

**SAS70 No More:
SSAE 16 Brings
Convergence and Change**

By

Rick J. Scarfino, CPA, CITP, CISA

&

Josh A Ayers, CPA, CITP, CISA

AUGUST 2010

The American Institute of Certified Public Accountants (AICPA) Auditing Standards Board (ASB) recently released **Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization (SSAE 16)**. SSAE 16 will supersede the requirements and guidance for service auditors that was previously included in Statement on Auditing Standards No. 70, *Service Organizations (SAS 70)*.

SSAE 16 brings U.S. auditing and attestation standards more in line with international auditing and attestation standards but retains much of the guidance that was already included in SAS 70. There will be a few practical changes to service auditor procedures, but there are some important changes service organizations should know when SSAE 16 becomes effective. Below are a series of frequently asked questions and answers that will help service organizations implement the relevant changes necessary to transition to SSAE 16.

1. If we have a SAS 70 Type I or II Report, when will we have to transition to the new standard and what happens if we do not?

Answer: The new standard must be applied to all reports that cover periods ending on or after June 15, 2011 with early adoption permitted. If a service organization does not transition to the new standard, its clients and its clients' auditors will be unable to rely on the report. This could result in the service organization incurring unnecessary costs related to the time and resources needed to accommodate additional on-site audits and requests for information by its clients or its clients' auditors.

It should be noted that by the time you read this article your first period under SSAE 16 may have already started.

2. Are all of the control objectives and specified controls we have in place for SAS 70 still relevant under SSAE 16?

Answer: Yes. At this point, no significant changes to control objectives and specified controls are considered to be necessary. As a result, the majority of the testing your auditor performed prior to SSAE 16 will be applicable once the new standard is in place.

3. What are the significant changes we will have to consider in preparing for our transition to SSAE 16?

Answer: Three significant changes will need to be considered by service organizations:

- Management's Assertion

The service organization will be required to provide the service auditor with a written assertion about the fairness of the presentation of the description of controls, the suitability of its design and, in a Type II engagement, its operating effectiveness. The assertion must either accompany the service auditor's report or

be included in the service organization's description of controls. Depending on its service auditor, the service organization may be required to have a responsible individual sign the management assertion.

SSAE 16 provides an example management assertion that your service auditor can help you tailor to your service organization.

- Suitability of Criteria

The service organization will be required to use suitable criteria to measure, present and evaluate the management assertion. The new SSAE 16 standard includes the suitable criteria to be used in a Type I or Type II engagement. The service organization should discuss these criteria with its current service auditor.

- Risk Assessment

The service organization will be required to perform a formal or informal risk assessment that identifies the risks that threaten the achievement of the control objectives and specified controls already established and, if applicable, identifies additional control objectives and specified controls needed to meet the users' needs. The risk assessment should include the consideration of changes to the description of controls and how the service organization monitors the effectiveness of its control environment.

4. Will there be changes in my service auditor's procedures under SSAE 16?

Answer: Yes. The service auditor will have to consider additional acceptance and continuance procedures to ensure the service organization has the ability to provide a reasonable basis for its assertion and the service organization has implemented a risk assessment methodology. The service auditor's application of materiality in SSAE 16 engagements will now consider both qualitative (the nature of observed deviations) and quantitative (the tolerable rate compared to the observed rate of deviations) components. The service auditor's use of a service organization's internal audit department will also be required to be disclosed with respect to the reliance on the specific tests performed.

5. My organization outsources certain processes to a sub-service organization. What impact will this relationship have on my report under SSAE 16?

Answer: Under SSAE 16, service organizations will still have to consider whether to include (inclusive method) or exclude (carve-out method) relevant sub-service organization control objectives and related controls in their report. However, choosing the inclusive method will have a greater impact on the service organizations under SSAE 16. When the inclusive

method is used, the requirements of SSAE 16 that apply to the service organization will also apply to the sub-service organization. This means the sub-service organization will also have to provide a written assertion regarding its description of controls relevant to the service organization and provide evidence of its effectiveness. In order to provide the appropriate evidence of its effectiveness the sub-service organization would need to supply its SSAE 16 report or be subject to additional procedures performed by the service auditor. As a result, service organizations will have to consider whether they will be able to coordinate and obtain the necessary information to use the inclusive method.

6. What changes can I expect to see in the service auditors' opinion letter?

Answer: Many of the changes to the service auditors' opinion letter will relate to the topics covered above. For example, there will be references to management's assertion, there will be an indication as to whether the carve-out or inclusive method is being used with respect to sub-service organizations, there will be specific reference to the complementary user control considerations, and, in Type II engagements, the opinion will now express whether the internal controls were properly designed and implemented for the entire period, not just as of the period end date as previously reported.

7. Are there any plans to publish additional guidance with respect to SSAE 16?

Answer: Yes. Keep in mind that the AICPA will issue an audit guide that provides additional guidance and clarity sometime in late 2010 and possibly early 2011. As a result, both service auditors and service organizations will still have some questions regarding the implementation and impact of the changes until this guidance is released to the public.

8. I am a service organization that feels SAS 70 is not relevant to my organization because the services I provide do not affect a user's financial statements, yet my clients continue to request one. Is there any relevant guidance for service organizations like data centers, software as a service providers, or electronic claims clearinghouses?

Answer: As mentioned above, the AICPA is scheduled to release audit guidance in late 2010 and possibly early 2011, which will address this concern as well. The expectation is they will allow service auditors to provide three different types of Systems of Controls (SOC) reports. SSAE 16 reports will be considered SOC 1 reports and AICPA Trust Services (WebTrust and SysTrust) reports will be issued as SOC 3 reports. SOC 2 reports will be available to service organizations that do not process transactions that affect their client's financial statements but are concerned with the security, availability, and/or confidentiality of their client's data (e.g. data centers).

