



SAS 70 Reports: Are They Useful and Can They Be Improved?

**AGA CPAG Research Series:
Report No. 15
July 2008**

ACKNOWLEDGEMENTS

About the Authors and Research

Anna D. Gowans Miller, MBA, CPA, was the primary researcher for this project. Miller has been with the Association of Government Accountants (AGA) since early 2004 and is currently the AGA Director of Research. She started her auditing career with Touche Ross (now Deloitte & Touche) in Houston, TX, and later was an auditor with the Corporation for Public Broadcasting in Washington, D.C. She served as technical manager for the Government Accounting and Auditing and Members in Government Committees at the AICPA in Washington, D.C. and as professional staff with responsibility for financial management and business improvement oversight for the U.S. House of Representatives Government Reform and Oversight Committee.

Views expressed in this report are those of the author and are not necessarily the views of AGA.

AGA wishes to thank **Werner Lippuner** and **James Merrill**, both with Ernst & Young LLP, for their valuable contributions to this research study.

AGA is Proud to Recognize the Firm Supporting this Effort:



Corporate Partner Advisory Group Leadership

Chairman

Hank Steininger, CGFM, CPA

Managing Partner, Global Public Sector,
Grant Thornton LLP

Vice Chairman

John Cherbini, CGFM, CPA
Partner, KPMG LLP

AGA Professional Staff

Relmond Van Daniker, DBA, CPA

Executive Director

Anna D. Gowans Miller, MBA, CPA

Director of Research

Susan Fritzlen

Director of Corporate Partner Program

Marie Force

Director of Communications

Christina Camara

Publications Manager

AGA's Corporate Partner Advisory Group Research Program: Building the Bridge Between Government and Industry

AGA's Corporate Partner Advisory Group (CPAG), executive director and director of research are creating research projects of value to governments, industry and the entire AGA membership. These studies are expected to result in reports assessing current and/or best practices and make recommendations for future improvements in federal, state and local governmental accounting, auditing and financial management. CPAG members support AGA research through either cooperative or sponsored research projects. "By undertaking research, AGA is fulfilling its mission as a thought leader in advancing government accountability," said AGA Executive Director Relmond Van Daniker, DBA, CPA. "This is one of numerous research initiatives that will benefit government and bridge the gap between the public and private sectors."

The CPAG was organized in 2001 as a business element within AGA. The mission of the CPAG is to bring industry and government executives together to exchange information, support professional development, improve communications and understanding, solve issues and build partnership and trust, thereby enhancing AGA's focus on advancing government accountability. Corporate member involvement in the CPAG is limited to organizations that sign up for the AGA Corporate Partner membership program. For more information on the research program, please visit www.agacgfm.org/research/default.aspx or contact Anna Miller at amiller@agacgfm.org.

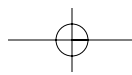
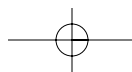


TABLE OF CONTENTS

Executive Summary	4
Introduction	5
Background	5
Key Findings	5
Recommendations	6
Thoughts for Future Consideration	6
Literature Review and Existing Accountability	6
Primary Audit Standards	6
Use of SAS 70 in Government	7
Other Governmental Audit Guidance	8
Survey Methodology and Overview of Analysis	8
Discussion of Results	9
Conclusion	12
Appendices	
Appendix A: Future State of SAS 70 Versus International Standards	13
Appendix B: References.	15
Appendix C: Outline of an SAS 70 Report	15
Appendix D: Survey Instrument	16



SAS 70 REPORTS: ARE THEY USEFUL

Executive Summary

This research paper addresses the usefulness to governments of the American Institute of Certified Public Accountants' (AICPA) Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, and whether improvements to the implementation of the standard could increase its usefulness. AGA and Ernst & Young LLP, the AGA Corporate Partner sponsoring this project, thought it was important and timely to review how SAS 70 reports are being used and whether they could be made more useful. The passage of the Sarbanes-Oxley Act caused an increase in use of SAS 70 reports as a way to better evaluate the control environment for outsourced functions. The AICPA is considering revisions to SAS 70 and the International Federation of Accountants has issued two exposure drafts for new international standards that are very similar in scope to SAS 70. Key findings of the research are:

- Service organizations, the subject of SAS 70 reports, are now a critical part of some user organizations' overall system of internal control over financial and operational reporting.
- SAS 70 reports are generally accepted as a method of communicating information and assurance about the controls that are of interest to the user organizations and their auditors as they relate to an audit of the financial statements.
- Generally, user organizations in government do not have significant input to the scope or systems to be covered by the SAS 70 report. The service organization usually determines the scope based on its contracts with the user organizations and/or discussions with individual user organizations or auditors.
- User organizations do not always have the skill set to understand or analyze the impact of the conclusions drawn or exceptions reported in the SAS 70 report. This could lead to misinterpreted results and unwarranted reliance upon a SAS 70 report that in fact may include reporting on a deficiency or other control weakness in the service organization's controls.
- User organizations do not always obtain the information they need from the SAS 70 report. The controls tested by the service organization's auditor may not be those that are considered important by the user organization; this appears to be especially true for information technology (IT) controls.
- Clarity is needed to differentiate between governmental audit standards and laws and regulations versus the standards issued by commercial and private auditing organizations such as the AICPA.

The research shows that the usefulness of SAS 70 reports could be improved by implementing the following recommendations:

- Understand the differences between the various federal audit guidelines that make reference to SAS 70 reports as a component of obtaining an understanding of an entity's system of internal control.
- Obtain training, if necessary, in the use and reading of SAS 70 reports, and understand where SAS 70 reports may not be appropriate.
- User organizations should be actively involved in a timely fashion in setting the appropriate scope for the SAS 70 report to enhance the report's usefulness.
- Service organizations should provide more outreach programs to educate their user organizations and auditors as to the content of their SAS 70 reports and the reasons for the particular report's scope.

Finally, as user organizations continue to use service organizations for financial processing functions, it is important to:

- Be aware of audit standards other than SAS 70 that may be appropriate for obtaining information and/or assurance about a service organization's controls.
- Be aware of potential and planned changes in the relevant professional standards that will enhance the overall concept of the service auditor's report from the SAS 70 examination level report to an attest report where management of the service organization will assert to their controls as a component of the audit report.

We hope that this research will provide information useful to auditors, organization management and standards-setters alike.

AND CAN THEY BE IMPROVED?

Introduction

This research effort focuses on how auditors' reports conducted in accordance with the American Institute of Certified Public Accountants' (AICPA) Statement on Auditing Standards No. 70, *Service Organizations* (SAS 70), are used and understood in a government environment. In the summer of 2007, AGA with the support of Ernst & Young LLP, an AGA Corporate Partner, decided that the topic was a timely one to be researched, considering that revisions to SAS 70 were being planned and the international standards-setters were developing guidance similar to that of SAS 70. AGA's Director of Research was the primary researcher, aided by subject matter experts from Ernst & Young who helped in identifying the interviewees, analyzing the results and developing the literature review and other sections of the report. The project consisted of three parts:

- a series of face-to-face and telephone interviews of selected users and auditors (both user auditors and SAS 70 auditors) at both the state and federal level;
- an Internet survey with numerous users intended to gauge the use of and understanding of SAS 70 reports in government, and;
- analysis of the results of the survey and the writing of this report.

Background

Today, the services of third-party service organizations are a critical part of some entities' overall system of internal control for financial and operational reporting. When an entity obtains an audit of its financial statements, the auditor must obtain an understanding of the entity's internal control system and how it is operating. If an entity obtains services from a third-party service organization, this has an impact on the entity's control environment.

