Keep Your SOCs On!!

June 13, 2013
• Introductions
• Service Organization Control Reports (SOCs)
  – SOC 1
  – SOC 2
  – SOC 3
• Dissecting a SOC Report
• Improving Your Review and Reliance on SOCs
• Questions
Neha S. Patel, CPA, CISA
Neha is a Senior Manager with more than nine years of experience in public accounting. She has experience in governance, risk, and compliance, including service organization control (SOC) audits and Sarbanes-Oxley (SOX) assessments. Her focus is on IT audit.

Brittany L. Teare, CISA
Brittany is a Manager in Weaver’s IT Advisory Services practice. Brittany has over eight years of experience IT auditing and consulting services. She performs security, SOC, IT audit (GRC), security and process improvement consulting services.
Largest independent accounting firm in the Southwest, with seven offices across all major Texas markets

Nationally ranked as a top 50 firm – named a “BEST of the BEST” CPA firm by *INSIDE Public Accounting* (2012)

Ranked #42 by *Accounting Today* (2013) and #39 by *INSIDE Public Accounting* (2012)

FY 2012 revenues of approximately $75 million

Founded in 1950 in Fort Worth, Texas

Approximately 500 employees, including 64 partners

Member of the Baker Tilly International network of firms
Our Services

• **Advisory:**
  - Internal Audit
  - IT Advisory
  - Forensics
  - Business Valuation
  - Service Organization Control Audits (SOC 1, 2 and 3)

• **Tax and Strategic Business Services:**
  - Tax Compliance
  - State and Local
  - Property Tax
  - Sales Tax
  - Refunds
  - International (transfer pricing)

• **Financial Statement Audit:**
  - Audits of Financial Statements
  - Benefit Plans
  - Reviews
  - IFRS
  - Agreed Upon Procedures
Industries Served

• Oil and Gas
• Renewable Energy
• Manufacturing and Distribution
• Financial Services
• Real Estate
• Construction
• Public Sector
• Healthcare
• Professional Services
• Retail
• Technology
SOC Terminology
Understanding Terminology

User Entity

Service Organization

It is important to understand who is being audited and who the report is ultimately being prepared for.
Any company that provides an outsourced service that is integral to the operations of its clients

- Application Service Providers (ASPs)
- Data Processing Services (DPs)
- Managed security providers
- Trust departments
- Claims processors
- Clearinghouses
- Credit processing companies
- Data hosting facilities
Service Organization Control Reports (SOCs)
What is a Service Organization Audit?

• First released in 1993 as the Statement on Auditing Standard No. 70 (SAS 70)

• In 2011, the American Institute of Certified Public Accountants (AICPA) refined the instructions and applicability of service organization audits by creating three report deliverables.
Standards and Names

<table>
<thead>
<tr>
<th>SERVICE ORG CONTROL 1 (SOC 1)</th>
<th>SERVICE ORG CONTROL 2 (SOC 2)</th>
<th>SERVICE ORG CONTROL 3 (SOC 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSAE16</strong> - Service auditor guidance</td>
<td><strong>AT 101</strong></td>
<td><strong>AT 101</strong></td>
</tr>
<tr>
<td>Restricted Use Report (Type I or II report)</td>
<td>Generally a Restricted Use Report (Type I or II report)</td>
<td>General Use Report (with a public seal)</td>
</tr>
<tr>
<td>Purpose: Reports on controls for F/S audits</td>
<td>Purpose: Reports on controls related to compliance or operations</td>
<td>Purpose: Reports on controls related to compliance or operations</td>
</tr>
</tbody>
</table>

**Note:** The SOC 3 report is the SystTust for Service Organizations.
• Report on controls at a service organization relevant to a user entity’s internal control over financial reporting

• Contents of report package:
  – Description of service organization’s system
  – CPA’s opinion on fairness of description, suitability of design, operating effectiveness of controls
SOC 1<sup>SM</sup> Reports – Type 1 and Type 2

• Both report on the fairness of the presentation of management’s description of the service organization’s system, and...
  
