

Minnesota ISACA Chapter Technical Roundtable

Service Organization Internal Control Audits:

The Future of Third Party Assurance Reporting Standards



April 28, 2009

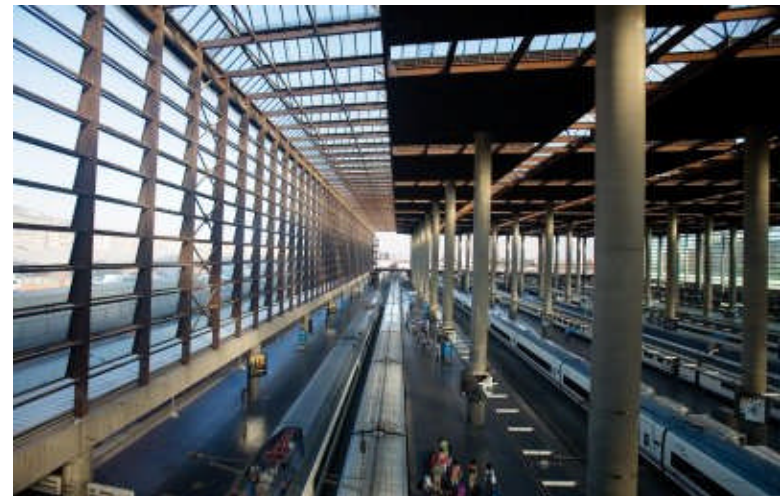
The Need for Change

- SAS No. 70 was originally written in early 1990s and was effective for service organization audits after March 31, 1993
- Many business events have altered the landscape since the issuance of SAS No. 70
 - Increased outsourcing including usage of shared service centers
 - Continued globalization and global processing models
 - Increased regulation and enhanced risk management requiring service organization customers to obtain controls comfort related to outsourced activities impacting their financial statements, regulatory requirements and overall business risk management



The Need for Change

- SAS No. 70 has served as the de facto standard on reporting on controls at a service organization on a global basis
- Other territories have steadily sought to adopt their own service organization audit standard (e.g., Canada – Section 5970, UK – Audit and Assurance Faculty Standard (AAF))
- Absence of a global standard(s) complicates engagements that cross borders
- Potential to take advantage of differing provisions within various third party control standards



THIRD PARTY ASSURANCE (TPA)

-- TPA is defined as SAS 70s (and successor standard) and Attestation Standards (e.g., SSAE10) primarily focused on reports on internal controls intended for third parties

Statement on Auditing Standards (SAS) No. 70

What a SAS 70 is:

- A report identifying the control structure, policies and procedures of a service organization
- An internationally recognized audit reporting standard used to communicate to user organizations that the service organization's internal controls are reasonable and effective
- Management's report on internal control, describing the control environment, risk assessment, control activities, information and communication and monitoring
- An auditor to auditor communication

What a SAS 70 is not:

- A Compliance Report
- An Attest Level Report (e.g., report on effectiveness of an entity's internal control over financial reporting)
- A Public Report

What is an Attestation?

- Practitioner is engaged to issue 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
- Attestation standards apply to a broad range of subject matter, financial or nonfinancial, not directly related to historical financial statements
- Intended to bridge the gap between standards established by other authoritative pronouncements and services not contemplated by those pronouncements that accountants are requested to perform
- Attestation standards are applicable only when Practitioner and the client intends the engagement to be an attest engagement

Attributes of an Attestation

The following attributes should be present for an attest engagement:

- Need to identify a responsible party – responsible for the subject matter (may or may not be the client)
- Evidence of responsible party's responsibility for the subject matter or a written assertion
- Suitable criteria exist (criteria should be objective, measurable, complete, and relevant)
- Need for assurance on reliability for specific subject matter – sufficient evidential matter exists
- Use attestation standards under Statements on Standards for Attestation Engagements (SSAE) 10

Attestation Standards

Overall, attestations are governed by Statements on Standards for Attestation Engagements (SSAE) 10:

- AT 101 - General Attest Engagements
- AT 201 - Agreed-Upon Procedures
- AT 501 - Reporting on an Entity's Internal Control Over Financial Reporting
- AT 601 - Compliance Attestation
- SSAE16 - will replace SAS 70

Common Types of Attestations

- SysTrust or WebTrust (Governed by AT 101 standards)
- Agreed upon procedures (Governed by AT 201 standards)
- XBRL (Governed by AT 101 standards)
- Rule 17ad-13 - Transfer Agent (Governed by AT 101 standards)
- Chief Compliance Officer (Governed by AT 101 standards)
- FISAP/BITS (Governed by AT 201 standards)
- Regulation AB (Governed by AT 601 standards)

SysTrust or WebTrust

- Attestation provides assurance that a company's controls over a system meet the Trust Services criteria for the principle(s) examined
- Based on Trust Services Principles and Criteria - were developed to build trust between business parties for the following:
 - Availability
 - Security
 - Processing Integrity
 - Online Privacy
 - Confidentiality
- SysTrust engagements are intended to provide assurance on the reliability of a system.
- WebTrust engagements are intended to provide assurance on an organization's system related to e-commerce.

