KPMG

# Service Organization Reporting – Changes Ahead

ADVISORY

AUDIT ▪ TAX ▪ 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 developed 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- SAS 70 to be superseded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 attestation 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 opinion will cover a period of time for all three areas (i.e., fairness of presentation, design and operating effectiveness of controls)

## Fundamentals of the Change

Under the new approach adopted by the IAASB and the ASB, SAS 70 has been replaced by two standards: an auditing standard that addresses the user auditor's consideration of internal control when processing is performed by a service organization; and a new attestation 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 attestation standard, the core framework for the service auditor is based on AT 101 in the United States and under ISAE3000 internationally. The new standard requires 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 minimum criteria that the service auditor must use to assess whether management has used suitable criteria in preparing its description and in evaluating the design and operating effectiveness of its controls. The new standard also includes a new service auditor's report, based on the attestation 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 is an assurance/U.S. attestation 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.)
- Specific considerations must be given by the service auditor regarding fraud and management overrides.

***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 attestation 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 attestation 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 proposed standards for a complete description (paragraphs 16-18 of the IAASB standard (ISAE 3402), and paragraphs 14-16 of the ASB standard (SSAE #16)).

## 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?***

Yes. Many aspects of the new standard come directly from SAS 70, however, there are some significant differences. The sidebar on the left highlights some of the similarities to, and differences from, the existing SAS 70 standard.

One significant difference is that there is now an international standard (ISAE 3402) that will be the basis for local standards including the U.S. standard (SSAE 16). This is important to note since service auditors across jurisdictions will be able to issue reports in accordance with locally developed standards, guidelines, and legal considerations that are based on ISAE 3402 for consistency. 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 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.*

***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. While management must have a reasonable basis for its assertion, it is not necessary that management put in place a "SOX-like" function to document and assess its controls. The application guidance contained in the standard states: "Management's monitoring activities may provide evidence of the design and operating effectiveness of controls in support of management's assertion. *Monitoring of controls* is a process to assess the effectiveness of internal control performance over time. It involves assessing the effectiveness of controls on a timely basis, identifying and reporting deficiencies to appropriate individuals within the service organization, and taking necessary corrective actions. Management accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of the two.…Ongoing monitoring activities are often built into the normal recurring activities of an entity and include regular management and supervisory activities. Usually, some combination of ongoing monitoring and separate evaluations will ensure that internal control maintains its effectiveness over time. The service auditor's report on controls is not a substitute for the service organization's own processes to provide a reasonable basis for its assertion."

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 local standard based on the international standard. However, it is anticipated that the significant majority of these standards will be substantially the same. While certain differences between the various standards will exist to accommodate the manner in which standards are framed and promulgated in each jurisdiction, it is anticipated that such differences will be minor and will not impact the intent or substance of the respective standards.

There are several subtle differences between SSAE 16 and ISAE 3402 which have been documented in Exhibit B of SSAE 16. The following is a summary of the more noteworthy differences:

- **Intentional Acts by Service Organization** – In the U.S. version, the service auditor is directed to perform additional follow-up procedures should he/she become aware of deviations resulting from intentional acts by service organization personnel. The international standard omits this guidance.
- **Anomalies** – ISAE 3402 enables the service auditor to conclude that a deviation identified in tests of controls involving sampling is not representative of the population from which the sample was drawn. The ASB believes the introduction of such language in the U.S. standard may have had unintended consequences and thus did not include it.
- **Direct Assistance** – SSAE 16 provides guidance on using members of the service organization's internal audit function to provide direct assistance and the international standard does not provide for the use of direct assistance.
- **Subsequent Events** – With respect to events that occur subsequent to the period covered by the description of the service organization's system up to the date of the service auditor's report, the U.S. standard requires the service auditor to disclose in our report, if not disclosed by management in its description, any event that is of such a nature and significance that its disclosure is necessary to prevent users from being misled. ISAE 3402 limits the types of subsequent events that would need to be disclosed to those that have a significant effect on the service auditor's report.

