Effects of Changes in Attest Standards on SOC 1 Examinations

Executive Summary

Subservice organizations, management's assertion responsibilities and other items are addressed in Statement on Standards for Attestation Engagements (SSAE) No. 18, *Attestation Standards: Clarification and Recodification.* SSAE 18, AT-C Section 320, "*Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting"* replaces SSAE 16, *"Reporting on Controls at a Service Organization"* (AT Section 801).

SSAE 18 Section 320 contains significant changes to management's responsibilities for Service Organization Controls (SOC 1) reports as well as providing clarification and guidance for service auditors. This paper covers changes to SOC 1 audit standards caused by SSAE 18 and their effect on service organization management.

The requirements are effective for audit reports dated on or after May 1, 2017.

Part I: Subservice Organizations

Outsourced services, such as payroll administration and third-party benefit plan administration, are services where the transaction processing extends beyond the user entity. When the controls of the service organization are likely to be relevant to user entities, a SOC 1 report is generally required. When the service organization outsources functions, such as IT hosting services, the complete processing system and related controls of the service organization include the relevant functions and controls at the subservice organization.

Management is responsible for understanding and documenting the service organization's **complete** transaction processing and control system and, for a Type 2 report, assessing control effectiveness—including consideration of subservice organizations. "Subservice organization" is mentioned 118 times in the new standard compared to 64 in SSAE 16. The underlying theme is that under SSAE 18, service organization auditors will expect the service organization's management to include in its system description these subservice organization elements:

- The functions performed by a subservice organization
- Whether the carve-out or inclusive method is used for each subservice organization
- Complementary Subservice Organization Controls (CSOCs)
- Activities at the service organization that provide evidence of the design and operating effectiveness of controls at the subservice organization

Complementary Subservice Organization Controls (CSOCs)

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

In other words, if a service organization's control system is designed with the assumption that CSOCs and complementary user entity controls (CUECs) are necessary to achieve the control objectives, management should identify those controls. For carve-out method examinations, management is not expected to describe the detailed processing or entire control structure at the subservice organization.

Service organizations generally process transactions. Subservice organizations may not process transactions. For example, a staffing organization (service organization) may contract with a data center to host its staffing and payroll applications. Because the data center's control system is a necessary component of the service organization's control system, it is considered a sub-service organization. Other vendors, such as the service organization's facility security guards, which are not considered a necessary component of the service organization's internal control over financial reporting, are not service organizations.

CSOC Risk Assessment

SSAE 18 clarifies that when a service organization's controls are designed with the assumption that user entities have implemented CUECs, or that subservice organizations have implemented CSOCs that are necessary to achieve the control objectives, management should identify risks that such controls were not implemented by user entities or subservice organizations or that those controls were not operating effectively.

Likewise, the service auditor is required to evaluate whether CSOCs are part of the service organization's risk assessment process. That means the auditor will evaluate whether management has identified and evaluated the risks that CSOCs—as well as CUECs—were implemented and operating effectively. The service auditor will assess how management addressed significant risks and the resulting effect on achievement of relevant control objective(s).

Practice Points:

- Monitoring activities, discussed below, may be an integral part of addressing significant subservice organization risks. If the risks that controls were not implemented or not operating effectively by user or subservice organization cannot be mitigated by the service organization's own controls, including monitoring controls, management may find it necessary to reassess whether achievement of the control objectives as worded is feasible. Management will be required to attest to control objective achievement as a precondition to the examination, also discussed below, which is expected to require significant resources.
- CSOCs are part of management's description of the service organization's system. Management may present CSOCs in a table supplementing its description or, alternatively, disclose them under the respective control matrices of the report with reference in management's description.

Complementary User Entity Controls (CUECs)

In addition to CSOCs, a service organization is required to design their system considering CUECs identified in the subservice organization's SOC 1 report as available. Service organization management is responsible for incorporating the subservice organization's CUEC into their own system design as necessary to achieve its control objectives. This entails ensuring controls identified by the subservice organization as CUECs are designed and operating effectively at the service organization.

Practice Point:

- Management can expect its service auditor to request a SOC 1 Type 1 or Type 2 report for carved-out subservice organizations. The service auditor will generally determine whether management's description adequately describes the functions performed by the subservice organization and whether CUECs are included in the service organization's system description, potentially as the service organization's own CUECs. Auditors will generally include in their examination procedures to determine whether the recommended subservice CUECs differ from those at the service organization. Service organization management is encouraged to prepare documentation supporting such differences, including why the applicable control objective(s) are still met.

