Mastering SOC-1 Attestation Reports Under SSAE 16: Auditing Service Organizations Controls in the Cloud

TUESDAY, AUGUST 9, 2016, 1:00-2:50 pm Eastern

IMPORTANT INFORMATION FOR THE LIVE PROGRAM

This program is approved for 2 CPE credit hours. To earn credit you must:

- Participate in the program on your own computer connection (no sharing) – if you need to register additional people, please call customer service at 1-800-926-7926 x10 (or 404-881-1141 x10). Strafford accepts American Express, Visa, MasterCard, Discover.
- **Listen on-line** via your computer speakers.
- **Respond to five prompts during the program plus a single verification code**. You will have to write down only the final verification code on the attestation form, which will be emailed to registered attendees.
- To earn full credit, you must remain connected for the entire program.

WHO TO CONTACT DURING THE LIVE PROGRAM

For Additional Registrations:
-Call Strafford Customer Service 1-800-926-7926 x10 (or 404-881-1141 x10)

For Assistance During the Live Program:
-On the web, use the chat box at the bottom left of the screen

If you get disconnected during the program, you can simply log in using your original instructions and PIN.

Tips for Optimal Quality

FOR LIVE PROGRAM ONLY

Sound Quality

When listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, please e-mail sound@straffordpub.com immediately so we can address the problem.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Program Materials

FOR LIVE PROGRAM ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides and the Official Record of Attendance for today's program.
- Double-click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

Mastering SOC-1 Attestation Reports Under SSAE 16

Aug. 9, 2016

Mitchell Evans, Director, Risk Consulting
Barr Assurance & Advisory, Salt Lake City
mevans@barradvisory.com

Brad Thies, Principal, Risk Consulting
Barr Assurance & Advisory, Kansas City, Kan.
bthies@barradvisory.com

Greg Ameden, CISA, Director of IT Assurance Services
Hancock Askew & Co., Norcross, Ga.
gameden@hancockaskew.com

Notice

ANY TAX ADVICE IN THIS COMMUNICATION IS NOT INTENDED OR WRITTEN BY THE SPEAKERS' FIRMS TO BE USED, AND CANNOT BE USED, BY A CLIENT OR ANY OTHER PERSON OR ENTITY FOR THE PURPOSE OF (i) AVOIDING PENALTIES THAT MAY BE IMPOSED ON ANY TAXPAYER OR (ii) PROMOTING, MARKETING OR RECOMMENDING TO ANOTHER PARTY ANY MATTERS ADDRESSED HEREIN.

You (and your employees, representatives, or agents) may disclose to any and all persons, without limitation, the tax treatment or tax structure, or both, of any transaction described in the associated materials we provide to you, including, but not limited to, any tax opinions, memoranda, or other tax analyses contained in those materials.

The information contained herein is of a general nature and based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your tax adviser.

Presenters

Greg Ameden, CISA

Greg is the Director of IT Assurance Services for Hancock Askew and leads the firm's IT-related internal audit, risk advisory, and Service Organization Controls (SOC) reporting services. He has over 14 years of experience working in various information technology environments, starting in the IT field and then most recently 10 years at public accounting and advisory firms. Advising and assisting many organizations from a range of industries has enabled Greg to develop a deep understanding of business processes, operational control, and risk management principles.

Brad Thies, CISA, CPA

Brad is principal at Barr Assurance & Advisory Inc., a risk consulting firm that simplifies compliance in an ubiquitously connected world. He specializes in helping clients assess, design, and implement processes and controls to address evolving risks in business. Brad is a certified public accountant and a certified information system auditor with more than 10 years of experience in the industry.

Mitch Evans, CISA

Mitch is director at Barr Assurance & Advisory, Inc and previously worked in KPMG's advisory practice. He has performed numerous IT attestation engagements including Sarbanes Oxley (SOX) and Service Organization Controls (SOC1, SOC2, and SOC3) examinations for both small and large organizations. He specializes in engagements within the Technology, Healthcare, Finance, Banking, and Retail industries. He is also a Certified Information System Auditor (CISA).