Refer to Exhibit B of SSAE 16 for a complete discussion of substantive differences between SSAE 16 and ISAE 3402.

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

ISAE 3402 has been issued by the International Auditing and Assurance Standards Board (IAASB), which has the authority to establish auditing and assurance standards within IFAC (the International Federation of Accountants). IFAC is the global organization for the accountancy profession. 122 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 their established protocols, similar to what the ASB has undertaken 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 a transition period during which both SAS 70 reports and reports under the new standard are acceptable?*

Early adoption is 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?*

We anticipate that the underlying effort to perform a service auditor's examination will affect service organizations 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 attestation standard permits reporting on non-financial systems; i.e., systems that are not part of the user organization's information systems relevant to financial reporting. Is this true?*

The new standard does not address reporting on non-financial systems and may not be used for that purpose. A report issued under this 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 standard 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 standard 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 standard. These issues include, for example, identification of suitable and available criteria, appropriate-

ness 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. Does the new attestation standard present any significant changes to the way user auditors will use a service auditor's report?*

No, it will not. The new SAS, *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. The SAS includes updated guidance that aligns it to corresponding elements of the new attestation standard 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? If so, when?*

We understand that such an update is planned by the AICPA. Given the required timelines for ASB review and approval, it is likely this will be available in early 2011.

### *What should we (the service organization) do?*

**1. Understand the change** — particularly the requirements 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:

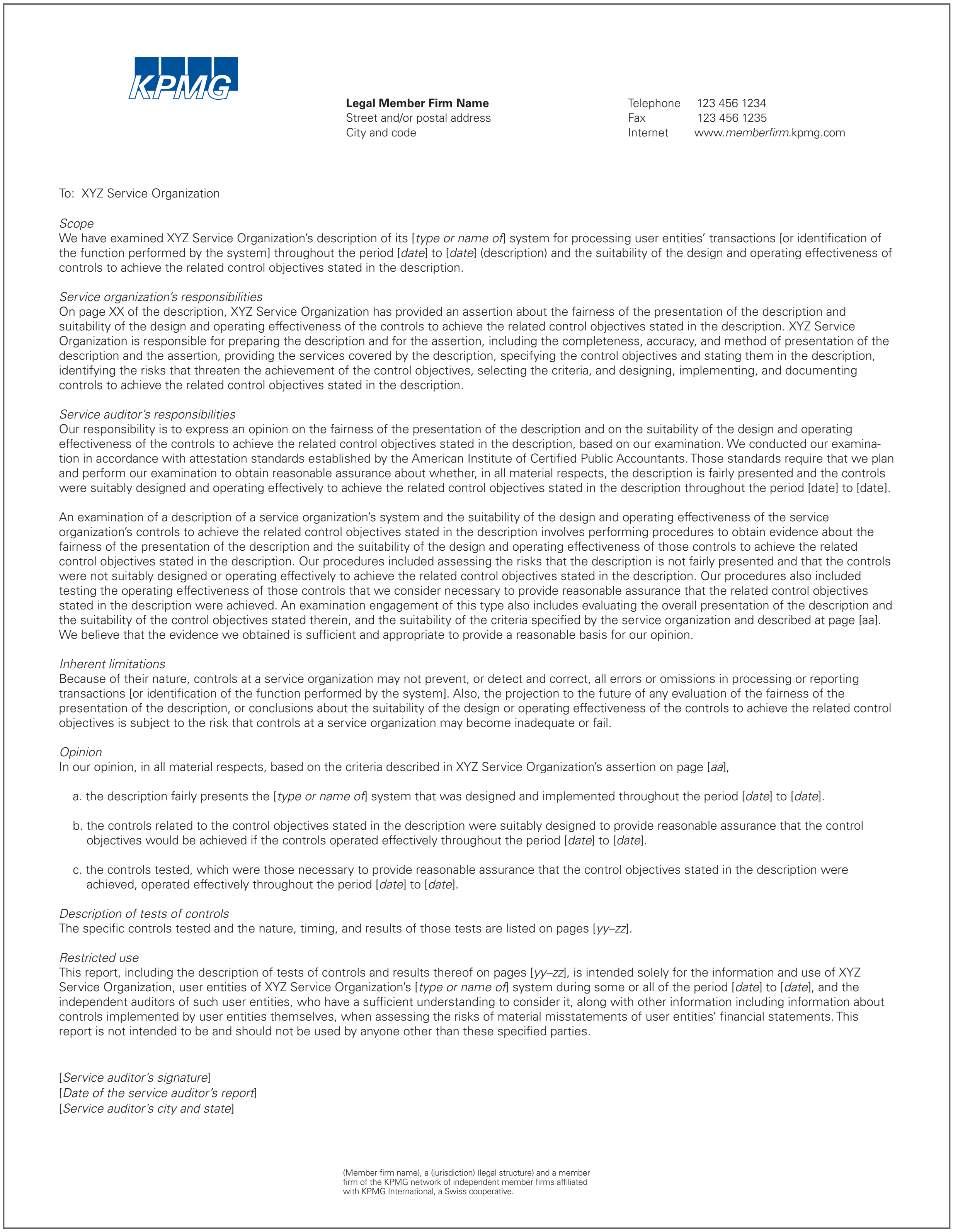
- Anticipated impact on their report and their work.
- Whether you are considering early adoption and the implications to their testing. Consider your customers' appetite for early adoption and the costs and benefits of early adoption.
- The impact of sub-service organizations that are or may be within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

