TESTIMONY OF
SUSAN J. PEIRCE, CPA

MEMBER OF THE
AICPA EMPLOYEE BENEFIT PLAN AUDIT QUALITY CENTER
EXECUTIVE COMMITTEE

BEFORE THE ERISA ADVISORY COUNCIL

WORKING GROUP ON PRIVACY AND SECURITY ISSUES AFFECTING EMPLOYEE BENEFIT PLANS

SEPTEMBER 1, 2011

I am pleased to appear before the Working Group on behalf of the American Institute of Certified Public Accountants for which I serve on the Employee Benefit Plan Audit Quality Center Executive Committee. The Employee Benefit Plan Audit Quality Center is a firm-based voluntary membership center with over 2,200 CPA member firms that audit employee benefit plans.

My remarks today will focus on the use by plan sponsors and auditors of a service organization's report on internal controls. Specifically, I will address the current SAS No. 70 report and the controls typically covered by the report, how the plan sponsor can best use these reports, and how these reports will change under the new SSAE No. 16 framework. Finally, I will conclude on the usefulness of these reports to plan sponsors in performing their fiduciary duties.

Background of SAS No. 70

Employee benefit plans and plan sponsors frequently use service providers for such services as participant recordkeeping, custodial/trustee, and payroll processing. Each of these service providers processes information and transactions that affect plan financial statements and, as such, it is critical that plan sponsors and plan auditors consider the service organization's controls that are relevant to the plan's internal control over financial reporting.

As it is inefficient and overly burdensome for each service organization customer to perform its own review of the controls of the service organization, Statement of Auditing Standards (SAS) No. 70 was issued in 1992 to alleviate this duplication of efforts. By engaging an independent CPA to examine and report on a service organization's controls, those service organizations can meet the needs of their user entities and their auditors who want and need an objective evaluation of the effectiveness of controls as specifically identified by the service organization that address operations and compliance, relating to financial reporting of the plans sponsored by the user entities.

Under SAS No. 70, a service auditor is engaged by a service organization to perform either a Type 1 or Type 2 engagement. In a Type 1 engagement, the auditor examines and opines on whether the description of the service organization's system is fairly presented and whether

controls at the service organization that may affect user entities' financial reporting are suitably designed. In a Type 2 engagement, the service auditor also examines and opines on whether the controls were operating effectively and describes tests of the controls performed by the service auditor to form that opinion and the results of those tests.

Because a Type 1 report does not address the effectiveness of the controls at the service organization, a Type 2 report is much more beneficial to the plan sponsor and auditor. As such, my testimony today will address Type 2 reports. And while SAS No. 70 reports can be used for any number of industries and service organizations, my testimony will focus on the use of these reports primarily by 401(k) Plan Sponsors (service organization customer) and their plan auditors (user auditor).

SAS No. 70 Reports

A SAS No. 70 report does not address all controls at the service organization. Rather, it encompasses the controls over transactions and processes relevant to financial reporting of the plan. The controls that a service auditor will typically test include access controls, participant transaction controls, and investment controls, such as the following:

a. Logical access and physical access to service organization
b. Logical access and availability of the system at plan sponsor, participant and advisor level
c. Integrity of the system to provide complete, accurate and timely processing of transactions
d. Set-up of plans new to service organization
e. Eligibility (initial and continuing), enrollment and participant data
f. Processing of employer/employee contributions at the plan level and participant level
g. Participant account income and expense allocations
h. Distributions and expenses at plan level and participant level
i. Marketable securities held – safekeeping and valuation (not fair value)
j. Investment changes at participant and plan level
k. Plan obligations, if a defined benefit plan
l. Reporting at plan and participant level
m. Complementary user control considerations

It is important to note that while the service auditor opines on the design and effectiveness of the relevant controls at the service organization, no assurance is given as to whether the information supplied to them by the plan administrator/sponsor is accurate. The controls at the plan sponsor over the transmission of the information (participant eligibility, salary, dates, contributions, etc.) are equally important in ensuring the integrity of the financial statements, and they are beyond the scope of the SAS No. 70 engagement. Additionally, controls over privacy and security issues, such as firewall security and cloud computing are addressed only as they relate to financial reporting controls. There are recently-issued guidelines for engagements covering privacy and security issues, which I will address later in this testimony.

