Moving to SSAE 18

A clearer view of attestation standards for service organizations

pwc

Introduction

The Auditing Standards Board (ASB) has revised the existing attestation standards "to address concerns over the clarity, length, and complexity" of the standards and released the new Statement on Standards for Attestation Engagements (SSAE) No. 18, *Attestation Standards: Clarification and Recodification*.

Specifically, the ASB's revisions affect the examination standard AT Section 801, *Reporting on Controls at a Service Organization* (AT 801), the standard under which Service Organization Controls (SOC) 1 reports are issued, as depicted in the table below. AT 801 has been superseded by AT-C Section 320 *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AT-C 320) of SSAE 18 and therefore affects SOC 1 reports dated on or after May 1, 2017. Early adoption is permitted.

Revisions to attestation standards

Existing attestation standards	Clarified attestation standards
AT Section 101	AT-C Section 105, *Concepts Common to all Attestation Engagements* AT-C Section 205, *Examination Engagements*
AT Section 801	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*

Who is affected and what the changes might mean to you

Generally, SOC 1 reports are requested by companies that outsource some aspect of their operations to third parties—service organizations—where those operations are likely to be relevant to their internal control over financial reporting. The revised standard will affect the service organizations providing SOC 1 reports to their customers, as well as the service auditors that issue the reports. We would not, however, categorize these revisions as significant.

As service organizations familiarize themselves with the revised standard, it might be helpful to categorize the changes into three buckets:

1. Revisions that may require a service organization to make adjustments to management's description.
2. Revisions that may require service auditors to alter their approach to SOC 1 engagements.
3. General changes that won't necessarily affect management's description or a service auditor's approach but of which the parties should be aware.

1. Changes for service organizations themselves

Revision	What service organizations need to do differently
CSOCs A complementary subservice organization control (CSOC) is a control that management assumes will be implemented by their subservice organization. It is also a control that is necessary to achieve a control objective stated in management's description. CSOCs are part of management's description but the service auditor's procedures do not extend to these controls.	Service organizations should assess the subservice organizations carved out of their SOC 1 reports and document those controls they assumed to be in place at the subservice organization when designing their system. In performing this assessment, they may consider reviewing SOC 1 reports received from their subservice organizations to understand the controls they have detailed within the description of their system. CSOCs are part of management's description; however, we suggest they be disclosed under the respective control matrices in Section IV of the report and that management's description refer to them.
Subservice organization monitoring Previously, the concept of monitoring the effectiveness of controls at subservice organizations applied only to subservice organizations presented using the carve-out method. Under AT-C 320, this monitoring now applies to subservice organizations presented using the inclusive method as well.	Service organizations should assess their monitoring controls for subservice organizations and ensure they cover all subservice organizations, including those presented under the inclusive method. Service organizations' monitoring should continue to be included in management's description of controls and not listed as a control tested by the service auditor within the control matrices in Section IV of the report.
Controls testing Within management's description, the service organizations themselves now identify the controls necessary to achieve the stated objectives. By including a control within management's description, service organizations signal that the control is necessary to achieve the stated control objectives and that their service auditor is required to test it.	Service organizations should review management's description and ensure that all controls that are necessary to achieve the control objectives are included. They should also review management's description and find and remove any non-key controls that are not necessary to achieve the control objectives.

Revision	What service organizations need to do differently
Management's assertion The standard now establishes a minimum set of required criteria—for the fair presentation, suitability of design, and operating effectiveness of controls—to be included in management's assertion. This minimum set of criteria is meant to drive consistency and enable comparison across SOC 1 reports.	This change should eliminate the need for service organizations to tailor the management's assertion, including, for example, the need to make modifications to management's assertion for an information technology general controls (ITGC)–only report. In fact, changes made to the assertion criteria should be either limited or none. These changes may only encompass those instances in which criteria beyond the specified minimum are included.

2. Changes that may alter the service auditor's approach

Revision	What service auditors will do differently
Definition of internal audit The revised definition, which closely mimics the one used in financial statement audits, more narrowly defines the internal audit function and does not include a reference to "others."	Service auditors that use or plan to use the work of groups other than a traditional internal audit function may need to revisit their evaluation of the competence and objectivity of such groups using the revised definition.
Reliability of information The new standard instructs service auditors to evaluate whether information produced by the service organization is sufficiently reliable and precise for the service auditor's purposes.	While some service auditors may have already been performing this evaluation, those that have not must now perform procedures to evaluate whether information produced by the service organization (e.g., population lists, reports used in the execution of controls, and reports provided to user entities) is complete, accurate, and sufficiently precise and detailed.

3. Changes that all parties should be aware of

In addition to the items noted above, there are other changes that may not have a substantial impact on service organizations or service auditors but that all parties should be aware of as they plan and prepare for upcoming SOC 1 engagements:

Revision	Impact to SOC 1 engagements
Definition of misstatement Misstatement is now defined as "*a difference between the measurement or evaluation of the subject matter by the responsible party and the proper measurement or evaluation of the subject matter based on the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions. In certain engagements, a misstatement may be referred to as a deviation, exception, or instance of noncompliance.*"	For SOC 1 engagements, misstatements are issues with fair presentation, design, or operating effectiveness of controls. Issues with fair presentation will be called "misstatements"; issues with design or operating effectiveness of controls will still be referred to as "exceptions." This change is principally a modification in terminology.
Added definition of risk of material misstatement Risk of material misstatement (ROMM) is a new term defined 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.*"	Service organizations have likely already been addressing the ROMM as they develop their management's description. Service auditors have likely been considering ROMM in developing and documenting their procedures to execute a SOC 1 engagement. This term is now formally defined in the standard.
The service auditor's opinion The service auditor's opinion has changed in format and now includes a revised restriction of use paragraph. To make the opinion more clear and concise, several additional items—particularly scope limitations, such as complementary user entity controls, CSOCs, and subservice organizations—now reside in the scope section. The restricted use paragraph of AT 801 identified the intended users of the report as the service organization, user entities of the service organization, and their independent auditors of financial statements. The intended users are now expanded to include those auditors who audit and report on internal controls over financial reporting (ICFR).	The ASB included this condition to recognize those instances in which different auditors may be engaged to audit the financial statements and ICFR.