Mastering SOC 1 Attestation Reports: Training Outline

- Uses and framework
- IT Considerations
- Testing and Sampling Guidance
- SOC 1 Reporting Special Considerations
- Additional Reporting Options and Use Cases

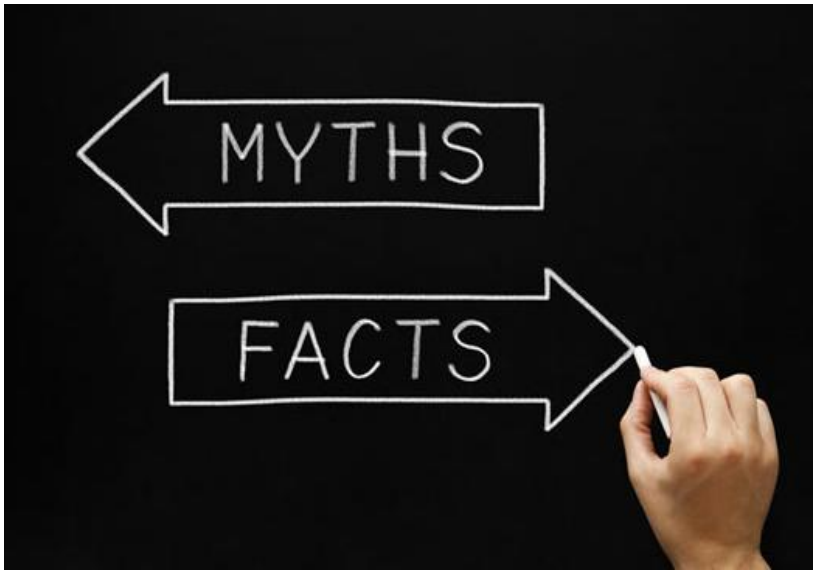
Uses and framework: Key Authoritative Guidance

- SAP 49—Reports on Internal Control (1971)
- SAS 30—Reporting on Internal Accounting Control (1980) (superseded by SSAE 2 (1993))
- SAS 44—Special-Purpose Reports on Internal Accounting Control at Service Organizations (1982)
- SAS 53—Special Reports—Applying Agreed-Upon Procedures to Specified
- Elements, Accounts, or Items of a Financial Statement (1981)
- SAS 70—Service Organizations (1992) SSAE 1—Attestation Standards (1986)
- SSAE 2—Reporting on an Entity's Internal Control Over Financial Reporting
- (1993)
- SSAE 4—Agreed-Upon Procedures Engagements (1995) (removed from the auditing standards by SAS 93 (2000))
- Attestation Standards: Revision and Recodification (2001)
- SSAE SSAE 10—16—Reporting on Controls at a Service Organization (2010) Guide—Reporting on Controls at a Service Organization Related to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC2 (SM)) (2011)

Source: AICPA Understanding the Clarified Attestation Standards (New SSAE No. 18)

Uses and framework: Why is SSAE 16 often misused?

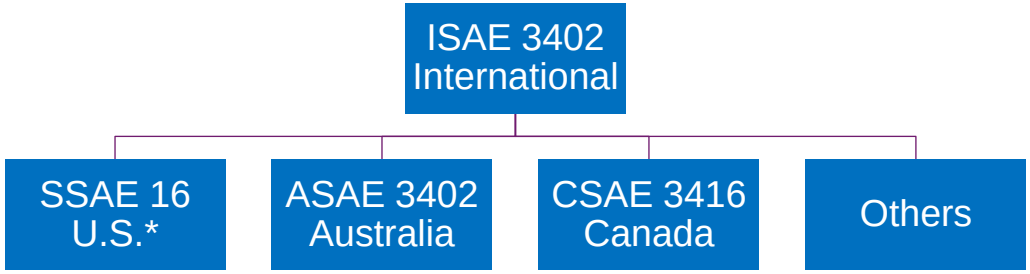
Vendor SSAE 16 Compliant?



