relevant section of the final standard for a complete description.

	<i>Subject Matter</i>	<i>Criteria</i>	<i>Comments</i>	
Opinion about the fair presentation of the description of the service organization’s system (Type I and Type II reports)	The service organization’s system that is likely to be relevant to user entities’ internal control as it relates to financial reporting and is covered by the service auditor’s assurance report	<p>The description is fairly presented if it:</p> <ul style="list-style-type: none"> a. Presents how the service organization’s system was designed and implemented including, as appropriate, the matters identified in paragraph 16(a) (i)–(viii) b. In the case of a Type II report, includes relevant details of changes to the service organization’s system during the period covered by the description c. Does not omit or distort information relevant to the scope of the service organization’s system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the service organization’s system that each individual user entity may consider important in its own particular environment. 	The specific wording of the criteria for this opinion may need to be tailored to be consistent with criteria established by, for example, law or regulation, user groups, or a professional body. Examples of criteria for this opinion are provided in the illustrative service organization’s assertion in Appendix 1. Paragraphs A21–A24 offer further guidance on determining whether these criteria are met. (In terms of the requirements of ISAE 3000, the subject matter information ¹ for this opinion is the service organization’s description of its system and the service organization’s assertion that the description is fairly presented.)	
Opinion about suitability of design, and operating effectiveness (Type II reports)	The suitability of the design and operating effectiveness of those controls that are necessary to achieve the control objectives stated in the service organization’s description of its system	<p>The controls are suitably designed and operating effectively if:</p> <ul style="list-style-type: none"> a. The service organization has identified the risks that threaten achievement of the control objectives stated in the description of its system b. The controls identified in that description would, if operated as described, provide reasonable assurance that those risks do not prevent the stated control objectives from being achieved c. The controls were consistently applied as designed throughout the specified period. This includes whether manual controls were applied by individuals who have the appropriate competence and authority. 	When the criteria for this opinion are met, controls will have provided reasonable assurance that the related control objectives were achieved throughout the specified period. (In terms of the requirements of ISAE 3000, the subject matter information for this opinion is the service organization’s assertion that controls are suitably designed and that they are operating effectively.)	The control objectives, which are stated in the service organization’s description of its system, are part of the criteria for these opinions. The stated control objectives will differ from engagement to engagement. If, as part of forming the opinion on the description, the service auditor concludes the stated control objectives are not fairly presented, then those control objectives would not be suitable as part of the criteria for forming an opinion on either the design or operating effectiveness of controls.

¹ The “subject matter information” is the outcome of the evaluation or measurement of the subject matter that results from applying the criteria to the subject matter.

About KPMG

KPMG has more than 137,000 professionals in KPMG member firms in 144 countries, located in or near the cities where our clients operate. This proximity means that KPMG's professionals know local laws, customs, and business practices so they can effectively help our clients achieve compliance. Turning knowledge into value for you is what differentiates KPMG.

KPMG's IT Advisory Services

KPMG's IT Advisory Services professionals work collaboratively with clients throughout the IT transformation life cycle to help them harness their IT investments to generate greater business value and manage risk more effectively. They provide advice independently from systems integration vendors, solutions vendors, and business process outsourcers. Our deep knowledge in the following areas can mean the difference between seeing the broad issues and focusing solely on the immediate problems:

- IT controls, including the requirements of Sarbanes-Oxley and the views of financial reporting regulators (e.g., SEC, PCAOB)
- Industry knowledge across various industry sectors to address your industry-specific business and regulatory requirements
- Regulatory requirements (e.g., privacy, integrity) that impact IT projects
- Finance, accounting, and taxation to facilitate IT decisions that are supported by CFO-approved business cases.

KPMG's IT Attestation Practice

KPMG's IT Attestation practice consists of a globally accredited network of partners and professional staff who provide a range of IT attestation services to help organizations satisfy their third-party assurance requirements. We have established a global accreditation process to help ensure consistency and quality in the delivery of attestation and assurance services including SAS 70 examinations, Agreed Upon Procedures, SysTrust, and WebTrust services. We have over 1,000 professionals fully trained on the SAS 70 examination process through our global IT Attestation Instructor network. Our extensive experience in delivering attestation services has enabled us to develop tools such as our Controls Repository Database (CRD), which contains a wide variety of control objectives and control activities across various service industries. We welcome the opportunity to open a dialogue with service organizations or user entities interested in learning more about the new standard.

Contacts

For more information about KPMG's service auditor assurance services, please contact:

David Wallace

Partner

Tel : +352 22 51 51 6332

david.wallace@kpmg.lu

Michael Hofmann

Partner

Tel : +352 22 51 51 7925

michael.hofmann@kpmg.lu

KPMG contributors to this publication include Tom Wallace, Han Boer, Dave Palmer, Ronald Van Langen, and Samantha Malackey.



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG LLP, the audit, tax, and advisory firm (www.us.kpmg.com), is the U.S. member firm of KPMG International. KPMG International's member firms have 137,000 professionals, including more than 7,600 partners, in 144 countries. Each KPMG firm is a legally distinct and separate entity, and describes itself as such.

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

© 2010 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved. 21352NSS_RCSO