Conclusion

Overall, while the revisions to the attestation standards are not significant, service organizations and service auditors should familiarize themselves with them and assess the impact to their SOC 1 reports. Service organizations will need to start reviewing their management descriptions and consider the changes noted above that could require them to revise management's description. Service auditors should be engaging in discussions with their service organizations to discuss the impact, if any, that the changes may have as they plan for the SOC 1 engagements.

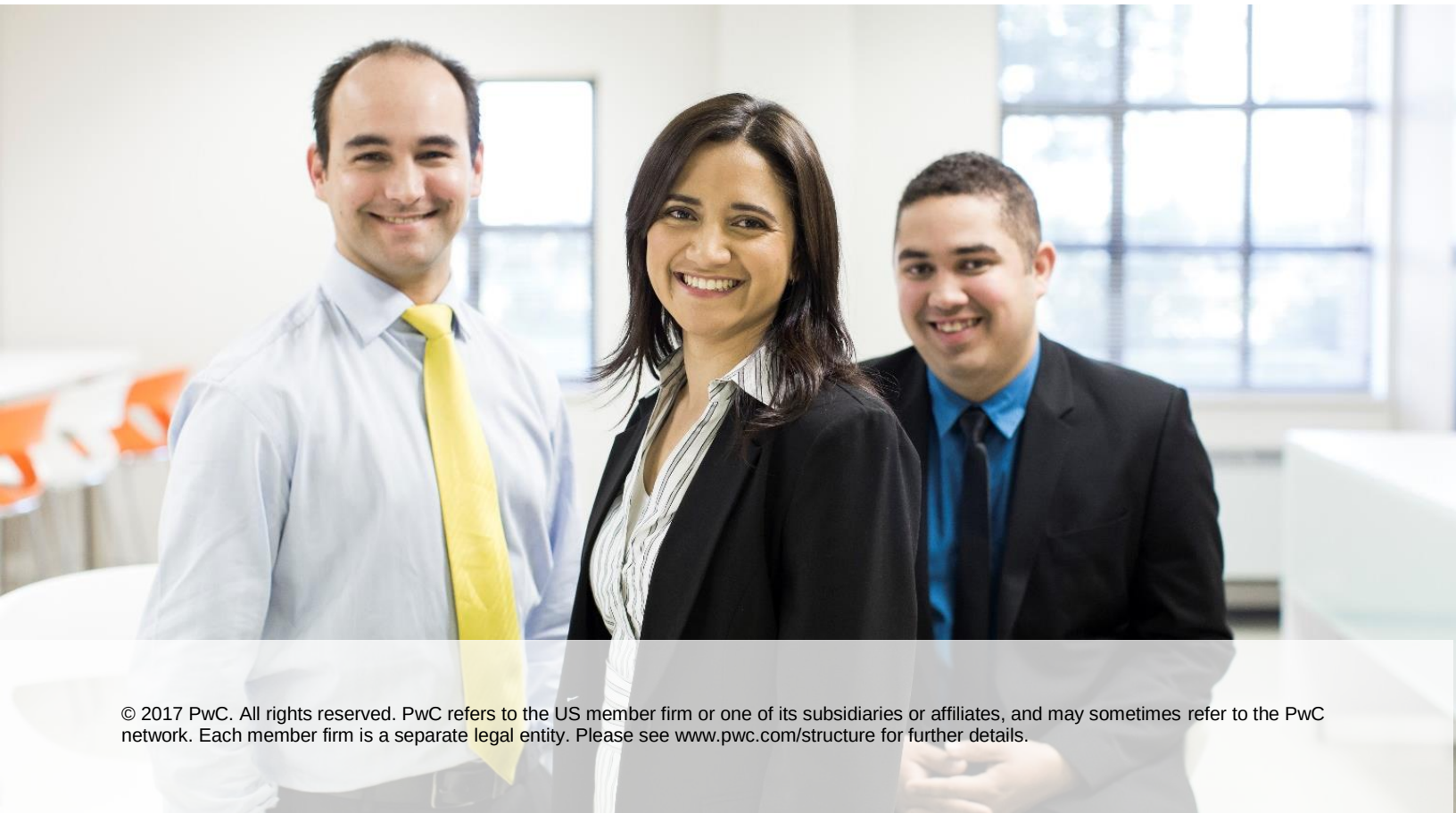
For a deeper discussion, contact:

Todd Bialick
Partner, US Trust and Transparency Solutions Leader
+1 973 236 4902
todd.bialick@pwc.com

Kevin O'Connell
Partner, US Trust and Transparency Solutions Financial Services Leader
+1 617 530 7785
kevin.w.oconnell@pwc.com

Anthony Graziano
Partner, Trust and Transparency Solutions
+1 646 471 3187
anthony.m.graziano@pwc.com

Rebecca Thomas
Managing Director, Trust and Transparency Solutions
+1 314 206 8732
rebecca.j.thomas@pwc.com



© 2017 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.