Uses and framework: SSAE 16 vs. International Standards

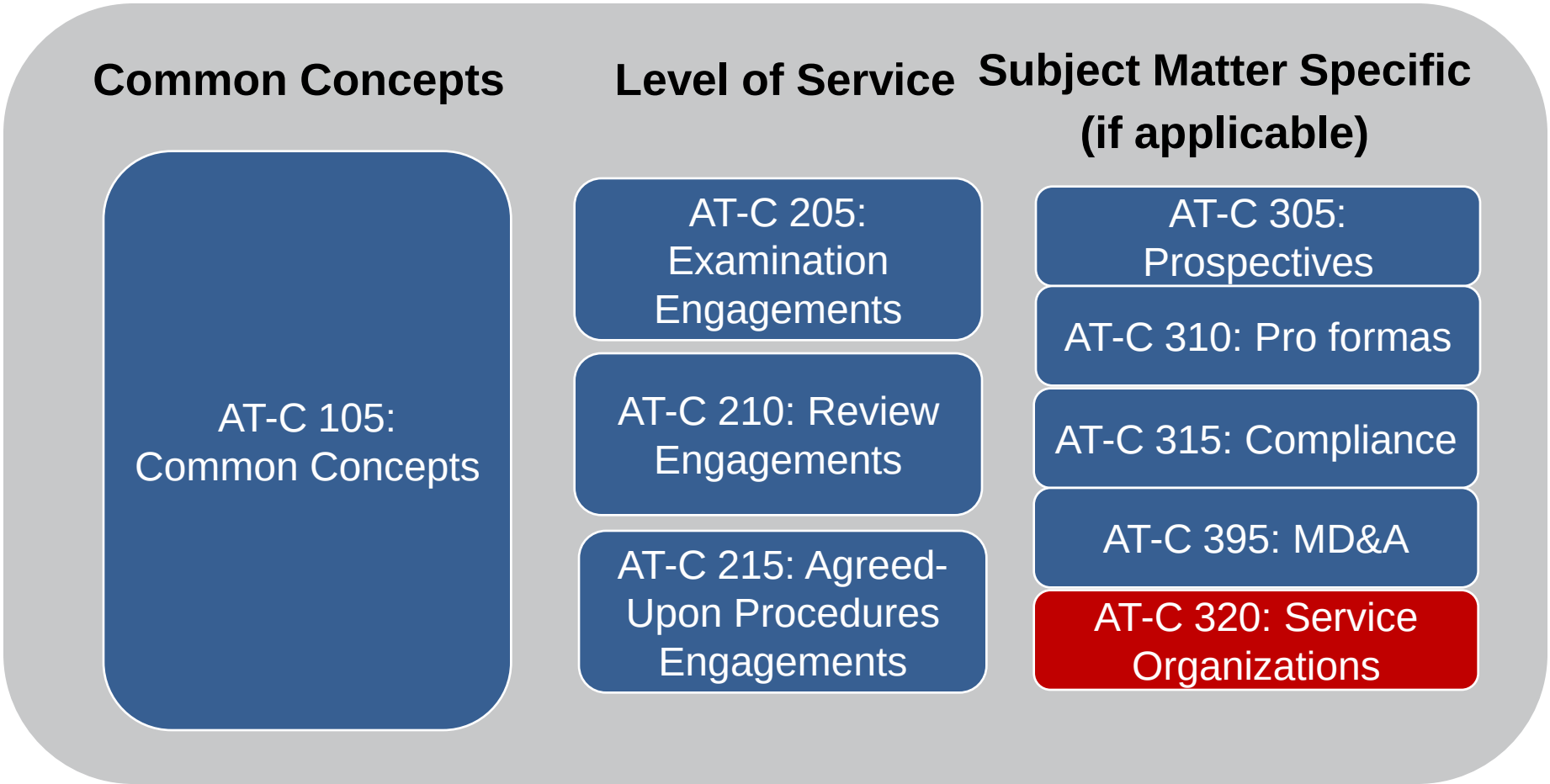
Historically…

Now…



***Note: SSAE 18 to take effect May 1, 2017**

Uses and framework: How Standards are Used (SSAE 18 change)