What is the best way to ensure that the entity's auditors obtain an adequate understanding of the service organization's control environment? For more than 25 years, standards-setters have focused on just how best to do this. The guidance currently available in the United States is in Statement on Auditing Standards (SAS) 70, *Service Organizations*, issued by the American Institute of Certified Public Accountants (AICPA) in April 1992. SAS 70 is intended for all entities that use a service organization for processing

transactions and maintaining related accountability and/or for recording transactions and information processing. It provides guidance to the auditor of the organization using the service (user auditor) and the auditor of the organization providing the service (service auditor). From the start, certain difficulties were perceived by practitioners.¹

However, when the standard was finally developed, the consensus was that in spite of the perceived difficulties shown in *Figure 1*, the guidance in SAS 70 should not be changed markedly from that in SAS 44. Currently, an AICPA task force is examining revisions to SAS 70, and the International Federation of Accountants' International Auditing and Assurance Standards Board has exposed two documents for public comment. One contains proposed guidance for the auditor of the service organization or service center; the other for the auditor of the entity (also called the user organization).

Service organizations are quite common in a governmental environment and are sometimes known as shared service providers or centers of excellence. They can be either internal governmental organizations or outside commercial organizations providing services to the state or federal user. The services provided can range from one particular function to replacing entire business units. Shared service providers or centers of excellence have been especially encouraged in the federal government environment in the past several years. They are seen as a way to reduce the costs of updating expensive computerized systems for financial management and reporting, reduce the number of disparate accounting systems, and create more efficient record-keeping and reporting. The objectives of this research effort are to determine how SAS 70 is being used in a government environment, what the problems are, if any, and how the guidance can be improved.

Key Findings

Results of the research show that:

- Service organizations, the subject of SAS 70 reports, are a critical part of some user organizations' overall system of internal control for financial and operational reporting. In a government environment, service organizations can be either internal governmental organizations or outside commercial organizations providing services to the state or federal user.

Figure 1: Difficulties with SAS 70 Reports

- The service center auditor will only review the controls selected by the service center for review.
- The service auditor will make a single, overall evaluation rather than a control-by-control evaluation, while the user auditor has to make risk assessments evaluations assertion by assertion.
- A control considered effective by the service auditor may not be considered effective by the user auditor or vice versa. A control-by-control evaluation would

provide the user auditor with better information on which to make risk assessments than would an overall opinion.

- The controls selected for review by the service organization may not include a control that may be considered critical by the user auditor.
- The scope of the service center auditor's testing may not be sufficient for the user auditor's purpose.

SAS 70 REPORTS: ARE THEY USEFUL

- SAS 70 reports are generally accepted as a method of communicating information and assurance about the controls that are of interest to the user organizations and their auditors as they relate to an audit of the financial statements. The reports have been used for more than 10 years. Use of SAS 70 reports has grown since the passage of the Sarbanes-Oxley Act.
- Generally, user organizations in government do not have significant input into the scope or systems to be covered by the SAS 70 report. The service organization usually determines the scope based on its contracts with the user organizations and/or discussions with individual user organizations or auditors.
- User organizations do not always have the skill set to understand or analyze the impact of the conclusions drawn or exceptions reported in the SAS 70 report. This could lead to misinterpreted results and unwarranted reliance upon a SAS 70 report that in fact may include reporting on a deficiency or other control weakness in the service organization's controls.
- User organizations do not always obtain the information they need from the SAS 70 report. The controls tested by the service organization's auditor may not be the ones considered important by the user organization; this appears to be especially true for information technology (IT) controls. However, little additional work is performed to compensate for the apparent lack of coverage in the SAS 70 report.
- Clarity is needed to differentiate between governmental audit standards and laws and regulations versus the standards issued by commercial and private auditing organizations such as the AICPA.

Recommendations

The research shows that the usefulness of SAS 70 reports could be improved by implementing the following recommendations:

- Understand the differences between the various federal audit guidelines that make reference to SAS 70 reports as a component of obtaining an understanding of an entity's system of internal control.
- Obtain training, if necessary, in the use and reading of SAS 70 reports, and understand where SAS 70 reports may not be appropriate.
- User organizations should get actively involved in a timely fashion in setting the appropriate scope for the SAS 70 report to enhance the report's usefulness.
- Service organizations should provide more outreach programs to educate their user organizations and auditors as to the content of their SAS 70 reports and the reasons for the particular report's scope.

Thoughts for Future Consideration

As organizations continue to use service organizations for financial processing functions, it is important to:

- Be aware of audit standards other than SAS 70 that may be appropriate for obtaining information and/or assurance about a service organization's controls. Examples include agreed-upon procedures reports and reports conducted in accordance with consulting standards, commonly known as findings and recommendations reports; such reports do not have an auditor's opinion on the suitability of design of or operating effectiveness of the relevant controls, but can be useful to a user organization and their auditor in planning an audit.
- Be aware of potential and planned changes in the relevant professional standards that will enhance the overall concept of the service auditor's report from the SAS 70 examination level report to an attest report where management of the service organization will assert to their controls as a component of the audit report. See Appendix A for a discussion of new international standards that will have an impact on future standards-setting activities in the United States.

Literature Review and Existing Accountability

Primary Audit Standards

Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, is included in Volume 1 of the Professional Standards of the American Institute of Certified Public Accountants (AICPA). It was initially issued in April 1992 and became effective after March 31, 1993. It replaced SAS 44, *Special-Purpose Reports on Internal Accounting Control at Service Organizations*, which had been issued 10 years before. SAS 70 brought a number of new concepts to reports on internal control, one of which was the coverage of a period of time by an independent service auditor, as compared to the one-day SAS 44 and SAS 30 reports in use at the time. SAS 70 provided for two basic types of reports as follows:

- Type I report—an auditor's opinion on the suitability of design and the description of controls placed in operation at a specific point in time.
- Type II report—includes the auditor's opinion on the suitability of design and the description of controls placed in operation at a specific point in time and includes the auditor's opinion on the results of testing the operating effectiveness of the controls for a period of time, generally not less than six months.

Each type of report may be useful in specific situations. Generally, Type II reports are more useful than Type I reports, because they cover a period of time rather than a point in time, and as a result are more commonly found in practice today. Type I reports may be useful in an initial evaluation of a service center by a potential user.

Certain basic terms are defined in the AICPA's Audit Guide, *Service Organizations*, Section I-08:

AND CAN THEY BE IMPROVED?

- *User organization.* The entity that has engaged a service organization and whose financial statements are being audited.
- *User auditor.* The auditor who reports on the financial statements of the user organization.
- *Service organization.* The entity (or segment of an entity) that provides services to a user organization that is part of the user organization's information system.
- *Service auditor.* The auditor who reports on controls of a service organization that may be relevant to a user organization's internal control as it relates to an audit of financial statements.

Since its release, SAS 70 has been amended several times by the AICPA; changes were made based on other developments in the audit profession related to internal control, such as the COSO (Committee of Sponsoring Organizations of the Treadway Commission) internal control report², the advent of the Sarbanes-Oxley Act in 2002³, and other refinements that were made to improve the content of an SAS 70 report. Because SAS 70 reports became increasingly more complicated in the 1990s, the AICPA began to provide more detailed guidance than that found in the standard itself in the form of audit releases. In the early 2000s, the AICPA began issuing SAS 70 guidance in the form of an industry audit guide, titled *Service Organizations*.

