

Insights on IT risk
January 2010

Planning for the new service organization reporting standards





With few significant modifications since it was issued in April 1992, SAS 70 has served the needs of service organizations, user entities and user auditors to report on the effectiveness of service organizations' internal control over financial reporting. While the importance of effective controls and reporting processes remains more critical than ever, globalization and regulatory changes have prompted the issuance of two new standards that combine to supersede SAS 70.

Service organizations are wondering how the new standards affect their business and what they need to do to prepare to implement them.



The New Standards – ISAE 3402 and SSAE 16

In December 2009, the International Auditing and Assurance Standards Board (IAASB) issued International Standard on Assurance Engagements ISAE 3402, *Assurance Reports on Controls at a Service Organization*. ISAE 3402 creates an international standard to address “engagements undertaken by a professional accountant to report on the controls at a third-party organization that provides a service to user entities when those controls are likely to be part of user entities’ information systems relevant to financial reporting.”

In January 2010, the American Institute of Certified Public Accountants (AICPA) Auditing Standards Board issued Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization*, that is substantially similar to the international standard and supersedes Statement on Auditing Standards No. 70, *Service Organizations (SAS 70)*.

These two standards are referred to here as “the New Standards.” The New Standards are effective for reports for periods ending on or after 15 June 2011, with early adoption permitted. Because many reporting periods cover 12 months and begin in July, the New Standards will affect many organizations as early as 1 July 2010.

While similar to SAS 70, the New Standards will require changes to service organizations’ reporting processes and reports. For some service organizations, these changes will be relatively minor. For others, significant efforts will be required to change their reports, reporting processes or both. To determine the impact and how best to plan for and implement the New Standards, service organizations need to understand:

- ▶ Reasons for the New Standards
- ▶ Service organization responsibilities under the New Standards
- ▶ Changes to service auditor responsibilities under the New Standards
- ▶ Impact on reports with inclusive subservice organizations
- ▶ Action steps to implement the New Standards

Reasons for the New Standards

While SAS 70 has worked well for many years, a number of factors drove the need for the New Standards, including:

- ▶ **Globalization of business process outsourcing.** Business process outsourcing has grown from regional shared service organizations created by specific industries to multinational and local organizations serving many different industries for a mixture of local, regional and international organizations. As a result, the information required in a SAS 70 report may no longer be sufficient for user entities.

- ▶ **SAS 70 is a US standard.** While SAS 70 is used globally, it is a US standard and engagements must be performed in accordance with the AICPA US Auditing Standards. Consequently, current reports may not respond to the needs of user entities and their auditors outside the US.
- ▶ **Service organization’s report versus service auditor’s report.** SAS 70 was developed as an auditor-to-auditor communication, a way for the service auditor to share audit workpapers with the user auditor, who then could rely on this work in planning and executing the financial statement audit. However, the regulatory landscape has seen significant changes, and governments, regulators, boards of directors and financial statement users are placing ever-increasing emphasis on internal control over financial reporting. These stakeholders, as well as the user auditors, now need a report from and by the service organization describing its internal control. This, in turn, significantly increases the importance of management’s description of its system. The independent service auditor’s opinion remains critical, but its role is as a provider of assurance, not the entity responsible for the communication.

Service organization responsibilities under the New Standards

Under the New Standards, service organizations have five primary responsibilities:

1. Prepare and present a complete and accurate description of the system
2. Specify the control objectives of the system and state those control objectives in the description of the system
3. Identify the risks that threaten the achievement of the control objectives (although these risks are not included in the service organization report)
4. Design, implement and maintain controls to provide reasonable assurance that the control objectives will be achieved
5. Provide a written assertion to accompany the description as to the completeness and accuracy of the information provided and state the criteria used as a basis for making the assertion

The following responsibilities represent the most significant changes from SAS 70.



