www.pwc.com/us/thirdpartyassurance

SOC 2 and 3: Building customer trust through controls reporting

Covers reporting on controls that go beyond internal control over financial reporting

Presents the three SOC reporting options and highlights recent SOC 2 and SOC 3 changes, observations, and trends

A brief introduction to SOC 1, SOC 2, and SOC 3

Companies have increasingly looked to outsourcing over the past few decades as a means of reducing costs and improving processing efficiency. From 2012 to 2017, the size of the US business process outsourcing market will increase by 23.3%.[1] The growing rates of adoption of software as a service, platform as a service, and other cloud-based infrastructure models to store customers' sensitive information will continue to drive increases in outsourcing. Because of those increases, the need for auditor reporting on internal controls at a third-party entity (or "service organization") has also increased. Also known as a Statement on Standards for Attestation Engagements (SSAE) 16 report, the Service Organization Control (SOC) Report 1 is designed to deal with internal controls over financial reporting (ICFR), but it does not cover broader operational and compliance control needs for user organizations.

The American Institute of CPAs (AICPA) and the Canadian Institute of Chartered Accountants (CICA) understand the need for reporting on controls in situations other than those directly involving ICFR, and to that end, they created two reporting vehicles to meet this need: SOC 2 and SOC 3. As described in this paper, SOC 2 and SOC 3 reports use the Trust Services Principles and Criteria as a framework for reporting on a service organization's operational and compliance controls relevant to user organizations.

SOC 2 and SOC 3 reports provide companies with an option to obtain the assurance they need over compliance and operational controls for functions they outsource to third parties.

What is the basic difference between SOC 1, 2, and 3 reports?

Reporting on internal controls over financial reporting

SOC 1: A direct replacement for the Statement on Auditing Standards No. 70, Service Organizations, report, a SOC 1 report opines on controls operating at a service organization that have a direct impact on user entities' ICFR. SOC 1 reports are not permitted to report on controls beyond ICFR. Because SOC 1 reports are more common in the marketplace, the focus of this paper is on SOC 2 and SOC 3 reports.

Reporting on controls beyond financial reporting

SOC 2: A SOC 2 report provides reporting options beyond ICFR. A SOC 2 opines on controls relevant to security, availability, processing integrity, confidentiality, and/or privacy (referred to in total as the Trust Services Principles) at a service organization and does so in a format similar in detail to a SOC 1 report.

SOC 3: A SOC 3 report is very similar to a SOC 2 but with a few main differences, such as (1) the information presented in a SOC 3 report is truncated (no controls, test procedures, or results) and (2) distribution of the SOC 3 report is unrestricted—meaning, it can be shared with anyone.

This paper explores the appropriate application and content of SOC 2 and SOC 3 reports.

[1] IDC, Worldwide and US Business Process Outsourcing Services 2013–2017 Forecast, May 2013, and PwC analysis.

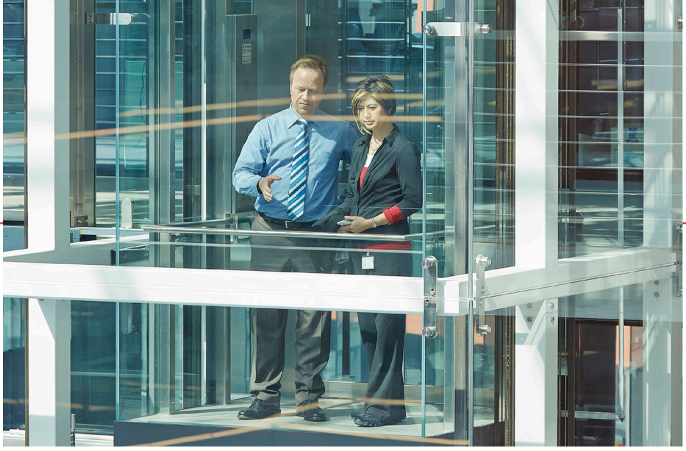
SOC reports compared

The following table compares the purpose and benefits of the three SOC reports.