Today, the SAS 70 audit guide is generally released annually and reflects various outside influences and activities, such as further refinement of the Sarbanes-Oxley legislation by the Securities and Exchange Commission (SEC), additional Public Company Accounting Oversight Board (PCAOB) guidance for registered public accounting firms, and additional AICPA standards and guidance related to internal control. It is important to note, however, that updated audit and accounting guidance from both the U.S. Government Accountability Office (GAO) and the Office of Management and Budget (OMB) has had little influence on these changes to the SAS 70 literature.

Other standards-making bodies in other countries have issued audit standards that are similar to SAS 70. The Canada Institute of Chartered Accountants introduced new assurance standards dealing with Service Organizations in the form of Sections 5970 and 5310. Section 5970 provides guidance to service auditors reporting on controls at a service organization and Section 5310 provides auditors with guidance on how to use Section 5970 as part of a financial statement audit. A year later, the Audit and Assurance Faculty of the Institute of Chartered Accountants of England and Wales introduced new assurance standards dealing with service organizations in the form of Technical Release AAF 01/06.

However, none of these have had the same level of acceptance as SAS 70. This is due in part to Sarbanes-Oxley federal legislation affecting U.S. public filers with overseas operations that use service organizations in locations outside the U.S. This means that for the performance of audits in accordance with existing U.S. audit standards, primarily

promulgated by the PCAOB for public filers, obtaining SAS 70s from service organizations in those countries has emerged as a de facto audit procedure. As a result of these activities, the use of SAS 70 has spread to numerous countries where the user organizations may not be public company filers, but SAS 70 has emerged as the de facto measure of control compliance for service organizations.

Today, SAS 70 reports are issued on every continent and have prodded country-specific audit and accounting standards-setting organizations to develop local audit standards that are similar to SAS 70. A partial list of these standards is included in an appendix to this report.

To address the inevitable overlap that arises from multiple similar standards, an initiative was started in 2007 by the International Auditing and Assurance Standards Board (IAASB), which operates under the auspices of the International Federation of Accountants (IFAC). The goal of the IAASB initiative is to issue two new international standards for reports on controls at service organizations. One of the two standards will be for user organizations and their auditors, while the second standard will be for service organizations and service auditors. The AICPA's SAS 70 Task Force is also looking at the matter and has issued exposure drafts to revise the standard.

In December 2007, the IAASB issued two exposure drafts: ISA 402, *Audit Considerations Relating to an Entity Using a Third Party Service Organization*, a proposed revised and redrafted international standard on auditing; and ISAE 3402, *Assurance Reports on Controls at a Third Party Service Organization*, a proposed international standard on assurance engagements. Comment deadlines were April 30, 2008 and May 31, 2008 respectively. While ISA 402 has a focus on third-party service organizations, the IAASB is of the view that it is also applicable to situations where an entity uses a shared service center that provides services to a group of related entities. The two proposed standards were developed concurrently to ensure that the reports issued under the new ISAE would meet the needs of a user auditor who would be applying proposed ISA 402 (revised and redrafted) and intending to use such a report. The IAASB believes that an assertion-based engagement and attest report is the appropriate model for its proposed standard, ISAE 3402. See Appendix A for more information on the IAASB's activities.

Use of SAS 70 in Government

Service organizations have been used in government for many years. Some of the key reasons for the recent increase in usage are:

- Increased need for efficient operations across multiple federal, state and local departments and agencies.
- Increased demands for standardized systems for financial reporting from the Congress and state legislatures.
- Ability to leverage existing commercial sector expertise and reduce costs.

SAS 70 REPORTS: ARE THEY USEFUL

- Ability to offload non-core systems to outsourcers to permit focus on business operations.

In government, service organizations exist in several forms:

- Within a department or an agency

Example: A data center supports operations for multiple agencies on a shared basis.

- Across department or agency lines

Example: A service organization in one department provides general ledger / payroll services not only to its own department but also to unrelated departments that can “purchase” the same service.

- External commercial organization

Example: A local government outsources its tax collection activities to a commercial organization that specializes in such systems.

- Multiple commercial and governmental service organizations supporting a common outsourced process

Example: Because of the size of the federal Medicare and Medicaid programs, multiple commercial and governmental service organizations are used to administer the programs.

Applying these definitions in government indicates that the likely candidates for outsourced services are repeatable, high-volume, routine business processes. Research conducted in accordance with this report identified the following outsourced services:

- General ledger/financial reporting
- Payments (accounts payable/purchasing)
- Payroll administration
- Medicare/Medicaid claims fiscal agents
- Pension/trust fund administration services
- Electronic benefit transfers (food stamps, for example)
- Highway toll collection systems
- General data processing centers
- Any IT services that are franchised as fee for service, for example data centers, general application development, ISS services, printing/audit visual services, telecom, help desk and wireless services.

It is important to note that the research indicated that most government user organizations are dependent upon multiple outsourced services to accomplish their business objectives. As a result, those who are responsible for financial auditing of these user organizations need to consider the impact of potentially multiple service organizations.

Other Governmental Audit Guidance

The increased presence of service organizations has caused certain rule-making organizations in government to recognize the presence and potential usefulness of SAS 70 reports. Specifically, OMB has included references to SAS 70 reports in its Circular A-133, *Compliance Supplement*, as it relates to audits conducted to support the Single Audit Act

for federal programs. For example, as it relates to the federal Medicaid program, of which about 40 percent is outsourced by the state governments to commercial third-party claims processors, OMB Circular A-133 (March 2007) specifically identifies SAS 70 reports in the audit planning phase as it relates to controls and IT security assessments, as follows:

“Review the State Medicaid agency’s policies and procedures, and document the frequency, timing, and scope of [automated data processing] ADP security reviews. This should include any reviews following Statement on Auditing Standards No. 70 (SAS 70) that may have been performed on outside processors.”

Other relevant OMB references to SAS 70 reports include:

- OMB Memorandum M-04-11 (April 30, 2004) recommends Type 2 SAS 70s be obtained for supporting financial management audits where transaction processing is outsourced. In M-04-11, OMB sought to indicate to user organizations and auditors that Type 1 reports may not provide the best way to determine the operating effectiveness of controls at the service organization since no testing of the controls has taken place.
- OMB A-123 references SAS 70s in connection with reviews conducted to comply with the Federal Information Security Management Act (FISMA) of 2002. Frequently, user organizations and their auditors have turned to SAS 70 reports as a method of obtaining information and assurance about information security control procedures at service organizations for FISMA compliance. Unfortunately, SAS 70 reports are not intended to include all of the required reporting elements of FISMA. OMB sought to clarify this in A-123 guidance to prevent unwarranted or inadvertent reliance upon SAS 70 reports as a substitute for FISMA testing.
- OMB A-133 references SAS 70s in connection with EBT testing.
- OMB Audit Guidance (Bulletin No. 07-04).

Survey Methodology and Overview of Analysis

Three different survey techniques were used to collect data related to the use of SAS 70s in government.

The first technique consisted of telephone interviews with certain state and federal groups, which included internal or legislative auditors, project administrators and controller/comptroller personnel.

The second technique consisted of a focused interview of certain federal and state organizations in proximity to the Washington, D.C. area. These interviews were structured around the questions contained in the Internet survey (discussed subsequently in this report). The AGA Director of Research was present at the majority of the interviews, which were with federal government agencies including oversight agencies, and state agencies and functions.