Benefits and Concerns of Using a SAS No. 70

The independent auditors' opinion on the SAS 70 report includes information which is critical to the plan sponsor, including:

- The date by which the controls were placed in operation
- The period of time from which the testing samples were selected
- Carve-outs of outside organizations used by the service provider that are not included in any testing
- No procedures have been performed to evaluate the effectiveness of internal controls at individual user organizations
- The projection of any conclusions, based on the report, to future periods is subject to the risk that changes may alter the validity of such conclusions.

Plan sponsors have a fiduciary duty to ensure that participant transactions are properly executed and recorded. Most plan sponsors outsource participant recordkeeping to service organizations, but that does not relieve them of their fiduciary duty with respect to participant transactions and records.

When used properly a SAS No. 70 can be very beneficial to the plan sponsor. A SAS No. 70 report can provide plan sponsors with reasonable assurance that the service organization has adequate controls in place relating to the audit of the plan's financial statement and they are working properly. The report also includes the complementary user controls which were contemplated in the design of the service organization's controls. And finally, auditors can use the SAS No. 70 report to reduce the cost of the plan audit by considering the results of the work performed by the service auditor.

Unfortunately, many plan sponsors do not understand how to use SAS No. 70 reports effectively or, worse, they incorrectly assume they have transferred their fiduciary responsibilities to the service organization and/or the SAS No. 70 report gives them absolute assurance that the service provider's records are complete and accurate. Oftentimes, plan sponsors obtain SAS No. 70 reports for the plan auditors and never actually read them themselves.

Plan sponsors should be aware that the service organization specifies which controls it wants the service auditor to review and test. It is imperative that the plan sponsor read the report to ensure that controls applicable to their plan are covered by the SAS No. 70 engagement. In addition, the plan sponsor should:

- ensure that the report covers the appropriate time period,
- follow up with service provider when key controls relevant to their plan are not tested,
- review the internal control test results to ensure that the no problems that would affect their plan were noted,
- follow up with the service organization to determine that any identified problems that would that would affect their plan were corrected, and

- review the required complementary user controls noted in the report and determine that they are in place at the plan.

If the plan sponsor uses multiple service providers for various tasks, it may need to obtain multiple SAS No. 70 reports. In addition, service providers can, and frequently do, use sub-service organizations to process transactions. The services provided by the sub-servicer typically are not covered by the primary service organization's SAS No. 70 report. Instead, these sub-service organizations will have their own SAS No. 70 reports, which they often times will release only to their direct users (the primary service organization). In such cases, the plan sponsor may need to ask the service organization to obtain the sub-servicer SAS No. 70 reports for their use.

SAS 70 reports help the plan sponsor and user auditor:

- develop an understanding of the controls in place at the service organization
- understand how effectively the designated controls operated during the testing period
- understand the complementary user controls that need to be in place

SAS 70 reports cannot be used:

- to determine whether the controls indicated are the "best" controls
- to make projections regarding the controls beyond the period covered in the report
- to eliminate due diligence procedures in regard to the service organization
- to make projections/assumptions about controls regarding privacy and security issues

Third party administrators may not truly understand how a SAS No. 70 report is to be used. The plan sponsor needs to be wary of any claims made that the SAS No. 70 engagement is an audit of the company or its financial statements. TPAs also frequently use SAS No. 70 reports for marketing purposes and may overstate the purpose and use of the SAS No. 70 report. Plan sponsors should consider these misstatements during their due diligence process.

