



RISK & COMPLIANCE

# Reporting on Controls at Service Organizations

*New Standard for Service Auditor Reporting*

ADVISORY

AUDIT ■ TAX ■ ADVISORY

# Agenda



- **SAS 70 (Service Reporting) Recap**
- **Brief History vs. Today**
- **New Standard Core Concepts**
- **New Terms to Learn**
- **Key Elements and Discussion Points**
- **What Should Service Organizations Do?**
- **What Should User Entities Do?**
- **Q&A / Frequent Questions**



## SAS 70 (Service Reporting) Recap



- Evaluation of the design and operating effectiveness of controls to achieve specific control objectives (but not a certification)
- Report includes detailed information about the processes, controls, tests performed, and results of the tests.
- Report also includes an opinion about whether each control objective was achieved.
- Must be performed by a CPA.
- Report is used by management, customers, and the auditors of customers.
- SAS 70 is the generally accepted report used by customers and their auditors that complies with PCAOB requirements.
- Incorporated as a requirement in many contracts between service organizations and their customers.

All of these bullets remain true given the changes in the new standards!



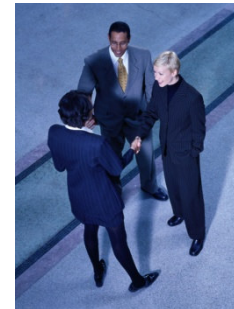
# Typical Parties to a SAS 70 review



Service Organization



Service Auditor



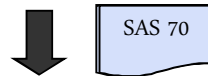
SAS 70



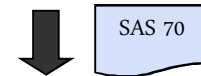
User Organizations



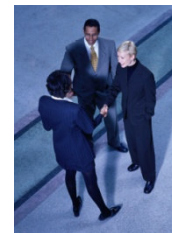
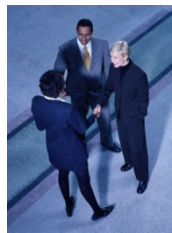
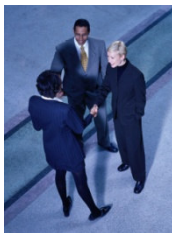
SAS 70



SAS 70



SAS 70



Independent Auditor  
of User Organizations



## Brief History vs. Today



- Service organization audit standards have evolved over 40+ years
- In the post-SOX era, SAS 70 became a de facto global standard
- The IAASB included service auditor reporting on its agenda over two years ago, resulting in the development of an international (IFAC) standard:
  - The current SAS 70 standard will be retired
  - The old standard will be bifurcated into two new standards: one that applies to user auditors; and one that applies to the service auditor
- U.S. Auditing Standards Board (ASB) agreed to conform to IAASB approach
- IAASB has approved the international version of new standards and the ASB reviewed a final version of the standards in January, 2010
- New standard is effective for reports covering periods ending on or after June 15, 2011

## Replacement, but Not a Re-Write



- The intent of service auditor reporting is not changing much
- Report will still serve the same basic purpose: auditor-to-auditor communication
- Underlying work effort for the service auditor will likely be ~95% the same for most engagements
- Will report on the same three elements based on the control objectives
  - Fairness of Presentation
  - Suitability of Design
  - Effectiveness of Operation
- Will still be restricted to current users of the system and their auditors



# New Standard Core Concepts



## Similarities and differences between SAS 70 and new standards

Similarities	Differences
<ul style="list-style-type: none"><li>▪ Underlying work effort expected to be substantially the same</li><li>▪ Two types of reports (Type I and Type II)</li><li>▪ Type II reports should cover a minimum of six months</li><li>▪ Restriction on use – remains the same</li><li>▪ Service auditor’s tests included in report</li><li>▪ Sample sizes disclosed only when exceptions are identified</li></ul>	<ul style="list-style-type: none"><li>▪ The new standard is composed of an attest standard (SSAE) and audit standard (SAS)</li><li>▪ Management will be required to provide <b>an assertion</b>, which will be included in the report</li><li>▪ In a Type II report, all three assertions/opinions will be <b>for a period of time</b>. (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)</li></ul>

## New Terms to Learn



- “User Entity” (Formerly user organizations)
- “Complementary User Entity Controls” (Formerly client control considerations)
- “Service Organization’s System” – definition:
  - The services provided
  - The period covered
  - The control objectives
  - All related controls (including relevant aspects of control environment, risk assessment and monitoring)
- “Criteria”
  - standards to measure the subject matter of the report
  - a defined term under AT101