Monitoring the Effectiveness of Controls at Subservice Organizations

Management's description of the service organization's system presents how the service organization's control system was designed and implemented. This may include aspects of the control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities when relevant to the services provided.

Management's monitoring activities may provide evidence supporting its assertion over the design and operating effectiveness of controls. SSAE 18 clarifies that a service organization's monitoring activities may include monitoring the effectiveness of controls at the subservice organization.

Some combination of ongoing monitoring and separate evaluations may be used to ensure that the internal control structure maintains its effectiveness over time. Ongoing monitoring generally determines that potential issues are identified timely, and separate evaluations generally determine that internal control effectiveness is maintained over time.

Examples of subservice monitoring activities include:

- Reviewing and reconciling output reports
- Making regular site visits with the subservice organization
- Testing controls at the subservice organization by a member of the service organization's internal audit function
- Reviewing Type 1 or Type 2 reports on the subservice organization's system
- Monitoring external communications, such as customer complaints relevant to the subservice organization's services

Subservice organizations that generally require monitoring are those with systems and controls required for the fair presentation of management's description of the service organization's system, the suitability of the design of controls that address the control objectives stated in the system description and, in the case of a Type 2 report, the controls' operating effectiveness.

Changes to the service auditor's report wording clarifies SSAE 18's intent to ensure management takes responsibility for its control system design, as follows:

Auditor's Report Regarding Controls Necessary to Achieve the Control Objectives	
SSAE 16	**SSAE 18**
Includes a statement that the examination included testing the operating effectiveness of those controls that the service auditor considers necessary to provide reasonable assurance that the related control objectives stated in management's description of the service organization's system were achieved	Includes a statement that the examination included testing of the operating effectiveness of those controls ***that management considers necessary*** to provide reasonable assurance that the related control objectives stated in management's description of the service organization's system were achieved

Aspects of the service organization's control environment, risk assessment process and monitoring activities may not be presented in the control objectives stated by management, although necessary to achieve the specified control objectives. Thus, deficiencies in these controls may affect the service auditor's assessment of whether the control system was suitably designed or operating effectively to achieve the specified control objectives.

Practice Point:

- As part of examination planning, management is encouraged to discuss with its auditor activities in place to monitor the effectiveness of controls at subservice organizations, if any. The service auditor's examination will include controls at the service organization that monitor the effectiveness of controls at the subservice organization—as it does other monitoring controls—when such controls are included in management's description of the service organization's system.

Other Service Auditor Requirements

In an examination of a service organization where the carve-out method is used, the service auditor's exam will not extend to controls of the subservice organization. Likewise, the service auditor will not evaluate the suitability of the design or operating effectiveness of CSOCs **at the subservice organization**. Rather, the service auditor examination will entail determining whether management has identified controls necessary—either at the service organization, subservice organization or at the user entity—to achieve the control objectives and whether they are effectively designed and, for a Type 2 engagement, operating effectively.

Thus, a SOC 1 examination where the carve-out method is used will include a statement from the service auditor that certain control objectives specified by the service organization may only be achieved if CSOCs (and CUECs) assumed in the design of the service organization's controls are suitably designed (and, for a Type 2 report, operating effectively).

In addition, the service auditor's report will include a statement that management's description of the service organization's system excludes the control objectives and related controls at subservice organizations and that the service auditor's examination did not extend to the subservice organization's controls.

Practice Point:

- Service organizations are encouraged to be prepared to explain to their SOC 1 report recipients that the service organization's control objectives can only be met if CSOCs assumed in the service organization's system design were designed effectively and, for a Type 2 report, operating effectively throughout the period. User organizations may want to explore obtaining an inclusive method report from the service organization, particularly in situations where a subservice SOC report is not available. If one is available, the user organization may request guidance on how to obtain the report and how to evaluate the combined information.

Only under the inclusive method does management's description include control objectives and controls of a subservice organization. Under the carve-out method, the service auditor will not evaluate the suitability of the design or operating effectiveness of controls at the subservice organization, including CSOCs.

