CSA Position Paper on AICPA Service Organization Control Reports℠

February 2013

cloud security alliance℠

AICPA American Institute of CPAs®

Contents

Acknowledgments

Lead Author

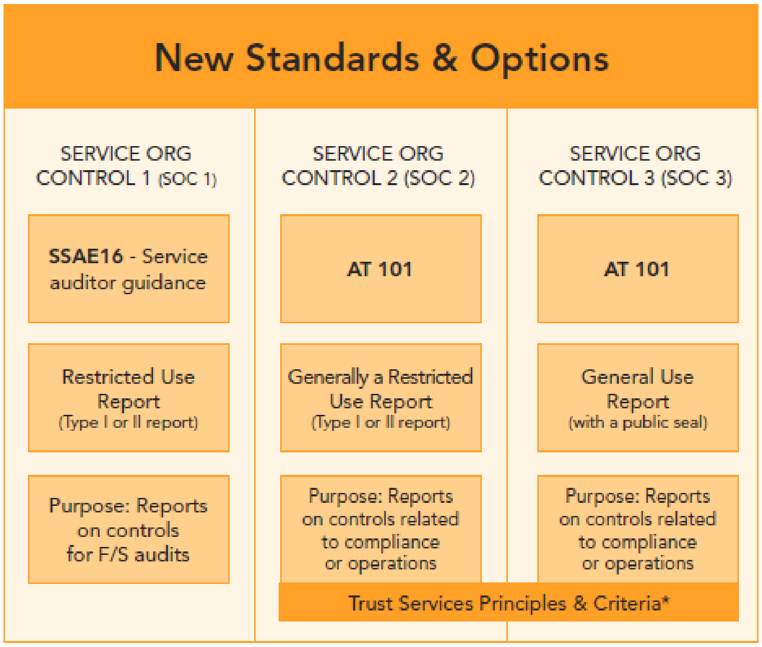
David Barton, Principal, UHY LLP

Contributors

Phil Agcaoili, CISO, Cox Communications
Daniele Catteddu, Managing Director EMEA, Cloud Security Alliance
Chris Halterman, Executive Director, Ernst & Young LLP
John Howie, Chief Operating Officer, Cloud Security Alliance
Audrey Katcher, Partner, RubinBrown, LLP
Jim Reavis, Executive Director, Cloud Security Alliance
Daniel Schroeder, Partner, Habif, Arogeti, & Wynne, LLP

1.0 Introduction

In June 2011, the American Institute of Certified Public Accountants (AICPA) issued SSAE 16, which replaced SAS 70, an auditing standard used by CPAs reporting on controls at a service organization, including information technology controls. At that time, the AICPA introduced three Service Organization Control (SOC) reporting options: SOC 1^{SM}, SOC 2^{SM} and SOC 3^{SM} reports.



New Standards & Options

SERVICE ORG CONTROL 1 (SOC 1)	SERVICE ORG CONTROL 2 (SOC 2)	SERVICE ORG CONTROL 3 (SOC 3)
SSAE16 - Service auditor guidance	**AT 101**	**AT 101**
Restricted Use Report (Type I or II report)	Generally a Restricted Use Report (Type I or II report)	General Use Report (with a public seal)
Purpose: Reports on controls for F/S audits	Purpose: Reports on controls related to compliance or operations	Purpose: Reports on controls related to compliance or operations
	Trust Services Principles & Criteria*	

Figure 1 - Overview of the Reporting Options

For additional information: See the link below in "Additional Resources"

The new AICPA reporting framework was created to eliminate confusion that management of a service organization (including management of cloud providers) might have regarding the type of engagement a CPA could perform to provide their customers with assurance on the service organization's controls. Part of this confusion stems from the lack of knowledge of customers, potential customers, and service organizations regarding the purpose of each type of SOC report and its intended use.

The Cloud Security Alliance (CSA) has drafted this position paper as a means of educating its members and providing guidance on selecting the most appropriate reporting option.