SysTrust or WebTrust, continued

- For each Trust Services Principle - a system can be evaluated against the following elements:
 - Policies
 - Communications
 - Procedures
 - Monitoring
- Report Audience is stakeholders of the system – known and unknown
- General (unlimited) distribution report
- Governed by AT 101 (*Attest Engagements*)

SysTrust or WebTrust, continued

Advantages

- Reports can be shared with any interested parties
- Reports can be posted on client's web site, through use of the SysTrust or WebTrust Seal programs (administered by AICPA/CICA)
- Reports can be structured to cover one or more of the Trust principles (as relevant to the organization)
- Provide the highest level of assurance
- Provide better comparability against other organizations providing similar services

Disadvantages

- Incorporates a standard set of control principles and control criteria that CANNOT be modified for specific reporting requirements.
- Failure of even one of the control criteria within a principle results in an adverse opinion.
- Existing security issues at the client may lead to an adverse opinion.
- Less known in the market place.

Agreed Upon Procedures (AUP)

- AT 201 – Agreed Upon Procedures (AUP) Engagements
 - Relates to the subject matter that is financial or non-financial, and historical or prospective
 - Unlike AT 101 attest engagements, agreed-upon procedures engagements do not involve our judgment as to the procedures to be performed which are provided by a third party
 - All parties who receive the auditors report need to agree to the procedures in advance of report receipt (limited distribution)
 - Sample size for each test defined by relevant parties
- Auditor expresses no opinion to the adequacy of procedures or controls; results are communicated in the form of procedures and findings.

Agreed Upon Procedures (AUP), continued

Examples of appropriate procedures include the following:

- Execution of a sampling application after agreeing on relevant parameters.
- Inspection of specified documents evidencing certain types of transactions or detailed attributes.
- Confirmation of specific information with third parties.
- Comparison of documents, schedules, or analyses with specified attributes.
- Performance of specific procedures on work performed by others (including the work of internal auditors).
- Performance of mathematical computations.

Examples of inappropriate procedures include the following:

- Evaluating the competency or objectivity of another party.
- Documentation of a subject or process.
- Interpreting documents outside the scope of the third party's professional expertise.

Third Party Assurance - Summary

<p style="text-align: center;">SAS 70</p> <ul style="list-style-type: none">• Non-attest level report, but an <u>auditor opinion</u> is issued• Auditor to auditor communication• Intended to support the financial reporting process	<p style="text-align: center;">SysTrust</p> <ul style="list-style-type: none">• Can be <u>published</u>• Can be tailored to address combinations of principles / criteria in the Trust Services framework• Attestation <u>opinion</u> issued
<p style="text-align: center;">WebTrust</p> <ul style="list-style-type: none">• Provide assurance over an organization's system(s) related to e-Commerce• Can be focused on e-Commerce objectives, i.e. consumer protection, online privacy, certification authorities• Attestation <u>opinion</u> issued	<p style="text-align: center;">AUP</p> <ul style="list-style-type: none">• Specific procedures agreed upon between the client and third party• Can only be distributed to specified parties• <u>No opinion</u> is issued

eXtensible Business Reporting Language (XBRL) Attestation

- Under the SEC Proposal, there would be no required auditor involvement with the XBRL-formatted information
 - No required assurance on the XBRL Exhibit or any required auditor consideration by the auditor of such information as part of standard procedures around SEC filings
- Companies have begun to consider auditor involvement, even though this is not required
- Attestation opinion of the XBRL data and related documents is expressed over conformity with the official EDGAR filings, applicable XBRL taxonomies and specifications, and with the SEC requirements for format and content
- Governed by AT 101 (*Attest Engagements*) & AT 9101

Rule 17ad-13 of Securities Exchange Act of 1934 - Transfer Agent

- SEC Rule 17ad-13 requires all registered transfer agents to annually file a report prepared by an independent accountant concerning the transfer agent's system of internal accounting control and related procedures for the transfer of record ownership and the safeguarding of related securities and funds
- Independent auditor provides and opinion on management's assertion that effective internal control over the transfer agent functions
- Auditors report is submitted with transfer agents registration
- Governed by AT 101 (*Attest Engagements*) & SSAE 15