Part II: Other Significant Management Responsibility Changes

Risk Assessment

SSAE 16's section pertaining to "*Identification of Risks"* has been retitled *"Management's Responsibility for Identifying Risks"* in SSAE 18. The service auditor guidance reads as follows:

Risks to Achieving Control Objectives	
SSAE 16	**SSAE 18**
Service auditor ***identifies*** risks that threaten the achievement of the control objectives stated in management's description of the service organization's system	Service auditor will "obtain an understanding of ***management's process*** for identifying and evaluating the risks that threaten the achievement of the control objectives and assessing the completeness and accuracy of ***management's identification*** of those risks"

Control objectives relate to the risks that controls seek to mitigate. Thoughtful identification by management of control objectives when designing, implementing and documenting the service organization's system may itself comprise an informal process for identifying relevant risks. Risk identification should encompass fraud as well as unintentional acts that threaten the achievement of the control objectives. The service auditor will evaluate whether CSOCs (and CUECs) are part of the service organization's risk assessment process. See discussion above (CSOC Risk Assessment).

Practice Points:

- When performing its assessment of management's work, the service auditor is guided to include risks related to new or changed controls, system changes, significant changes in processing volume, new personnel or significant changes in key management or personnel, new types of transactions, new products or technologies or modifications to the service auditor's opinion in the service auditor's report from the prior year—and management is encouraged to do the same*.*
- The service auditor is newly required to *"include risks arising from each of the described classes of transactions, and risks that IT poses to the user entity's internal control over financial reporting"* when evaluating the linkage of controls identified by management with risks identified by management. Management is encouraged to do the same.

Control Determination

Management's responsibility for determining controls necessary to achieve the control objectives has been clarified in SSAE 18 by modifying the service auditor's report wording, as follows:

Evaluation of Controls Necessary to Achieve the Control Objectives	
SSAE 16	**SSAE 18**
Service auditor is required to obtain an understanding of the organization's system ***to determine*** which controls are necessary to achieve the control objectives stated in management's description of the service organization's system, whether controls were suitably designed to achieve those control objectives and, in the case of a Type 2 report, whether controls were operating effectively throughout the period to achieve those control objectives	Service auditor is required ***to understand*** which controls are necessary to achieve the control objectives stated in management's description of the service organization's system, whether controls were suitably designed to achieve those control objectives and, in the case of a Type 2 report, whether controls were operating effectively throughout the specified period to achieve those control objectives

Practice Point:

- Management may develop controls through a process of identifying "what could go wrong" that could hinder achievement of the control objectives.

Precondition to Acceptance (& Continuance) of the SOC 1 Engagement

The conditions under which a service auditor accepts or continues a SOC 1 engagement are clarified as *"Preconditions"* in SSAE 18. In other words, a service auditor should accept or continue an engagement to report on controls at a service organization **only** if the preconditions are met and continue to be met.

Among the preconditions, the service auditor is required to obtain management's written acknowledgement (assertion) that it fairly presents the service organization's system description, has identified risks that threaten the achievement of control objectives, has designed and implemented suitably designed controls and, for Type 2 engagements, the controls are operating effectively throughout the period. The service auditor's responsibility is to plan and perform the examination to obtain reasonable assurance about the components of management's assertion, in all material respects, and provide an opinion.

If management of the service organization refuses to provide a written assertion, the service auditor is required to withdraw from the engagement (when withdrawal is possible under applicable law or regulation). When the inclusive method is used, service organization management is responsible for precondition items of the subservice organization as well as its own.

Practice Points:

- Service organization management relying on the service auditor to "review and approve" its assertion elements—system description, control objectives, risks, control design and operating effectiveness—and offer suggestions for improvement are cautioned against this practice. The SOC 1 examination objective is for the service auditor to independently evaluate the risk that the subject matter prepared by management, *e.g.*, the organization's system description, is not in accordance with (or based on) the criteria management prepared, in all material respects, and that management's assertion is not fairly stated, in all material respects. Thus, management is expected to document, evaluate and attest to these components prior to the examination. Engagement criteria is discussed below.
- The service auditor is not prohibited from assisting management or other responsible party in developing or presenting the examination subject matter, but management or the responsible party remains responsible for the subject matter. This is required for the service auditor to express an independent opinion.

Management is encouraged to devote resources to understanding engagement preconditions. SSAE 18 clarifies the service auditor's responsibility to evaluate management's description of the organization's system, control design and operating effectiveness against management's criteria (discussed below). More than ever, service organizations should expect their SOC auditors to "push back" and ensure all items are prepared by management as a precondition to the engagement.

Evaluation Criteria

Management is required to include in its written assertion a statement about the criteria it used to prepare its description of the service organization's system and conditions upon which the auditor should evaluate whether the controls were suitably designed and operating effectively.