Describing the service organization's system

Under SAS 70, a service organization provides a "description of controls." Under the New Standards, a service organization provides a "description of its system" as designed and implemented. While the term "system" has many different definitions, a common and useful definition is "the procedures, people, software, data and infrastructure organized to achieve a specific objective." Controls are only one aspect of a system so the New Standards require a broader management description. Under the New Standards, the service organization's description of its system includes:

- ▶ **Description of the services provided, including classes of transactions processed.** This description should contain a sufficient level of detail to permit the user to understand the nature of the services provided. For service organizations that process transactions for user entities, a description of the classes of transactions processed and should provide the ability to identify a user entity's significant accounts to which the transactions are posted. The description of the services provided should provide the ability to identify the significant user entity processes that are affected by the services (e.g., payroll expenses, cash disbursements, accounts payable and payroll tax reporting for the payroll function). For service organizations that provide IT platform and infrastructure services, the description should include the IT and other services that the user entities are likely to find significant.
- ▶ **Description of the procedures by which services are provided, including transaction initiation, authorization, recording, processing and correction.** The description of the system should provide an understanding of the flow of transactions or activities from start to finish, as well as the processes by which information errors are corrected.
- ▶ **Description of the capturing of significant events and conditions other than transactions.** The description of the system should enable the identification of other types of events and conditions that affect the processing of transactions and services, such as information technology general controls.
- ▶ **Description of the process used to prepare reports or information provided to user entities.** The reports provided to user entities are often key components of a user entity's financial reporting and controls. A description of the process used to prepare reports and provide information relates the other controls in the report to the transactions reflected in the financial statements and the information that user entity management relies on to run the business.

The above requirements are in addition to the requirements that previously existed in SAS 70:

- ▶ Description of control objectives and related controls, including complementary user entity controls.

- ▶ Description of aspects of the service organization's control environment, risk assessment process, information and communications systems, control activities and monitoring controls. These aspects, which follow the elements of the COSO Internal Control Framework, are the most common means to articulate controls that achieve the control objectives.

Other responsibilities

- ▶ **Providing a written assertion in the report.** The most visible difference between a report prepared under SAS 70 and a report prepared under the New Standards is management's written assertion. Similar to management's assertion report on internal control over financial reporting in an integrated financial audit, the assertion is a separate component of the report, typically on the service organization's letterhead and signed by a member of management. The assertion communicates:
 - ▶ Service organization management's responsibility for the description of the system
 - ▶ The achievement of the evaluation criteria for the report – standards used by the service auditor to provide its opinion.
- ▶ **Identifying risks that threaten the achievement of the control objectives.** The New Standards require the service organization to support its assertion by:
 - ▶ Identifying the risks that threaten the achievement of the control objectives
 - ▶ Determining whether the controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives from being achieved

Note that these risks do not need to be described or otherwise identified in the service organization's description of the system.

While many SAS 70 reports contain descriptions that meet most or all criteria of the New Standards, others that focus only on the minimum requirements of SAS 70 may require substantial additional descriptions.



Changes to service auditor responsibilities under the New Standards

The service auditor's responsibilities under the New Standards do not change as dramatically as the service organization's responsibilities. However, there are several changes that service organizations and user entities should understand.

Moving the standard from an audit standard to an assurance/attestation standard. SAS 70 is a US auditing standard, whereas ISAE 3402 is part of the IFAC assurance standards and the new SSAE is part of the AICPA attestation standards. This technical change was made to help service auditors by eliminating certain inconsistencies and ambiguities that resulted from mixing the service organization reporting standard with financial audit guidance.

Using the work of internal audit. Like SAS 70, the New Standards permit the service auditor to use the work of an internal audit function. The use must comply with the requirements in the New Standards that provide guidance to the service auditor.

The major change in the use of the work of internal audit is that for Type 2 reports the service auditor is required to describe the work performed by the internal audit function, as well as the procedures used to test that work. How this information is presented is not prescribed. The description can be provided in one of two ways:

- ▶ Using a narrative description summarizing the processes tested by internal audit, the nature of the work performed and the procedures performed by the service auditor to test that work. This description can be provided in the introduction to the service auditor test section
- ▶ Attribution of individual tests in the service auditor's testing section of the report to internal audit, along with a description of the specific procedures performed by the service auditor to test the work of internal audit

When internal auditors provide direct assistance to the service auditor and that assistance is planned and supervised by the service auditor, the assistance need not be disclosed.

The impact on reports with inclusive subservice organizations

A subservicer is a service organization used by another service organization. Similar to a SAS 70, under the New Standards the "carve-out" and "inclusive" methods are still available for dealing with services provided by subservice organizations in the report.