**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 timeline that considers key implementation activities such as:

- Conduct 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 new standard. Such activities should include briefings with sales, support, and other customer-facing personnel so they can effectively articulate changes to and answer questions from customers.
- Coordinate with your legal department to review contracts with customers and, as necessary, sub-service organizations to identify required modifications that may be needed due to the new standard.
- Develop a customer communication plan to help alleviate unnecessary customer anxiety over the transition to the new standard and be responsive to customer inquiries.
- Review 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 supporting compliance.

# Revised Attestation Examination Report

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls. *The following is an example of an unqualified Type II report under the new standard SSAE #16. This report is illustrative and is not intended to be exhaustive or applicable to all situations.*



**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

To: XYZ Service Organization

*Scope*
We have examined XYZ Service Organization's description of its [*type or name of*] system for processing user entities' transactions [or identification of the function performed by the system] throughout the period [*date*] to [*date*] (description) and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

*Service organization's responsibilities*
On page XX of the description, XYZ Service Organization has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. XYZ Service Organization is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

*Service auditor's responsibilities*
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period [date] to [date].

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control 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 obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

*Inherent limitations*
Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions [or identification of the function performed by the system]. 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 achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

*Opinion*
In our opinion, in all material respects, based on the criteria described in XYZ Service Organization's assertion on page [*aa*],

a. the description fairly presents the [*type or name of*] system that was designed and implemented throughout the period [*date*] to [*date*].

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period [*date*] to [*date*].

c. 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 [*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*].