The third and final technique centered on an Internet-based survey of several groups of questions around the use of SAS 70 reports in government. The survey was open on the public Internet for about 60 days. About 100 surveys

AND CAN THEY BE IMPROVED?

were completed by individuals representing various federal, state, local and private organizations.

Analysis of Internet Survey Demographics

Figure 2 illustrates the breakdown of the respondents by type of organization. Figure 3 illustrates the categories of job responsibilities held by the survey respondents.

Figure 2: Percentage of Respondents

- Federal 19%
- State 47%
- Local 2%
- Non-public 15%
- Not Specified 17%

A total of 31 states and territories were represented in the survey.

Figure 3: Percentage of Categories of Job Responsibilities

- Users of SAS 70s 28%
- User Auditors 37%
- Service Auditors 8%
- Service Organizations 7%
- Not Specified 20%

The survey was designed such that certain questions were intended for certain types of respondents. Users and user organization auditors were asked to complete one section of the survey, a second section was intended for service organizations and the third section was intended for the service auditors (independent auditors that perform a SAS 70 project).

Generally, the respondents that were user organizations of the SAS 70 reports relied on the following general categories of content:

- General ledger processing
- Tax payments processing
- Payroll / pension administration
- Data center outsourcing
- Medicaid fiscal agent systems.

Discussion of Results

We analyzed the information collected about the use of SAS 70 reports in government from both the interviewees and the survey respondents. We noted a wide range of responses, which reflects the different backgrounds and interests of the respondent groups. However, several themes stood out and some of them echo the difficulties identified when SAS 70 was first issued (see page 5). These themes are discussed in this section in no particular order, as they are all relevant to the further understanding of SAS 70 reports

and the determination of whether their usefulness in government needs to be further enhanced.

Education on the SAS 70 Standard—Several responses indicated a need for further education, especially for user organization personnel. User organizations sometimes do not consider the need for a SAS 70 audit when contracting with a service organization; in fact the user organization may not be aware of the need for these audits. Respondents commented that they ask for them for the external auditor or because the external auditor requires the report. Some said they were getting more familiar with the reports; others said they are looking for potential audit use. One commented that at least one large private sector consulting firm needs to be better educated on the usefulness of SAS 70 reports, because it is an outspoken critic of the reports to many organizations, despite the SAS 70 reports' widespread and increasing global acceptance as an effective third-party assurance tool to service organizations. One interviewee stated the auditors do not use the SAS 70 reports they receive.

User organizations do not always understand the need for a SAS 70 report. More education is needed to ensure that user organizations are aware of the need for a SAS 70 report and that they request SAS 70 reports as part of the RFP⁴ process. One comment was, "No SAS 70s are performed specifically for the agency or its servers at its service provider, but sometimes we get coverage from reviews performed for other clients of the service provider. But it is uncertain for any particular year whether the agency has coverage."

User organizations do not always have the skill set to understand or analyze the impact of the conclusions drawn or exceptions reported in the SAS 70 report. This could lead to misinterpreted results and unwarranted reliance upon a SAS 70 report. A user organization may mistakenly rely on a report that in fact may include reporting on a deficiency or other control weakness in the service organization's controls. As one respondent said, "read the report." Another said, "Look at the details for any risks that you may need to address in your audit." Others thought that the reports were "too long and should be more concise. Users do not know what they are looking at."

Usefulness of SAS 70 Reports—Some found them very useful. There is a caveat here. Respondents found only Type II (see page 6) to be useful because they helped them understand the operating effectiveness of the controls. One user reported that "the SAS 70 reports required are essential to our review of pass-through entities utilizing service organizations to process payments for Medicaid and non-Medicaid payments of federal funds. We also have a SAS 70 organization processing many of our own grant payments to recipient agencies of state and local government." Another said, "This is a report that lets you know where or what you have to improve in order to be in compliance and reduce the risk of errors and inaccuracies that could affect the financial statements." One respondent's advice was, "Assure that only controls over financial reporting are

SAS 70 REPORTS: ARE THEY USEFUL

included in the description of control activities and that the service organization is educated on the difference between process and controls. Also, use the service level agreement, contract, or other controlling document to establish the control objectives and to keep them more focused.”

Service organizations respondents saw benefits from SAS 70 reports in that they reduced the need for multiple audits, increased the effectiveness of internal controls, and aided compliance with laws and regulations. They also saw problems with them. Since the scope is not consistent for SAS 70 audits based on customer assertions, competing providers are not on a level playing field. In addition, as long as FISMA regulations require independent assertions in the form of 800-53 audits, incorporating SAS 70 controls to meet the function is a duplication of effort, time and requirement. Another said the SAS 70 auditors are late and there were problems with the time it took to issue the report from the IG’s Office. We asked whether there had been problems with outside organizations asking for the report and not being given it, but most did not see this as a problem. One respondent noted that, “SAS 70 reports are not readily available to the user community.”

Perceived Problems with SAS 70 Reports—User auditors see several problems with SAS 70 reports. The service auditor will make a single, overall evaluation rather than a control-by-control evaluation, while the user auditor has to make risk assessment evaluations assertion by assertion. Also, the service center auditor will only review the controls selected by the service center for review. If the user auditor does not find this sufficient, he or she may have to do additional or alternative procedures to obtain information on which to make risk assessments. These two issues are still creating problems for user auditors as shown in Figure 4 below. They show the barriers that will have to be overcome before SAS 70 reports are truly useful.

Figure 4: Barriers to Usefulness

“Controls [in the SAS 70 report] not related to the financial statement assertions or compliance objectives.”

“Insufficient disclosure of the controls and testing completed to support the contention that the control is working as intended.”

“Insufficient internal control testing. Test more relevant controls and distribute to all users and their auditors.”

“Insufficient in-depth procedures performed and reported on, particularly in relation to operational controls.”

“Insufficient breadth of control objectives. Sometimes they are too narrow. For example, the controls objectives cover only general controls when application controls and manual assertion level controls would also be useful.”

User organizations do not always obtain the information they need from the SAS 70 report. The controls tested by the service organization’s auditor may not be those that are considered important by the user organization; this appears to be especially true for information technology (IT) controls. However, little additional work is performed to compensate for the apparent lack of coverage in the SAS 70 report. Observations made by interviewees and survey respondents addressing this issue included:

“Lack of adequate support for conclusions in any one area.”

“No consistency in presentation of the information between entities providing such reports.”

“Ensure that SAS 70 auditors are implementing the risk-based standards and relate their controls to financial statement assertions and compliance objectives (like A-133).”

“I would love to see some testing of IT procedures at the entities upon which we perform agreed-upon procedures. Also, better assurance of both technical and control procedures could allow us to better focus our current test work.”

“In conducting a performance audit, we hoped to rely on SAS 70 audit work to reduce the amount of audit work we did. The SAS 70 audit we tried to rely on made so much use of “discrete corroborative inquiry”—ask two people and if they tell you the same thing, you’re done—that we found it unhelpful.”

“They do not cover all the controls that we would rely on.”

“Sometimes it is just better for our external auditors to do additional test work to satisfy their needs than pay the high price of an SAS 70 report.”

“Facilitate better input by user auditors and user organizations on the control objectives being audited by the service audit. Incorporate guidelines/requirements for a minimum threshold or accreditation for SAS 70 audits, similar to FISMA compliance.”