Reporting Option	Service Organization Control Report No. 1 (SOC 1/SSAE 16)	Service Organization Control Report No. 2 (SOC 2)	Service Organization Control Report No. 3 (SOC 3)
Purpose	Report on internal control over financial reporting	Report on controls at a service organization that are relevant to the Trust Services principles: security, availability, processing integrity, confidentiality, and privacy	
Benefits	• Familiarity in marketplace • Provides transparency on the system description, the controls, the test procedures and the results thereof • Restricted in use to the user entity and its auditors	• Provides a level of transparency similar to that of a SOC 1—specifically, description of the system, test of procedures, and results • Restricted in use to the user entity, its auditors, and other specified parties that have knowledge of the system	• General distribution of report yields marketing benefits • Abbreviated report is missing auditors' testing and results
Report Sections	Section 1—Report of Independent Service Auditor Section 2—Management's Assertion Section 3—Description of the Service Organization's System Section 4—For Type 2 reports, description of tests and related results		Section 1—Report of Independent Service Auditor Section 2—Management's Assertion Section 3—Description of scope, or boundaries of system
Opinion	• Whether the description of the service organization's system is presented fairly • Whether the controls are suitably designed to provide reasonable assurance that the applicable control objectives/Trust Services criteria would be met if the controls operated effectively • For type 2 reports, whether the controls were operating effectively during a defined period to achieve/meet applicable control objectives/Trust Services criteria		Whether the entity maintained effective controls over its system as it relates to the Trust Services Principle(s) being reported on

A SOC report can be issued as a type 1 (point-in-time opinion addressing mainly the design of controls) or a type 2 (opinion spanning a defined period of time to address operating effectiveness).

What are the Trust Services Principles?



There are *five* Trust Services Principles. Each principle is supported by defined criteria that must be met in order to have a suitably designed system in place. Following is an overview of each principle with a non exhaustive list of specified criteria for reference purposes. Note: These principles were updated effective December 15, 2014.

	Principle	Criteria
Security	The system is protected against unauthorized access (both physical and logical).	Focuses on the implementation and dissemination of a security policy and accompanying procedures that include but are not limited to: • Security requirements of authorized users • Communication and risk assessment • Assignment of responsibility and accountability • Training and compliance with laws and regulations • Handling of security breaches and other incidents
Availability	The system is available for operation and use as committed or agreed.	Focuses on the definition of availability requirements for systems, and in its policies and procedures, requires but is not limited to: • Implementation of measures that prevent or mitigate threats • Exception-handling procedures regarding system availability • Procedures that provide for the integrity of backup data and systems maintained to support related security policies
Confidentiality	Information designated as confidential is protected as committed or agreed.	Focuses on the definition of confidentiality requirements for systems, and in its policies and procedures, requires but is not limited to: • Procedures related to confidentiality of inputs, data processing, and outputs that are consistent with policies • Understanding of ways that confidential information gets accessed, used, and disclosed • Protection of confidential information during change management activities
Processing Integrity	System processing is complete, accurate, timely, and authorized.	Focuses on the documentation and implementation of controls to confirm that system processing takes place as appropriate, and in its policies and procedures, requires but is not limited to: • Procedures related to completeness, accuracy, timeliness, and authorization of inputs consistent with policies • Procedures for exception handling of issues that is consistent with policies **Note:** additional requirements apply to e-commerce systems
Privacy	Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in the GAPP issued by the AICPA and CICA.*	The Privacy Trust Services Principle is the largest of the principles and requires the definition, documentation, and communication of, as well as accountability for, privacy-related policies and procedures. As part of the privacy policies and procedures, the service organization must consider and have in place such procedures and accompanying disclosures as: • management of privacy policies and procedures • collection, use, retention and disposal of personal information • disclosure of personal information to third parties • privacy incident and breach management *At the time of publication, generally accepted privacy principles (GAPP) are currently under AICPA review.

