



cutting through complexity™

Welcome to  
today's seminar

*The Retirement of  
SAS 70: A New Breed  
of SOC Reports*

Thursday, October 20, 2011



SAS 70 report retired June  
15, 2011...

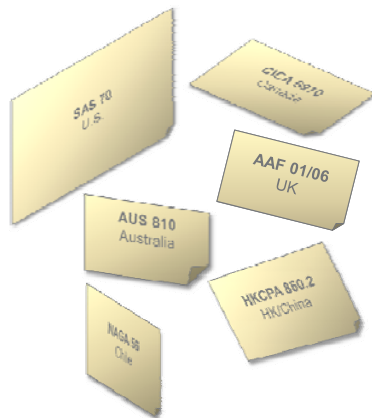


## Agenda

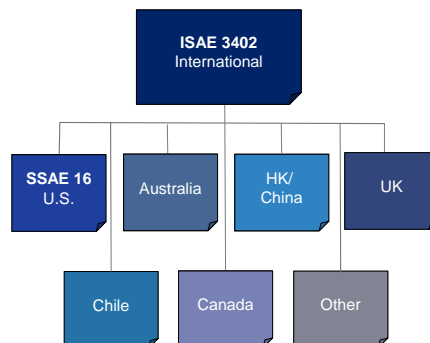
- What's staying the same?
- What's changing?
- Understanding the Impact as a Service Organization
- Understanding the Impact as an User Entity
- How to read a SOC 1 report
- Service Auditor Responsibilities
- SOC 2 and SOC 3

## Why are we here?


### Historically...



### Now...



## SOC Review – Service Organization Control (SOC) Reports

Report	Scope/Focus	Summary	Applicability
<b>SOC1</b>	Internal Control Over Financial Reporting	Detailed report for customers and their auditors	<ul style="list-style-type: none"> <li>■ Focused on financial reporting risks and controls specified by the service provider.</li> <li>■ Applicable where the service provider performs financial transaction processing or supports transaction processing systems.</li> </ul>
<b>SOC2</b>	Security, Availability, Processing Integrity, Confidentiality and/or Privacy	Detailed report for customers and specified parties	<ul style="list-style-type: none"> <li>■ Focused on Security, Confidentiality, Availability, Processing Integrity and/or Privacy.</li> <li>■ Applicable to a broad variety of systems.</li> </ul>
<b>SOC3</b>	Same as SOC2 	Short report that can be generally distributed, with the option of displaying a web site seal	<ul style="list-style-type: none"> <li>■ Same as above without disclosing detailed controls and testing.</li> <li>■ Optionally, the service provider can post a Seal if it receives an unqualified opinion.</li> </ul>

**Note:** The traditional SAS 70 construct of a Type 1 (point in time design-focused) and a Type 2 (period of time effectiveness-focused) report also applies to SOC 1, 2 and 3 reports (point in time for initial report).

- What's staying the same?
- What's changing?
- Understanding the Impact as a Service Organization
- Understanding the Impact as an User Entity
- How to read a SOC 1 report
- Service Auditor Responsibilities
- SOC 2 and SOC 3

## What's staying the same?

- Purpose of the report
- Intended users of the report
- Two types of reports: Type 1 and Type 2
- Core elements of the report
  - Auditor's Opinion
  - Management Description
  - Detailed Tests of Controls (Type 2 reports)
- Service Auditor's testing

- What's staying the same?
- What's changing?
- Understanding the Impact as a Service Organization
- Understanding the Impact as a User Entity
- How to read a SOC 1 report
- Service Auditor Responsibilities
- SOC 2 and SOC 3

## What's changing?

- Based on Management's Assertion(s)
  - Management provides a written assertion for inclusion in the report
  - Management must have a reasonable basis for the assertion
- The Service Auditor's Report
  - Expanded wording on management's responsibilities
  - One opinion addressing all three elements
  - Opinion on fairness of presentation and design in a Type 2 report will now cover the entire period
- Requirement to disclose use of Internal Audit
- Inclusive Method for Subservice Organizations
  - Subservice Organizations must supply an assertion addressing the same elements

- What's staying the same?
- What's changing?
- Understanding the Impact as a Service Organization
- Understanding the Impact as a User Entity
- How to read a SOC 1 report
- Service Auditor Responsibilities
- SOC 2 and SOC 3

## Impact on Service Organizations

### Key Discussion Points:

- Management Assertion
- Reasonable Basis
- Risk Assessment
- Suitable Criteria
- Use of Internal Audit
- Subservice Organization
- Report Distribution

### Paraphrased:

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 achieve the specified control objectives. Criteria used were:
  - Risks that threaten the achievement of the control objectives.
  - Controls identified were designed to mitigate those risks.
  - Controls were consistently applied by appropriate individuals.