If a service organization wishes to include a description in the report of a subservice organization's role and controls (inclusive method), the subservice organization must prepare a management assertion report similar to the assertion report prepared by the service organization's management. Getting subservice organization management to agree to provide this assertion may be more difficult than obtaining a letter of representations. (Note: a letter of representations from the subservice organization is still required.) This is even more likely to be a challenge when the subservice organization is a small unit of a much larger organization.

Action steps to help your company implement the New Standards

Determine the implementation date for the adoption of the New Standards

The New Standards are required to be adopted for periods ending 15 June 2011, with earlier adoption permitted. Service organizations should consider the potential benefits of early adoption. Consider whether:

- ▶ Non-US user entities have a preference for reports issued under the international standard
- ▶ Market benefits exist for early adoption of the New Standard
- ▶ Benefits exist for delaying adoption costs by waiting until the New Standards are effective

Determine whether subservice organizations will be treated under the inclusive method

If a current SAS 70 report uses the inclusive method for one or more subservice organizations, early discussions with the subservice organization(s) are critical. An assertion report from subservice organization management may be difficult to obtain. Early communication with subservice organization management will reduce the risk of the subservice organization refusing to provide an assertion report when the final report is issued.



Key steps in this activity include:

- ▶ **Determine whether all subservice organizations that affect user entities' financial statements have been identified.** A careful review of processes will occasionally identify subservice organizations that have not been identified in prior reports or new subservice organizations.
- ▶ **Determine whether any of the subservice organizations have existing service organization reports (prepared under either SAS 70, the New Standards or other acceptable standard) or would be willing to provide one to your customers.** If a subservice organization has an acceptable report for the services it provides to you and your customers, it is usually cheaper and easier to provide your customers with a copy of the subservice organization's report and limit your report to only your processes.
- ▶ **Discuss your reporting strategy with your subservice organization.** You will need the assistance and cooperation of your subservice organization whether you are using the inclusive method or packaging a copy of the service organization's report along with yours. Obtain agreement with your subservice organization regarding this strategy, and get this agreement in writing. You may be able to include the commitments in the service agreement if the agreement is renewed between now and your implementation date, or you may need to prepare an addendum to the agreement. In addition, you may need to educate your procurement personnel on the new requirements and your strategy to ensure the contracts contain the appropriate language.
- ▶ **If you are a subservice organization, discuss with the primary service organization how the needs of their clients will be met.** Using the carve-out approach, a separate report can be issued. If the inclusive method is used, the subservice organization will need to provide a description of its system, a management assertion and a written representation letter. Discuss these matters with your service organization clients to better understand their needs and strategies.

Develop a change management plan for dealing with your clients

Your service organization report is one part of your service portfolio. The term "SAS 70 report" has become the generic term for service organization reports and has developed its own brand identity. However, as of the effective date of the New Standards, SAS 70 will be superseded. In preparing for the New Standards you should consider:

- ▶ How you will communicate the changes in the New Standards to your clients. Multiple communications may help them understand the nature of the change, including a cover letter attached to the first report issued under the new standard explaining the change. If you do not early-adopt the New Standards in 2010, you should consider communicating your implementation plans in the 2010 report.
- ▶ Review your standard contracts to determine whether the term SAS 70 is used. Consult with your legal counsel regarding any required changes and assess the impact on existing contracts.
- ▶ Make sure that your sales and client service personnel understand the pending change and its impact to your clients. Their ability to explain the change can reduce client confusion and uncertainty.

Review your system description and identify any necessary changes

As mentioned, many existing SAS 70 reports will need only minor modifications to comply with the New Standards, but some reports will require extensive modification. In updating your reports for the New Standards, you should:

- ▶ Identify the criteria used to evaluate the description of the system. While the standard sets minimum criteria for the description, other criteria may be appropriate. Consult with your service auditor as part of this process.
- ▶ Evaluate your current report using your criteria and identify required changes to your description. Consider whether it may be cost-effective to phase in the changes to the report now and the effective date of the New Standards.
- ▶ Consider preparing all new reports using your criteria. A report prepared using the minimum description criteria required by the New Standards can be used for a SAS 70 report. If a report will be issued on a recurring basis through at least 2011, consider drafting the system description so that it will not need to be updated for the New Standards.



