Service Organization Control Reports

What Did We Learn from Year One?

experience BKD
CPAs & Advisors

Agenda

- Definitions
- Service Organization Reports – What are they?
- Year One Experiences – SSAE 16
- Year One Experiences – SOC 2
- Reading a Report
- Questions / Discussion

What are Service Organizations?

- Service Organization – provider of services that may impact a risk to a user's financial reporting, or that pose a business or compliance risk
  - Services such as:
    - ✓ Cloud computing (SaaS, IaaS, PaaS)
    - ✓ Managed security
    - ✓ Boutique AR / AP / Tax Outsourcing
    - ✓ Financial services customer accounting
    - ✓ Customer support
    - ✓ Sales force automation
    - ✓ Health care claims management and processing
    - ✓ Enterprise IT outsourcing

Common Terms

- Service auditor – a CPA who examines and reports on controls at a service organization
- Users – typically considered clients of service organization
  - May need assurance regarding controls over ICFR, security, availability, processing integrity, confidentiality or privacy
- User Auditor – a CPA who performs a audit on the users financial statements
  - Needs assurance regarding the controls in place at the service organization that impact user financial statements (ICFR)

Service Organization Control Reports

experience BKD CPAs & Advisors

Changes: SAS vs. SSAE

- June 15, 2011 – sunset date for SAS 70
- Attest standard (Assertion), not an audit standard (GAAP)
- Consistency with international standards and existing attestation standards
- Increased focus on service organizations with services relevant to a user organizations internal control over financial reporting (ICFR)
- Some SAS 70 reports will move to SOC 2 or SOC 3 reports
- By the way…
  - ❖ No such thing as a SAS 70 or SSAE 16 “certification”

Service Organization Control Reports

	SOC 1	SOC 2	SOC 3
Purpose	Report on controls relevant to user entities ICFR [1]	Report on controls related to compliance and operations	Report on controls related to compliance and operations
Use of Report	Restricted [2]	Restricted [3]	General
Report Detail	Includes Testing Detail *Type 1 or Type 2*	Includes Testing Detail *Type 1 or Type 2*	No Testing Detail
AICPA Interpretive Guidance & Reporting Vehicle	SSAE 16, AICPA Guide	AT 101, AICPA Trust Services Principles, AICPA Guide	AT 101, AICPA Trust Services Principles TSP 100

[1]Internal Control Over Financial Reporting
[2]Service Organization Management, Users, Users Auditor
[3]Service Organization Management, Users, Knowledgeable Parties

experience BKD CPAs & Advisors

Type 1 and Type 2 Reports

- Type 1
  - Reports on fairness of presentation of management's description of the service organization's system
  - The suitability of design of controls
  - Unlikely to provide sufficient information to assess risks
  - Provides an understanding system and controls
- May be useful when:
  - Organization is new
  - Recently made significant changes
  - Other reason insufficient time or history to perform Type 2

Type 1 and Type 2 Reports

- Type 2
  - Same as Type 1 plus
  - Service auditor opinion on operating effectiveness
  - A detailed description of service auditor's tests of controls and results
  - Reporting on compliance with selected TSPs (SOC 2)
  - Most frequently requested type of report

SSAE 16 – Year One Experiences and Key Issues

experience BKD CPAs & Advisors

Which Report Do I Use?

- ICFR – SOC 1 (SSAE 16)
- Limited Use / Trust Principles – SOC 2
- General Use / Trust Principles – SOC 3
- Discussion
  - Cloud Services
  - Data Centers
  - Electronic Medical Record SaaS
  - TPAs
- Driver – Who is the intended user?

Scoping

- Included/excluded services
- Services that impact your client's financial reporting
- Key third parties (sub-service organizations)
  - Identify all relevant 3rd party service organizations
  - Existence and use of their SSAE 16/SOC 2 Report
  - Commitments from 3rd party relative to carve out or inclusive method
- Treatment of subservice organizations
  - Included (inclusive method)
  - Excluded (carve-out method)

Key Issues:

Management Assertion - New

A Management Assertion will be included in or attached to the SSAE 16 report

- States*:
  - System fairly represented
  - System suitably designed and implemented
  - The related controls activities were suitably designed to achieve the stated control objectives
  - That the control activities are operating effectively (Type 2 only)

*The auditor opinion attests to these statements. Type 1 specified date/Type 2 throughout the period

Key Issues:
Management Assertion

- The report will reference that <u>management</u> is responsible for:
  - Preparing the system description
  - Providing the stated services
  - Specifying the control objectives
  - Identifying the risks
  - Selecting and stating the criteria for their assertion (e.g. monitoring activities)
  - Designing, implementing and documenting controls that are suitably designed and operating effectively

Key Issues:
Management Assertion

- Auditor's Opinion – remains in the role of providing assurance regarding management's assertions (same but more emphasis)
- Auditor is not the entity responsible for the communication (same but more emphasis)
- Subservice organizations must provide a similar assertion when the inclusive method is used

Management Assertion - Issues

- “Boilerplate” – with edits for inclusive / exclusive treatment of subservice organizations
- Management’s basis for assertion
- Sufficiency of current monitoring processes
- Need for direct testing of controls not sufficiently monitored