## Impact on Service Organizations (continued)

### Key Discussion Points:

- Management Assertion
- Reasonable Basis
- Risk Assessment
- Suitable Criteria
- Use of Internal Audit
- Subservice Organization
- Report Distribution

- Management must have basis for assertion:
  - Not intended to be "SOX-Like"; however, must be more than a 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.

## Impact on Service Organizations (continued)

### Key Discussion Points:

- Management assertion
- Reasonable Basis
- Risk Assessment
- Suitable Criteria
- Use of Internal Audit
- Subservice Organization
- Report Distribution

### Management is responsible for:

- Identifying the risks that threaten the control objectives.
  - Process to identify risks may be formal or informal.
  - Process may include estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them.
- Designing and implementing controls to mitigate those risks.
- Consideration of risks that threaten the achievement of the control objectives is explicitly required in SSAE 16.

## Impact on Service Organizations (continued)

### Key Discussion Points:

- Management Assertion
- Reasonable Basis
- Risk Assessment
- Suitable Criteria
- Use of Internal Audit
- Subservice Organization
- Report Distribution

- Introduction of criteria as the standard for evaluating the subject matter.
- Management is responsible for:
  - Selecting the criteria and stating them in its assertion.
  - Using the criteria as the basis for making their assertion.
- The criteria expand the requirements for the description in several areas. For example:
  - Classes of transactions processed.
  - How significant events are captured.
  - Process for preparing reports for user entities.
  - Changes during the period.

## Impact on Service Organizations (continued)

### Key Discussion Points:

- Management Assertion
- Reasonable Basis
- Risk Assessment
- Suitable Criteria
- Use of Internal Audit
- Subservice Organization
- Report Distribution

- Relevance of Internal Audit must be understood:
  - Service auditor should understand the relevance of Internal Audit to the engagement. Internal Audit work may be assessed and evaluated for use in performing the work.
- If the work of Internal Audit is used, it must be disclosed in report:
  - May be included as introductory material to the description of tests of controls.
  - Certain tests attributable to Internal Audit may be included.

## Impact on service organizations (continued)

### Key Discussion Points:

- Management Assertion
- Reasonable Basis
- Risk Assessment
- Suitable Criteria
- Use of Internal Audit
- Subservice Organization
- Report Distribution

- If management of the subservice organization is unwilling or unable to provide an assertion on all of the required elements, they **MUST** be carved out.
- If a subservice organization is carved out, the service organization should consider the following:
  - Contract between the service organization and the subservice organization.
  - Controls at the service organization that monitor the effectiveness of the subservice organization.
  - Does the subservice organization have a service organization report?
- Materiality of the subservice organization should be considered.

## Impact on service organizations (continued)

### Key Discussion Points:

- Management Assertion
- Reasonable Basis
- Risk Assessment
- Suitable Criteria
- Use of Internal Audit
- Subservice Organization
- Report Distribution

- Possible scenarios for inclusive method reporting:
  - Related party
  - Contractual obligation
  - Cooperative third party
- However, inclusive method subservice organizations must meet the same requirements as the service organization:
  - Description of its system
  - Providing a written assertion, based on suitable criteria
  - Providing a Representation Letter
  - Communicating significant changes to the system