  – Type 1 also reports on the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date
  
  – Type 2 also reports on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period
• Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy

• Contents of report package same as SOC 1\textsuperscript{SM}
  – Also two versions: Type 1 or Type 2

• Example:
  – A Software-as-a-Service (SaaS) or Cloud Service Organization that offers virtualized computing environments or services for user entities and wishes to assure its customers that the service organization maintains the confidentiality of its customers’ information in a secure manner and that the information will be available when it is needed.
SOC 2<sup>SM</sup> Report – 5 Trust Services Attributes

- **Security**
  - The system is protected against unauthorized access (both physical and logical)

- **Availability**
  - The system is available for operation and use as committed or agreed

- **Processing integrity**
  - System processing is complete, accurate, timely and authorized

- **Confidentiality**
  - Information designated as confidential is protected as committed or agreed

- **Privacy**
  - Personal information is collected, used, retained, disclosed and disposed of 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 Canadian Institute of Chartered Accountants
• Trust Services Report for Service Organizations

• Contents of report package:
  – CPA’s opinion on whether entity maintained effective controls over its system
  – A seal can be issued on service organization’s website

• SOC 2\textsuperscript{SM} vs. SOC 3\textsuperscript{SM} report
  – The key difference: a SOC 2\textsuperscript{SM} report is generally a \textit{restricted-use} report, while a SOC 3\textsuperscript{SM} report has less detail and in a format that lends itself to a \textit{general-use}
Main Differences

- Type 1 is a snapshot in time (i.e. as of June 30, 2013)
- Type 2 tests controls over a period of time (6 to 12 months)
Dissecting a SOC Report
Sections in the Report

- Section I: Independent Auditor’s Report (i.e., Opinion)
- Section II: Management Assertion
- Section III: Description of the System
- Section IV: Description of Test of Controls and Results
- Section V: Additional Information (optional / unaudited)
What Matters to Users?

- Section I: Independent Auditor’s Report (i.e., Opinion)
- Section II: Management Assertion
- Section III: Description of the System
- Section IV: Description of Test of Controls and Results
- Section V: Additional Information (optional / unaudited)
• Section I: Independent Auditor’s Report (i.e., Opinion)
  – Provides user entities with the overall evaluation over the areas reviewed in the report.
  – If qualified, the opinion will outline the areas that could not be achieved (i.e., failure) or the areas that were not available for review (i.e., scope limitation).
• Section IV: Description of Test of Controls and Results
  – Provides user entities with detail regarding the individual criteria, testing procedures performed and results by control / criteria.
  – SOC 3 reports will NOT include this detail.
Making SOCs Fit Your Needs
Key Steps for Users

• Determine the type of service is being relied upon and what matters to your organization from an operations and regulatory requirement
• Get as much transparency as possible; if nothing else, at least get a copy of the last relevant audit report
• Familiarize yourself with the limits of the vendor's responsibility

Source: Bloomberg Businessweek
Key Steps for Users

• As with any other service provider, make sure there are solid agreements in place that protect you as a user
• Make sure you have recourse and the service provider has some ‘skin’ in the game
Summary
• Audits over service organizations are **NOT** new
  – SAS 70 has been around for more than 20 years
  – Trust Services existed for non-financial services

• SSAE 16 does not equal a SOC 2 or SOC 3
SOC Reporting

• SOC reporting can provide users with the **transparency and assurance** they need
  – SOC 1 can be designed to focus on transactional processing (if performed in relation to **financial reporting**) in addition to IT areas
  – SOC 2 can be focuses on specific **principles** to demonstrate coverage from a technical standpoint
  – SOC 3 can provide a high-level report to provide a summary of the service
Questions?

Neha S. Patel
Senior Manager, IT Advisory Services
Tel: 972.448.9804
Email: Neha.Patel@weaverllp.com

Brittany L. Teare
Manager, IT Advisory Services
Tel: 972.448.9299
Email: Brittany.Teare@weaverllp.com