KFI WHITE PAPER:

Statement on Standards for Attestation Engagements (SSAE) No. 18

The AICPA's attestation standards contain the requirements and application guidance for performing and reporting on examination, review and agreed-upon procedures engagements. Since Service Organization Controls (SOC) reports are classified as "examinations," the attestation standards apply to these engagements.

In April of 2016, the Auditing Standards Board (ASB) began the process of redrafting the attestation standard into one statement. Statement on Standards for Attestation Engagements (SSAE) No. 18, *Attestation Standards: Clarification and Recodification,* with the goal of making the standards easier to read, understand and apply. SSAE No. 18 replaces SSAEs No. 10 through 17. The new standard is intended to increase convergence with the International Auditing and Assurance Standards Board, which makes it more efficient and effective for audit firms to report under both the US and international standards. In fact, the foundation for certain sections of SSAE No. 18 is International Standards on Assurance Engagements (ISAE) 3000, *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information.* SSAE No. 18 is effective for SOC reports dated on or after May 1, 2017 and early adoption is permitted.

While SSAE No. 16 generally applied only to SOC 1 reports, SSAE No. 18 applies to SOC 1, 2 and 3 reports. SSAE No. 18 restructures the attestation standards so that the applicability of any section to a particular engagement depends on the type of service provided and the subject matter of the engagement. For example:

- AT-C section 105 contains requirements and application guidance applicable to any attestation engagement.
- AT-C section 205 contains requirements and guidance for examinations (SOC 2 and 3).
- AT-C section 320 establishes the requirements and application guidance for reporting on controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting (SOC 1).

SSAE No. 18 impacts auditors more than the service organizations that receive SOC reports. Auditors will be required to enhance their workpaper documentation and perform additional procedures in certain areas, such as risk assessment. SSAE No. 18 requires auditors to obtain an understanding of the subject matter that is sufficient to enable them to identify and assess the risks of material misstatement in the subject matter and provide a basis for designing and performing procedures to respond to the assessed risks.

Under SSAE No. 18, one of the most significant changes for service organizations is that controls are required to be implemented and described in the system description for monitoring of subservice organizations. A subservice organization is defined as a service organization used by another service organization to perform some of the services provided to user entities.

One of the most common examples of a subservice organization is a data center. Many service organizations use data centers to outsource some or all of their IT infrastructure, and most data centers these days have their own SOC 1, SOC 2 and/or SOC 3 report. The "carve-out method" of reporting is generally appropriate when this is the case. This means that the service auditor will not be required to test physical security and environmental controls at the data center, assuming that these controls were covered/tested in the data center's SOC report. But even under this approach, monitoring of the subservice organization is still required.

One of the most common types of monitoring that we generally recommend to our SOC clients includes the following:

1. Obtain SOC reports from subservice organizations annually. Did they issue a Type 2 report and is it updated annually?
2. Read the *Independent Service Auditor's Report*, which includes the auditor's opinion. This is generally Section 1 of the SOC report. Was a clean/unqualified opinion issued?
3. Read the complementary user-entity controls, which are generally found towards the end of Section 3 of the report. Are each of the relevant user-entity controls being performed by the service organization? Is there documentation in place to substantiate the performance of relevant user-entity controls?
4. Scan the "Results of Testing" in Section 4 of the report and evaluate all exception items. For each exception, were compensating or mitigating controls identified and successfully tested? Or, were remediation plans identified in the report relative to the exception items?
5. Document the results of the review of the SOC reports in a memo and include responses to the 4 questions above. If any of the responses are "No," then management should consider additional monitoring procedures, such as site visits to the service organization to independently evaluate relevant controls.

By Taylor Marsden and Jamie Kilcoyne, CPA, CISA, CITP, CIA, CFE - K Financial

Other examples of subservice organization monitoring activities include the following:

- Reviewing and reconciling output reports.
- Holding periodic discussions with the subservice organization.
- Making regular site visits to the subservice organization.
- Testing controls at the subservice organization by members of the service organization's internal audit function.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

SOC auditors will be responsible for determining if the description of the system includes activities at the service organization to monitor the effectiveness of controls at subservice organizations.

In conclusion, the impact of SSAE No. 18 on service organizations and their auditors is not expected to be significant. Some service organizations, however, will need to develop more robust subservice organization monitoring controls and document them in their system description.

Although SOC reports prepared under the carve-out method will exclude the controls of subservice organizations, the reports should include the monitoring controls that are performed by the service organization.