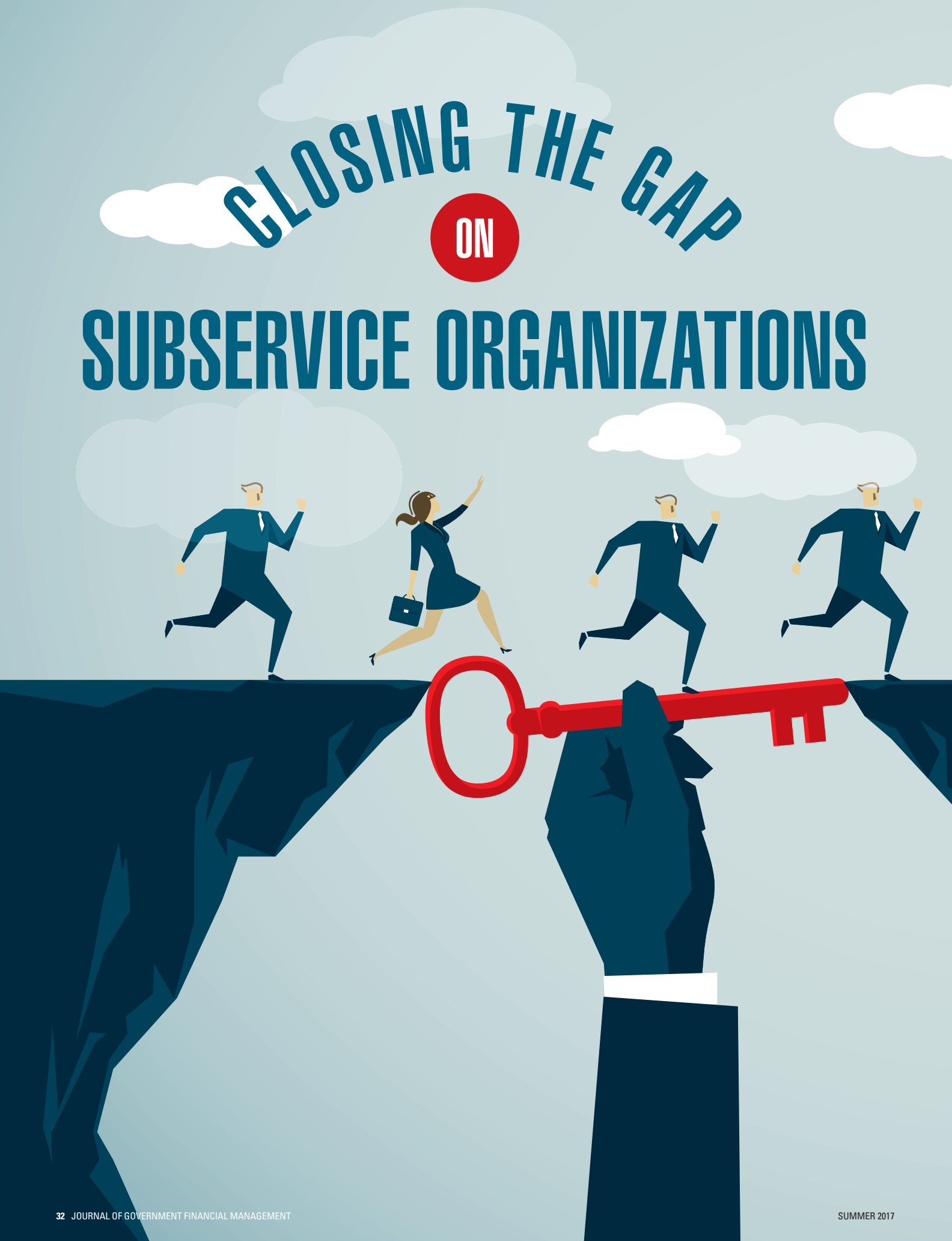
CLOSING THE GAP ON SUBSERVICE ORGANIZATIONS



