Service Organization Control Reports and Attestation Standards

This document is intended to be read by anyone that may be a part of the purchasing/contract negotiation process (where a third party is assuming responsibility for processing transactions or hosting infrastructure/data), may be involved in contract/vendor management, or who directly requests or reviews service organization control (SOC) reports provided to Penn by third parties.

1) I hear that SSAE 16 is a SOC 1 report. What is a SOC 1 report?

The American Institute of Certified Public Accounts (AICPA) recently introduced a new naming convention, Service Organization Control℠ (SOC) reports, and identified three types of engagements for reporting on controls at a service organization: SOC 1, SOC 2, and SOC 3.

A SOC 1 report is issued for engagements that follow Statement on Standards for Attestation Engagements No. 16 (SSAE 16) guidance. SOC 1 (SSAE 16) reports retain the original purpose of SAS 70 reports in that they provide a vehicle for reporting on a service organization's controls that may affect a user organization's financial reporting. SOC 1 reports are considered "restricted use" reports (i.e., auditor-to-auditor communication) just like SAS 70 reports. SOC 1 engagements will still have the report objectives and related controls defined by the service organization. This provides little to no comparability across similar providers when reading SOC 1 reports.

SOC 1 reports will have nearly the same elements as SAS 70 reports, but specific content will depend on the service auditor and the service organization's internal processes and controls.

Key Terms

- **Service Organization:** an organization (third party) providing services to a user organization, such as ADP for payroll services or Verizon for data center/hosting services
- **User Organization:** an organization, such as Penn, that receives services provided by a service organization
- **Service Auditor:** The auditors who have been engaged to examine the service organization
- **User Auditor:** The auditors (e.g., PwC) of the user organization, such as Penn, who use the service auditor's report to gain an understanding of the internal controls performed at the service organization because they affect Penn's overall internal control environment

2) What is a SOC 2 report?

The purpose of a SOC 2 report is to report on controls other than those likely to be relevant to a user organization's financial reporting (e.g., compliance/operations). These reports address controls at a service organization relevant to the joint AICPA-Canadian Institute of Chartered Accountants (CICA) Trust Services Principles and Criteria: security, availability, processing integrity, confidentiality and privacy. Management identifies one or more Trust Services Principles that it believes it has achieved and the criteria upon which it will base its assertion of achievement.

Although SOC 2 reports are generally considered "restricted use" reports, other stakeholders (e.g., business partners, customers) and regulators knowledgeable about the subject matter and the criteria may also be appropriate parties to view a SOC 2 report. The report contains many of the same elements as a SOC 1 report.

3) What is a SOC 3 report?

Similar to a SOC 2 report, the purpose of a SOC 3 report is to report on controls other than those likely to be relevant to a user organization's financial reporting. The biggest difference between a SOC 2 and SOC 3 report is the intended audience of the report and the content.

In the past, the AICPA has used the terms SysTrust or WebTrust to denote a service organization control report that is made available to the general public through a link posted to a service organization's website. A SOC 3 report now allows a service organization to make their report publicly available. Like a SOC 2 report, SOC 3 reports focus on controls relevant to one or more of the Trust Services Principles.

In terms of content, the SOC 3 report does not include the detailed description of tests of controls and results that are included in SOC 1 or SOC 2 reports. Unlike the SOC 1 and SOC 2 reports, SOC 3 reports are short-form, publicly available reports, which contain a statement about whether the system achieved the applicable criteria outlined in the "Trust Services Principles Criteria and Illustrations."

Additionally, unlike a SOC 1 examination, SOC 2 and 3 engagements require the service organization to meet pre-defined criteria for one or more of the Trust Services Principles, thus allowing comparability across providers when reading SOC 2 and SOC 3 reports.

4) Are all SOC reports the same?

No. SOC 1 and SOC 2 reports can be either a Type I or a Type II report. A SOC 3 report is neither a Type 1 nor a Type II report; it is a short-form report that does not contain all of the sections that are included in SOC 1 and SOC 2 reports.

How are Type I and Type II reports different? The short answer is a Type I report provides an opinion as of a specified date (e.g., as of 09/30/20xx) whereas a Type II report expresses an opinion for the period specified (e.g., for the period 10/01/20xx – 09/30/20xx). Type II reports are considered more meaningful because a service auditor tests the effectiveness of controls over a period of time versus verifying that controls simply existed as of a specified date.

5) Could an organization be SSAE 16 "certified"?

No. There is no such thing as an organization being SSAE 16 "compliant" or "certified". An organization could only indicate that it was subjected to a SOC 1 (SSAE 16) or SOC 2/SOC 3 Type I or Type II examination. If an organization chose to share their report through a link posted to a service organization's website, a SOC 3 report would be the appropriate report.

6) What happened to SAS 70? Isn't this the report I need to ask for?

No. SSAE 16 was issued in April 2010 and supersedes SAS 70 as the guidance for service auditors to use when reporting on controls at the service organization that are

relevant to user organizations' financial reporting.

SSAE 16 became effective for all reports issued on or after June 15, 2011.

SAS 70 was the leading standard for guidance regarding assurance reports for service organizations since 1992. However, over time, SAS 70 reports were asked for and shared with parties that were not authorized recipients of these reports. In many cases, SAS 70 often became a "check the box" exercise without a true understanding of what the report was intended to communicate. As a result, SAS 70 often was misused as a means to obtain assurance regarding compliance and operations to addressing control concerns, i.e., "one size fits all".

The SAS 70 standard did not completely disappear. It still provides guidance for independent auditors when performing financial statement audits.

7) What does this mean for me? What can I do to make sure that Penn receives the right report?

Since these changes to the attestation standards and reporting options are still fairly new, the industry will need to become more familiar with the differences in SOC reports. As a result, expect to see a majority of SSAE 16 (SOC 1) reports issued, even if the subject matter is not reporting on controls that may affect user organizations' financial reporting.

a) Revisit existing contracts (and address in new contracts) with third parties performing transaction processing/hosting services to Penn. Is there a requirement for the third party to provide Penn with a SOC report? If not, have we included a "right to audit" clause?

b) Continue to discuss with third parties what SOC report benefits Penn and provides the most value. For example, a data center providing physical hosting of Penn infrastructure really should not be providing a SOC 1 report. As noted earlier, it will take time for the industry to become familiar with the changes in attestation standards and reporting options. Organizational maturity will likely be linked to willingness to change.

c) For a SOC 1 (SSAE 16) report, review the User Control Considerations section. User Control Considerations are controls that the service organization states that user organizations must also have in place for the service organization's "system" of controls to be effective. This is an area that was usually neglected by parties who received SAS 70 reports. An example of a User Organization Consideration could be: "*User organizations should have controls in place to restrict access to the secure web portal that is used to transmit data to the service organization to only authorized individuals. Controls should include notifying the service organization when an individual's access is no longer required or if authentication credentials have been compromised."* In other words, the service organization is communicating to the user organization that the service organization is not responsible for the design, implementation, and effectiveness of this control.

8) **Who can I contact with questions about SOC reports?**

When in doubt, seek assistance from OACP and ISC Security (and OGC, as appropriate). OACP, ISC Security, and OGC can review contracts to ensure that Penn has a means to assess the third party's control effectiveness. Similarly, OACP and ISC Security can assist in discussions with third parties about the differences in SOC engagements and review SOC reports provided by third parties to determine their usefulness to Penn and whether there are issues that should be discussed.

For more information, contact:

- Kevin Secrest, IT Audit Manager
  ksecrest@upenn.edu
  215-573-4495

- Josh Beeman, University Information Security Officer
  jbeeman@isc.upenn.edu
  215-746-7077