Recent and Proposed Changes to SOC Reports Impacting Service and User Organizations.

March 3, 2015

Presenters:
Sayontan Basu-Mallick
Lori Johnson
Agenda

► SOCR Overview
  ► Difference between SOC1, SOC2 and SOC3
► Changing SOCR Community
► Update to ISAE 3402
► Changes to the AICPA attestation standards
► SOC 2 Trust Principal Update
  ► SOC 2 Plus
► Updates from an user organization perspective
► Independence
SOC 1 – elements

System description
► Services provided
► Procedures
► Accounting records
► Significant events
► Entity-level controls
► Reporting
► User control considerations

User entities’ financial statement assertions

Control objectives
“Reasonable basis” for management asserting controls were consistently applied

Risk assessment
Existing testing/validation
On-going monitoring
Limited additional testing

Management’s written assertion
Service auditor’s report
SOC 1, SOC 2 or SOC 3?

**Financial System**
- Restricted Distribution
  - Testing Description
  - Opinion
  - Assertion
  - SOC 1

**Non Financial System**
- Limited Distribution
  - Testing Description
  - Opinion
  - Assertion
  - SOC 2

- General Distribution
  - Short Description
  - Opinion
  - Assertion
  - SOC 3

(Scope: Control Objectives)
(Scope: Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and/or Privacy)

Other
SOC 1, SOC 2 or SOC 3?

Who will use the communication?
- Direct consumer
- User entity
- Business Partner
- Management/BOD
- User service organization
- Regulator
- Other

User’s areas of interest?
- Controls relevant to financial audits
  - Security
  - Availability
- Processing integrity
- Confidentiality
- Regulatory/self regulatory
- Contractual compliance
- Privacy
- Other

User’s business Purpose?
- Meet audit needs
  - Governance/risk management
  - Vendor management
  - Regulatory compliance
- Contractual compliance
- Internal report – management confidence
- Enhance trust regarding service
- Other

What ‘criteria’ will the report measure against?
- Financial statement assertions
  - Industry standards
  - Contractually specified
  - Regulatory requirements
  - Other

Conclude on report type and distribution method?
- SOC 1
- SOC 2
- SOC 3
  - Agreed upon procedures
    - AT 101, AT 601
- Findings and recommendations (internal-use, no assurance provided)
SOC 2 and SOC 3

- SOC 2 - Provides information about internal control at the service organization related to the Trust Services Principles - security, availability, processing integrity, confidentiality, or privacy (restricted use)

- SOC 3 - Provides information about the service organization’s achievement of the Trust Services criteria related to security, availability, processing integrity, confidentiality, or privacy (general use)
## A Service Provider Perspective

### Why do you provide independent assurance to your user organizations?

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows us to manage the audit process and the resulting messages that are sent to our clients</td>
<td>37%</td>
</tr>
<tr>
<td>Provides valuable feedback on how our teams are operating</td>
<td>53%</td>
</tr>
<tr>
<td>Reduces number of supplier audits</td>
<td>53%</td>
</tr>
<tr>
<td>Seen as providing competitive advantage in winning work (competitors do not provide this independent assurance)</td>
<td>71%</td>
</tr>
<tr>
<td>Contractual or compliance requirement to provide independent assurance</td>
<td>84%</td>
</tr>
</tbody>
</table>

*Source: 2014 EY Service Organization Controls Reporting Survey Results*
Changing SOCR Community
We are in the midst of significant changes for SOCR

<table>
<thead>
<tr>
<th>Alerts, changes, and guidance</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCAOB Staff Audit Practice Alert #11</td>
<td>October 2013 (published)</td>
</tr>
<tr>
<td>ISAE 3402 – international guidance update</td>
<td>December 15, 2015 (effective date)</td>
</tr>
<tr>
<td>AT 801 – US guidance update</td>
<td>December 2015 or later (anticipated effective date)</td>
</tr>
<tr>
<td>Updated Trust Services Principles and Criteria</td>
<td>December 15, 2014 (effective date)</td>
</tr>
</tbody>
</table>
Changing Standards and Guidance

► New and Pending Guidance
  ► PCAOB Staff Audit Practice Alert No. 11
  ► SOC 2 Guide—Winter 2014
  ► SOC 3 Guide—Winter 2014/2015
  ► Revised AICPA attestation standards, including AT 801—2014
  ► Trust Services Privacy currently under revision
    ► Exposure provided in June 2014
    ► Effective 2015
PCAOB SAPA 11 observations – other observations

While the PCAOB has not directly focused on the quality of SOC 1 reports, many reports may not be deemed sufficient if subject to the scrutiny given to other audit documentation. Alert 11 identifies areas for specific improvement.