2.0 The Cloud Security Alliance Position

After careful consideration of alternatives, the Cloud Security Alliance has determined that for most cloud providers, a type 2 SOC 2 attestation examination conducted in accordance with AT section 101 of the AICPA attestation standards is likely to meet the assurance and reporting needs of the majority of users of cloud services, when the criteria for the engagement are supplemented by the criteria in the CSA Cloud Controls Matrix (CCM). AT 101 provides the following key strengths for the cloud industry's consideration:

- AT 101 is a mature attest standard (it serves as the standard for SOC 2 and SOC 3 reporting)
- Allows for immediate adoption of the CCM as additional criteria and the flexibility to update the criteria as technology and market requirements change
- Provides for robust reporting on the service provider's description of its system, and on the service provider's controls, including a description of the service auditor's tests of controls in a format very

similar to the now obsolete SAS 70 reporting format, and current SSAE 16 (SOC 1) reporting, thereby facilitating market acceptance

3.0 Further Background

Although many cloud providers currently issue SOC 1 (SSAE 16) reports, which are intended for reporting on controls over financial reporting, the services being provided do not typically have a direct effect on, or relevance to, internal control over financial reporting (ICFR). If the controls being examined are not directly relevant to ICFR, then SOC 2 is a more suitable reporting standard. SOC 2 reports cover controls relevant to the security, availability, or processing integrity of a system or the confidentiality or privacy of the information processed by the system. The standard for performing and reporting on such engagements is provided in AT section 101 and the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2).*

Controls at private cloud and SaaS providers *may* affect their customers' internal control over financial reporting, especially when the service (or software) involves initiating, authorizing, recording, processing, or reporting financial transactions that are included in the user entities' financial statements. Each cloud provider should determine if its services affect the items above and should determine whether a SOC 1 (SSAE 16) report is appropriate for its circumstances. In some cases, the cloud provider may need to obtain ***both*** a SOC 1 (SSAE 16) report (for those controls that affect ICFR) and a SOC 2 (AT 101) report to adequately address all of the controls that are important to their customers.

This conclusion is supported by the AICPA Technical Practice Aid titled "*TIS Section 9530: Service Organization Controls Reports*," published in November 2011. Paragraph .19 of this publication states:

> ### Issuing Separate Reports When Performing Both a SOC 1 and SOC 2 Engagement for a Service Organization
>
> *Inquiry*—Going forward, will service organizations that include control objectives relevant to user entities ICFR along with control objectives that are not relevant to user entities' ICFR in their descriptions need to request two separate reports—SOC 1℠ and SOC 2℠?
>
> *Reply*—Yes. Service organizations will now need to request two separate SOC reports if the service organization would like to address control objectives relevant to user entities' ICFR and control objectives (criteria) that are not relevant to user entities' ICFR. See paragraph 1.23 of the SOC 2℠ guide.

SOC 2 engagement is appropriate for reporting on controls relevant to the security, availability, or processing integrity of a system or the confidentiality, or privacy of the information processed by the system. When deciding which reporting approach is best for your environment, it is important to remember that non-financial reporting controls, such as controls relevant to security, availability, processing integrity, confidentiality, and privacy, are intended to be covered in a SOC 2 report, not a SOC 1 report.