## New Terms to Learn



- **Attestation Standards**
  - “an examination, a review, or an agreed-upon procedures report on subject matter, or an assertion about the subject matter, that is the responsibility of another party.”
- **Other Types of Attest Reports**
  - SysTrust® and WebTrust®
    - AICPA defined attestation over the Security, Availability, Processing Integrity, Confidentiality, and Privacy of a system
  - Agreed Upon Procedures
    - report of findings based on specific procedures performed on subject matter
  - Compliance Report
    - engagements related to either (a) an entity's compliance with requirements of specified laws, regulations, rules, contracts, or grants or (b) the effectiveness of an entity's internal control over compliance with specified requirements

# Fundamentals of Change



- Old standard will be split into 2 new standards:
  - Reporting on Controls at Service Organizations - Statement on Standards for Attestation Engagement 16 (SSAE 16)
  - Audit Considerations Relating to an Entity Using a Service Organization – Statement on Auditing Standards (SAS)
- Attestation-based engagement
- Follows the core tenets of AT101
  - Management’s assertion
  - Suitable criteria
  - Subject matter
  - Intended users

# Key Elements and Discussion Points



## •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

- Layout will be similar with:
  - *Opinion*
  - *Description of System and Controls*
  - *Control Objectives, Activities, Testing and Results*
- Report will also include management's assertion
- Opinion will “look and feel” very different (See example in Appendix)
- All three elements cover the entire period of the report
  - *SAS 70 only required an evaluation of fairness of presentation and suitability of design at the “as-of” date for the report. These will now be evaluated throughout the period.*

# The Service Auditor's Report



- **Scope**
  - Initial definition of the “system” covered in the report including period covered.
- **Service Organization's Responsibilities**
  - References management's assertion as well as responsibility over control objectives, identifying risks, and implementing and maintaining controls designed to meet the objectives.
- **Service Auditor's Responsibilities**
  - Examine system and express an opinion over the period indicated in accordance with professional standards.
- **Inherent Limitations**
  - Note that controls may not detect all issues, and continuing operation into the future may not be accurate.
- **Opinion**
  - The system is fairly presented, suitably designed, and operating effectively for the period.
- **Description of tests of controls**
- **Restricted Use**

## Key Elements and Discussion Points (continued)



### •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

Paraphrased (See example in Appendix):

*We (management) have prepared this description of the “system” and confirm:*

- *Presents fairly the ‘system’ used for processing transactions for user entities and includes all relevant information.*
- *Relevant changes for the period are included.*
- *Controls are suitably designed, implemented and operating effectively for the period to meet the specified control objectives and this was measured by:*
  - *Risks to the control objectives were identified*
  - *Controls were designed to mitigate the risks*
  - *Controls were understood and executed by individuals appropriately.*

## Key Elements and Discussion Points (continued)



### •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

### • Basis for Assertion

- *Not intended to be “SOX-Like”; however, must be more than passive interest in effectiveness.*
- *Monitoring activities may provide evidence (assesses effectiveness over time)*
- *Can be ongoing monitoring or separate evaluations, or combination of the two.*
- *Could include Internal Audit or ongoing monitoring for information provided by external parties (regulators, customers, etc.)*
- *Consider risks to achieving objectives and how management would identify failures.*

### • Risk Assessment

- *Formal or informal process for evaluating risks and likelihood of achieving the control objectives.*
- *Assists with the evaluation of controls and assessing management’s process and basis for assertion.*

*(See Appendix for references to the Standard)*

## Key Elements and Discussion Points (continued)



### •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

- The focus of this SSAE is on controls at service organizations **LIKELY** to be relevant to user entities' internal control over financial reporting.
- Not intended for non-financial systems
- The new standard may be “helpful” to a practitioner performing an engagement under AT 101 to report on controls at a service organization (provides a framework that may be formalized.)
  - *Suitable and available evaluation criteria must exist*
  - *The needs of the user of the report must be identified*
  - *The relevance of the control objectives to non-financial reporting must be considered*
  - *Other matters*

## Key Elements and Discussion Points (continued)



### •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

### • Subservice Provider

- *Entity used by Service Organization that performs some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting .*
- *In other words, another provider that is part of the "system."*