► Roll-forward of controls
  ► Obtain sufficient evidence to update the results of testing of controls from an interim date to year-end

► Using the work of others
  ► Sufficiently perform procedures regarding the use of the work of others

► Evaluating control deficiencies
  ► If a deviation exists and we conclude a control is not effective, do the remaining controls address the identified risks?
  ► Sufficiently evaluate identified control deficiencies
Update to ISAE 3402
Update to ISAE 3402

► Updated ISAE3000 and ISAE3402
  ► Released in December 2013 - effective for reports dated on or after 15 December 2015
  ► Most changes are technical reporting matters that will not be visible to the service provider
  ► ISAE3402 now a supplement to ISAE 3000 rather than a stand-alone standard
  ► “Management’s Assertion” now “Management’s Statement”
  ► Requirement that the service auditor’s report contain a statement that the service auditor applies ISQC (International Standard on Quality Control) 1
  ► Requirement that the service auditor’s report contain a statement that the service auditor complies with independence and other IESBA (International Ethics Standards Board for Accountants) code requirements
Significant changes (continued)

► Concept of “engagement partner” introduced
  ► “Where required, has the appropriate authority from a professional, legal or regulatory body”
► Engagement quality control review
► Risk-based approach
Changes to the AICPA attestation standards
Proposed changes to the AICPA attestation standards, including SOC 1

- The AICPA Attestation Standards (published in the Statements on Standards for Attestation engagements or SSAEs) establish requirements for examining, reviewing, and applying agreed-upon procedures to subject matter other than financial statements.
- The Auditing Standards Board (ASB) is undertaking significant effort to improve the clarity and quality of the attestation standards.
- The revised standards are expected to be finalized during the 4th quarter 2015.
- Anticipated effective date is reports with an opinion date on or after May 1, 2017.
Summary of key changes for SOC 1 (AT 801)

► Changes to description
  ► Inclusion of complementary subservice organization controls—when carve-out method is used
  ► Disclosure of monitoring controls over subservice organizations
  ► Sufficiency of descriptions of controls
  ► Descriptions of reports
  ► Definition of subservice organization—still being discussed
  ► Definition of complementary user entity controls—still being discussed
Summary of key changes for SOC 1 (continued)

► Changes in auditor responsibilities
  ► Clarifying the use of a risk-based approach to the service auditor’s examination
  ► Understanding the internal audit function and reading all relevant reports
  ► Identification of the risk of material misstatement and evaluation of whether the description meets the needs of user auditors
  ► Evaluating control objectives and performing separate identification of the risks that threaten the achievement of the control objectives
  ► Excessive use of the work of internal audit—still being discussed
Changes to the attestation standards

► Many similarities with revisions to ISAE 3000
  ► Engagement “partner”
  ► Engagement risk-based approach
  ► Engagement quality control review
► Intended to be self-contained – minimal reference to US auditing standards
Subservice organization challenge

► ISA 402/AU-C 402

*If the user auditor plans to use a type 1 or a type 2 report that excludes the services provided by a subservice organization and those services are relevant to the audit of the user entity’s financial statements, the user auditor shall apply the requirements of this ISA with respect to the services provided by the subservice organization.*

► PCAOB inspections have identified failure to perform procedures on carved-out subservice organizations as an issue.