“The opinion states that the controls are in place to meet the company’s control objectives. It would be helpful if these control objectives were related to the compliance objectives that we need to test or the financial statement assertions that we are testing. It is very broad-based and difficult to take that information and relate it to our audit objective. We do not have all the details to do this and more information on the SAS 70 auditors doing this would help in the reliance.”

One solution to this is for the user to detail his or her requirements as part of the RFP process. As one respondent said, “... use the service level agreement, contract, or other controlling document to establish the control objectives and to keep them more focused.”

Timing Issues—Another observation is that the timing of the audit report and the SAS 70 report can create problems. As one respondent pointed out, “... the timing of the reviews and reports has, in the past, not been useful to the agency’s financial statement audit cycle.” Another said, “Make audit periods coincide.”

AND CAN THEY BE IMPROVED?

With the right planning, users can exert some control over this and our respondents had advice on how to do so. They suggested that the user organization contact the service provider early to request a SAS 70. One alternative use in state and local government environments is that the government auditors step in and do the additional work. One respondent mentioned the “lack of standardization of the timeframe of the report scope. Some reports are every year, others every other, which then causes our financial statement auditors concern.”

Scope of Testing—The scope of the service center auditor’s testing may not be sufficient for the user auditor’s purpose. It appears that many user organizations in government do not have significant input into the determination of the scope. The service organization usually determines the scope based on its contracts with the user organizations and/or discussions with individual user organizations or auditors.

Possible solutions could be to include user requirements in RFPs and/or contracts and negotiate with the service organization auditors.

Impact of Regulations and Other Requirements—Some respondents were confused about what SAS 70 reports can accomplish and the impact that other regulations and requirements have on the SAS 70 procedures. Several referred to the fact that SAS 70 reports now incorporate IT security as well as financial controls. A concern expressed by some was that the duplication of effort required by doing this was almost equivalent to waste, fraud and abuse. “They have been expanded beyond financial services to any franchise service available. They also integrate FISMA audits which are already required through FISMA in the form of system certifications thereby duplicating workload and time to support external audit activities, and they provide very little value from a FISMA perspective since the NIST 800-53A assessments provide the expectation for detailed security controls required by IT systems.” Others opined:

“SAS 70 reports should be limited to only financial services as originally intended. It should be required that GAO auditors use one set of COTR⁵ deliverables required for any external audit process (financial, FISMA, FISCAM, etc.) and rotate auditors within the agency to assure consistent standards/audit practices are deployed throughout government.”

“Stick to financial services only as originally required. It appears that SAS 70 vendors are extending their services to increase their profits while not ... required. This creates a disconnect in the audit process due to lack of experience. Lack of experience was not an issue when the focus has been financial functional assessments. In addition it creates a conflict for the IGs. They see it as a priority to consolidate their workloads/costs for regulatory audit requirements.”

Regarding the impact that the Sarbanes-Oxley Act (SOX), FISMA or other law or regulation has or has had on the issuance of SAS 70 reports, typical responses were:

“The IG (inspector general) has tried to integrate multiple audit functions to save time and money but requires the customer to pay for the services while maintaining COTR responsibilities. This is a conflict of interest per the policies that have been established and the IG should only procure services to assess the audit products required by law for system owners to provide through third party services.”

“Burdensome!!!”

“There is substantial overlap in the evaluations of controls.”

“It has created a need for more internal control work to be done.”

“Increases cost to companies needing such documents to satisfy either SEC requirements or management and the development of a specialized SAS 70 auditor discipline.”

“In my opinion, the requirements in SOX have elevated the reliance on SAS 70 audits because of internal control reporting requirements and the financial impact due to insufficient and inadequate controls. It is my understanding that FISMA and FIPS requirements are mandated for federal agency systems and provide guidance toward certification and accreditation of secure systems, however states and private industry are only encouraged to use federal guidelines.”

“I think the impact of recent legislation has required auditors to perform additional work regarding the information included in the SAS reports. From experience, we have performed walk-throughs at the service provider to enhance our understanding of their operations to assist in developing relevant audit procedure.”

“Both management and the auditor need to pay closer attention to the adequacy of the description of controls and the selection of control objectives. SAS 70s are designed for financial auditors. FISMA goes into [many] other areas where an agreed-upon procedures report would be more appropriate.”

Conflict of Interest—We asked about any potential conflict of interest when an auditor is the financial statement auditor for a client who is an outsourcing service provider and also issues the SAS 70 report. Eighty three percent said there was none.

Future of SAS 70 Reports—Would it be helpful if SAS 70 reports were to be mandated? And if they are mandated, should they be consistent with international standards? OMB encourages their use but does not require agencies to use them if they can use alternative procedures. Some believe that they should be required:

“I believe it should be required by OMB that for any outsourced service center services procured, the contract must include a requirement for SAS 70 reviews. There is far too much outsourcing of computer center services with no regard to this useful tool. These service centers are such costly contracts to procure, that I imagine the cost of an SAS 70 review would be insignificant to the contract as a whole.”

SAS 70 REPORTS: ARE THEY USEFUL

Some believe that they should be better aligned with international standards:

“Include other internationally recognized standards into the SAS 70 report (like ISO 17799 and BS 7799 standards) to make them more internationally appealing and more useful to global organizations.”

Conclusion

- Service organizations, the subject of SAS 70 reports, are now a critical part of some user organizations' overall system of internal control for financial and operational reporting.
- SAS 70 reports have been used in government for several years and are generally accepted as a method of communicating information and assurance about the controls that are of interest to the user organizations and their auditors as they relate to an audit of the financial statements.
- Some agencies have found them useful in the performance of financial statement audits.
- Parties involved in the SAS 70 process appear in some cases to have conflicting perceived objectives for the reports.
- Generally, user organizations in government do not have significant input to the scope or systems to be covered by the SAS 70 report. The service organization usually determines the scope based on its contracts with the user organizations and/or discussions with individual user organizations or auditors.
- User organizations do not always have the skill set to understand or analyze the impact of the conclusions drawn or exceptions reported in the SAS 70 report. This could lead to misinterpreted results and unwarranted reliance upon the SAS 70 report that in fact may include reporting on a deficiency or other control weakness in the service organization's controls.
- User organizations do not always obtain the information they need from the SAS 70 report. The controls tested by the service organization's auditor may not be the ones considered important by the user organization; this appears to be especially true for IT controls.
- Automatic default to SAS 70 reports by a service organization may not always be appropriate nor necessary.
- Increased presence of certain federal compliance and audit standards is blurring the line regarding the scope of the SAS 70 reports.
- Clarity is needed in ownership for report and content, and to differentiate between governmental audit standards and laws and regulations versus the standards issued by commercial and private auditing organizations, such as the AICPA.
- Increased involvement by the service organization management is needed.

We recommend that:

- User organizations understand the differences between the various federal audit guidelines that make reference to SAS 70 reports as a component of obtaining an understanding of an entity's system of internal control.
- User organizations obtain training, if necessary, in the use and reading of SAS 70 reports, and understand where SAS 70 reports may not be appropriate.
- User organizations should get actively involved in a timely fashion in setting the appropriate scope for the SAS 70 report to enhance the report's usefulness.
- Service organizations should provide more outreach programs to educate their user organizations and auditors as to the content of their SAS 70 reports and the reasons for the particular report's scope.