## Impact on Service Organizations (continued)

### Key Discussion Points:

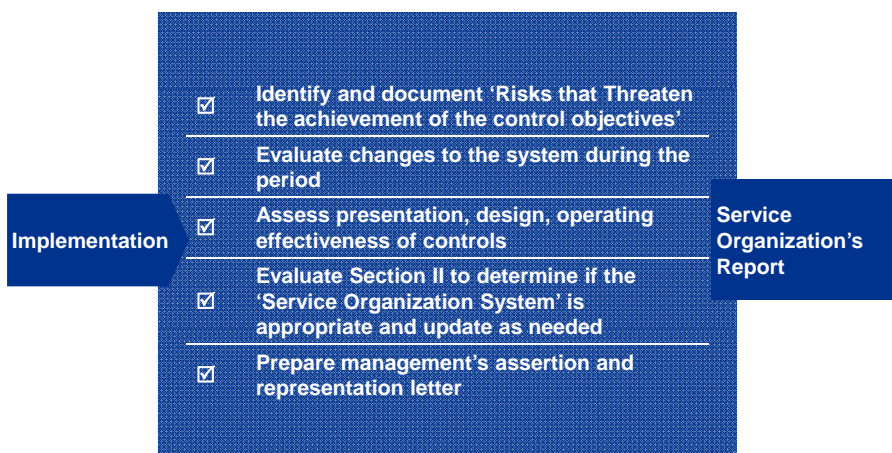
- Management Assertion
- Reasonable Basis
- Risk Assessment
- Suitable Criteria
- Use of Internal Audit
- Subservice Organization
- Report Distribution

- Reports are intended for 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 that used the system during that period to understand the "system" in place and determine its effectiveness.
- The independent auditor (of user entities) 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.
  - Consistent guidance with the PCAOB Standard #5 (Appendix B) for use in a SOX Audit.

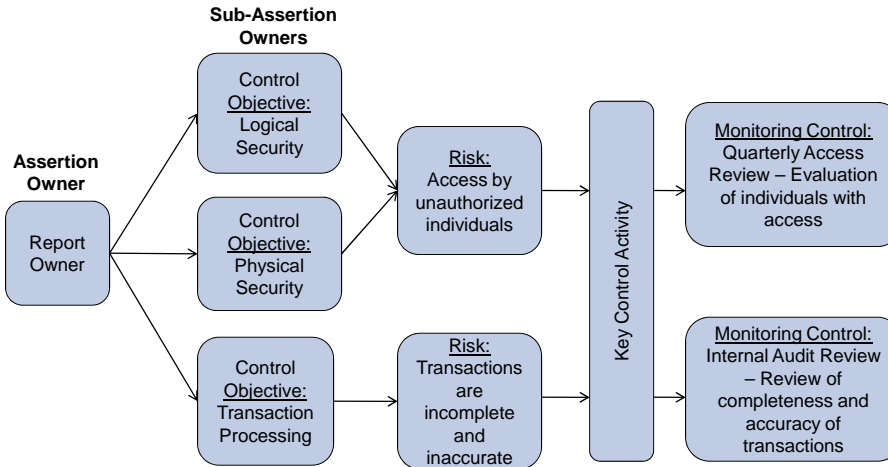
## Next steps – Service Organizations



## Next steps – Service Organizations (continued)



## Management Assertion – Example Assessment



© 2011 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

20

- What's staying the same?
- What's changing?
- Understanding the Impact as a Service Organization
- **Understanding the Impact as an User Entity**
- How to read a SOC 1 report
- Service Auditor Responsibilities
- SOC 2 and SOC 3

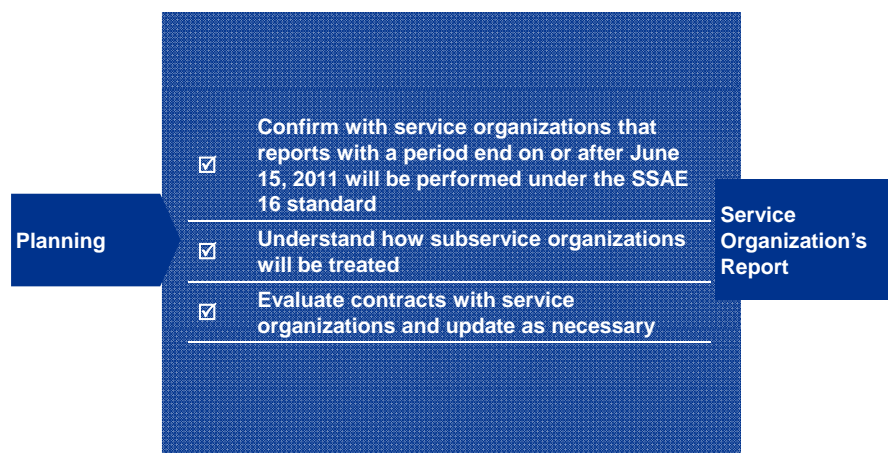
© 2011 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