Source: AICPA's Understanding the Clarified Attestation Standards (New SSAE No. 18)

Uses and framework: SSAE 18 Update and SOC 1 Application

ATs	AT-Cs
• Sampling guidance now only in 205 • Internal audit guidance now only in 205, reduced from guidance provided in AT801 • Most written representation guidance in 205 but some in 320 • Other accompanying information guidance in 205 • Report dating guidance in 205	• Title of the report changed • Complementary subservice organization controls • Inclusive method, all applicable 104, 205 and 320 • Consideration of internal audit function • Changes to the wording of criteria requirements • Description includes monitoring of subservice organizations • Change in definition of CUEC • Read applicable internal audit reports • Evaluating the reliability of IPE • Change to report contents

Source: AICPA's Understanding the Clarified Attestation Standards (New SSAE No. 18)

Uses and framework: SOC reporting overview

Scope	Report	Summary	Applicability	Timing
Internal control over financial reporting (ICOFR)	SOC 1	▪ Detailed report for users and their auditors ▪ Sometimes also referred to as an SSAE 16, AT 801 or ISAE 3402 report	• Detailed report for users, their auditors, and specified parties	Period of time report (Type II) Point in time report (Type I)

Operational controls	SOC 2	▪ Detailed report for user organizations, their auditors, and specified parties	• Focused on:
			  • Security
			  • Availability
			  • Confidentiality
			  • Processing Integrity
			  • Privacy.
			• Applicable to a broad variety of systems such as managed services, cloud service providers, SaaS, and colocation systems.	

	SOC 3	▪ Short report that can be more generally distributed		

Uses and framework: Type I versus Type II

- There are two variations of SOC reports (type 1 and type 2):
  - A **Type I** – Point in time report over the suitability of the design of controls
  - A **Type II** – Report over a specified period of time over the suitability of the design and operating effectiveness of controls

IT Considerations: System Components

Description of the service organization's system, system includes five key components	Infrastructure	The physical and hardware components of a system.
	Software	The programs and operating software of a system.
	People	The personnel involved in the operation and use of a system.
	Procedures	The programmed and manual procedures involved in the operation of a system.
	Data	The information used and supported by a system.

IT General Controls need to consider control objectives for the following

- Information Security
  - Logical access
  - Physical access

Listed in table 4-3 IT General Control Objectives and Risks That Threaten the Achievement of the Control Objectives of the AICPA SOC 1 guide.

IT General Controls need to consider control objectives for the following

- Change Management
  - Application
  - Infrastructure

Listed in table 4-3 IT General Control Objectives and Risks That Threaten the Achievement of the Control Objectives of the AICPA SOC 1 guide