By: Leah Southers, CGFM, CPA, CISA, CFE

As part of its effort to make auditing standards easier to read, understand and apply,[1] the American Institute of Certified Public Accountants (AICPA) Auditing Standards Board (ASB) recently issued Statement on Standards for Attestation Engagements (SSAE) 18, *Attestation Standards: Clarification and Recodification*,[2] which supersedes several statements, including SSAE 16, *Reporting on Controls at a Service Organization*.[3]

Issued in April 2010, SSAE 16 became the authoritative guidance on reporting on service organizations, replacing Statements on Auditing Standards (SAS) 70. SSAE 16 was issued by the AICPA to better align U.S. standards with International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*.[4] In SSAE 16, the ASB defines a service organization as "an organization or segment of an organization that provides services to user entities, which are likely to be relevant to those user entities' internal control over financial reporting." From a government financial management perspective, a service organization is an organization that hosts key functions applicable to the financial reporting of an entity, such as payroll processing, application hosting, accounting or financial reporting. Service organizations typically obtain a service organization controls (SOC) report to provide assurance to their customers (the "user entities") that controls relating to these services are suitably designed and operating effectively.[5]

SSAE 18, effective for attestation reports dated on or after May 1, 2017, takes the objectives of SSAE 16 a step further by providing improved guidance in several areas: subservice organization management, evidence validation, risk assessment and written assertion requirement.

SSAE 18, effective for attestation reports dated on or after May 1, 2017, takes the objectives of SSAE 16 a step further by providing improved guidance in several areas: subservice organization management, evidence validation, risk assessment and written assertion requirement. The greatest impact of the SSAE 18 changes will be felt at the service organization, subservice organization and service auditor levels. The user entities and user auditors will not likely notice a substantial difference in the information provided in the report or the amount of testing required because of these changes.