Finally, as organizations continue to use service organizations for financial processing functions, it is important for management to:

- Be aware of audit standards other than SAS 70 that may be appropriate for obtaining information and/or assurance about a service organization's controls.
- Be aware of potential and planned changes in the relevant professional standards that will enhance the overall concept of the service auditor's report from the SAS 70 examination level report to an attest report where management of the service organization will assert to their controls as a component of the audit report.
- Take more interest in how the report is developed and actually read the report. Then if necessary, in future years, use the contract vehicle to require more coverage of relevant controls.

In conclusion, we hope that this research will provide information useful to auditors, service organization management, user organization management and standards-setters.

End Notes

1. SAS 70: *Reports on the Processing of Transactions by Service Organizations*, Warner, Paul D., CPA Journal Online, November 1992.
2. Internal Control—Integrated Framework
3. Public Law 107-204
4. Request for Proposal
5. Contracting Officer's Technical Representative

APPENDIX A: THE FUTURE STATE OF SAS 70

Appendix A—The Future State of SAS 70 Versus Other International Standards

Introduction

In the global economy, companies continue to focus on providing services tailored to their specific customer requirements. Frequently, such businesses find that focusing on the customer may be more easily achieved by outsourcing routine processes to external service organizations.

This outsourcing of processes presents challenges to financial and regulatory auditors of businesses that use service organizations. As part of a financial audit, an auditor is required to evaluate the internal control environment of its client. However, when processing is outsourced, portions of the client's internal control are performed at the service organization rather than at the company's place of business. Often clients have more than one service organization that may perform the same service, different services, or different parts of the same transaction.

The international nature of business has further complicated the auditor's evaluation of internal controls as a service organization may be in a different country or continent than the client. For example, a Canadian bank may outsource the data center operations to a service organization headquartered in the United States, but whose main data center is in Australia, while the data security function resides in Brazil, and the application developers reside in India. This presents significant challenges to companies and their auditors.

The American Institute of Certified Public Accountants (AICPA) recognized the challenges presented to auditors by outsourcing and issued Statement of Auditing Standards No. 70 Service Organizations (SAS 70) to aid auditors in the assessment of internal control. Other countries developed their own standards to meet local needs, some of which were based on SAS 70 and the International Federation of Accountants (IFAC)'s International Auditing and Assurance Standards Board (IAASB) developed a standard on how user auditors could rely on SAS 70-like reports. With passage of the Sarbanes-Oxley Act, SAS 70 quickly became the global *de facto* standard for service organizations' reporting. Today, it is estimated that more than 1,000 SAS 70 reports are issued globally for a myriad of outsourced services and in multiple languages.

The Sarbanes-Oxley Act increased management accountability, by requiring the management of U.S. registrants to assess and make an assertion as to the effectiveness of internal control over financial reporting. This assessment included internal controls that had been outsourced to service organizations. Auditors are required to audit these internal controls in conjunction with a financial audit of a registrant.

The Public Company Accounting Oversight Board (PCAOB), which assumed responsibility for establishing auditing standards related to registrants in 2004, has issued Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (AS 2) and its subsequent update, Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements* (AS 5). These standards incorporate by reference the previously existing audit standards established by the AICPA that did not require immediate modification in response to Sarbanes-Oxley. These audit standards specifically identified SAS 70 reports as a means for management to perform its assessment, and the auditor to perform its audit, of internal controls.

In 2004, the IAASB issued ISA 402—*Audit Considerations Relating to Entities Using Service Organizations*—which provided user organizations and their auditors with guidance on the impact of service organizations on the audits of financial statements and the use of SAS 70-like reports; however this standard did not provide guidance to the service auditor on performing these engagements. In 2006, IAASB initiated a research project with two focuses: update and enhance ISA 402 and develop a new global standard for service organization examination reports, tentatively designated ISAE 3402, *Assurance Reports on Controls at a Third Party Service Organization*. In doing so, the IAASB wanted to make the report more useful to a wider range of users, not just the management of user organizations and user organization auditors. In addition, the IAASB wanted to broaden the types of controls that could be subject to examination beyond controls over financial reporting.

Currently, the IAASB is concluding its work on ISA 402 and ISAE 3402 and, as mentioned on page 7, released them as new standards in final draft form in late 2007 for public comment. After the comments are evaluated and applied, the final standard will be issued. The AICPA is working on a parallel effort to incorporate elements of ISA 402 and ISAE 3402 into U.S. auditing standards. Issuance of the new AICPA standard is also currently anticipated for 2010.

A Comparison Between SAS 70 and ISAE 3402

Because of SAS 70's success in meeting the needs of user organizations and their auditors, the IAASB is proposing to adopt most of its tenets rather than completely revising the standards. This will reduce the effort required by service organizations and their service auditors in adopting the new standards and smooth the transition for user organizations and their auditors. However, the IAASB has introduced several proposed differences that are intended to increase the overall usefulness of the service organization's report to users who are interested in controls related to the effectiveness and efficiency of operations and compliance with applicable laws and regulations. In addition, the IAASB has proposed a requirement that management make a written assertion as to the controls that are the subject of the examination.

APPENDIX A: THE FUTURE STATE OF SAS 70

Aside from some terminology differences in ISAE 3402 compared to SAS 70, some differences between ISAE 3402 and SAS 70 include:

- *Management's Assertion*—now required in the report immediately after the service auditor's opinion. A standard model has been developed for management to formally assert to the existence and operating effectiveness of its controls. Currently, SAS 70 only includes the auditor's opinion. SAS 70 also requires a manager to provide the service auditor with letter containing certain representation but this letter is provided only to the service auditor and is not made public.
- *Assessing the Criteria*—a requirement for the service auditor to assess the appropriateness of the criteria used by the service organization to develop its description of the system controls, the control objectives, and related controls. The IAASB intended to include this measurement of the criteria to parallel the managerial assertion to help ensure that the content of the report (control objectives and controls) would be relevant to the intended audience. SAS 70 has no requirement for the service auditor to assess the appropriateness of the criteria used in the development of the report.
- *Distribution of the Report*—the report will be appropriate for general use and usually will not need to be restricted to specified parties. Currently, distribution of a SAS 70 report is restricted to service organization management, user organizations and the auditors of user organization. With this proposed change, other persons may obtain and rely on the report. In its current deliberations, the AICPA has signaled its intention to continue this restriction on the use of reports in the updated version of SAS 70.
- *Auditor's Opinion*—ISAE 3402 will combine "design" and "operating" exceptions in the auditor's opinion. This reflects the idea that there is a more direct linkage between the design of controls and the operation of those controls. SAS 70 separates these two concepts; the IAASB believes that combining the two will be more meaningful in an evaluation of the total set of internal controls at the service organization.

Similarities between ISAE 3402 and SAS 70 include:

- *Provision for Different Types of Reports*—Both standards permit the auditor to issue a report on controls placed in operation (referred to as Type I or Type A) or a report on controls placed in operation and their operating effectiveness (referred to as Type II or Type B). Type II reports are expected to continue to be the most common, as they are usually more useful to users.
- *Use of Internal Audit*—Both standards permit the use of internal audit in the performance of the service auditor's procedures. Similar to SAS 70, ISAE 3402 does not permit the auditor to state in the report opinion that procedures were performed by internal audit.
- *Representation Letter*—Both standards require the service organization to provide a letter of representation to the service auditor prior to issuance of the report.

- *Format of the Report*—Formats and presentation will be consistent with SAS 70.
- *Subsequent Events*—Both require the service auditor to update understanding of the controls through the report date to determine if any changes have occurred that might impact the auditor's evaluation of the controls or that should be communicated to report users.