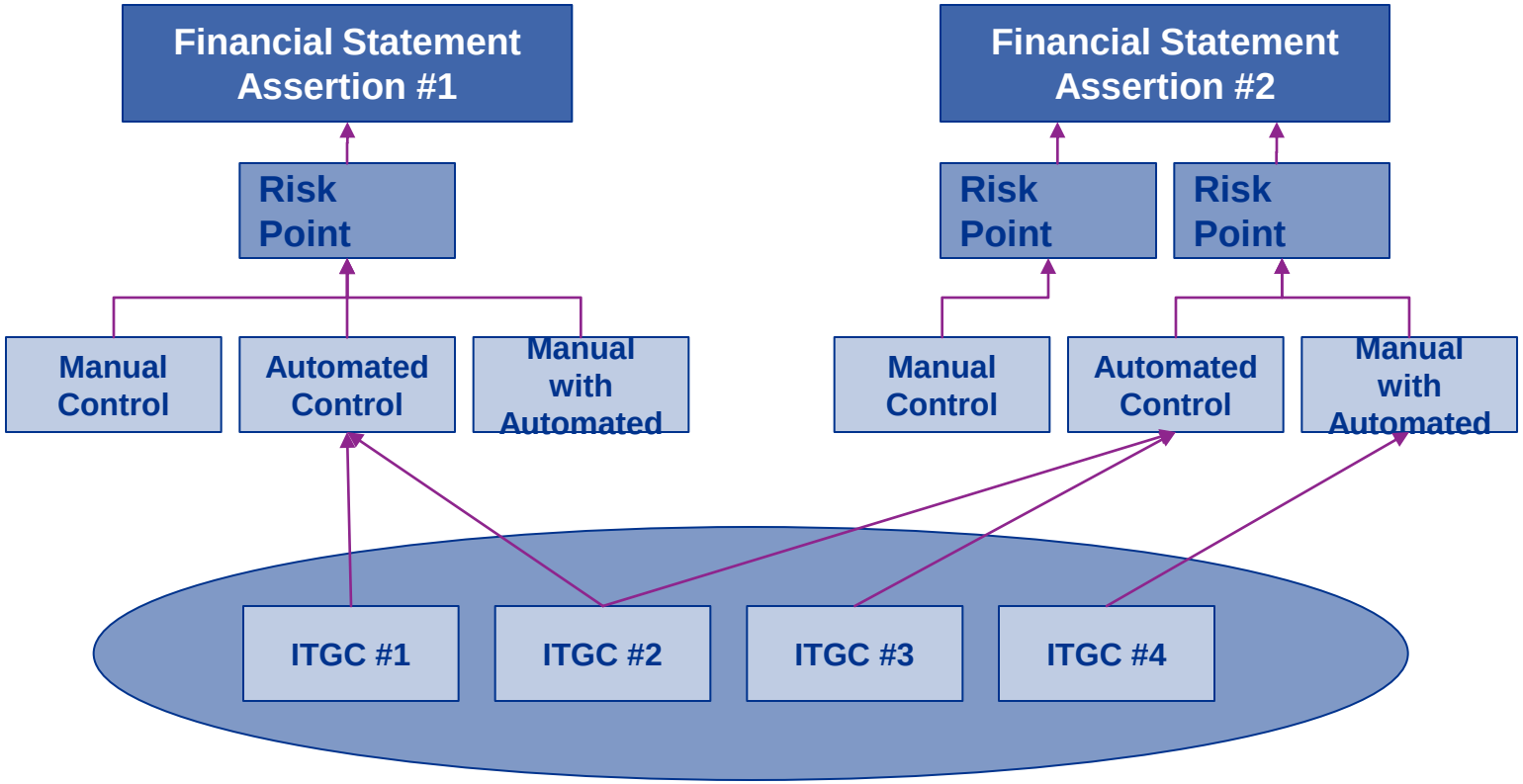
IT General Controls need to consider control objectives for the following

- Computer Operations
  - Application and system processing
  - Data transmissions
  - Data backup

Listed in table 4-3 IT General Control Objectives and Risks That Threaten the Achievement of the Control Objectives of the AICPA SOC 1 guide

IT Considerations: Linkage to Business Process Controls

IT General Controls – Linkage to Business Process Controls



Testing and sampling guidance: Sampling

Sampling

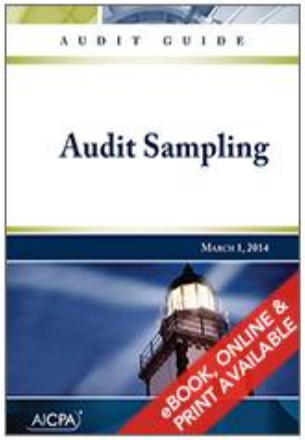
The AICPA SOC Guide

- For tests of controls using sampling, the service auditor determines the tolerable rate of deviation and uses that rate to determine the number of items to be selected for a particular sample.