SSAE 18 clarifies that the service auditor's responsibility is to plan and perform the examination to obtain reasonable assurance about management's assertions in all material respects, based on the criteria in management's assertion. The service auditor will evaluate management's criteria for suitability. SSAE 18 clarifies that assessment of management's criteria is not a precondition to accepting the engagement. Instead, it is part of the engagement.

Evaluation Criteria	
SSAE 16	**SSAE 18**
The service auditor is required to have preliminary knowledge, as a precondition to accepting or continuing a SOC 1 engagement, indicating that the criteria used **will be suitable**	The service auditor will assess whether management has used suitable criteria in preparing its system description, evaluation of control design suitability and, in a Type 2 report, operating effectiveness

Misstatements occur when the service auditor's evaluation of the subject matter differs from the assessment criteria management has established. Material misstatements are generally termed "exceptions" or "deviations" by the service auditor.

Practice Points:

- Establishing criteria against which to evaluate assertion items can be daunting for management. SSAE 18 provides the service auditor with guidance for assessing the suitability of criteria by providing a list of minimum components, and management may refer to the same list. For example, as part of the examination, the service auditor will determine whether management has considered whether controls were consistently designed and applied throughout the period by individuals who have the appropriate competence and authority.
- Certain aspects of management's criteria may be included within the assertion components themselves. For example, management's control objectives are often the criteria against which the risk assessment and control design are evaluated. However, control objectives will be evaluated against their own criteria—their adequacy and suitability for SOC 1 report users. Thus, management is encouraged to approach the examination with the expectation that the service auditor will include deficiently worded control objectives, *e.g.*, when it assesses the risk of material misstatement.

Management is responsible for understanding the examination expectations early in its SOC1 engagement planning. Because criteria assessment is part of the SSAE 18 examination, management can expect the service auditor to concurrently perform its evaluation of the service organization's internal control system and suitability of management's evaluation criteria. The service auditor's work is based on it.

Request to Change the Scope of the Engagement

Under SSAE 18, a request to change the SOC 1 engagement's scope may be reasonably justified because of a change in circumstances that affects the requirements of the responsible party—or, if different, the engaging party—or a misunderstanding concerning the nature of the engagement **originally** requested.

A change may not be considered reasonable by the service auditor if it appears the change relates to information that is incorrect, incomplete or otherwise unsatisfactory.

Practice Point:

- Defining the "assertion" as a precondition emphasizes management's responsibility to document all aspects of its system design and operating effectiveness prior to examination. Service organization management should expect incomplete, incorrect or unsatisfactory information to delay the examination. Relevant details of changes to the control system's design and implementation should be included in its assertion. If not, differences from, or changes to, the original assertion may be viewed as control design or operating effectiveness misstatements.

Part III: Other Significant Service Auditor Changes

Internal Audit

SSAE 16's section on *"Using the Work of the Internal Audit Function"* has been removed. Under SSAE 18, service auditors are required to understand the internal audit function as part of understanding the service organization's system related to the services provided to user entities and scope of the SOC 1 engagement. Thus, service auditors will generally take internal audit findings into consideration as part of their risk assessment and determining the nature, timing and extent of testing. This replaces the requirement under in SSAE 16 for the service auditor to understand the internal audit function to determine whether and how the department's work could be relied upon for examination execution.

Practice Point:

- The service auditor will generally read the reports of the internal audit function—as well as regulatory examinations—related to services provided to user entities and scope of the SOC 1 engagement to understand the nature and extent of procedures performed and related findings. Accordingly, management is encouraged to consider including relevant internal audit examination functions in its system description, *e.g.*, monitoring activities.

Obtaining Evidence Regarding the Operating Effectiveness of Controls

The service auditor's opinion is still owned by the service auditor, but management's role in the engagement is clarified in it. The auditor's opinion will include a statement that *"the service auditor believes the **evidence obtained** is sufficient and appropriate to provide a reasonable basis for the service auditor's opinion."* This replaces the SSAE 16 requirement to include a statement that *"the service auditor believes **the examination** provides a reasonable basis for his or her opinion."*

The new language clarifies management's responsibility for identifying fraud. Procedures that are effective for detecting unintentional misstatements in the management's description, and instances in which control objectives were not achieved, may be ineffective for detecting fraudulent misstatements or instances involving collusion. That means the service auditor's evaluation of information produced by the service organization is limited to determining whether the information is sufficiently reliable for the auditor's purpose.