The Impact on a Service Organization

The service organization that is considering reporting on controls in accordance with ISAE 3402 at one or more of its operations needs to address the following:

- *Management's Assertion*—A written assertion will be necessary before the report can be issued. The content of the assertion will vary depending on the nature of the services provided. The IAASB has developed several examples that will be included in the ISAE 3402 standard.
- *Criteria*—An analysis of the criteria used by the service organization to the development of the control objectives and controls will need to be prepared. The IAASB has indicated that criteria need to be specific, measurable and relevant to the intended user organizations' reliance on the report.
- *Planning*—An international service organization with multiple locations may have to continue issuing a combination of SAS 70 reports, local standard reports (common in the U.K. and Japan) as well as ISAE 3402 reports. Designated personnel at the service organization should carefully plan for the implementation of ISAE 3402 within their operations.

The actual activities by the service organization and of the auditor in all likelihood will not vary significantly from current practices; controls must be identified, documented and tested by the service auditor. However, there is no substitute for adequate planning; any service organization considering reporting on controls in accordance with ISAE 3402 in its organization is advised to begin planning early in 2009 as the new standard is prepared for final issuance. Similarly, close attention to the AICPA's parallel efforts to enhance SAS 70 is also warranted.

APPENDIX B—C: REFERENCES, OUTLINE OF SAS 70 REPORT

Appendix B—References

Volume 1 of the *Professional Standards* of the American Institute of Certified Public Accountants (AICPA), Section AU 324, *Service Organizations*, May 1993, as amended.

AICPA Audit Guide, *Service Organizations*, May 2007, as amended.

OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*.

OMB Circular A-123, *Management's Responsibility for Internal Control*.

OMB Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*.

International Federation of Accountants (IFAC), International Auditing and Assurance Standards Board (IAASB), International Standard on Auditing 402, *Auditing Considerations Relating to an Entity Using a Service Organization*, (DRAFT).

International Federation of Accountants (IFAC), International Auditing and Assurance Standards Board (IAASB), International Standard on Auditing 3402, *Service Organizations*, (DRAFT).

United Kingdom—Technical Release, AAF 01/06 (superceding FRAG 21/94 guidance), *Assurance Reports on Internal Controls of Service Organizations Made Available to Third Parties*, Audit and Assurance Faculty of the Institute of Chartered Accountants of England and Wales.

Canada—CICA Handbook Section 5970, *Audit Reports on Controls at a Service Organization* and Section 5310, *Audit Evidence Considerations When an Entity Uses a Service Organization*, both issued by the Canadian Institute of Chartered Accountants (CICA), April 2005.

FIPS stands for Federal Information Processing Standards

Appendix C—Outline of an SAS 70 Report

The AICPA did not provide a required format for a SAS 70 report but did specify certain elements of SAS 70 reports that must be present to be considered a complete document. The elements for a Type II—Report on Controls Placed in Operation and Tests of Operating Effectiveness are as follows, by section:

1. Independent Service Auditor's Report
 - Auditor's Opinion on Letterhead
2. Example Computer Service Organization's Description of Controls
 - Overview of Operations
 - Relevant Aspects of the Control Environment, Risk Assessment and Monitoring
 - Control Environment
 - Risk Assessment
 - Monitoring
 - Information and Communication
 - Information Systems
 - Application(s) Description
 - Control Objectives and Related Controls
 - The organization's control objectives and related controls are included in section 3 of this report, "Information Provided by the Service Auditor." Although the control objectives and related controls are presented in section 3, they are an integral part of the organization's description of controls.
 - User Control Considerations
3. Information Provided by the Service Auditor
 - Overview of Control Objectives, Related Controls and Tests of Operating Effectiveness
 - General Computer Controls
 - Systems Development and Maintenance
 - Logical and Physical Access
 - Computer Operations and Backup of Data
 - Application Controls
 - Application Controls—System 1, 2, 3, etc.
4. Other Information Provided by the Service Organization (unaudited)
 - Description of Other Applications
 - Description of Planned Changes to Applications
 - Description of Business Continuity Plans

APPENDIX D: SURVEY INSTRUMENT

Appendix D—Survey Instrument

SAS 70 Reports: Are They Helpful and Can They be Improved?

The AGA Corporate Partner Advisory Group (CPAG) Research Program is undertaking a research project to evaluate the current usefulness of SAS 70 audits and identify recommendations for how they could be made more useful. Statement on Auditing Standards (SAS) 70 audits are conducted in accordance with AU Section 324, Service Organizations. The title of SAS 70 is *Reports on the Processing of Transactions by Service Organizations*.

In the federal environment, SAS 70 audits may not meet all the requirements of the Federal Information Security Management Act (FISMA). In the private sector, SAS 70 audits are getting more attention since the passage of the Sarbanes-Oxley Act and the requirements of Section 404 of that Act.

This project demonstrates the commitment of AGA and its Corporate Partners to be at the “leading edge” of issues that face the government financial community. Ernst & Young, a CPAG member, is sponsoring the research. The project has three phases: review of existing literature; interviews with selected subject matter experts and surveys sent out to other interested parties; and finally, a report summarizing recommendations and containing suggestions as to best practice.

The research is being conducted by the Director of Research at AGA, Anna D. Gowans Miller, who has been an auditor with Touche Ross and the Corporation for Public Broadcasting, Technical Manager at the AICPA, a House of Representatives Committee on Government Reform and Oversight Professional Staff Member, and independent contractor with the Office of the Secretary of Defense Quality Management Office.

You have been identified as an individual with experience and knowledge in one or more aspects of service providers, in federal, state or local government or in the private sector. In our attempt to get the experiences of as many individuals as possible, we request that you complete this survey. We have attempted to make the survey as easy to use as possible. Please provide as many comments as you can, and add your personal experiences as appropriate. Such information will add to the substance of the final result.

This research will result in one or more publications and presentations, such as a published research report in AGA’s CPAG Research Series, an article in AGA’s *Journal of Government Financial Management* and a presentation at AGA’s Annual Professional Development Conference (PDC).

Please note that AGA surveys like this one do not attribute thoughts and quotations to individuals. This preserves anonymity and encourages individuals to speak freely.

Please be assured that your name and that of your organization will not be used in any publication or presentation materials without your specific permission.

You can go into the survey more than once and answer the questions in stages, if you prefer. Just do not click the DONE button until you have completed all the questions you can answer.

Demographics

1. Please provide the following information:

Name of respondent

Your title or function

Federal Government Agency/Dept/Organization

State Government Agency/Dept/Organization

Local Government Agency/Dept/Organization

Private Sector Organization

If your organization is part of a larger organization or agency, please list name of the larger organization or agency, e.g. DHS for TSA or Treasury for IRS

Name of Respondent’s Bureau/Office/Service/etc.

Address

Phone

Fax

E-mail

2. Please indicate your function as it relates to SAS 70 reports:

User Organization

Service Organization

User Organization Auditor

Service Auditor (performs the SAS 70 Report)

Other (please specify)

3. What is your level of direct involvement in SAS 70 reports in your organization?

I provide input to the scope and the control objectives of the report

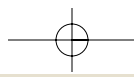
I contribute to the description of controls and other information provided by the service organization

I am a user of SAS 70 reports

I am a SAS 70 auditor

I have no direct involvement

Other (please specify)



APPENDIX D: SURVEY INSTRUMENT

Users of Outsourced Services provided by Service Organizations

4. From the list below, please select the services for which you receive (either through request or contractually) a SAS 70 report.