- The service auditor's selection of sample items should result in a sample that is representative of the population. All items in the population should have an opportunity to be selected. Random-based selection of items represents one means of obtaining such samples.

AICPA Audit and Accounting Guides Audit Sampling – Clarified (Updated as of March 1, 2014)

- Includes tables for sample size based on tolerable deviation rate



Testing and sampling guidance: Nature of Testing

Nature of Tests of Controls

Perform procedures in combination with **inquiry** to obtain evidence about:

- How the control was applied
- The consistency with which the control was applied
- By whom or by what means the control was applied

Procedures the service auditor should perform in combination with inquiry to obtain evidence about the operating effectiveness of controls include

- **Observation** of the application of the control
- **Inspection** of documents, reports, or electronic files that contain evidence of the performance of the control
- **Reperformance** of the control

Testing and sampling guidance: Timing and Extent

Type 1 or Type 2 Testing

Type 1 point in time does not require sampling when performing the test of the controls.

Type 2 test of controls, tests the effectiveness of controls for a period of time typically at least six months

- Identify the occurrence of the controls during the period and test a sample of the occurrences
- What six months should the report include?
  - The period that the report covers should cover six months of the user entity's fiscal year.
  - For the remaining six month period the service organization often will provide a **bridge letter or gap letter**
    - Communicates if were any changes in their controls

Special Considerations: AICPA Peer Reviews Common Issues

Service Organization Control (SOC) Reports

•Failure to obtain the experience and training required under SSAE 16 to properly complete a Service Organization Control Report

•Failure to include required elements in the report such as:

- Management assertions o Complementary user entity controls
- Carve outs
- Inclusion of all controls in control activity section

•Failure to have sufficient working paper support for information included in the report, such as lack of or poor documentation of:

- Procedures to assess the nature, timing, and extent of the procedures (specifically sampling methodology)
- Procedures to test carve outs
- Procedures to support the Other Information included in the report

Examples of Matters in Peer Reviews Engagements with Year-Ends between 12/31/14 and 3/31/16 - AICPA Peer Review July 2016

Special Considerations: AICPA Peer Reviews Common Issues

- **Failure to sufficient test controls, including:**
  - Failure to address the elements of the control, all IT general controls and change management controls
  - Failure to document which controls at the service organization were necessary to achieve the control objectives stated in management's description of the service organization's system and assess whether those controls were suitably designed to achieve the control objectives

- **Failure to document how sample sizes were selected**
- **Failure to coordinate the use of inquiry with other procedures**

