



The Transition from SAS 70 to SSAE 16

Organizations that provide services to their customers that impact financial reporting processes are often subject to audits of the processes executed on behalf of their customers. Statement on Auditing Standards (SAS) No. 70 has long been the governing standard in the US for performing these audits, and giving the service organization a mechanism for providing an independent audit report to their customers and their customers auditors. The requirements and guidance for US auditors reporting under SAS 70 will be superseded by Statement on Standards for Attestation Engagements 16 (SSAE 16). Globally, many countries do not have their own standard for performing such audits, which led to the creation of an international standard, International Standard on Assurance Engagements 3402 (ISAE 3402). The international standard will provide a reporting option for service organizations with the need for a global attestation standard to deliver consistent reporting worldwide.

Although initial discussions on these new standards considered broadening the scope beyond financial reporting, the final standards both focus on controls at service organizations likely to be relevant to a customer's internal control over financial reporting. The standards are effective for reports with periods ending on or after June 15, 2011, and permit early adoption. While SSAE 16 and ISAE 3402 have some differences, they are substantially the same.

KEY SIMILARITIES AND DIFFERENCES BETWEEN SSAE 16 AND SAS 70

Similarities	Differences
<ul style="list-style-type: none">• Scope is focused on controls that are likely to be relevant to user entities' internal control over financial reporting	<ul style="list-style-type: none">• New standard is an attest standard, not an audit standard; a separate audit standard will be issued to address the requirements of the user auditor
<ul style="list-style-type: none">• Type 1 and Type 2 reports may be issued by the service auditor	<ul style="list-style-type: none">• Management is required to provide a written assertion
<ul style="list-style-type: none">• Reports may include (inclusive method) or exclude (carve-out method) services provided by subservice organizations	<ul style="list-style-type: none">• Subservice organizations are required to provide a similar assertion when the inclusive method is used
<ul style="list-style-type: none">• Service organization's description of controls under SAS 70 generally will provide a basis for the system description under SSAE 16	<ul style="list-style-type: none">• In a Type 2 report, the service auditor opines on the suitability of the design of controls related to the control objectives throughout the entire period
<ul style="list-style-type: none">• Service auditor's report is restricted to service organization management, user entities of the service organization and the user auditors	<ul style="list-style-type: none">• Service auditor is required to disclose any reliance on the work of Internal Audit (or other independent management testing functions) within the report
	<ul style="list-style-type: none">• Format of service auditor's opinion will change



Overall assessment of key changes to the standard

SSAE 16 includes several new requirements and changes to previous requirements of SAS No. 70. The following pages include an evaluation of the differences identified above.

ASSESSING KEY CHANGES TO THE STANDARD

Management Assertion

Under the new standard, the service organization has additional responsibilities. Most notable is the requirement to provide a written assertion, which will state that the controls are fairly presented, suitably designed and operating effectively to achieve the specified control objectives.

- Management's assertion will be included in, or attached to, management's description of the system and documented within the report.
- Management's assertion should be based on suitable criteria.
 - Management should select the criteria to be used to make their assertion and should state them within the assertion.
 - A service auditor is precluded from issuing a report if management does not provide a written assertion.
 - The standard provides typical suitable criteria and a sample assertion, which should make this requirement straight-forward to implement.
- Management should have a reasonable basis for its assertion, which may be achieved through on-going monitoring activities that provide evidence of the design and operating effectiveness of controls.

SSAE 16 includes example management assertions, which are attached to this document as Appendix 1. Management's representation letter signed at the completion of a SAS 70 engagement today includes the required items within management's assertion.

Description of the System

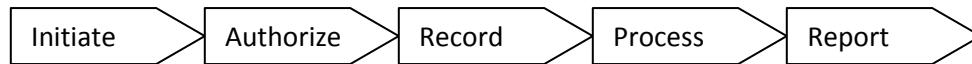
In addition to a written assertion, management is responsible for preparing its description of the service organization's system ("the system"). The system is defined as the policies and procedures designed, implemented, and documented by management to provide customers with the services covered by the service auditor's report. Management's description should identify (as applicable):

- services covered,
- period covered by the report,
- description of the classes of transactions processed,
- control objectives and related controls,
- complementary user controls,
- controls performed by the subservice organization (inclusive reports),
- the process used to prepare reports provided to customers,
- changes to the system during the period covered by the report, and
- other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls, as



defined by the Committee of Sponsoring Organizations' (COSO) internal control framework, that could be relevant to user entities.