Evaluation procedures entail obtaining evidence about the information's accuracy and completeness and evaluating whether the information is sufficiently precise and detailed.

Practice Point:

- Service organization management is encouraged to be alert to the service auditor opinion wording changes. Management should expect the service auditor to request information evidencing the accuracy and completeness of all evidence, including internally produced evidence. For system-produced reports, this generally will entail examination of application-specific controls as well as general computer controls over the applicable software applications and system(s). A service auditor is not expected to perform more or alternative work when management is unable to provide sufficient and appropriate evidence to support the system description's fair presentation or suitability and operating effectiveness of controls to achieve the control objectives.

Use of Audit Report Clarified

Report distribution is within management's control, but SSAE 18 requires the service auditor to specify the intended distribution recipients in the audit report as follows:

Changes to the Service Auditor's Report Wording Regarding Report Distribution	
SSAE 16	**SSAE 18**
The report is solely intended for the information and use of management of the service organization, user entities of the service organization's system during some or all the period covered by the report **and the independent auditors of such user entities**	The report is solely intended for the information and use of management of the service organization, user entities of the service organization's system during some or all the period covered by the report **and the auditors who audit and report on such user entities' financial statements or internal control over financial reporting. The report is not intended to be, and should not be, used by anyone other than the specified parties**

Conclusion

Examination preparation is more important than ever for a successful SOC engagement. SSAE 18 clarifies, among other topics, that describing the service organization's system and determining the necessary controls is management's responsibility. Understanding the organization's system, including related controls, is the service auditor's responsibility.

BKD will continue to monitor practice and implementation issues of SSAE 18.

For more information, contact your BKD advisor.

Contributor

Connie L. Spinelli, CPA, CIA, CISA, CISSP

Responsibilities in an Attest Engagement – Responsible Party (Management of the Service Organization)	
All Attestation Engagements (SOC 1, SOC 2 and SOC 3 reports)	**Specific to SOC 1 Engagements**
▪ The subject matter—and, if applicable, the preparation and presentation of the subject matter—in accordance with (or based on) the criteria ▪ Its assertion about the subject matter ▪ Measuring, evaluating and, when applicable, presenting subject matter that is free from material misstatement, whether due to error or fraud ▪ Providing the auditor with: • Access to all information of which the responsible party is aware that is relevant to the measurement, evaluation or disclosure of the subject matter • Access to additional information that the practitioner may request for the engagement • Unrestricted access to people within the appropriate party(ies) from whom the practitioner determines it is necessary to obtain evidence ▪ Management's written assertion that is included in or attached to management's description of the service organization's system	▪ Prepare an accurate and complete description of the service organization's system* relevant to user entities' internal control over financial reporting, which includes control objectives, risks and system assertions as well as: • CUECs necessary to achieve the control objectives • CSOCs, if any, necessary to achieve the control objectives** • Services performed by a subservice organization, if any, and whether the carve-out method was used** • Criteria against which the fairness of the presentation of the description and the suitability of the design or operating effectiveness of the controls to achieve the related control objectives in the description is evaluated ▪ Evaluate whether its controls were suitably designed to achieve the control objectives stated in the description and the criteria against which the fairness of the presentation of the description and the suitability of the design is evaluated*** • Evaluate whether its controls operated effectively throughout the specified period to achieve the control objectives stated in the description of the service organization's system, in the case of a Type 2 report, and the criteria against which the operating effectiveness of the controls to achieve the related control objectives in the description is evaluated*** ▪ Disclose: • Instances of noncompliance with laws and regulations or uncorrected misstatements attributable to the service organization that may affect one or more user entities • Knowledge of any actual, suspected or alleged fraud by management or the service organization's employees that could adversely affect the fairness of the presentation of management's description of the service organization's system or the completeness or achievement of the control objectives stated in the description *The guidelines and activities for providing transaction processing and other services to user entities, including the infrastructure, software, people and data that support the policies and procedures *If the application of complementary user entity or subservice organization controls is necessary to achieve the related control objectives **For engagements, which exclude or "carve out" subservice organizations, management's description excludes control objectives and related controls of the relevant subservice organization ***When the engagement excludes or "carves out" subservice organizations, management's evaluation includes a discussion of control objectives that can only be achieved if CSOCs assumed in the design of the service organization controls are suitably designed and operating effectively