Key Change #1: Subservice Organization Management

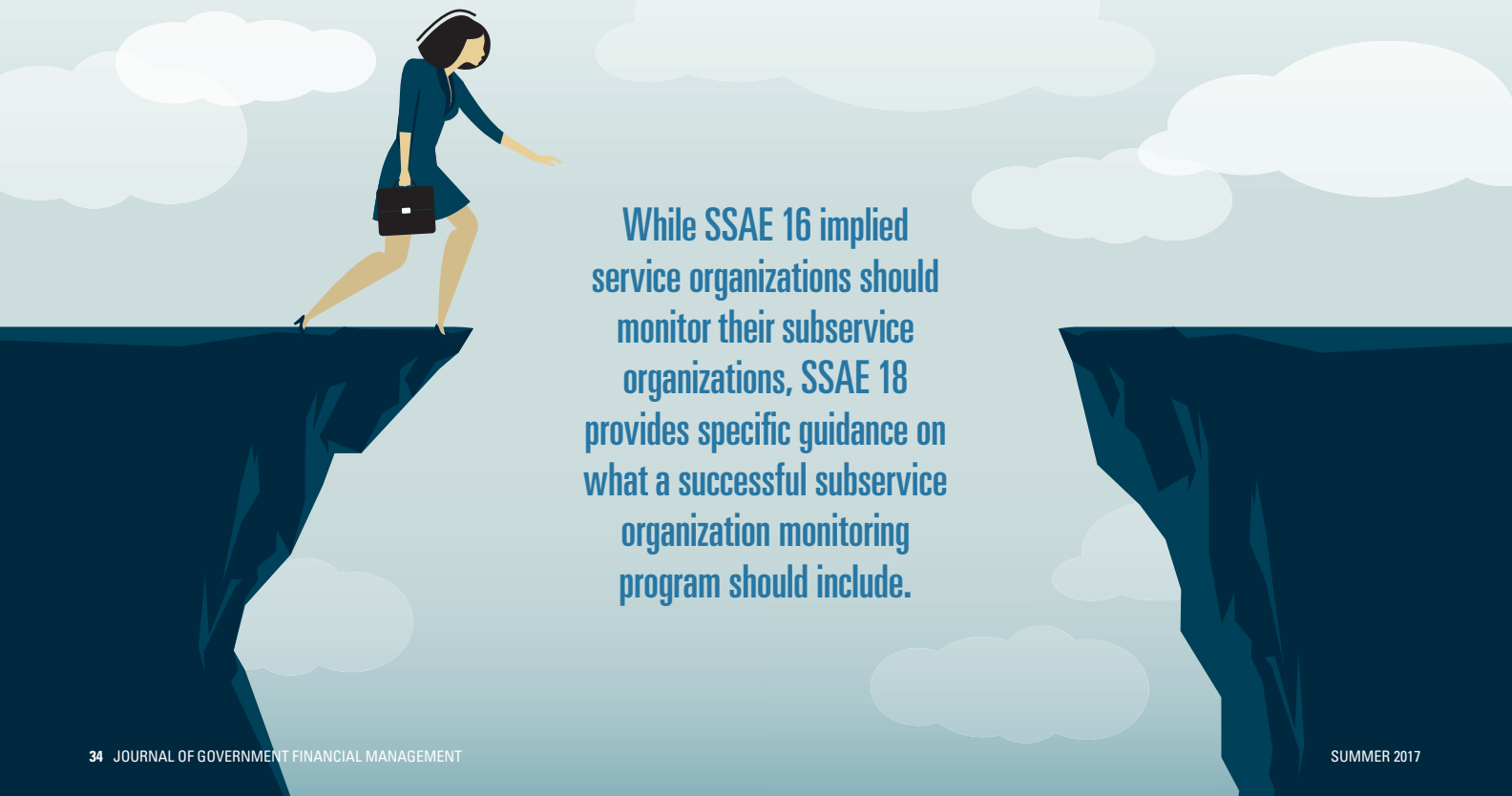
The biggest change introduced by the issuance of SSAE 18 is the increased emphasis on subservice organization management and the introduction of complementary subservice organization controls (CSOCs). A subservice organization is defined as a "service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting." SSAE 16 mentioned subservice organizations, but didn't provide much guidance related to the relationship between the two organizations and how this relationship and the division of controls affects the control objectives. Under SSAE 18, there is greater emphasis placed on service organizations' processes for monitoring the effectiveness of their subservice organizations. While SSAE 16 implied service organizations should monitor their subservice organizations, SSAE 18 provides specific guidance on what a successful subservice organization monitoring program should include. The statement provides examples of several monitoring activities the service organization could implement, such as:

- 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;
- reviewing SOC type 1 or type 2 reports on the subservice organization's system; and
- monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization.

The updated guidance in SSAE 18 requires service organizations to develop, document and implement a plan for monitoring subservice organizations, if not part of their existing process. Service auditors will likely verify that these monitoring procedures are in place and effective at the service organizations.

To address the new monitoring requirement, many service organizations will expect subservice organizations to have undergone or to undergo a SOC audit. Obtaining a SOC audit report from the subservice organization reduces the amount of time, effort, and money the service organization needs to spend meeting this new requirement. Instead of testing these controls themselves, service organizations will review a SOC report to verify subservice organization controls are operating effectively.

Service organizations are already familiar with complementary user entity controls (CUECs), which are controls that the service organization assumes will be implemented by the user entities that are necessary to



While SSAE 16 implied service organizations should monitor their subservice organizations, SSAE 18 provides specific guidance on what a successful subservice organization monitoring program should include.

achieve stated control objectives. Now, SSAE 18 introduces the concept of CSOCs. CSOCs are controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management's description of the service organization's system.

Overall, SSAE 18 provides additional information regarding requirements related to subservice organization monitoring, hopefully providing uniformity across entities and auditors.