Trust Services Principles reporting

SOC 2 and SOC 3 reports use the same framework: the Trust Services Principles and Criteria. The Trust Services Principles to be reported on are selected by a service organization, meaning that the service organization can select any single Trust Services Principle or combination of Trust Services Principles to be included in the scope of its SOC 2 or SOC 3 Report. Such flexibility creates unique advantages by enabling a service organization to strategically assess its organizational components and to target the principles that are of greatest interest to its user entities and potential user entities. Once a principle gets included in the scope, all related criteria are required to be addressed in the SOC 2 or SOC 3 Report.

Comparison of users of the report

SOC 2: SOC 2 reports are intended for knowledgeable parties and stakeholders with broad understanding of internal controls and their limitations, of the specific services being provided, and of the ways that user entities use the service organization's system and that potential user entities could use it. Those users could include but are not limited to:

- Management of the service organization
- Existing customers
- Prospective customers
- Regulators

SOC 3: SOC 3 reports are general-use reports, which means anyone can be a user of these reports.

Testing and content of SOC 2/SOC 3 reports

Although the scope can be the same, SOC 3 reports contain less detail than SOC 2 reports do, and they're often valued for their marketing benefits. SOC 3 reports do not contain detailed description of the service organization's system, nor do they contain description of the service auditor's tests of operating effectiveness or results of those tests.

As part of both reports, the service organization provides a management assertion, which gets validated by the service auditor and which must include the following five components: infrastructure, software, people, procedures, and data.

Components of the Service Organization's System

Infrastructure

The physical hardware components of a system (facilities, equipment, and networks)

Software

The programs and operating software of a system (system, applications, and utilities)

People

The personnel involved in the operation and use of a system (developers, operators, users, and managers)

Procedure

The programmed and manual procedures involved in the operation of a system (automated and manual)

Data

The information used and supported by a system (transaction, streams, files, databases, and tables)

Updated criteria for 2014

In January 2014, the AICPA recognized the need for a revision to the Trust Services Principles and Criteria after receiving feedback from both user entities and service auditors that increases in clarity and reductions in redundancy would benefit the reports.

Many of the criteria applied in the evaluation of a system are shared among all of the principles—for example, the criteria related to risk management apply to the security, availability, processing integrity, confidentiality, and privacy principles.

As a result, the criteria for the security, availability, processing integrity, and confidentiality principles are organized into (1) criteria applicable to all four principles (or “common criteria”) and (2) criteria applicable to only a single principle.

The common criteria constitute the complete set of criteria for the security principle. For the principles of availability, processing integrity, confidentiality, and privacy, a complete set of criteria is composed of all of the common criteria and all of the additional criteria applicable to the principle(s) being reported on.

Historically, because of the interrelated nature of the Trust Services Principles, a trend PwC has observed is that service organizations are including both the security principle and the availability principle in their initial SOC 2 or SOC 3 reports. Doing so enabled service organizations to address multiple items required by their user entities; however, the inclusion created a considerable amount of redundancy throughout the principles and resulted in a voluminous report. Updated criteria, released in 2014, removed those redundancies and will lead to streamlined and more-efficient reporting.

The privacy principle is being revised, and reporting on the privacy principle is not currently affected by alignment to the common criteria.

The updated Trust Services Principles and Criteria are effective for periods ended on or ending after December 15, 2014.

Updated criteria for 2014 *(continued)*

The common criteria are organized into seven categories that align with the key concepts of the Committee of Sponsoring Organizations of the Treadway Commission's framework.

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.

SOC 2 reporting observations and trends

Demand for SOC 2 reports

Demand for SOC 2 reports has increased greatly in the past 12 months. Unlike demand for SOC 1 reports, demand for SOC 2 reports is not typically coming from user entities' accounting or finance organizations or the user entities' auditors. Instead, we see demand being driven mainly by user entities' technology, risk management, operations, and line-of-business organizations. Service organizations should always seek to understand the reasons for requests they receive from their user entities because such understanding helps facilitate the structuring of the principles included in the report.

