Service Organization Controls

From Wikipedia, the free encyclopedia

Service Organization Controls are a series of accounting standards that measure the control of financial information for a service organization. They are covered under both the SSAE 16 and the ISAE 3402 professional standards.

SOC 1 reports are examination engagements undertaken by a service auditor to report on controls at an organization that provides services to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting.

SOC 1 overview [edit]

SOC 1 reports, which have effectively replaced SAS 70 reports as of June 15, 2011, will be prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. SOC 1 reports retain the original purpose of SAS 70 by providing a means of reporting on the system of internal control for purposes of complying with internal control over financial reporting. SOC 1 reports are restricted use reports, which mean use of the reports is restricted to:

- Management of the service organization (the company who has the SOC 1 performed),
- User entities of the service organization (service organization's clients), and
- The user entities' financial auditors (user auditor). The report can assist the user entities' financial auditors with laws and regulations such as the Sarbanes-Oxley Act. A SOC 1 enables the user auditor to perform risk assessment procedures, and if a Type II report is performed, to assess the risk of material misstatement of financial statement assertions affected by the service organization's processing.

For reports that are not specifically focused on internal controls over financial reporting, SOC 2 and SOC 3 reports should be used. These reports will focus on controls at a service organization relevant to security, availability, processing integrity, confidentiality, and/or privacy. In the past, SAS 70 reports often encompassed financial reporting controls, operational controls, and compliance controls.[1]

SOC 1 type I and type II Reports [edit]

As with SAS 70 reports, both SOC 1 type I and type II reports can be issued:[2]

- Type I – a type I is a report on policies and procedures placed in operation as of a specified point in time. SSAE 16 type I reports evaluate the design effectiveness of a service provider's controls and then confirms that the controls have been placed in operation as of a specific date.
- Type II – a type II is a report on policies and procedures placed in operation and tests of operating effectiveness for a period of time. SSAE 16 type II reports include the examination and confirmation steps involved in a type I examination plus include an evaluation of the operating effectiveness of the controls for a period of at least six consecutive calendar months. Most user organizations require their service provider to undergo the type II level examination for the greater level of assurance it provides.

SOC 2 overview [edit]

In January, the AICPA Assurance Services Executive Committee (ASEC) released the revised version of the Trust Services Principles and Criteria (TSP). The new 2014 version of the TSP, now referenced as TSP Section 100, supersedes the 2009 version and is mandatory for examination periods ending on or after December 15, 2014. With these new modifications enacted, the AICPA offers significant changes for auditors, partners, customers, and regulators to bring confidentiality and security measures in line with current security concerns worldwide. While no specific changes have been finalized for the Privacy Principle criteria, major changes to the non-privacy principles include changes in definitions, an all-encompassing Security principle, and updated risk definitions. By compartmentalizing the security principle into seven unique categories, the AICPA increases the relevance of these documents for stakeholders by providing increased organizational oversight and corporate governance, a comprehensive risk management processes, and increased regulatory oversight. BrightLine reviewed the changes and below is a synopsis of the major changes:[3]

The new security principle [edit]

One major difference is that the Security Principle now consists of "Criteria Common to All Principles." The Common Criteria are applicable to four of the five TSPs, known as the non-privacy principles, and are addressed only once in the report, rather than each principle addressing portions of common criteria, allowing for greater efficiency in the report. As a result, all SOC 2 examinations performed under the new standards must couple the Security Principle with any non-privacy principle. For instance, a SOC 2 that includes the Availability Principle must also include the Security Principle. Prior to the 2014 updated TSP Section 100, just one of the four non-privacy principles could be included in scope.

The Security Principle was restructured into the following seven categories:

- **Organization and management:** The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.
- **Communications:** The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
- **Risk management and design and implementation of controls:** The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
- **Monitoring of controls:** The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.
- **Logical and physical access controls:** The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.
- **System operations:** The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.
- **Change management:** The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

The other non-privacy principles, Availability, Processing Integrity, and Confidentiality, have also been modified to include criteria that is only applicable the specific principle. This greatly reduces the redundancies found in the old TSPs when more than one non-privacy principle was in scope for the SOC 2 examination.

New definitions [edit]

TSP Section 100 now includes modifications, or clarifications, to the definitions of the four non-privacy principles. The definitions listed below include these modifications:

- Security: The system is protected against unauthorized access, use, or modification
- Availability: The system is available for operation and use as committed or agreed
- Processing Integrity: System processing is complete, valid, accurate, timely, and authorized
- Confidentiality: Information designated as confidential is protected as committed or agreed
- Privacy: The system's collection, use, retention, disclosure, and disposal of personal information are in conformity with the commitments in the service organization's privacy notice and with criteria set forth in the Generally Accepted Privacy Principles (GAPP) issued by the AICPA and CICA

References [edit]

1. ^ "SSAE 16 (SOC 1) Overview" .
2. ^ "SOC Reports Information for Service Organizations" . AICPA.
3. ^ "Comparison: Old TSP to New TSP" .

Categories: Standards by organization