Chief Compliance Officer (“CCO”)

- SEC adopted Rule 38a-1 under the Investment Company Act of 1940 and Rule 206(4)-7 under the Investment Advisers Act of 1940.
 - Funds and advisers must adopt and implement policies and procedures (P&P)
 - P&P’s reviewed at least annually for adequacy and effectiveness
 - Appointment of CCO to be responsible for administering the P&P’s and report to the funds Board of Directors
- As operations of funds and advisers are carried out by service providers, P&P’s at the service provider may be a part of the funds/advisers internal control over compliance
- Examination report is restricted to management and Board of Directors of the service provider; service providers’ clients
- Relevant guidance: AICPA SOP 07-2 & AT 101 (Attest Engagements)

Financial Institution Shared Assessments Program (FISAP) / BITS AUP

- BITS is a not-for-profit, CEO-driven financial service industry consortium made up of 100 of the largest financial institutions in the U.S
- BITS' member financial institutions created the Financial Institution Shared Assessments Program (FISAP) in 2006 to streamline the service provider security assessment process
- The Shared Assessments program consists of two documents—the Standardized Information Gathering (SIG) questionnaire and the Agreed Upon Procedures (AUP):
 - SIG - Completed by the service provider and provided to the Financial Institutions that utilize their services.
 - AUP - Completed by the service provider's designated assessment firm as an objective test of the company's control procedures.
- AUP governed by AT 201; AT 201.10; SSAE 10 and SSAE 11

Regulation Asset Backed Securities (AB) Attestation

- Regulation AB addresses the registration, disclosure and reporting requirements for asset-backed securities (ABS)
- Required annual servicing assertion and accountant's attestation report for parties participating in the servicing function of ABS
- Attestation report expresses an opinion, or states that an opinion cannot be expressed, concerning the asserting party's assessment with the compliance of applicable servicing criteria set forth by Item 1122(d) of Reg AB platform
- Attestation report is included in the Trusts Form 10K of the ABS issuer
- Both AT 101 - *Attest Engagements* and AT 601 - *Compliance Attestation*

New International & US Standards

International Auditing and Assurance Standards Board (IAASB)

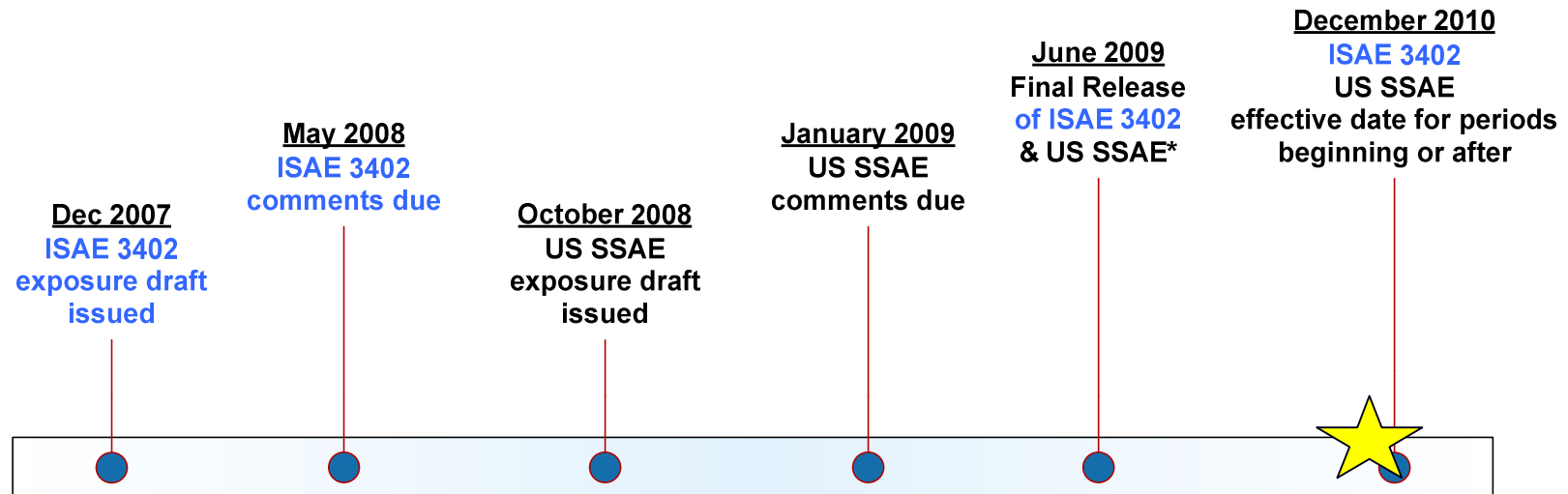
- Commenced a project in 2006 to develop an international standard for reports on controls at a service organization
- The proposed International Standard on Assurance Engagements (ISAE 3402) is entitled, “Assurance Reports on Controls at a Service Organization”
- The proposed standard complements International Standards on Auditing (ISA 402), “Audit Considerations Relating to Entities Using Service Organizations”