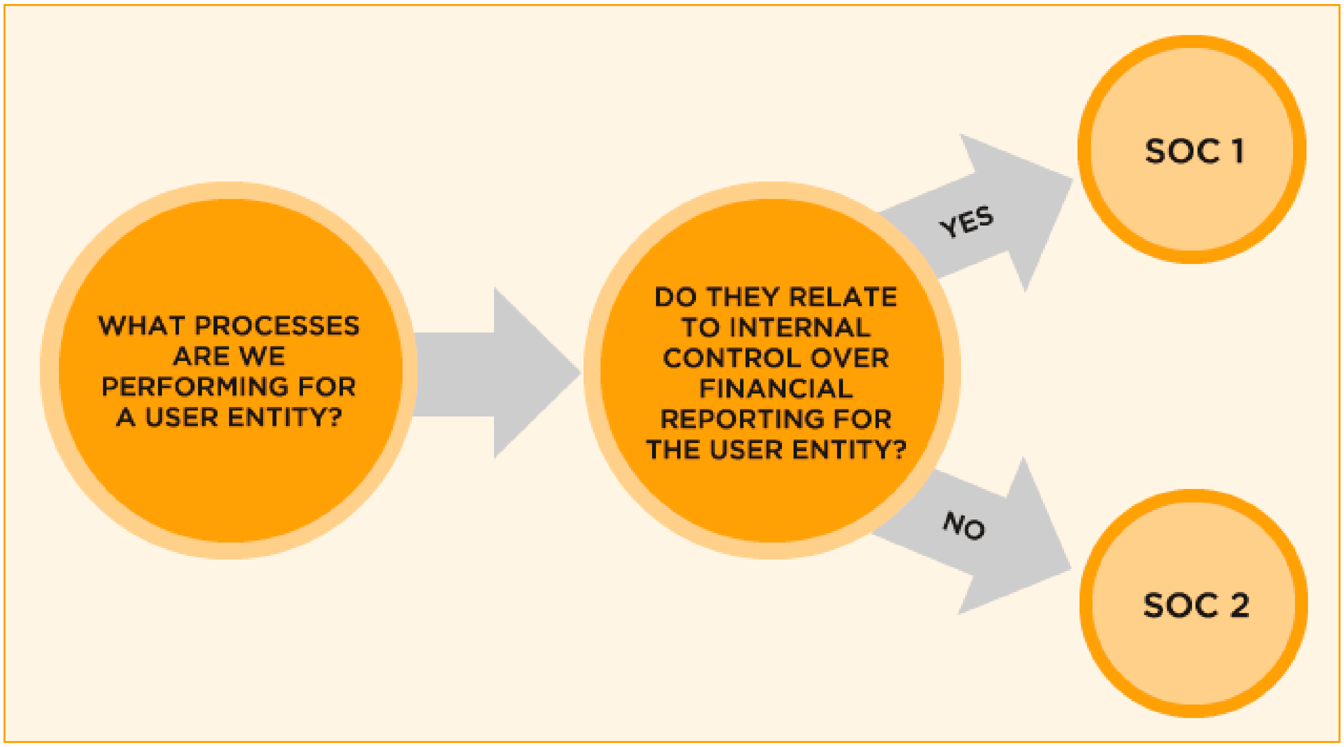

WHAT PROCESSES ARE WE PERFORMING FOR A USER ENTITY?
DO THEY RELATE TO INTERNAL CONTROL OVER FINANCIAL REPORTING FOR THE USER ENTITY?
YES
SOC 1
NO
SOC 2

Figure 2 - Selecting SOC 1 or SOC 2

The AICPA Technical Practice Aid, "*TIS Section 9520: SSAE No. 16, Reporting on Controls at a Service Organization*," provides clarification:

> ## Reporting on Controls at a Service Organization Relevant to Subject Matter Other Than User Entities' ICFR
>
> *Inquiry*—May AT section 801 be used for reporting on a service organization's controls relevant to subject matter other than user entities' ICFR?
>
> *Reply*—No. AT section 801 does not apply to examinations of controls over subject matter other than user entities' ICFR. The increasing use of cloud computing companies (that provide user entities with on-demand network access to a shared pool of computing resources, such as networks, servers, storage, applications, and services) has created an increasing demand for CPAs to report on a cloud computing service organization's controls relevant to subject matter other than user entities' ICFR.

4.0 Conclusion

By providing this position paper, the Cloud Security Alliance hopes to provide relevant and timely guidance to its members. The Cloud Security Alliance supports the use of SOC 2 engagements and the ability to use the Cloud Controls Matrix as additional suitable criteria in order to produce an attestation report that will provide the most pertinent and comprehensive evaluation of controls for customers and users of cloud computing services.

5.0 Additional Resources

SOC Whitepaper:

http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/TrustServices/DownloadableDocuments/10957-378%20SOC%20Whitepaper.pdf

TIS Section 9520:

http://www.aicpa.org/InterestAreas/FRC/DownloadableDocuments/TIS_Sections/TIS_Section_9520.pdf

TIS Section 9530:

http://www.aicpa.org/InterestAreas/FRC/DownloadableDocuments/TIS_Sections/TIS_Section_9530.pdf