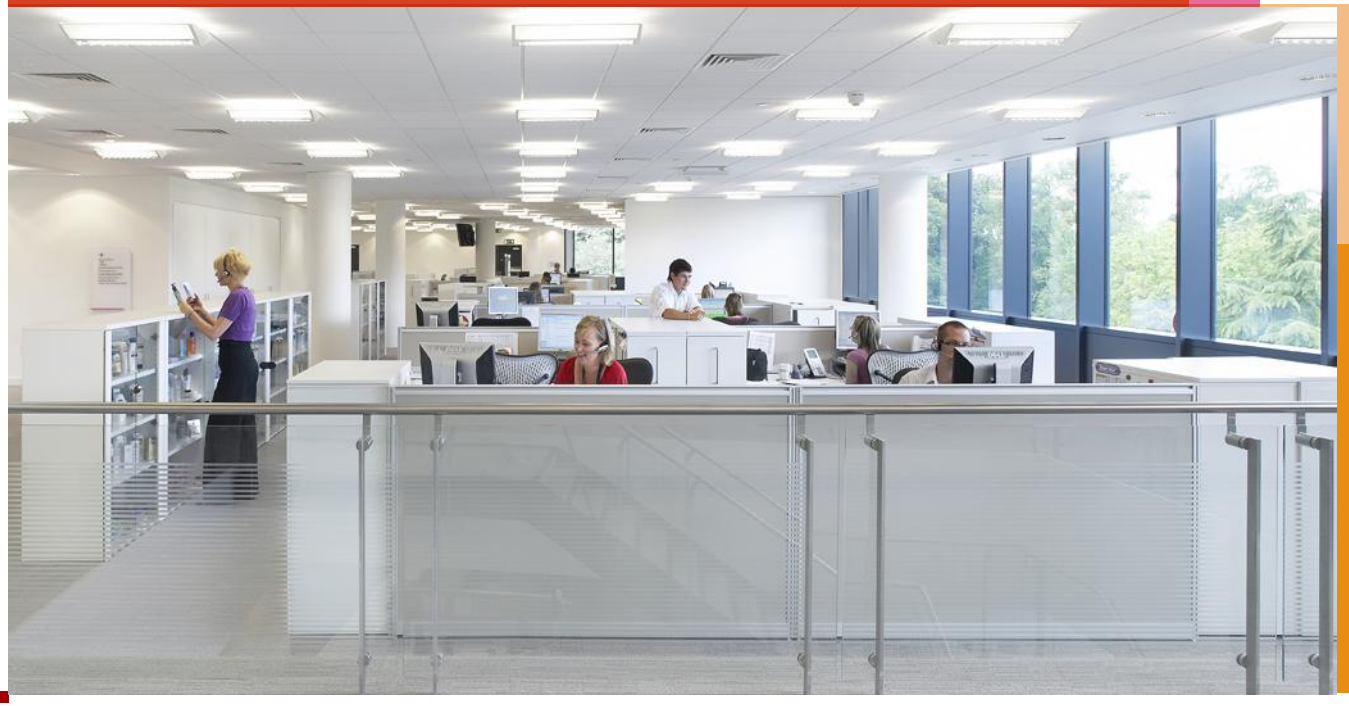
www.pwc.com

Fiduciary & Investment Risk Management Association

Getting the Right Fit on SSAE16

May 1, 2013



pwc

Agenda

- Introduction
- What is driving the need for increased transparency?
- Overview of Third Party Assurance Options
- Comparing Various Reporting Options
- What is Included and What Does it Mean?
- What you can do and Questions to Ask
- Questions

Introduction

George Galindo is a managing director in PwC's Risk Assurance practice in Dallas and serves as the national practice director for Third Party Assurance. George has nearly 20 years of experience assisting organizations assess and report on complex IT environments, internal controls, business and IT strategy and regulatory compliance.

What is Driving the Need for more Transparency

- Promises made between organizations

- Increase in the need for, use of and quality of Data

- Increased outsourcing and off-shoring of core business functions

*Seeing increase in transparency reporting in two categories – Reports **over** financial reporting and Reports **beyond** financial reporting*

Overview of Reporting Options

	Reports Over Financial Reporting	Reports Beyond Financial Reporting
Standard	AICPA – SSAE16 / SOC	AICPA – AT101
Purpose of Report	Controls at a service organization related to internal control over financial reporting	Reports over management's assertion over internal controls or other subject matter (e.g., compliance, operations, security, performance, etc.)
Level of Comfort	Positive Assurance over the subject matter covered in the report	Positive Assurance over an assertion made by management
Criteria and Scope	Fair presentation, design and operating effectiveness of control objectives covering internal controls over financial reporting	Custom or specified criteria based on subject matter of the report
Intended Users	Current user entities of service organization and their auditors	Can be restricted to known users/entities or general use (distributed to unknown third parties)
Marketplace Awareness	Well known in marketplace, however, often misunderstood in belief that report covers items beyond financial reporting	Not as well known in the marketplace, however, knowledge is rapidly growing due to need for transparency beyond traditional financial reporting
Reporting Period	Generally, annual or semi-annual reports are issued over operating effectiveness (Type 2) or point in time over design (Type 1)	Can range from point in time (results based report) to a period of time, generally no longer than a one year period.

