Deloitte.

Adopting SSAE 18 for SOC 1 reports

Overview

Since its adoption in 2011, service auditor reports issued in accordance with SSAE 16 have become increasingly common in the marketplace. In April 2016, the Auditing Standards Board issued SSAE No. 18, *Attestation Standards: Clarification and Recodification*, which seeks to clarify the requirements and provide application guidance for performing and reporting on examinations, reviews, and agreed-upon procedure engagements (attestation engagements). This document focuses on the impact of SSAE 18 on SOC 1 examinations and the re-codified attestation standards, specifically AT-C Section 105 and AT-C Section 205, which are common concepts across all attestation and examination engagements and AT-C Section 320, *Reporting on an examination of controls at a service organization Relevant to User Entities' Internal Control over Financial Reporting.* The updated attestation standards emphasize the requirement for service organizations to understand, consider, and demonstrate oversight of service providers they use that are relevant to a user entity's financial reporting (subservice organizations). It highlights the importance for a service auditor to evaluate whether information provided by the service organization is "sufficiently reliable" for the service auditor's purposes; the requirement for service auditors to evaluate the relationship between risks of material misstatement and controls; and the requirement to design audit procedures in response to assessed level of risk of material misstatement.

Monitoring the effectiveness of controls at subservice organizations

The updated standards emphasizes that the service organization's description of the system and scope of services should include controls performed by management to monitor the effectiveness of controls at the subservice organizations. Oversight of subservice organizations relevant to the description of the system may be demonstrated through:

- Controls that monitor services provided by the subservice organizations, such as reviewing and reconciling output reports, periodic meetings, site visits, etc.
- Review of SOC 1 reports of the subservice organizations
- Direct testing of controls at the subservice organization
- Monitoring of external communications and customer complaints relevant to the service organization

Impact: The description of the system should reflect the controls performed by management to demonstrate oversight over subservice organizations. Service auditors' test procedures will test the effectiveness of such controls performed by management.

Identifying complementary subservice organization controls

SSAE 18 introduces the concept of Complementary Subservice Organization Controls (CSOCs) which represents controls that management of the service organization expects will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management's Description of the System, when the carve-out method of reporting has been used.

Impact: When using the carve-out method to report on subservice organizations, the service auditor's scope and opinion will reflect that the control objectives specified by the service organization can be achieved only if the CSOCs assumed in the design of controls were suitably designed and operating effectively along with the related controls at the service organization.

Similar considerations will be reflected in the written assertion by management and the management representation letter that the description does not extend to the controls and control objectives of subservice organizations.

Changes are effective for service auditors' reports dated on or after **May 1, 2017.** Early adoption is permitted.

SOC 1 reports will be prepared in accordance with the American Institute of Certified Public Accountants' (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 18, *Attestation Standards: Clarification and Recodification.*

These changes will be applicable to service auditor reports currently issued under SSAE 16 and reports issued under both SSAE 16 and ISAE 3402 standards.

To meet these requirements, we anticipate that the description of the system will include a sub-section for CSOCs to provide transparency over the services provided by the subservice organizations. This will be relevant for users' consideration in evaluating the effectiveness of the control objectives defined in the scope of the report.

Clarification of complementary user entity control considerations

Complementary user entity control considerations (CUECCs) within a SOC 1 report are controls and procedures that a user entity of the report should design, implement, and place in operation. The updated standards clarify that the CUECCs should *only* include those controls and procedures that are relevant to achieve the control objectives within the service organization's report.

Impact: Service organizations should assess the CUECCs in the report to determine if they are relevant to the achievement of the control objectives described in the report. Service organizations could consider including a mapping of the CUECCs to the control objectives as a leading practice.

Evaluating reliability of information produced by the service organization

The revised standard requires that the auditor evaluate whether the information provided by the service organization is "sufficiently reliable" for the service auditor's purposes. This implies that the service auditor will have to obtain evidence about the accuracy and completeness of the information received during the examination and will have to evaluate whether that information is sufficiently precise and detailed.

Examples of information produced by the service organization that could be commonly used by the auditor include population lists, exceptions reports, transaction reconciliations, and user access lists.

Impact: The auditor needs to establish accuracy and completeness and reliability of data through:

- Routine test procedures performed as part of the examination
- Testing of controls over the preparation and maintenance of such data
- Additional targeted procedures as determined by the service auditor

The auditor's test of controls in the report will describe the procedures performed to confirm accuracy and completeness of the data.

Assessing the risk of material misstatement

SSAE 18 defines "risk of material misstatement" as the risk that the subject matter is not in accordance with (or based on) the criteria in all material respects, or that the assertion is not fairly stated in all material respects.

The updated standards place emphasis on the service auditor to consider risks and likely sources of misstatement, including those related to fraud at planning or during the course of the examination. They should also consider the impact of any subsequent events to assess the risk of material misstatement.

Impact: The service auditor will obtain internal audit and regulatory reports and work with management to understand the likelihood of material misstatement. Based on the assessed level of risk of material misstatement, the service auditor will design and perform procedures whose nature, timing, and extent are based on and responsive to the assessed level of risk of material misstatement.

Next steps

Your service auditor will be able to provide insights related to the impact of SSAE 18, and communication with them should be a key part of planning for your next examination.

Re-codified AT-C sections applicable to SOC 1 reporting under SSAE 18

Prior relevant attestation standard section under SSAE 16	Relevant attestation sections under SSAE 18 and after recodification
AT Section 801: Reporting on controls at a service organization	**AT-C Section 105** Concepts common to all attestation engagements
	AT-C Section 205 Examination engagements
	AT-C Section 320: Reporting on an examination of controls at a service organization relevant to user entities' internal control over financial reporting

Contact us:

Laurent Berliner
Partner | Risk Advisory Leader
+352 45145 2328
lberliner@deloitte.lu

Martin Flaunet
Partner | Banking Leader
+352 451 452 334
mflaunet@deloitte.lu

Roland Bastin
Partner | Risk Advisory
+352 451 452 213
rbastin@deloitte.lu

Michael Blaise
Director | Risk Advisory
+352 45145 2562
mblaise@deloitte.lu

Jerome Sosnoswki
Director | Risk Advisory
+352 45145 4353
jsosnowski@deloitte.lu

Laurent de la Vaissiere
Director | Risk Advisory
+352 45145 2010
ldelavaissiere@deloitte.lu

Arnaud Barosi
Director Risk Advisory
+352 45145 2875
abarosi@deloitte.lu

Sophie Binninger
Senior Manager | Risk Advisory
+352 45145 3463
sbinninger@deloitte.lu