WHAT THIS MEANS FOR
Service Organizations

Service organizations will need to develop, document and implement proper subservice organization monitoring procedures, the results of which should be documented and made available to the auditor during the SOC audit. In addition, service organization management will need to consider which subservice organization controls are necessary to achieve control objectives and document these controls in management's description of the service organization's system. These controls will also need to be clearly communicated to the subservice organization.

If the service organization doesn't have subservice organization monitoring procedures in place, or if management decides to enhance its existing procedures to meet the new requirement, it may incur costs to develop, enhance, and/or implement the new procedures. Using the subservice organizations' SOC report as a monitoring tool could reduce these costs, since the service organization would be relying on a report paid for and supplied by the subservice organization instead of conducting the testing themselves.

However, if the service organization decides to use a SOC report to monitor their subservice organizations, the service organization will need to pay close attention to the CUECs included in the SOC report and ensure those controls are in place at their organization.

WHAT THIS MEANS FOR
Subservice Organizations

Subservice organizations should expect additional monitoring by their customers. To minimize the cost of monitoring their subservice organizations, many service organizations may soon require their vendors undergo their own SOC audit. This means the subservice organization, which previously may not have obtained a SOC audit, may now need to obtain one at its own expense or risk being at a competitive disadvantage.

WHAT THIS MEANS FOR
Service Auditors

Service auditors will now be required to obtain an understanding of the service organization's processes for monitoring subservice organizations and ensure proper procedures are being implemented. Auditors will also need to include a statement in the audit opinion about whether CSOCs are necessary to achieve the related control objectives.

Key Change #2: Evidence Validation

SSAE 18 now requires auditors to evaluate the reliability of information produced by the service organization. This requirement includes obtaining evidence about the accuracy and completeness of the information produced, and evaluating whether the information is "sufficiently precise and detailed" for the auditor's purposes. To achieve this objective, auditors may need to obtain more information about how the reports were produced and the system that produces them.

This change may not be as significant as the other changes, since most auditors already perform this type of evaluation, even though the standard did not explicitly require them to do so. Therefore, the effect of this change at the service organization, subservice organization, and auditor level will likely be minimal.

WHAT THIS MEANS FOR
Service Organizations

Service organizations may be required by their auditors to provide additional information on their reports and monitoring of subservice organizations. Service organizations may also be subject to additional testing of evidence provided as auditors strive to determine whether the evidence is sufficiently reliable for their purposes. Although this effort may not have a large impact on the service organization, since many auditors already make such determinations as a matter of due diligence, it may result in a few additional requests or questions from the auditor.

WHAT THIS MEANS FOR
Subservice Organizations

If the subservice organization undergoes a SOC audit, there may be some additional requests from the subservice auditors to validate the reliability of evidence. If the subservice organization does not undergo a SOC audit, it may encounter additional requests from its customers to satisfy the service auditor's requests.

WHAT THIS MEANS FOR
Service Auditors

If service auditors were not already doing so, they will need to ask additional questions of, and obtain additional documentation from, the service organization regarding the source and reliability of evidence provided. Based on the information obtained, the service auditors will need to determine whether the evidence is sufficiently reliable for their purposes.

Key Change #3: Risk Assessment

SSAE 18 provides additional guidance and requirements for performing risk assessments during SOC audits. SSAE 16 only required service auditors to obtain an understanding of the service organization's system, including controls included in the scope of the engagement. SSAE 16 did not specifically address the risk of

material misstatement or provide risk assessment procedures or guidelines.

SSAE 18 builds on the requirements of SSAE 16 in requiring the auditor to conduct a more detailed risk assessment. Specifically, the auditor now needs to gain further understanding of the entity, enough to identify and assess the risk of material misstatement and to provide the basis for designing and performing procedures to address that risk.