	Yes	No
General Ledger/Financial Reporting		
Receivables and Payment Management Systems		
Purchasing/Travel Card SmartPay Systems		
Grant Accounting		
Payroll and Pension Administration		
Trust and Custody—Investment Management		
Highway Toll Systems—EZPass		
Medicaid and Medicare Contractor		
Data Center Outsourcing		
Electronic Benefits Transfer (EBT)		
Electronic Tax Payments		
Child Support Enforcement—Collection and Disbursement		
State Lottery Systems		
Other		

5. Which statement best reflects why you obtain SAS 70 reports from your service organization provider?
 The requirement is included in our RFP process.
 Our external financial statement auditors ask for SAS 70 reports.
 Our internal auditors (and OIG) ask for SAS 70 reports.
 We are required to do so by law, regulation or other guidance.
 We use them to select service providers.
 Other (please specify)

6. If your organization obtains SAS 70 reports, please indicate your level of agreement with the following statements. If you are not sure of the answer, please enter N/A.

	Do Not Agree	Somewhat Agree	Neutral	Agree
SAS 70 reports are generally useful to our management.				
We use SAS 70 reports to assist in the selection of a service provider.				
SAS 70 reports assist in reducing our risk of errors and inaccuracies in our financial statements.				

SAS 70 reports are only used by our auditors.
 SAS 70 reports do not provide enough information on IT security but no additional work is done.
 We have to ask for additional procedures to be performed because of timing between our fiscal year-end and the year-end of the entity receiving the SAS 70 Audit.

7. If you do not find SAS 70 reports useful, please describe some of the reasons why.

8. Please describe any best practices, lessons learned or future plans related to using SAS 70 reports based on your experience and knowledge.

Service Organizations

9. Do you arrange to have a SAS 70 report on your organization's services or systems?

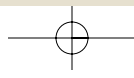
10. From the list below, please select the services you provide to your user organization for which they may request or contractually require a SAS 70 report.

	Yes	No
General Ledger/Financial Reporting		
Receivables and Payment Management Systems		
Purchasing/Travel Card SmartPay Systems		
Grant Accounting		
Payroll and Pension Administration		
Trust and Custody—Investment Management		
Highway Toll Systems—EZPass		
Medicaid and Medicare Contractor		
Data Center Outsourcing		
Electronic Benefits Transfer (EBT)		
Electronic Tax Payments		
Child Support Enforcement—Collection and Disbursement		
State Lottery Systems		
Other		

11. If none of the services listed above are applicable, briefly describe your specific service here.

12. What is the "as of" date of your SAS 70 report?

- 3/31
- 6/30
- 9/30
- 12/31
- Other (please specify)



APPENDIX D: SURVEY INSTRUMENT

13. What is the duration of the period under review of your SAS 70 report?

- 3 month
- 6 month
- 9 month
- 12 month
- Other (please specify)

14. SAS 70 reports are limited distribution reports. Has there ever been a situation where you (as the service organization) were asked to provide a SAS 70 report to an outside party that was not a user organization?

Yes No

15. If you answered "Yes" to the previous question, were you able to comply

Yes No

16. If you answered "No" to the previous question, please explain.

17. How do you distribute your report?

- Paper report only
- Electronic (document, PDF)
- Download from service organization website (no password)
- Download from service organization website (password required)

18. The AICPA has defined two types of SAS 70 reports: Type I and Type II.

Type I includes the auditor's opinion on the fairness of presentation of the service organization's description of controls relevant to the services provided. The Type I also includes a conclusion as to the suitability of design to meet specified control objectives. A Type II report includes the same information as a Type I report. It also has the auditor's opinion on the operating effectiveness of the controls specified by the service organization during the period covered by the report (generally at least six months) and whether they provide reasonable assurance that the control objectives were achieved during the period specified. Which type of SAS 70 Report are you currently receiving?

Type I _____ Type II _____

Control Objectives

19. Who develops the control objectives for the SAS 70 report?

- Service Organization management
- Third-party regulator
- User organization
- External auditors
- OIG/State auditors
- Other (please specify)

20. Do you receive questions or requests for clarifications from your user organizations or their auditors?

- Yes, relative to the scope of the audit
- Yes, relative to the results of the auditor's tests
- Yes, relative to control updates since the end of the auditor's reporting period
- Yes, relative to other items (see below)
- No
- Other items (please specify)

21. For how many user organizations do you provide a SAS 70 report?

- 0-5
- 6-10
- 11-25
- 25+

22. Do you provide different reports to different clients or the same report to all your clients?

- Different reports to different clients
- The same report to all clients
- Management is willing to obtain custom reports tailored to client requirements for clients who request them
- Other (please specify)

23. How long have you had SAS 70 reports issued on your organization?

- New in 2007
- 2006
- 2005
- 2004
- 2003
- 2002
- 2001
- 2000
- Prior to 2000

APPENDIX D: SURVEY INSTRUMENT

24. How important to you are the following benefits of SAS 70 reports? Please answer all items.

Not Important Neutral Important

Reduces need for multiple audits
Increases the effectiveness of controls
Compliance with laws and regulations
Compliance with contract
Service differentiation in RFPs and bids

25. If you have experienced problems or difficulties with providing SAS 70 reports to user organizations, please describe them here. Examples could include an ill defined scope, excessive time to issue the report, numerous previously unknown control deficiencies, etc.

User Organization Auditors and Service Organization (SAS 70) Auditors

26. From the list below, please select the services for which you are performing financial statement audits.

	Yes	No
General Ledger/Financial Reporting		
Receivables and Payment Management Systems		
Purchasing/Travel Card SmartPay Systems		
Grant Accounting		
Payroll and Pension Administration		
Trust and Custody—Investment Management		
Highway Toll Systems—EZPass		
Medicaid and Medicare Contractor		
Data Center Outsourcing		
Electronic Benefits Transfer (EBT)		
Electronic Tax Payments		
Child Support Enforcement—Collection and Disbursement		
State Lottery Systems		
Other		

27. For SAS 70–service auditors only: SAS 70 reports are limited distribution reports. Has there ever been a situation where you were asked to provide a SAS 70 report to an outside party that was not a user organization?

Yes No

28. If you answered “Yes” in the previous question, were you able to provide the report to the requesting entity?

Yes No

29. If you answered “No” in the previous question, please explain.

30. Do you find the SAS 70 reports you receive from service organizations useful in your financial statement audit work for the user organization?

Yes No

31. If you answered “No” to the previous question, what can be done to make them more useful?

32. In some cases, an auditor may be the financial statement auditor for a client who is an outsourcing service provider and also issue the SAS 70 report. If the SAS 70 report is distributed to the service organization’s clients and one of these is also one of your clients, do you see any potential conflict of interest?

Yes No

33. If you answered “Yes” please suggest below how such conflict of interest could be mitigated or eliminated.

34. What do you see as the impact the Sarbanes-Oxley Act, FISMA or other law or regulation has or has had on the issuance of SAS 70 reports? Please describe below.

35. What do you think can be done to make SAS 70 reports more useful and more effective in mitigating risk to the user of financial management shared services?

Conclusion

36. Can we contact you to get more information?

Yes No



*Advancing
Government
Accountability*

Association
of Government
Accountants

2208 Mount Vernon Avenue
Alexandria, VA 22301

PH: 703.684.6931
TF: 800.AGA.7211
FX: 703.548.9367

www.agacgfm.org
agamembers@agacgfm.org