9. Will the new standard provide us with any additional advantages?

Answer: Yes. The new standard converges U.S. and International auditing and attestation standards. Depending on the needs of the users and/or their auditors, those service organizations that have been required to provide a separate report under the International Standards on Attestation Engagements (ISAE) 3402 in addition to their SAS 70, may now be able to meet their reporting obligations with a single SSAE 16 report.

10. The new SSAE 16 standard mentions early adoption as an option for service organizations. Are there benefits to early adopting?

Answer: Those that choose to early adopt will have more time to assess and evaluate whether the service organization has implemented the processes necessary to comply with SSAE 16. There are certainly challenges to be faced in organizations transitioning from SAS 70 to SSAE 16 however, service organizations that choose to early adopt could be perceived as market leaders and their users may consider their control environment to be stronger than their competitors.

You may be thinking about the most important question, what do I do now? The answer is to take charge of the transition process. Ask your service auditor to educate you on the new standard and help you start planning your course of action. Start discussing whether early adoption is appropriate, who in the organization is responsible for the management assertion, and if there are any additional compliance and risk assessment processes that need to be implemented to comply with the new standard. Developing a communication plan for sub-service organizations, clients, and users will allow key individuals within those organizations to know what to expect when your SSAE 16 report is issued. Gaining an early understanding of SSAE 16 and taking charge of the transition process will help your organization avoid the stress and disruption of costly mistakes and missed opportunities associated with delaying the transition to the new compliance requirements.

Rick Scarfino, CPA, CITP, CISA is a Senior Manager with Stone Carlie & Company, LLC. Rick can be reach at rscarfino@stonecarlie.com. Josh Ayers, CPA, CITP, CISA is a Manger with Stone Carlie & Company, LLC. Josh can be reached at jayers@stonecarlie.com. Stone Carlie & Company, LLC (www.stonecarlie.com) is a full service accounting firm that specializes in SAS70 engagements for TPAs and other entities within the insurance industry.



This article was published in the September 2010 edition of The Self-Insurer. For more information, contact Josh Ayers of Stone Carlie at (314) 889-1173 or email him at jayers@stonecarlie.com.

Joshua A Ayers, CPA, CITP, CISA

Manager Assurance Services



Responsibilities

Josh is a manager at Stone Carlie and helps oversee all activities and services performed at or on behalf of a client organization in the Firm's Assurance Services Department.

- Manage audit, internal audit, SAS 70, SysTrust and WebTrust services
- Plan, perform & review fieldwork, and provide technical support for audit, internal audit, SAS 70, SysTrust and WebTrust services
- Monitor services on an ongoing basis
- Provide technical support to clients on an ongoing basis
- Meet with client executives on a periodic basis

Qualifications

- Certified Public Accountant – Missouri
- Certified Information Technology Professional
- Certified Information Systems Auditor
- Member of Stone Carlie System Security and Process Assurance Group
- Possesses four years of professional experience in the assurance services field with commercial and not-for-profit entities, including audits, reviews, compilations, agreed-upon procedures, due diligence, and consulting engagements for industries such as manufacturing, construction, retailers, distribution, logistics, life sciences, financial institutions, application service providers, data storage companies, website hosting, development companies, web browsers, document imaging companies, health care, and large governmental agencies.
- Possesses almost two years of professional experience in financial reporting and compliance with a leading global life reinsurance company, which included identifying, researching, and documenting technical issues that ensured compliance with appropriate United States Generally Accepted Accounting Principles (US GAAP) and Securities and Exchange Commission (SEC) regulations. In addition to providing general US GAAP and SEC compliance support, served as primary accounting liaison to an investment department that managed over \$16 billion in invested assets that included traditional fixed maturity securities, mortgage loans, derivatives and other emerging investment vehicles. Accomplishments included the research, development and implementation of the Company's first hedge accounting policies as it related to a \$300 million net investment in a foreign operation and a fair value hedging strategy to convert \$50 million in fixed rate investments to floating rate investments.

Education and Selected Memberships

- Saint Louis University – St. Louis, MO B.S. – Business Administration with an emphasis in Accounting
- Member, American Institute of Certified Public Accountants (AICPA)
- Member, Missouri Society of Certified Public Accountants (MSCPA)
- Member, Information Systems Audit and Control Association (ISACA)
- Extensive continuing professional education

Richard J. Scarfino, CPA, CITP, CISA

*Senior Manager
Assurance Services*



Responsibilities

Richard will serve as the Audit Engagement In-Charge, coordinating audit services and staff support during fieldwork. He will plan, supervise and perform fieldwork as well as provide technical support on industry specific, accounting and tax related issues.

- Manage audit, internal audit, SAS 70, SysTrust and WebTrust services
- Plan, perform & review fieldwork, and provide technical support for audit, internal audit, SAS 70, SysTrust and WebTrust services
- Monitor services on an ongoing basis
- Provide technical support to clients on an ongoing basis
- Meet with client executives on a periodic basis

Qualifications

- Certified Public Accountant – Missouri
- Certified Information Technology Professional
- Certified Information Systems Auditor
- Member of the Stone Carlie System Security and Process Assurance Group
- Member of the Stone Carlie Manufacturing and Distribution Group
- Member of the Stone Carlie Not-for-Profit Services Group
- Possess nine years of audit and internal audit experience in a variety of industries including professional service, retail, distribution, manufacturing and not-for-profit
- Possess five years of experience providing SAS 70, SysTrust and WebTrust services

Education and Selected Memberships

- Saint Louis University, Business Administration – Accounting, Finance and Management Information Systems
- Member, American Institute of Certified Public Accountants
- Member, Missouri Society of Certified Public Accountants
- Member, Information Systems Audit and Control Association
- Extensive continuing professional education