### • Inclusive Method or Carve-Out Method

- *The inclusive method requires that the management of the subservice provider meet all the requirements of the service organization including providing an assertion on the relevant controls (and a basis for the assertion).*
- *When a subservicer's controls are not sufficient to achieve a control objective on its own, management of the subservice organization may be unwilling or unable to provide an assertion. In such situations, the subservice organization must be carved out.*

## Key Elements and Discussion Points (continued)



### •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

### • Internal audit may be evaluated

– *Not a new element. Internal audit work may be assessed and evaluated for use in performing the work.*

### • Report must indicate the use of Internal Audit

– *When Internal Audit is used to test the effectiveness of the controls, the description of that work and the service auditor's procedures to validate the work must be presented within the report.*

– *May be included as introductory material to the description of tests of controls, OR*

– *Certain tests attributable to Internal Audit may be included.*

## Key Elements and Discussion Points (continued)



### •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

### • Effective Date

- The effective date for the new standard is for reporting periods ending on or after June 15, 2011.
- Since service auditor reports cover 6-12 months, reports may fall under the new standard as early as 2<sup>nd</sup> quarter of 2010.

### • Early Adoption

- IAASB and ASB are permitting early adoption; reports may be issued under the new standard as early as latter half of 2010.
- For a period of time after issuance of the standard and before June 15, 2011, both standards will be in place and may be used.

## Key Elements and Discussion Points (continued)



### •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

- Some reports are designated for the “system” of processing transactions for an individual user entity.
  - *Designation of a single user entity does not remove management’s responsibility to assess the design of the controls to meet the control objectives, and provide the corresponding assertion.*
  - *Impacts management’s risk assessment and evaluation of controls.*
  - *Consider procedures applied to ensure complete and accurate reporting to the user entity, and consider the appropriate control objectives for that entity.*

## Key Elements and Discussion Points (continued)



### •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

- Reports are restricted for intended use by the service organization, its user entities, and the independent auditors of the user entities.
  - *The reports are intended to be used by clients during that period to understand the “system” in place and determine its effectiveness.*
- The independent auditor may use these reports in planning a risk assessment and performing an audit for the user entity of a service organization.
  - *Auditing standard (SAS) will address user auditor’s consideration of internal control when processing is performed by a service organization*
  - *Update is planned in third or fourth quarter of 2010 for new AICPA Audit Guide*
  - *Consistent guidance with the PCAOB Standard #5 (Appendix B) for use in a SOX Audit.*

## Key Elements and Discussion Points (continued)



### •Key elements and discussion points

- Format of the report
- Management assertion
- Assertion basis and risk assessment
- Scope of controls
- Subservice organizations
- Internal audit
- Effective date and early adoption
- Single user reports
- User entities and auditors
- Global aspects

- ISAE 3402 is the global standard (December 2009)
- The US Standard is substantially the same as the International Standard with differences to reflect US based standards and definitions:
  - **Intentional acts** identified under the US standard must be specifically evaluated for overall impact.
  - The ISAE allows for the evaluation of exceptions as **anomalies** that may be excluded from the report.
  - The ISAE does not include reference to **direct assistance**.
  - The ISAE has differences on **subsequent events**.
  - The ISAE does not require the **restricted use** language in the auditor's report.
- Anticipated that most countries will adopt the international standards, or adopt a similar standard.
  - Example: Canada is expected to replace the 5970 (SAS 70 equivalent) with a similar standard to the US.
  - Example: The UK is expected to replace with a standard that includes all the elements of the global standard, but includes additional performance requirements (like the specification of particular control objectives).

# What Should Service Organizations Do?



1. Understand the change
  - Assertion requirement
  - Review your risk assessment processes, controls and control objectives, and details related to monitoring
2. Engage your service auditor
  - Anticipated impact on their report and their work
  - Their approach for assessing management's assertion
  - Early adoption and implications
  - Impact of subservice organizations
3. Plan for the transition
  - Conduct internal training
  - Coordinate with legal department, contracts may need to change
  - Develop customer communication plan, educate them on current changes and prepare them for differences
  - Review internal processes and current report(s)

# What Should User Entities Do?



## 1. Discuss reporting need with Compliance and Audit

- Identify key service organization relationships, and how they are evaluated by interested stakeholders (Management, Internal Audit and Compliance teams, External Auditors)
- Understand other reporting requirements from regulators, customers, etc.