► User auditors are expressing greater concern over carved-out subservice organizations.
Subservice organizations - Issues in inclusive and carved-out reports

▶ **Inclusive reports**
  ▶ Subservice organizations are often reluctant to participate
    ▶ Provide services to multiple primary service organizations
    ▶ Contractual concerns
  ▶ Coordination of testing

▶ **Carve-out reports**
  ▶ No contractual relationship between users and subservice organization
  ▶ Report period
  ▶ Timing of report availability
  ▶ User organizations can monitor primary service providers, usually cannot monitor subservice organizations
  ▶ Users need to tie the subservice organization CUECs to controls at the primary service organization
Analysis of monitoring

- Understand user-entity financial statement assertions
- Identify control objectives
- Identify risks that threaten the achievement of the control objectives
- Identify the risks that are directly addressed by controls at the subservice organization
- Identify monitoring/reporting and other evidence that the controls at the subservice organization are functioning as designed
- Consider testing
Subservice organizations – Resolving issues

- SOC 1 guide encourages description of monitoring controls even when carving-out
- Monitoring may be sufficient to make controls at vendor not relevant to users

**Examples of effective monitoring controls:**

**Colocation Facility**
- Controls: Physical access and environment
- Monitoring controls: physical access approvals, periodic evaluations

**Securities Pricing Services**
- Controls: Valuation of investments
- Monitoring controls: Pricing comparison
Carved-out subservice organization CUECs

► Identifies risks that threaten the achievement of the control objectives
► Includes risks that arise from using a subservice organization
► Usually will include risk that subservice organization CUECs need to address
► If a SOC 1 report is not available from the subservice organization, consider manuals, contracts or other communications from the subservice organization
SOC2 Trust Principal Update
## SOC reporting trends – Current State

### Which of the following areas are seeing an increased interest / demand for independent assurance from your clients?

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes not related to financial transaction (e.g., customer management)</td>
<td>20%</td>
</tr>
<tr>
<td>Regulatory Compliance (e.g., Financial Market Supervisory Authority)</td>
<td>67%</td>
</tr>
<tr>
<td>Cloud Services</td>
<td>22%</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>59%</td>
</tr>
<tr>
<td>Availability / business continuity</td>
<td>71%</td>
</tr>
<tr>
<td>Data Privacy</td>
<td>59%</td>
</tr>
</tbody>
</table>

Source: 2014 EY Service Organization Controls Reporting Survey Results
The 2014 Trust Services principles and criteria

- Issued January 2014
- Effective for periods ending on or after December 15, 2014, but early adoption encouraged
- Established by the Assurance Services Executive Committee (ASEC) of the AICPA
- Consolidates the common criteria across the Trust Services principles, security, availability, processing integrity, and confidentiality
# The 2014 Trust Services principles and criteria SOC 2 principles and criteria

<table>
<thead>
<tr>
<th>PRINCIPLES</th>
<th>CRITERIA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Organization</td>
</tr>
<tr>
<td>Security</td>
<td>X</td>
</tr>
<tr>
<td>Availability</td>
<td>X</td>
</tr>
<tr>
<td>Processing Integrity</td>
<td>X</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>X</td>
</tr>
</tbody>
</table>
The 2014 Trust Services principles and criteria principles

- Established by the Assurance Services Executive Committee (ASEC) of the AICPA:
  - **Security:** The system is protected against unauthorized access, use, or modification.
  - **Availability:** The system is available for operation and use as committed or agreed.
  - **Processing integrity:** System processing is complete, valid, accurate, timely, and authorized.
  - **Confidentiality:** Information designated as confidential is protected as committed or agreed.
  - **Privacy:** Addresses the system’s collection, use, retention, disclosure, and disposal of personal information
SOC 2 — expected 2015 changes

- Updated for 2014 Trust Service criteria
- Increased guidance to service auditors on how to plan and perform an engagement
  - Sufficiency of description
  - Suitability of design of controls
    - Guidance by trust services grouping
    - Principle
  - Controls that did not operate during the period
  - User entity responsibilities vs. complementary user entity controls
  - Subservice organizations
# New SOC 2 reporting opportunities

## SOC 2 reporting options

<table>
<thead>
<tr>
<th>Report</th>
<th>Level of effort</th>
<th>Opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 2</td>
<td>Baseline</td>
<td>Standard opinion</td>
</tr>
<tr>
<td>SOC 2 with a mapping to another framework</td>
<td>Not likely to require additional controls outside of Trust Services Principles</td>
<td>Standard opinion</td>
</tr>
<tr>
<td>SOC 2 Plus</td>
<td>Controls required to align to Trust Services Principles and the selected framework(s)</td>
<td>Standard opinion plus an opinion on the selected framework(s)</td>
</tr>
</tbody>
</table>
## New SOC 2 reporting opportunities (continued)