The diagram below illustrates the elements management should consider when describing the flow of transactions through the system:



In many cases, a majority of the elements to be included in management's description of the system as required under SSAE 16 have been included in existing SAS 70 reports. In such cases, there should not be a significant additional work effort required of the service organization.

Identification of risks to achieving control objectives

Similar to guidance under SAS 70, management's description of the system should specify control objectives and related controls. Management should identify the risks that threaten the achievement of the control objectives stated in management's description of the system. SSAE 16 allows for management to have a formal or informal process for identifying the relevant risks and does not require that management explicitly include such risks within the report. However, our perspective on leading practice is that management conduct and formally document their consideration of the relevant risks. As many companies have already performed this risk assessment as part of the creation of the control objectives and control activities for their historical SAS 70 efforts, identifying the relevant risks factors should not be a significant additional work effort.

Subservice Organizations

Consistent with the prior standard, SSAE 16 allows the service organization to describe the use of subservice organizations through either an inclusive or carve-out method of presentation.

When using the inclusive method, management's description of the system should include a description of, and clearly distinguish, the services provided by the subservice organization. Additionally, the subservice organization is subject to the same requirements as the service organization and should provide the following:

- a description of the related control objectives and controls at the subservice organization,
- a written assertion, to be included in, or attached to, management's description of the service organization's system, and
- a letter of representation.

The requirement that the subservice organization provide a written assertion, when employing the inclusive method, may present the greatest challenge, which management should proactively coordinate well in advance of a service auditor engagement. The representation letter signed at the completion of a SAS 70 engagement today includes the required items within the assertion.



Using work of internal audit

The service auditor may use the work of internal audit or other independent control-related functions that has been performed independent of the service auditor's work to support their testing. However, there are often challenges in finding sufficient alignment of the scope and timing of work performed by internal audit or other independent control-related functions with that of the service auditor. If the service auditor is able to overcome such challenges and relies upon this work in performing their tests of controls, additional disclosure is required within the report. Such disclosure is not required when internal audit or another control-related function is used in the more common direct assistance capacity (e.g., under the direction of the service auditor).



Appendix 1

Example 1: Assertion by Management of a Service Organization for a Type 2 Report

XYZ Service Organization's Assertion

We have prepared the description of XYZ Service Organization's [*type or name of*] system (description) for user entities of the system during some or all of the period [*date*] to [*date*], and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the [*type or name of*] system made available to user entities of the system during some or all of the period [*date*] to [*date*] for processing their transactions [*or identification of the function performed by the system*]. The criteria we used in making this assertion were that the description
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including
 1. the classes of transactions processed.
 2. the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system.
 3. the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system.
 4. how the system captures and addresses significant events and conditions, other than transactions.
 5. the process used to prepare reports or other information provided to user entities of the system.
 6. specified control objectives and controls designed to achieve those objectives.
 7. other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
 - ii. does not omit or distort information relevant to the scope of the [*type or name of*] system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the [*type or name of*] system that each individual user entity of the system and its auditor may consider important in its own particular environment.



- b. the description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.
- c. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period [date] to [date] to achieve those control objectives. The criteria we used in making this assertion were that
 - i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;
 - ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
 - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Example 2: Assertion by Management of a Service Organization for a Type 1 Report

XYZ Service Organization's Assertion

We have prepared the description of XYZ Service Organization's [type or name of] system (description) for user entities of the system as of [date], and their user auditors who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when obtaining an understanding of user entities' information and communication systems relevant to financial reporting. We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the [type or name of] system made available to user entities of the system as of [date] for processing their transactions [or identification of the function performed by the system]. The criteria we used in making this assertion were that the description
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including
 1. the classes of transactions processed.
 2. the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system.
 3. the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports provided to user entities of the system.



4. how the system captures and addresses significant events and conditions, other than transactions.
 5. the process used to prepare reports or other information provided to user entities of the system.
 6. specified control objectives and controls designed to achieve those objectives.
 7. other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
- ii. does not omit or distort information relevant to the scope of the [*type or name of*] system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the [*type or name of*] system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. the controls related to the control objectives stated in the description were suitably designed as of [*date*] to achieve those control objectives. The criteria we used in making this assertion were that
- i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization.
 - ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.