## 2. Evaluate current reports with Service Organizations

- The current changes are a good time for re-evaluation of scope of services for reporting and control objectives for current reports
- Understand the scope of the reports provided and your needs for reporting

## 3. Coordinate for changes

- Coordinate with legal department, contracts may need to change
- Develop internal communication plan, educate them on current changes and prepare them for differences
- Plan for new reports and using them for gaining an understanding of service organizations
- Work with your Service Organization early to proactively anticipate and address any delays as the new standard and processes are established

## Frequent Questions



- 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 U.S., the service auditor must issue the report in accordance with AICPA standards. Reports issued outside the U.S. would be issued in accordance with applicable international standards. 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.

## Frequent Questions (continued)



- 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.

## Frequent Questions (continued)



- 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 subservice 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.

## Frequent Questions (continued)



- 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 system 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 use, application of the concept of materiality, and development of the language to be used in the practitioner's report.

# Q&A



## Appendix – References and Excerpts



- AICPA ([www.aicpa.org](http://www.aicpa.org))
- Meeting materials from January meeting of the Auditing Standards Board, including the latest drafts of the standards.  
(<http://www.aicpa.org/Professional+Resources/Accounting+and+Auditing/Audit+and+Attest+Standards/Auditing+Standards+Board/ASB+Meeting+Agenda+and+Materials+January+11-14+2010.htm>)
  - Navigate:
    - » AICPA
    - » Professional Resources
    - » Accounting and Auditing
    - » Audit and Attest Standards
    - » Auditing Standards Board
    - » ASB Meeting Agenda Materials

## Appendix – References and Excerpts



### Example: Type 2 Service Auditor's 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

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.*



## Appendix – References and Excerpts



### (Continued – Type 2 Service Auditor’s Report)

#### *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 and the description of tests of controls and results thereof on pages [yy–zz] are 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]

From AICPA Proposed Statement on Standards for Attestation Engagements *Reporting on Controls at a Service Organization*



## Appendix – References and Excerpts



### Example Assertion by Management of a Service Organization for a Type 2 Report

#### XYZ Service Organization's Assertion

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*

(1) *presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including*

- *the classes of transactions processed.*
- *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.*
- *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.*
- *how the system captures and addresses significant events and conditions, other than transactions.*
- *the process used to prepare reports or other information provided to user entities' of the system.*
- *specified control objectives and controls designed to achieve those objectives.*
- *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.*

(2) *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*

(1) *the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;*

(2) *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*

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

**From AICPA Proposed Statement on Standards for Attestation Engagements *Reporting on Controls at a Service Organization***



## Appendix – References and Excerpts



### *Reasonable Basis for Management's Assertion (Ref: par. 7, definition of service organization's system; par. 9(c) (2) and 14(a) (7))*

**A17. 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. Internal auditors or personnel performing similar functions may contribute to the monitoring of a service organization's activities. Monitoring activities may also include using information communicated by external parties, such as customer complaints and regulator comments, which may indicate problems or highlight areas in need of improvement. The greater the degree and effectiveness of ongoing monitoring, the less need for separate evaluations. 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.**

### *Identification of Risks (Ref: par. 9c (4))*

**A18. Control objectives relate to risks that controls seek to mitigate. For example, the risk that a transaction is recorded at the wrong amount or in the wrong period can be expressed as a control objective that transactions are recorded at the correct amount and in the correct period. Management is responsible for identifying the risks that threaten achievement of the control objectives stated in management's description of the service organization's system. Management may have a formal or informal process for identifying relevant risks. A formal process may include estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. However, since control objectives relate to risks that controls seek to mitigate, thoughtful identification by management of control objectives when designing, implementing, and documenting the service organization's system may itself comprise an informal process for identifying relevant risks.**

From AICPA Proposed Statement on Standards for Attestation Engagements *Reporting on Controls at a Service Organization*



## Presenters



### **Alan Beaton**

IT Attestation Partner  
Office: (214) 840-2567  
Fax: (214) 292-9499  
e-mail: [awbeaton@kpmg.com](mailto:awbeaton@kpmg.com)

### **Keith Hamilton**

IT Attestation Manager  
Office: (214) 840-4964  
Fax: (214) 889-8426  
e-mail: [khamilton@kpmg.com](mailto:khamilton@kpmg.com)