Comparing SOC1, SOC2, and SOC3

Service Organization Control (SOC) reports are designed to bridge the gap between a report on financial reporting controls and the need to cover a broader set of business, commercial, and regulatory risks

- **SOC 1:**
  - Performed under SSAE 16
  - Direct replacement for SAS 70
  - Focuses on a service organization's internal controls over financial reporting
  - Contains a description of the service organization's system
  - Primarily and auditor-to-auditor communication

Comparing SOC1, SOC2, and SOC3

- **SOC 2:**
  - Reporting options that go beyond financial controls, such as technology-related areas like privacy, availability, confidentiality, processing integrity and security
  - Contains a description of the service organization's system
  - Allows for detailed description of the service auditor's tests & results
  - Intended for parties knowledgeable of the service organization
- **SOC 3:**
  - Encapsulates reporting on areas like privacy, availability, confidentiality, processing integrity and security
  - Often results in the issuance of a "branded report," e.g. "SysTrust"
  - Does not contain a description of testing and results
  - Can be distributed to anyone

Reports Beyond Financial Reporting

All reports beyond financial reporting are based on an Attest Standard called AT101

AT101 is a **flexible standard** and can be used for reports covering a wide variety of different subject matters, for example:

- Regulatory and compliance (PCI, ISO frameworks, NIST frameworks, etc)
- Business operations and results
- Technology and application outsourcing
- Privacy, sustainability and other emerging hot topics (GAPP)

Although AT101 is general standard over subject matter beyond financial reporting, the AICPA has some identified specific uses of AT101 over certain activities performed at service organizations.

Reports beyond financial reporting

Other custom attestation reports

When one of the three SOC based reports may not be the right fit, another option exists to provide comfort and assurance.

Customized attestations, are meant to allow for assurance reporting across a wide spectrum of different subject matter and are flexible enough to meet a wide variety of needs.

A customized attestation provides positive assurance and although generally limited to specified or knowledgeable users, in certain circumstances, can be unlimited in distribution.

Customized attestations can provide opinions covering either controls or specific results.

Requirements for customized attestations generally require suitable criteria, which must be objective, measurable, complete and relevant.

What is Included and what does it mean?

Most Common Type of Report – SOC1

- Report has two parts -- “audited” and “unaudited”
- Audited portion includes the opinion and the tests performed by the auditor
- Unaudited portion includes management’s description of the system and User Entity Control Considerations

Within the ‘unaudited’ areas, the auditor continues to have an obligation to ensure information is fairly presented.

What is Included and what does it mean?

Management's Description of the System

- It is very important to understand and align service expectations against the management description within the report
- Service organizations are placing more emphasis on strengthening this description to meet broader user needs
- User Entity Control Considerations are also key to ensure alignment between internal processes and services provided by the service organization

What is Included and what does it mean?
SOC2 Reports

- Similar to SOC1 – an “audited” and “unaudited” portion
- Criteria is pre-established by the AICPA – therefore, reports are comparable from organization to organization
- Key differences between reports will be management’s description of the system, and other activities performed that go beyond the standard principle

What Your Organization Can Do?

- Think about the transparency needed from your service provider – if they made a mistake, how would **you** detect it – what impact might it have on **your** brand
- You can gain a significant amount of comfort without receiving an independent auditor's report
  - Direct communication
  - Questionnaire and performance analytics
  - Requests for documents/transparency
  - Right to audit clause

An independent auditor's report can and does provide the highest level of comfort and assurance for mission critical functions and activities performed by another party

Questions to ask your service providers

1. What is the nature of the service organization, what are its intended services?
2. What types of attestation reporting is currently being performed at the service organization?
3. What is the scope of work being performed and does that cover the relevant risks that are of primary concern to the user organization?
4. What time frame will the report cover?
5. Have there been any recent incidents or concerns around data security or privacy?
6. Is the service organization using mobile devices, social media, cloud computing?
7. How are service organizations addressing regulatory concerns?
8. Does the service organization have a contractual responsibility to provide you with transparency over operations, controls and results?
9. Does the service provider use any other service providers or third-party vendors, and how do you derive comfort over these parties?

Aligning your ask with transparency received

- Read the report with a specific eye on how your organization utilizes the service provider – don't just read or rely solely on the auditor's opinion
- Understand the difference between an unqualified and qualified opinion – and how that may affect your processes and reliance on the service organization
- Engage with your service organization to include areas of concern to your organization in their next reporting cycle
- Ask for assurance that goes beyond financial reporting – as financial reporting controls only provide one window into the operations of your service organization

Questions

Presenter: George Galindo

Email: george.a.galindo@us.pwc.com

Phone: (214) 754-4831