21

## Impact on User Entities

- Timing of SSAE 16 – Required for all reports with periods ending on or after June 15, 2011 (early adoption is permitted)
- Understanding management’s assertion
- Understanding complementary user entity controls
- Understanding subservice organizations and reporting approach
  - Inclusive
  - Carve-out
- Users should expect control objectives, control activities, and testing to be consistent with that of historical SAS 70

## Next steps – User Entities



- What's staying the same?
- What's changing?
- Understanding the Impact as a Service Organization
- Understanding the Impact as an User Entity
- How to read a SOC 1 report
- Service Auditor Responsibilities
- SOC 2 and SOC 3

## How to read a SOC 1 report

- Review opinion
- Review complementary user entity controls
  - Determine key vs. non-key
  - Identify existing controls for key complementary user entity controls
  - Document analysis
- Review adequacy of testing by the Service Auditor
- Review exceptions and determine impact
- Acting upon SOC 1 Report information
  - Identify any gaps in controls related to complementary user entity controls
  - Request "bridge letter" if end of report period does not correspond with the end of the fiscal year end
  - Provide to auditors for their review and evaluation
  - Determine whether subservice organization reports should be requested

- What's staying the same?
- What's changing?
- Understanding the Impact as a Service Organization
- Understanding the Impact as an User Entity
- How to Read a SOC 1 report
- **Service Auditor Responsibilities**
- SOC 2 and SOC 3

## Service Auditor Responsibilities

- 1) Gain an Understanding of Management's Assertion
  - The Service Auditor is responsible for gaining an understanding of management's risk assessment process and approach related to assertion that is signed and included in the SSAE 16 report.
- 2) Suitability of Criteria
  - The Service Auditor is responsible for assessing whether management utilized suitable criteria to assess fairness of presentation, suitability of design, and operating effectiveness.
- 3) Opine
  - The Service Auditor is responsible for opining on the fairness of presentation, suitability of design, and operating effectiveness for the duration of the period.

- What's staying the same?
- What's changing?
- Understanding the Impact as a Service Organization
- Understanding the Impact as an User Entity
- How to Read a SOC 1 report
- Service Auditor Responsibilities
- SOC 2 and SOC 3

## SOC2 and SOC3 Background

- There is a large market need for SAS 70-style reports for services with limited or no relevance to financial reporting.
  - SOC2 has been developed to have the look and feel of a SOC1 report but using criteria that are applicable to non-financial reporting subject matter.
  - SOC2 leverages the Trust Services principles and criteria<sup>1</sup> that have historically supported SysTrust® and Web Trust® reporting.
  - SOC3 is a short form report like a traditional SysTrust report and uses the same principles and criteria as SOC2.

<sup>1</sup> *Trust Services Principles and Criteria*, the American Institute of Certified Public Accountants (AICPA), January 2009

SYSTRUST® and WEBTRUST® are registered trademarks of the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants.

## Overview of Trust Services Principles

Domain	Principles
<b>Security</b>	<ul style="list-style-type: none"> <li>The system is protected against unauthorized access (both physical and logical).</li> </ul>
<b>Availability</b>	<ul style="list-style-type: none"> <li>The system is available for operation and use as committed or agreed.</li> </ul>
<b>Confidentiality</b>	<ul style="list-style-type: none"> <li>Information designated as confidential is protected as committed or agreed.</li> </ul>
<b>Processing Integrity</b>	<ul style="list-style-type: none"> <li>System processing is complete, accurate, timely, and authorized.</li> </ul>
<b>Privacy</b>	<ul style="list-style-type: none"> <li>Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and CICA.</li> </ul>

© 2011 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

30

## Layers of Activity Covered by a SOC2 or SOC3 Examination

Topic	Summary
<b>Policies</b>	<ul style="list-style-type: none"> <li>Policies are defined and documented.</li> </ul>
<b>Communications</b>	<ul style="list-style-type: none"> <li>Defined policies are communicated to responsible parties and authorized users of the system.</li> </ul>
<b>Procedures</b>	<ul style="list-style-type: none"> <li>Procedures have been placed in operation to achieve the service provider's objectives in accordance with its defined policies.</li> </ul>
<b>Monitoring</b>	<ul style="list-style-type: none"> <li>The service provider monitors the system and takes action to maintain compliance with its defined policies.</li> </ul>