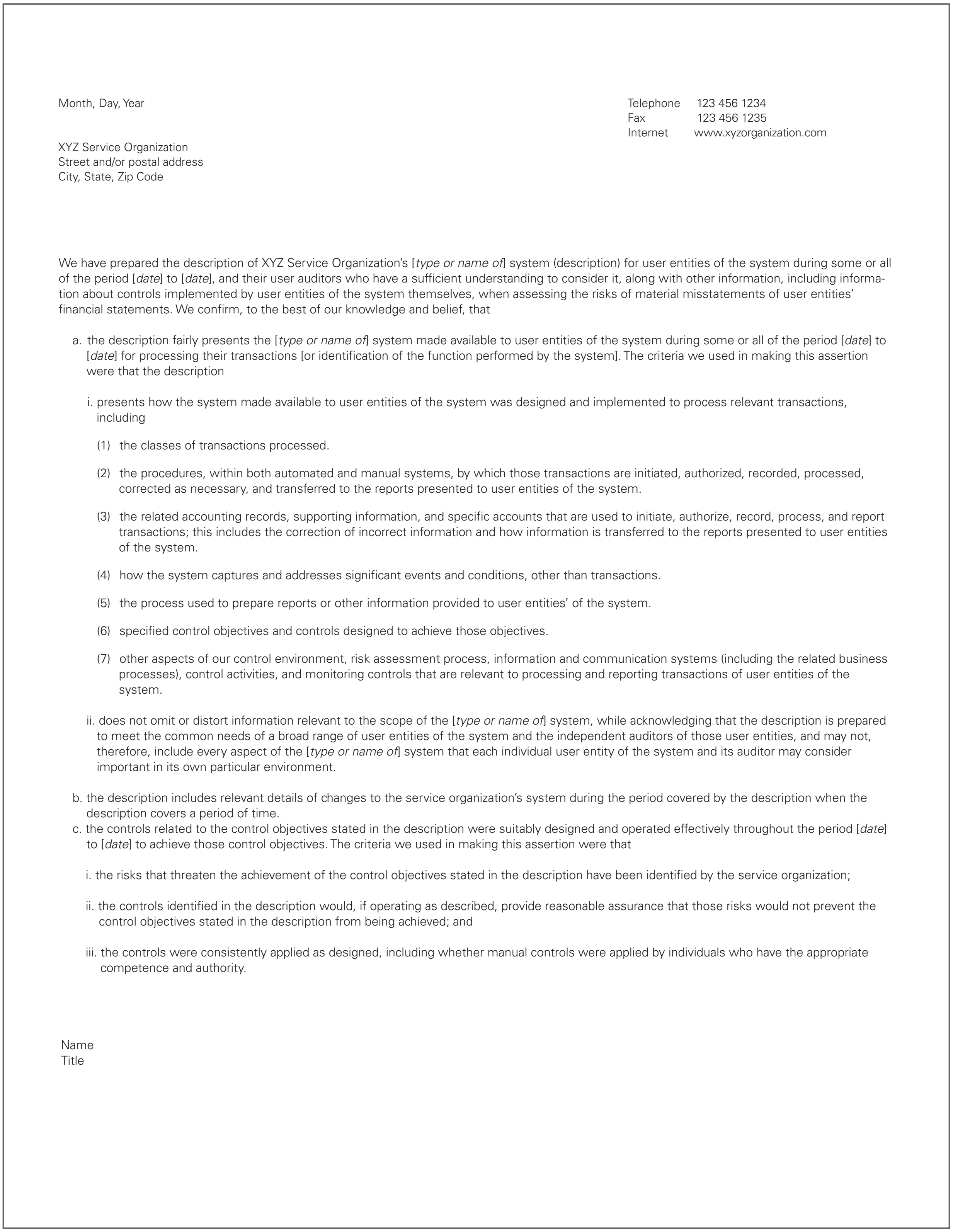
*Restricted use*
This report, including the description of tests of controls and results thereof on pages [*yy–zz*], is intended solely for the information and use of XYZ Service Organization, user entities of XYZ Service Organization's [*type or name of*] system during some or all of the period [*date*] to [*date*], and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

[*Service auditor's signature*]
[*Date of the service auditor's report*]
[*Service auditor's city and state*]

(Member firm name), a (jurisdiction) (legal structure) and a member
firm of the KPMG network of independent member firms affiliated
with KPMG International, a Swiss cooperative.