Identify assertions regarding suitability of design and operating effectiveness

The minimum criteria include requirements regarding assertions about whether:

- ▶ The risks that threaten the achievement of the control objectives stated in the description have been identified
- ▶ The identified controls would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved
- ▶ The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority

While making these assertions may require additional procedures, service organizations should consider that most of these criteria are met by their existing procedures as part of their service-level agreement and quality processes. However, because of the ability to rely on existing processes, you should plan to identify the processes that support these assertions early in your adoption process. In doing so, consider the following:

- ▶ **Review your control objectives.** Control objectives describe the objectives of the services you provide and the manner in which you provide them. They should focus only on those aspects of your services that can affect your clients' financial statement assertions. Consider whether your control objectives are complete, and evaluate whether all of them are necessary.
- ▶ **Use your risk assessment process.** Most organizations perform regular risk assessments, either formally or informally. These risk assessments address both financial and operating risks, including risks of not meeting service-level agreements. During your next risk assessment, consider the risks associated with the control objectives and determine whether any additional risks exist. One effective way to help you identify risks is to ask what could go wrong. Remember that risks should be reasonably possible to receive consideration during this process. To help reduce costs in future years, make sure to document your considerations.
- ▶ **Compare the controls you have identified in your current SAS 70 to the risks.** Each of the risks identified above should be addressed by one or more controls at your organization, or by controls that you believe should be in place at a user entity. If a risk has not been addressed in your prior report, look for existing controls rather than immediately implementing a new control. Your service auditor can assist you with this effort.

- ▶ **Consider how you know that the controls are consistently applied as designed.** For the controls identified above, you need to be able to assert that the controls were operating effectively. The basis for making this assertion should be separate from work that has been or will be performed by the service auditor.

Most service organizations have many processes to monitor the services provided to their clients. Often your control environment, monitoring, and information and communication controls provide sufficient evidence as to the application of controls. These include:

- ▶ Supervisory review of control procedures
- ▶ Management oversight
- ▶ Quality assurance programs
- ▶ Management reports
- ▶ Service-level agreement reporting
- ▶ Regular internal audits
- ▶ Complaint/incident management

These processes, individually or in combination, may provide sufficient evidence to determine that the controls were applied consistently as designed. Compare your existing processes to the list of controls in your current report to prepare for reporting under the New Standards.

- ▶ **Leverage your Sarbanes-Oxley compliance testing.** Some controls in scope for Sarbanes-Oxley compliance address your own financial reporting risks as well as the control objectives for services you provide to your clients. To the extent possible, reuse and rely on these efforts for both your Sarbanes-Oxley compliance and your service organization report assertion.
- ▶ **Avoid direct testing of controls.** Direct testing of controls, while an appropriate basis for making your assertion, is often costly and may provide limited benefit. Restrict the use of direct testing to only those controls for which you can find no other basis for making an assertion. Before performing direct testing ask: if this control is critical to achieving the control objective and consequently proper client service, why is its effectiveness not already monitored? Usually the answer to this question is one of the following:
 - ▶ An unidentified monitoring process helps ensure that the control is functioning
 - ▶ The risk that the control addresses has been assessed incorrectly or another control is more effective at addressing the risk
 - ▶ The control is periodically failing but the failure is not being detected, or if detected, the problem management process has not identified the control failure as a contributing cause of problems

Only in the last case is direct testing necessary, and usually additional monitoring should be implemented to reduce the risk of control failure. In future periods, this monitoring can replace direct testing.



Develop a project plan

Like any significant project, proper project management is a key enabler of efficient and effective implementation of the New Standards. Your project management process can be used to help achieve these goals. We are including a checklist to help you develop a project plan.

Conclusion

While SAS 70 met the needs of service organizations and user organizations for many years, the New Standards represent a needed evolution to increase the usefulness of service organization reports in the future. Your company can be well-prepared to implement the New Standards and serve your clients with minimal disruption while controlling the costs of adoption by understanding:

- ▶ Reasons for the New Standards
- ▶ Service organization responsibilities under the New Standards
- ▶ Changes to service auditor responsibilities under the New Standards
- ▶ Impact on reports with inclusive subservice organizations
- ▶ Action steps required to implement the New Standards

We encourage you to monitor development of both New Standards to take the actions necessary to achieve your goals.