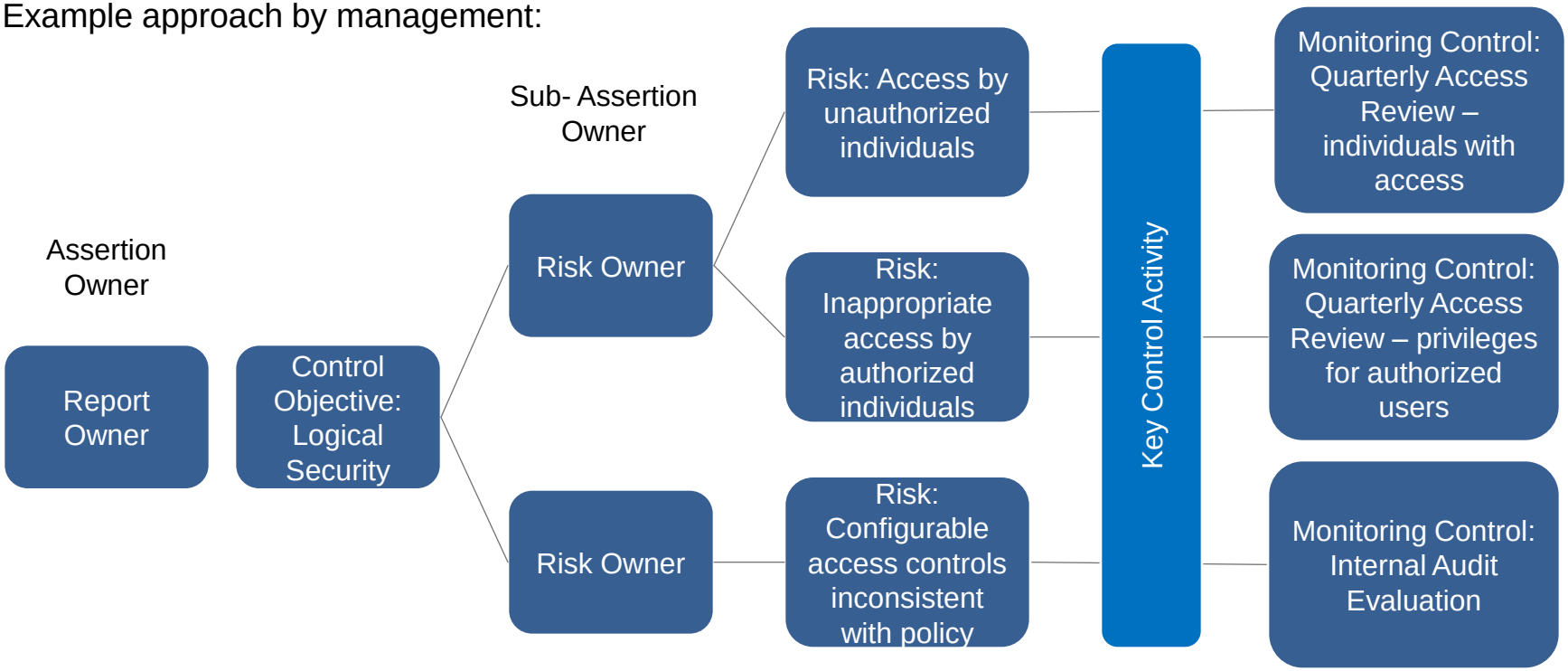
Examples of Matters in Peer Reviews Engagements with Year-Ends between 12/31/14 and 3/31/16 - AICPA Peer Review July 2016

Special Considerations: Use and Evaluation of Internal Audit

- Direct Assistance:
  - Competence and objectivity of the internal auditors
  - Clear responsibilities, objectives, and timing of procedures
  - Communication of all issues and AICPA standards
  - Supervise, review, and evaluate
- Reliance/Re-performance:
  - Risk based
  - Competence and objectivity
  - Internal audit supervision, review, and documentation expectations
  - Sufficient evidence
  - Ability to conclude from internal audit reporting

Special Considerations: Management's Assertion

Example approach by management:



Special Considerations: Subservice organization reporting

When the service organization use a service provider they need to be identified in the SOC report

There are two options:

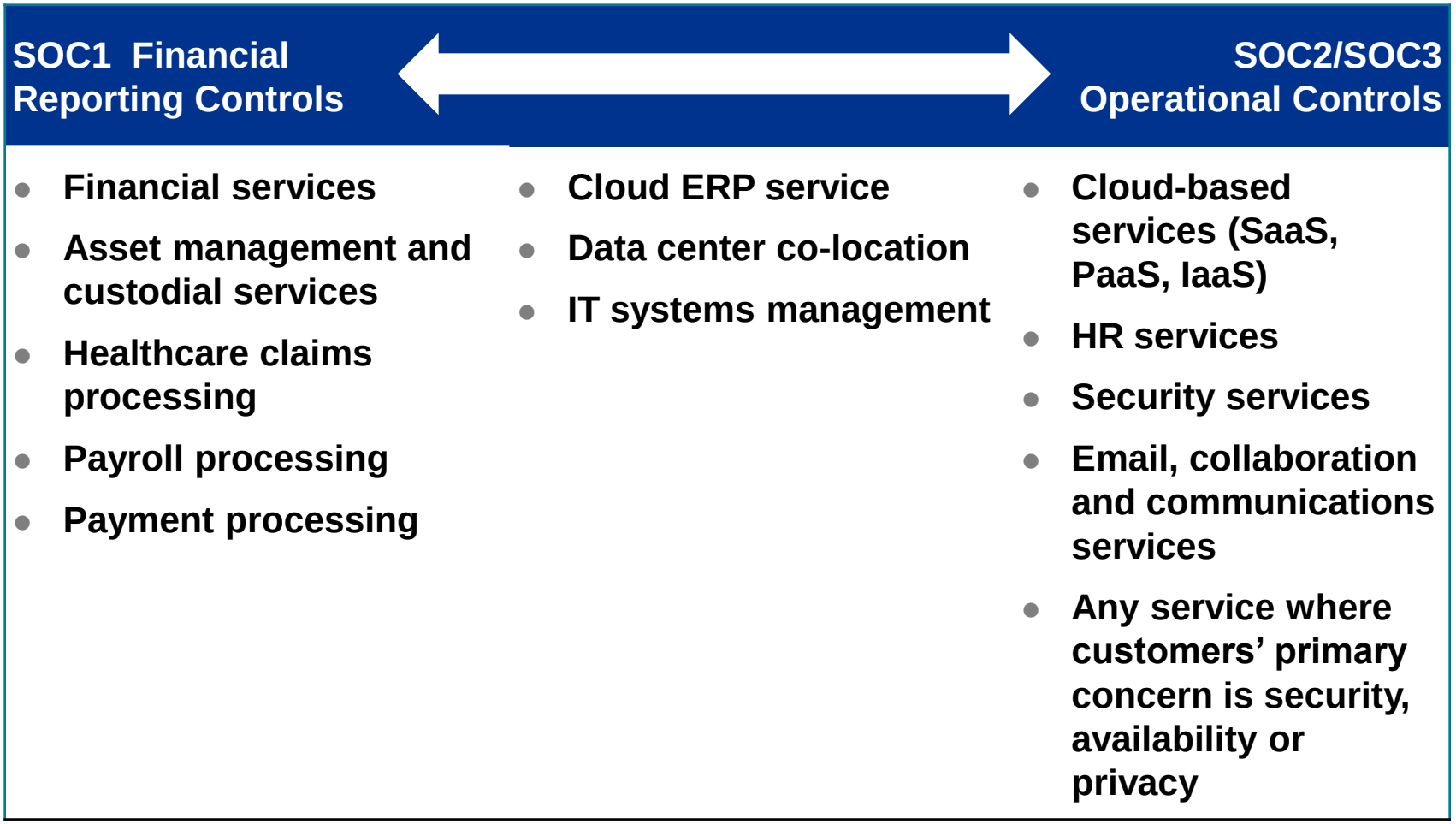
1.Carve-out Method (most common)

- The description of the service organization's system identifies the nature of the services performed by the subservice organization but excludes from the description and from the scope of the engagement the subservice organization's relevant control objectives and related controls.
- Often the subservice organization will have a separate SOC report.

2.Inclusive Method

- The description of the service organization's system includes a description of the nature of the services provided by the subservice organization as well as the subservice organization's relevant control objectives and related controls.
- This results in a separate assertion and testing of the subservice organization

Additional Reporting Options: Case Study



Source: KPMG Overview of SOC Reporting

SOC Report Knowledge Check

- Client has the need to make the report generally available (unrestricted distribution).
- Report is used by the service organization's customers and their auditors to plan and perform an audit or integrated audit or customer's statements SOC 1 Report audit of your customer's financial statements.
- Report is used by the service organization to report on compliance with regulations.
- Broker-dealer firm that buys and sells securities on its own on behalf of its customers

Questions?