Management Assertion - Issues

- Audit Firm Formats
  - Signed
  - Unsigned
  - Dated
  - What date?
  - No Date

Key Issues:
System Description

- SAS 70 was a narrative description of controls
- SSAE 16 requires a description of the system
  - Infrastructure
  - Software
  - People
  - Procedures
  - Data

Key Issues:
System Description

- Components common to existing Descriptions of Controls
  - Organizational Overview
  - Types of Services covered
  - Period covered
  - Control objectives and related control activities
  - Complementary user controls

Key Issues:
System Description

- Other relevant aspects of the organization's:
  - Control environment
  - Risk assessment process
  - Information and communication systems
  - Control activities and monitoring controls

Key Issues:
System Description

- Additional elements for the Description of the System
  - Classes of transactions and details on related procedures and accounting records
  - The capturing and addressing of significant events other than transactions
  - Report preparation processes
  - Changes to the system during the period (Type 2)

Key Issues:
System Description

- Identify excluded subservice organizations
- For inclusive subservice organizations, add
  - Related system description
  - Related control objectives
  - Related control activities

Key Issues:
Supporting Control Design

- Management should:
  - Identify the risks that threaten the achievement of the stated services
  - Identify the risks that threaten the achievement of the stated control objectives
  - Evaluate whether the identified controls sufficiently address the risks to achieving the control objectives
- Risks to Services ➡ Control Objectives
- Risks to Control Objectives ➡ Control Activities

Design of Controls: Based on Risk

Risk Assessment Supporting Control Design

Services Provided

Assessment of risks to services leads to:

Control Objectives

Assessment of risk to control objective leads to:

Control Activities

Key Issues:

Design of Control Objectives

- Identification of Service Process Areas
- Completeness of objectives to address risks
- Types of Control Objectives
  - Entity
  - Program Development / Change Management
  - General IT
  - Business Process
- Use existing frameworks / SOX efforts / compliance requirements

Key Issues:

Design of Control Activities

- Specificity of activities
  - Controls vs. processes
  - Specific
  - Testable
- Identifying supporting documentation
- Relating user considerations
- Management assertion considerations

Other Key Issues

- Service auditor use of internal audit
  - Reliance on / must disclose
  - Direct use / no disclosure
- Certain aspects of opinion apply to entire period rather than a point in time
  - Narrative
  - Control design
  - Control implementation

SOC 2 – Year One Experiences and Key Issues

experience BKD CPAs & Advisors

SOC 2 Reporting

- TSP Criteria
  - Security: The system is protected against unauthorized access (physical and logical)
  - Availability: The system is available for operation and use as committed or agreed
  - Processing Integrity of the system: System processing is complete, accurate, timely and authorized
  - Confidentiality of information processed: Information designated as confidential is protected as committed or agreed
  - Privacy of information processed: Personal information is collected, used retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice

Unique SOC 2 Key Issues

- Most Issues the same as SSAE 16
- Identification of applicable Trust Service Principles / Criteria
- Narrative
  - Discussion of TSP at included and excluded subservice organizations
  - Identification of compliance of relevant subservice organizations with key TSP criteria
- Report
  - Display of control activities supporting selected TSP criteria

Reporting to Multiple Audiences

- Multiple reports scenarios
  - ❖SOC 1 and SOC 2
    - ✓Services impacting ICFR of user and other services with trust services principles concerns
  - ❖SOC 2 and SOC 3
    - ✓Services not impacting ICFR and need to use beyond current users such as marketing to prospects
  - ❖SOC 1 and SOC 3
    - ✓Services impacting ICFR of user and other services with trust services principles concerns or marketing needs
- **Note** – must be separate reports

Reading a SOC Report

experience BKD CPAs & Advisors

Report Components

- Opinion
  - Qualified (Modified)
    - ✓Modifications are specific
    - ✓Not pass/fail
    - ✓User must assess impact of modification
  - References to subservice organizations
    - ✓Inclusive or Exclusive
- Assertion
  - Subservice Organizations
  - Inclusive or Exclusive

Report Components

- Narrative
  - Organization overview
  - Scope / related services not included as compared to services obtained by user
  - Sufficiency of description / controls for services obtained by user
- User Considerations
  - Assess if you have implemented user considerations
  - Consider sufficiency and applicability to services utilized

Report Components

- Control Objectives
  - Organization / scope of objectives
  - Sufficiency of service process areas compared to services utilized
  - Completeness for your purpose
- Control Activities
  - Completeness
  - Description of testing
  - Results / exceptions
  - Impact of exceptions on your services

Report Components

- Other Information
  - Changes between end of period and report date
  - Management responses to opinion modifications or testing exceptions
  - Other unaudited information relevant to user
    - ✓Glossary
    - ✓BCP / DR executive overview
    - ✓Organizational information

Questions / Discussion

experience BKD CPAs & Advisors

Thank you for attending. Learn more at bkd.com

Rod Walsh | Director | 816.221.6300
rwalsh@bkd.com

experience BKD CPAs & Advisors