# Example Management Assertion

Following is an example management assertion letter under the new standard SSAE #16.
*This letter is illustrative and is not intended to be exhaustive or applicable to all situations.*



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

We have prepared the description of XYZ Service Organization's [*type or name of*] system (description) for user entities of the system during some or all of the period [*date*] to [*date*], and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the [*type or name of*] system made available to user entities of the system during some or all of the period [*date*] to [*date*] for processing their transactions [or identification of the function performed by the system]. The criteria we used in making this assertion were that the description

i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including

(1) the classes of transactions processed.

(2) the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system.

(3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system.

(4) how the system captures and addresses significant events and conditions, other than transactions.

(5) the process used to prepare reports or other information provided to user entities' of the system.

(6) specified control objectives and controls designed to achieve those objectives.

(7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

ii. does not omit or distort information relevant to the scope of the [*type or name of*] system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the [*type or name of*] system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c. 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. 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 service organization;

ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

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 attestation literature (i.e., AT101/ISAE3000).

| | *Subject Matter* | *Criteria* | *Comments* |
|---|---|---|---|
| **Opinion on the fair presentation of management's description of the service organization's system (Type I and Type II reports).** | Management's description of the service organization's system that is likely to be relevant to user entities' internal control over financial reporting and is covered by the service auditor's report, and management's assertion about whether the description is fairly presented. | Management's description of the service organization's system is fairly presented if it:<br>*a.* presents how the service organization's system was designed and implemented including, as appropriate, the matters identified in paragraph 14(a) and, 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.<br>*b.* does not omit or distort information relevant to the service organization's system, while acknowledging that management's description of the service organization's system 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, regulation, user groups, or a professional body. Criteria for evaluating management's description of the service organization's system are provided in paragraph 14. Paragraphs 19–20 and A31–A33 offer further guidance on determining whether these criteria are met. |
| **Opinion on suitability of design and operating effectiveness (Type II reports).** | The design and operating effectiveness of the controls that are necessary to achieve the control objectives stated in management's description of the service organization's system. | The controls are suitably designed and operating effectively to achieve the control objectives stated in management's description of the service organization's system if:<br>*a.* management has identified the risks that threaten the achievement of the control objectives stated in management's description of the service organization's system.<br>*b.* the controls identified in management's description of the service organization's system would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.<br>*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 stated in management's description of the service organization's system were achieved throughout the specified period.<br>The control objectives stated in management's description of the service organization's system are part of the criteria for these opinions. The control objectives stated in the description will differ from engagement to engagement. If the service auditor concludes that the control objectives stated in the description are not fairly presented, then those control objectives would not be suitable as part of the criteria for forming an opinion on the design and operating effectiveness of the controls. |

## About KPMG

### KPMG LLP

KPMG LLP, the audit, tax and advisory firm (www.us.kpmg.com), is the U.S. member firm of KPMG International Cooperative ("KPMG International"). KPMG International's member firms have 137,000 professionals, including more than 7,600 partners, in 144 countries.

### 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 and auditing 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 is comprised 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 services including Service Auditor Examinations, Agreed-Upon Procedures, SysTrust, and WebTrust services. We have over 1,000 professionals fully trained on the service auditor 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) that 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 attestation services, please contact:**

James DeVaul
Washington D.C.
+1 202 533 3024
jdevaul@kpmg.com

Eddie Holt
Dallas TX
+1 214 840-2116
eeholt@kpmg.com

David Lewis
Tampa FL
+1 813 301-2102
rdlewis@kpmg.com

Mark Lundin
San Francisco CA
+1 415 963-5493
mlundin@kpmg.com

Sandy Stein
Philadelphia PA
+1 267 256-2720
sstein@kpmg.com

Frank Taylor
New York NY
+1 212 872-2166
fwtaylor@kpmg.com

Robert Wolf
Kansas City MO
+1 816 802 5632
rkwolf@kpmg.com

KPMG contributors to this publication include Eddie Holt, Dave Palmer, Gene Ozgar, Keith Hamilton, and Stephen Camara.

us.kpmg.com

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.

Document code: GSC-AD090