Note, although SSAE 18 provides additional guidance for the auditor's risk assessment, service organizations are still required to identify and assess risks that threaten the achievement of their control objectives as required by both SSAEs 16 and 18. However, SSAE 18 now explicitly requires the auditor to obtain an understanding of management's process for identifying and evaluating these risks, and to assess the completeness and accuracy of management's identification of these risks.

WHAT THIS MEANS FOR

Service Organizations

The auditors' requests to the service organization may increase to complete their risk assessment. An enhanced risk assessment process may lead to additional testing in areas the auditors consider high risk. In addition, the service organization should ensure it has a proper risk assessment process in place, and should be prepared to provide evidence of the process and the methodology to the auditors upon request.

WHAT THIS MEANS FOR

Subservice Organizations

This change may not have a direct impact on the subservice organization other than through its own SOC audit, should it elect to have one.

WHAT THIS MEANS FOR

Service Auditors

Service auditors will likely feel the greatest impact from this change as they will now be required to conduct and document their risk assessment of the entity under audit, if they are not already doing so. To meet this requirement, service auditors may need to expand their planning procedures to obtain a sufficient understanding of the entity to conduct their risk assessment. In addition, the results of the risk assessment may change or increase the test procedures to be performed.

Key Change #4: Written Assertion Requirement

A written assertion from service organization management is nothing new; both SSAE 16 and SSAE 18 require management to assert in writing that its description of the system is fairly presented. The primary change instituted by SSAE 18 is that the written assertion must include more information about the relationship between the service and subservice organizations, as well as the service organization and the user entity. SSAE 18 AT-C Section 320, Exhibit B, provides the revised content for management's written assertions for both SOC 1 and SOC 2 reports.

Organizations that use a carve-out method for their subservice organizations are now required to include a paragraph identifying the type of service provided by the subservice organization and state that control objectives in the description can only be achieved if certain CSOCs are adequately designed and operating effectively.[6] The revised assertion also requires management include a statement that certain control objectives specified in the description can be achieved only if CUECs assumed in the design of the organization's controls are suitably designed and operating effectively. Requiring management to discuss CSOCs and CUECs in their written assertion better delineates which controls management assumes responsibility for and which controls are included in their description.

WHAT THIS MEANS FOR

Service Organizations

Service organizations will need to clearly define CSOCs and CUECs in their description and be prepared to provide a written assertion related to that description.

WHAT THIS MEANS FOR

Subservice Organizations

This change should not affect subservice organizations other than the requirement to implement CSOCs.

WHAT THIS MEANS FOR

Service Auditors

Service auditors will need to ensure that written assurances from management are appropriately drafted in accordance with the revised standard.

Conclusion

SSAE 18 does not substantially change the requirements of SSAE 16; rather, it builds upon it to create simplified, more comprehensive guidance for service organizations, subservice organizations and their auditors. It provides these entities with additional guidance related to certain key areas that SSAE 16 did not explicitly address, particularly the management of subservice organizations. Closing the gap on subservice provider management will result in more reliable, consistent reports for user organizations and their auditors.]

Endnotes

1. AICPA's *Clarification and Convergence — An AICPA Auditing Standards Board Project*, July 2008, www.aicpa.org/InterestAreas/FRC/AuditAttest/DownloadableDocuments/Clarity/Archive/ASB_Clarity_%20and_Convergence_(8.5x11).pdf
2. SSAE 18, *Attestation Standards: Clarification and Recodification*. www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/SSAE_No_18.pdf, accessed April 20, 2017.
3. SSAE 16 — *Reporting on Controls at a Service Organization*, www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00801.pdf, accessed April 20, 2017.
4. www.journalofaccountancy.com/issues/2010/aug/20103009.html, accessed April 18, 2017.
5. www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/CPAs.aspx, accessed April 18, 2017.
6. SSAE 18, Section 320, Exhibit B.

Leah Southers, CGFM, CPA, CISA, CFE is a manager in Williams Adley's Assurance & Advisory Practice Group. She has more than 11 years' experience providing assurance services to federal, state and local government clients.