New service organization reporting standards planning checklist

- ☑ Make a preliminary decision on whether to wait until the effective date or adopt early
- ☑ If you rely on subservice organizations, determine whether you plan to use the inclusive method:
 - ▶ Determine whether your subservice organizations currently have an appropriate SAS 70
 - ▶ Discuss the plan for an inclusive report with subservice organization leadership
 - ▶ Modify your service agreements as needed
- ☑ Review and modify your customer contracts:
 - ▶ Review your standard contract to see if the language is sufficiently flexible to permit the provision of reports under the New Standards
 - ▶ Evaluate whether existing customer contracts will need to be amended to address the change in the standards
- ☑ Brief sales and client handling teams on the New Standards and your approach to adopting them so they can have informed conversations with clients and targets
- ☑ Develop a communication plan for your customers:
 - ▶ Identify your communication channels and develop a plan for communicating with them repeatedly
 - ▶ Those not adopting early may wish to inform customers of the pending changes for 2011 when they issue their 2010 reports under the current standards
 - ▶ Inform your personnel about the pending changes so that they are not caught unaware
- ☑ Draft new reports using the New Standards
 - ▶ Identify your evaluation criteria
 - ▶ Review your current description of controls and consider whether it addresses the criteria
 - ▶ Review your control objectives
 - ▶ Update your risk assessment process as necessary
- ☑ Compare your current controls to the risk assessment
- ☑ Identify your basis for knowing that your controls are functioning and that you are serving your customers in accordance with contractual terms
- ☑ Develop a formal project plan for issuing reports under the New Standards

About Ernst & Young

At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that every need and issue is unique to that business.

Information technology is one of the key enablers for modern organizations to compete. It gives the opportunity to get closer, more focused and faster in responding to customers, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective information technology risk management helps you to improve the competitive advantage of your information technology operations to make these operations more cost-efficient and to manage down the risks related to running your systems. Our 6,000 information technology risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your information technology risk or to deal with a specific risk and information security issue. We understand that to achieve your potential you need a tailored service as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or any of the people listed in the table below.

Contacts

| Global | | |
|---|--------------------|-------------------------------|
| Paul van Kessel (IT Risk and Assurance Services Leader, Amsterdam) | +31 88 40 71271 | paul.van.kessel@nl.ey.com |
| IT Risk and Assurance Services | | |
| Bernie Wedge (Americas Leader, Atlanta) | +1 404 817 5120 | bernard.wedge@ey.com |
| Paul van Kessel (Europe, Middle East, India and Africa Leader, Amsterdam) | +31 88 40 71271 | paul.van.kessel@nl.ey.com |
| Troy Kelly (Far East Leader, Hong Kong) | +81 2 2629 3238 | troy.kelly@hk.ey.com |
| Giovanni Stagno (Japan Leader, Chiyoda-ku) | +81 3 3503 1100 | stagno-gvnn@shinnihon.or.jp |
| Iain Burnet (Oceania Leader, Perth) | +61 8 9429 2486 | iain.burnet@au.ey.com |
| Service Organization Reporting | | |
| Chris Halterman (Global and Americas, Des Moines) | +1 515 362 7026 | chris.halterman@ey.com |
| Herbert Engelbrecht (Europe, Middle East, India and Africa, Stuttgart) | +49 711 9881 14579 | herbert.engelbrecht@de.ey.com |
| Jerry Wertelecky (Far East, Hong Kong) | +85 2 2629 3598 | jerry.wertelecky@hk.ey.com |
| Ryan Loughins (Japan, Chiyoda-ku) | +81 3 3503 1100 | loughins-ryn@shinnihon.or.jp |
| Susan Steedman (Oceania, Sydney) | +61 2 9248 4392 | susan.steedman@au.ey.com |



About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 144,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

For more information, please visit www.ey.com.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

The Ernst & Young organization is divided into five geographic areas and firms may be members of the following entities: Ernst & Young Americas LLC, Ernst & Young EMEA Limited, Ernst & Young Far East Area Limited and Ernst & Young Oceania Limited. These entities do not provide services to clients.

About Ernst & Young's Advisory Services

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 18,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2010 EYGM Limited.
All Rights Reserved.

EYG no. AU0430

www.ey.com



In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.