© 2011 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

31

## Use of SOC Reports – Summary of SOC2/3 Criteria Topics

Security	Availability	Confidentiality	Processing Integrity	Privacy
<ul style="list-style-type: none"> <li>■ IT security policy</li> <li>■ Security awareness and communication</li> <li>■ Risk assessment</li> <li>■ Logical access</li> <li>■ Physical access</li> <li>■ Environmental controls</li> <li>■ Security monitoring</li> <li>■ User authentication</li> <li>■ Incident management</li> <li>■ Asset classification / mgt.</li> <li>■ Systems development and maintenance</li> <li>■ Personnel security</li> <li>■ Configuration mgt.</li> <li>■ Change management</li> <li>■ Monitoring / compliance</li> </ul>	<ul style="list-style-type: none"> <li>■ Availability policy</li> <li>■ Backup and restoration</li> <li>■ Disaster recovery</li> <li>■ Business continuity management</li> </ul>	<ul style="list-style-type: none"> <li>■ Confidentiality policy</li> <li>■ Confidentiality of inputs</li> <li>■ Confidentiality of data processing</li> <li>■ Confidentiality of outputs</li> <li>■ Information disclosures (including third parties)</li> <li>■ Confidentiality of Information in systems development</li> </ul>	<ul style="list-style-type: none"> <li>■ System processing integrity policies</li> <li>■ Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs</li> <li>■ Information tracing from source to disposition</li> </ul>	<ul style="list-style-type: none"> <li>■ Management</li> <li>■ Notice</li> <li>■ Choice and consent</li> <li>■ Collection</li> <li>■ Use and retention</li> <li>■ Access</li> <li>■ Disclosure to third parties</li> <li>■ Quality</li> <li>■ Monitoring and enforcement</li> </ul>

© 2011 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

32

## SOC Report Structure

Traditional SAS 70	SOC1	SOC2	SOC3
Auditor's opinion	Auditor's opinion	Auditor's opinion	Auditor's opinion
–	Management assertion	Management assertion	Management assertion
Description of system and controls	Description of system and controls	Description of system and controls	Description of system
Controls, tests of operating effectiveness and results of tests	Controls, tests of operating effectiveness and results of tests	Controls, tests of operating effectiveness and results of tests	–

© 2011 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

33

## Examples of SOC Report Scenarios

### SOC1 Financial Reporting Controls

- Financial services – Custodial services
- Healthcare claims processing
- Payroll processing



### SOC2/SOC3 Operational Controls

- Cloud ERP service
- Data center co-location
- Enterprise cloud email
- Cloud collaboration
- Software-as-a-service

## Considerations for Cloud Service Providers (CSP) – Control Requirements

### Information Security Management System

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

### Areas of Added Emphasis for CSPs

- Data Protection/Segregation
- Privacy
- Encryption Standards
- Logging
- Authentication to the Cloud
- Configuration Management
- Monitoring/Compliance Function

## Key Takeaways

### ■ 2011 will be a year of transition

- SAS 70 report retires on June 15, 2011
- SAS 70 reports will be replaced by SOC1 reports, and SOC2/3 will provide a new framework for reporting on non-financial reporting subject matter.
- Varying levels of awareness

### ■ Service providers and their customers will need to determine what type of reports they require going forward

- SOC1 if significant financial reporting impact
- SOC2 or SOC3 if security, availability, processing integrity, confidentiality, or privacy focus
- Determine which principles to cover for SOC2/SOC3

## Leading Practices

### ■ Customers will need to prepare for the transition

- Revisit contractual audit provisions
- Communicate with your service providers early
- Build into due diligence/vendor management processes

### ■ Service providers will need to prepare for the transition

- Determine which report(s) will best meet the needs of their customers and potential customers
- Re-validate scope
- Identify any areas not previously covered, assess audit-readiness
- Communication plan/FAQs for educating users on the new standards and the rationale for the service provider's approach



**Thank You**

Emily Frolick  
513-763-2453  
efrolick@kpmg.com

© 2011 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.