Service Organization Control Reporting

Andrew Wittig CISA, CIA, MBA, MSIM

ParenteBeard
CONFIDENCE THROUGH CLARITY

an independent member of
BAKER TILLY
INTERNATIONAL

Learning Objectives

- Differences Between the 3 SOC reports
- Components of a SOC Report
- SOC Review Process

Overview

- What is a SOC Report?
  - “Service Organization Controls” Report
  - Independent Service Auditor’s Report on Controls at a Service Organization
  - Standards established by the AICPA

Overview

- SAS70 vs. SOC
- SOC1 vs. SOC2/3
- SSAE-16
- Type 1 / Type 2
- Definitions / Examples
  - Service Organization – ADP Payroll
  - User Organization – ADP's clients
  - Service Auditor – Firm that performs the SOC exam
  - User Auditor – Auditors of ADP's clients
  - Subservice Organization – Data center hosting ADP's servers

Overview

- Why Perform a SOC examination?
  - Prevent teams of individual auditors from duplicating efforts
- Are Companies Required to Have a SOC Report?
  - No, but it is in their best interest
- What Determines if a Company Gets a SOC Report?
  - Customer demand such as SOX or contractual obligation

Components of a Report

- Section 1 – Opinion
- Section 2 – Management Assertion
- Section 3 – Overview of Operations, COSO Components, UCC's
- Section 4 – Controls / Testing / Results
- Section 5 – Other Information

Components of Section 1

- Opinion Covers:
  - Fairness of Presentation
  - Design of Controls
  - For Type 2 – Test of Operating Effectiveness over a period of time
- Qualification
  - SOC 1 is qualified at the objective level
  - SOC 2 is qualified at the criteria level
  - Pervasiveness of failure and presence of compensating controls help determine qualification
- Subservice Providers
- Reference to Section 5

Components of Section 2

- Management's Assertion
- Similar to Opinion
  - Fairness of Presentation
  - Design
  - Operating Effectiveness

Components of Section 3

- Overview of Operations
- System Description / Components / Transaction Processing
- COSO Components – Relevant Aspects of:
  - Control Environment
  - Risk Assessment
  - Monitoring
  - Information and Communication
- User Entity Control Considerations

Components of Section 4

- SOC1 – Control Objectives Relevant to Financial Reporting
- SOC 2/3 – Trust Services Principles
  - Each principle includes policies, procedures, communication, monitoring
  - Can choose any or all principles, but must address all prescribed criteria for that principle
    - Security
    - Availability
    - Processing Integrity
    - Confidentiality
    - Privacy

Components of Section 5

- Other Information Provided by Management
  - Management Responses to Testing Exceptions
  - Disaster Recovery
  - Not covered by Opinion

SOC Review Process (User Organizations)

- For audits or vendor management
  - Scoping
  - Opinion
  - Testing Exceptions
  - Reporting Period
  - User Control Considerations

SOC Review Process - Scoping

- In-scope SOC reports should be determined by the user organization – i.e. SOX only, high/medium risk vendors, etc.
- You may only be concerned about certain controls in the report
- You may be concerned about controls not included in the report
- What if my service provider doesn't have a SOC report?
  - Additional procedures may be necessary

SOC Review Process - Opinion

- Opinion – Qualified or Unqualified?
- Qualified Opinion means they are not achieving one or more control objectives (SOC1) or criteria (SOC2) – may require additional procedures.
- Unqualified does not mean “no exceptions”
- A qualified opinion in a SOC report is not as serious as a qualified opinion for financial statements.

SOC Review Process – Testing Exceptions

- Test of Control = what the service auditor did to verify control was working
  - Inquire of management
  - Observe activity
  - Inspect documentation
  - Re-perform

SOC Review Process – Testing Exceptions

- Test Results
  - “No (relevant) exceptions noted”
  - “Inspected a selection of 25 new hires during the period and determined that 3 of the new hires did not complete…”

SOC Review Process – Testing Exceptions

- Testing Exceptions – Consider:
  - Nature of exceptions
  - Volume/Frequency
  - Compensating Controls
  - Remediation
  - Management Response

SOC Review Process – Reporting Period

- Reporting Period
  - Usually 6-12 months
- “Comfort Letter” or “Gap Letter” may be required (Also called “Negative Assurance Statement”)
- Additional Test Procedures may be required

SOC Review Process – UCC's

- User Control Considerations – Things the user organization must do in order for entire process to work:
  - Review reports from the service organization
  - Report errors timely
  - Administer security locally
  - Encrypt data transmissions

- How you address UCC's should be documented in your review

Questions?

Feel free to contact me at

Andrew.Wittig@ParenteBeard.com