

## SOC and SAS

### The New Standards for Service Organization Controls Reporting

David E. Barton, CRISC and Jeffrey S. Solis, CPA

Last April, the American Institute of Certified Public Accountants (AICPA) announced that Statement on Auditing Standards Number 70 (SAS 70) was going away, to be replaced by Statement on Standards for Attestation Engagements Number 16 (SSAE 16). Since that time, additional discussion and guidance from AICPA has resulted in better understanding of the standards. It turns out that AICPA has done a lot more than just renumber and reorganize SAS 70. It has created three new Service Organization Control (SOC) reports intended to provide a framework for CPAs to examine controls at a service organization.

These new reporting standards are important to the PEO industry because they finally address some of the issues with the old SAS 70. Your larger clients may request these reports, or they can be used as a way to differentiate yourself from your competition.

The main problem with SAS 70 is that no two audits and no two reports are the same. When an auditor performs a SAS 70 audit, what is he auditing

against? What are the criteria for the audit? Most people are surprised to learn that the PEO is responsible for identifying and describing the controls that the auditor will render an opinion on. So, in essence, the PEO is writing the test!

Every report is unique and the controls described are not standardized in any way. This makes it very difficult to compare reports (and controls) at two different PEOs.

Somehow, over time, the completion of an audit based on SAS 70 be-

came the equivalent of being “SAS 70 certified.” Never mind that—AICPA has no such certification and never will.

#### **SOC 1: SSAE 16 is the New SAS 70**

SOC 1 reports will result from attestation engagements focused on the PEO’s controls that are likely to be relevant to an audit of a user entity’s (client’s) financial statements (privacy of data, timely and accurate payroll tax payments, and payroll processing as a whole). These en-

gagements will be conducted in accordance with SSAE 16. As with the old SAS 70, SOC 1 reports will be available as Type 1 or Type 2 reports. Type 1 reports present the auditors’ opinion regarding the accuracy and completeness of management’s description of the system or service as well as the suitability of the design of controls as of a specific date. A Type 2 SOC 1 report provides the auditors’ opinion about the accuracy and completeness, the suitability of the design of controls, and the operating effectiveness of the PEO’s controls throughout a declared time pe-



riod, generally between six months and one year.

SOC 1 reports are restricted-use reports intended only for user entities (existing clients) and their auditors, not potential customers or the general public. Although many PEOs do not get requests for these reports, as the industry becomes more competitive, clients may start requiring that their PEO be that much better than the rest.

## SOC 2

SOC 2 reports are based on AT Section 101 of the AICPA professional standards. A SOC 2 report covers the PEO's controls relevant to security, availability, processing integrity, confidentiality, and/or privacy. The criteria upon which these examinations will be based are contained in "Trust Services Principles, Criteria and Illustrations" (AICPA, "Technical Practice Aids"), established jointly by AICPA and the Canadian Institute of Chartered Accountants (CICA). The criteria are organized into five key attributes, or principles:

- Security—the system is protected against unauthorized access (physical and logical).
- Availability—the system is available for operation and use as committed or agreed.
- Processing Integrity—system processing is complete, accurate, timely, and authorized.
- Confidentiality—information is classified and protected as committed or agreed.
- Privacy—personal information is collected, used, retained, disclosed, and disposed of as committed or agreed.



SOC 2 reports can be based on one or more of the principles listed above.

As with SSAE 16, a SOC 2 report can be issued as a Type 1 or as a Type 2. A Type 1 report presents the auditor's opinion as to the accuracy and completeness of the system description as well as the design of the controls. A Type 2 report includes all aspects of a Type 1 report plus a description of the tests performed by the service auditor and the results of those tests. A SOC 2 report is also a restricted-use report intended for existing clients and their auditors.

## SOC 3

SOC 3 reports are also based on AT Section 101 of the AICPA professional standards and follow the Trust Services Principles. The primary difference between a SOC 2 report and a SOC 3 report is that a SOC 3 report

provides only the system description provided by management and the auditor's opinion on whether the system achieved the trust services criteria. The SOC 3 report does not contain any details about the service auditor's testing or the results of the testing. A SOC 3 report is a general use report, available to existing and potential clients as well as the general public.

If the service auditor believes the PEO achieved the trust services criteria, the PEO may then distribute the SOC 3 report to clients and may publicly display the SOC 3: SysTrust for Service Organizations seal. This seal is recognition that the PEO's controls meet the pre-established criteria established by AICPA and CICA. This can be a great tactic to show your current and potential clients that their information is safe and being processed with integrity.

## Conclusion

The new reporting standards for controls at service organizations, such as PEOs, have been developed in an attempt to provide alternatives that will better match the type of report to the primary interests of its user organizations or clients. The use of pre-defined controls criteria for SOC 2 and SOC 3 reports will enable potential clients to have a greater level of assurance that the service providers carrying the SOC 3 seal have adequate controls in place to protect their information assets.

*David E. Barton, CRISC is principal and Jeffrey S. Solis, CPA is senior accountant for UHY LLP, Sterling Heights, Michigan*