<u>Monitoring a Service Organization</u>

The plan sponsor has a fiduciary duty to monitor its service providers. While obtaining and reading the SAS No. 70 report is an important part of this monitoring, it is not the only step the plan sponsor should take. In addition to reading the SAS No. 70 report, following are best practices that a plan sponsor should adopt in monitoring its plan service providers:

- Meet with the service provider regularly, and where possible hold at least one meeting at the service provider's location
- Review service provider reports
- Ask questions about policies and procedures
- Follow up on participant complaints
- Review their complaint file and how issues were resolved
- Review published reports on service providers

SSAE No. 16

Recently, SAS No. 70 has been superseded and replaced by two new standards. One is a Statement on Standards for Attestation Engagements (SSAE) also known as an attestation standard; the other is a SAS (an auditing standard). The requirements for examining and reporting on controls at service organizations have been placed in SSAE No. 16, *Reporting on Controls at a Service Organization.* The requirements for auditing the financial statements of entities that use service organizations remain in the auditing standards in a new SAS, *Audit Considerations Relating to an Entity Using a Service Organization.* Moving the requirements for CPAs reporting on controls at service organizations to the attestation standards better reflects the nature of the work being performed. SASs primarily provide guidance on auditing and reporting on historical financial statements, whereas the SSAEs primarily provide guidance on reporting on other subject matter.

SSAE No. 16 was effective for reports issued on or after June 15, 2011. It establishes a Service Organization Control (SOC) framework, which allows for three engagement types:

- SOC 1 Engagement – This engagement is performed in accordance with SSAE No. 16, and results in a restricted use report on controls at a service organization that may be relevant to user entities' internal control over financial reporting. This engagement is the same as the current SAS No. 70 engagement described above.
- SOC 2 Engagement – This engagement is performed under AT section 101, an attestation engagement using the guidance provided under *Reporting on Controls at Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. In other words, a SOC 2 engagement examines and reports on controls at a service organization other than those relevant to user entities' internal control over financial reporting and is a restricted use report as well.
- SOC 3 Engagement – This engagement is the same as a SOC 2 engagement except that it uses a short form report that is intended for general use.

The SOC 2 engagement was developed to address concerns over nonfinancial controls, such as privacy and security controls that are outside the realm of financial reporting. This was done in direct response to more and more information being transmitted and maintained over the internet and the need to address these controls for the plan participants and their privacy. This engagement also allows more flexibility with respect to the types of controls reported on at the service organization.

Similar to SAS No. 70 reports, the SOC 1 and SOC 2 reports will be issued as Type 1 or Type 2 reports. For a Type 2 SSAE No. 16 engagement, management at the service organization is required to provide publicly a written assertion to confirm, to the best of management's knowledge and belief, that the description of the controls is fairly stated, and that the controls were suitably designed and were operating effectively throughout the period.

COBIT and ACH Guidance Controls

SSAE No. 16 does not mandate the specific controls that must be placed into operation at a service organization, nor does it identify a precise control framework to follow. Many user organizations use existing information technology (IT) guidelines in establishing their internal computer system process and procedures, customizing them to their own unique system. You've asked me to comment specifically on two specific frameworks as they relate to SAS No. 70 and I shall. However, please be aware the AICPA does not recommend or endorse any such framework.

Control Objectives for Information and Related Technologies (COBIT) is a framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. Automated Clearing House (ACH) Guidance Controls is another framework that is used for processing ACH transactions and interacting with various financial institutions. These guidelines are frequently used by service organizations to establish controls and by service auditors in determining appropriate tests of internal controls.

As mentioned earlier, controls over privacy and security issues, such as firewall security and cloud computing are addressed in SAS No. 70 reports only as they relate to financial reporting controls. Thus, controls related to privacy and security issues in employee benefit plans, other than those likely to be relevant to user entities' internal control regarding financial reporting, would be covered by a SOC 2 or a SOC 3 report.

Conclusion

In conclusion, when used appropriately and in conjunction with other monitoring procedures, the SAS No. 70 report (and the subsequent SOC 1 report) is a very useful tool. The new SOC 2 report will enhance the plan sponsor's review and evaluation of controls at service organizations by including the controls that do not relate to financial reporting, such as controls relating to privacy and security issues.

Thank you for your interest in this important matter and the opportunity for me to testify before the Working Group today. I will be happy to answer any questions.

* * * * *