Common frameworks requested by our clients and their stakeholders:

<table>
<thead>
<tr>
<th>Framework</th>
<th>Mapping to SOC 2 available</th>
<th>SOC 2 Plus possible</th>
<th>Other Attestation report</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001</td>
<td>✓</td>
<td>✓</td>
<td>ISO Certification</td>
</tr>
<tr>
<td>Cyber Security for Critical Infrastructure</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NIST 800-53 R4</td>
<td></td>
<td>In progress</td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PCI</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Security Alliance Cloud Control Matrix</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>FISMA</td>
<td></td>
<td></td>
<td>AT101</td>
</tr>
<tr>
<td>Federal Risk and Authorization Management Program (FedRAMP)</td>
<td>✓</td>
<td>✓</td>
<td>AT101—in progress</td>
</tr>
</tbody>
</table>
Multi-framework SOC2 Reporting

SOC 2
Common Criteria/Security

FISMA/FedRAMP
Privacy
PCI
Processing Integrity
Confidentiality
HIPAA/Hitech
Availability
ISO 27001
Updates from an user organization perspective
## A User Organization Perspective

**Why do user organizations still perform their own audits on the services covered by independent assurance reports?**

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not applicable - clients do not perform their own audits</td>
<td>33%</td>
</tr>
<tr>
<td>The regulatory agenda is not covered in the assurance report</td>
<td>10%</td>
</tr>
<tr>
<td>The assurance report period is inappropriate</td>
<td>8%</td>
</tr>
<tr>
<td>The independent assurance report does not cover all client relevant service parts</td>
<td>46%</td>
</tr>
<tr>
<td>Other reason*</td>
<td>23%</td>
</tr>
</tbody>
</table>

*Other reasons include:
- Clients' own auditors include reports as part of their own broader audits.
- Independent assurance report does not cover the requirements for internal control (Governance).
- The assurance report period covers only 9 months (not 12).
- Client specific details have to be covered with a specific audit.

Source: 2014 EY Service Organization Controls Reporting Survey Results
AICPA SOC 1 Guide 3.40 states that

The degree of detail included in the description (SOC 1) generally is equivalent to the degree of detail a user auditor would need if the user entity were performing the outsourced services themselves.

This applies to all aspects of the SOC 1 report:

- Auditor opinion
- Management assertion
- Description
- Evaluation of
- Carved out sub service providers
- Identified deficiencies
- Wording of controls
- Wording and results of testing
A User Organization Perspective (6)
User auditor viewpoint on SOC report

► The description – should be documented as if the user entity were performing the outsourced service
  ► Clear description of the process flow – consider a flowchart
  ► Identification of key process owners, inputs, outputs, reports
  ► Control objectives related to financial statement and IT risks
► Description of relationship with “carved out” subservice providers, including the affected control objectives
► Increased level of detail provided in the test procedures and results section
  ► When describing controls
  ► Of the auditor’s tests and results
  ► Identified deviations
Recent changes/trends that impact user organizations and user auditors

► Sufficiency of coverage provided by the Type 2 SOC report

► The PCAOB is increasingly questioning reliance on SOC reports when the SOC report does not cover an adequate period of the company’s audit period. Adequacy is determined based on period covered in the SOC report, the nature of services provided, the risk of impacted accounts at the user organization, among other factors.

► Use of SOC 2 reports in support of financial statement audit

► This is becoming more acceptable where transaction processing and reporting services are not performed and the system description and controls can be adequately represented in a SOC 2 report.
Independence update
Independence update

➡️ SEC matters

➡️ Reports included in SEC filings or prepared to meet an SEC requirement (e.g., custody rule)

➡️ “bookkeeping services” has been interpreted to include word processing and printing services and are prohibited

➡️ Single user reports

➡️ SEC has taken the position that a EY audit client user entity should not use an EY prepared single user SOC 1 report as its basis for SOx assessment.
Questions?
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2014 Ernst & Young LLP.
All Rights Reserved.

1405-1254075
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com