The Auditing Standards Board (ASB)

- Resurrected the AICPA SAS 70 Task Force in 2007 to develop a successor set of standards to AU 324 (SAS No. 70)
- One proposed standard will be a Statement on Standards for Attestation Engagements (SSAE) (i.e., attest standard), “Reporting on Controls at a Service Organization”
- Second proposed standard complements the proposed Statement on Auditing Standards (SAS) (i.e., auditing standard), “Auditing Considerations Relating to an Entity Using a Service Organization”

Enhances the consistency of auditor performance in relation to assurance reports on controls at third party service organizations, particularly in those jurisdictions that have adopted IAASB standards and have not, to date, had a specific standard on this topic.

International & US Standards: *Estimated* Timeframes



*PwC Estimate

International & US Standards: Key Provisions

US SAS 70 standard to be superseded by proposed SSAE standard:

- To expand current scope beyond financial reporting
- Assertion based engagement
- Disclosure of the work of internal audit
- US service providers will still execute under US standards

Management Assertion Requirement

Management Assertion:

- Assertion would accompany description of service organizations description of controls
- Management is responsible for selecting criteria, for determining whether it is appropriate, and it must be available to the intended users
- Nature, timing and extent of service auditor procedures would be expected to be the same
- ASB believes assertion-based engagements are more appropriate because of the explicit acknowledgement by management of its responsibility for the matters contained within the assertion
- ASB specifically sought perspective where situations may arise where it isn't possible or practicable for management to provide an assertion



What Does It All Mean? *Questions to Consider*

Potential for Expanded Reporting Scope:

- User organizations may seek additional comfort in a particular areas that hasn't historically been incorporated in a SAS 70 either because;
 - limitations with the existing control standards; or
 - concern that the area is not prepared for a review (e.g., compliance, specific operations areas of concern, security, privacy, business resumption)
- Incorporate contractual and/or service level requirements into future control reports
- Compliance or operational audit requirements of new or existing service offerings that could be combined with financial reporting "audits"



What Does It All Mean? *Questions to Consider*

Potential Cost Reductions:

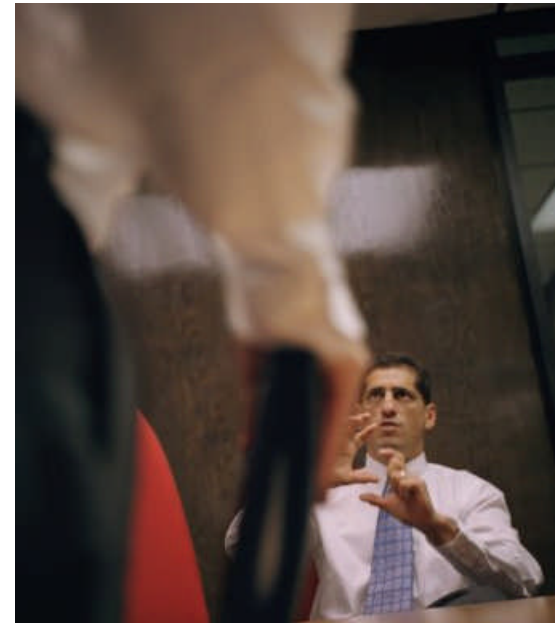
- Reduce existing "audit" activity and/or site visits executed by user organizations within a single report
- Consolidation or elimination of several different types of third-party assurance reports issued by service organization under the proposed standards
- Reduce service organization customer risk management and compliance costs through simplified and consolidated reporting under the proposed standards



What Does It All Mean? *Questions to Consider*

Other Considerations:

- Has service provider management considered what processes it has in place to evaluate and assess the performance of its controls to support a formal assertion on its controls?
- Has service provider management identified suitable criteria that will be used in preparing and presenting the description of controls and in evaluating the suitability of design and operating effectiveness of the controls for existing control reporting?



Questions?

Brian Strittmater

PricewaterhouseCoopers, LLP

b.strittmater@us.pwc.com

612.596.3908