Starting with security

It has been our experience that most companies are opting to report on one or two Trust Services Principles in their first SOC 2 report—namely, Security and one other principle, if required. Such a practical and measured approach has enabled clients to focus on meeting the criteria of each selected principle while continuing to strengthen their businesses' maturity in other areas so as to better position themselves to increase the scope of their reports in future reporting cycles, if necessary. Year over year, service organizations can consider adding new processes, facilities, or principles to the scope of their reports. Generally, the decision to add to the scope of SOC 2 reports results from explicit requests received from user entities, or from changes in business risks, or from changes in the organization's products and services.

Privacy

The complexity of the Privacy Principle and related criteria as well as the high level of effort required from the service organization and the respective service auditor has led many organizations to avoid and/or delay including the privacy principle in their reports. Therefore, very few reports that include the privacy principle have been issued.

To date, the most common reporting request is for the Security Principle, followed by the Availability Principle.

Clients attempting to achieve compliance with the Privacy Principle have required the most preparation because of the depth and breadth associated with this principle.

Dual Reporting

Occasionally, service organizations request that SOC 2 and SOC 3 reports be issued for the same environment. Service organizations are finding that by having both reports issued, they can provide current user entities with the level of details they require in the SOC 2 report while using the SOC 3 report for marketing purposes. This helps differentiate themselves from their competition.

What’s next?

Determining the right fit

When a company is deciding on the most appropriate reporting option, the first question to ask is whether the existing control report, or lack thereof, is satisfying users’ needs. If user entities’ focus is limited to internal controls over financial reporting, a SOC 1 report may be sufficient. If a user is concerned about processes that are not related to financial reporting including security, availability, processing integrity, confidentiality, or privacy, a SOC 2 or SOC 3 report would be a better fit. In situations when a SOC 2 or SOC 3 has been determined to be the right solution based on users’ needs, an evaluation should be made about whether users will need detail around the system description, the tests performed by the auditor, and the results of the testing performed. If that level of detail is determined to be required, a SOC 2 would be appropriate. If a branded report without all of the details would be adequate, a SOC 3 may be the right choice.

Executing the engagement

When an organization plans to issue a SOC 2 or SOC 3 report, we typically recommend a phased approach from readiness through to the ultimately execution of a type 2 engagement. The phased approach to obtain a SOC 2 or SOC 3 report helps:

- Properly define customers’ reporting needs and expectations.
- Identify and assess appropriate controls.
- Pave the way for an efficient SOC engagement.
- Minimize the potential risk of exceptions being reported.

What if a SOC 2 report would cover almost everything you need?

If you or your customers believe that the Trust Services Principles and Criteria cover most of your collective areas of concern, but the framework is still missing certain areas that you would want to include in a SOC 2 report (e.g., system development life cycle controls, vendor management controls, etc.), you may be interested in our companion thought leadership piece entitled “Vendor Controls Assurance (SOC 2+): A cost effective approach to building customer trust.” This article presents a new controls reporting solution that builds upon the SOC 2 framework and provides vendors/service organizations with an opportunity to further reduce costs, decrease customer audits, and differentiate itself from its peers.

Although the service auditor can assist in any or all of the following phases, the typical progression of phases that an organization goes through is as follows.

Phase 1

Determine the reporting type: Discussed earlier, this includes determining your reporting objectives and agreeing on the appropriate report type and Trust Services Principles for inclusion.

Phase 2

Readiness assessment: The primary benefits of a readiness assessment are to assess the current-state environment, identify relevant controls, and reduce the risk of reporting exceptions in the final report. The service auditor will work to understand your current control environment, identify any gaps in your control environment, and provide recommendations to address any gaps identified.

Phase 3

Management remediation: Utilizing the results of the readiness assessment, management develops and implements remediation plans in order to be ready for reporting. The service auditor can assist management throughout this process by providing advice and reviewing the remediation plans developed and implemented by management.

Phase 4

Type 1 report: An attestation engagement is performed over the agreed-upon Trust Services principles. The auditor will perform testing over management's control activities, and an opinion will be issued regarding whether those controls are suitably designed and placed in operation as of a point in time (e.g. December/31/2013).

Phase 5

Type 2 report: An attestation engagement is performed over the agreed-upon Trust Services Principles. The auditor will perform testing over management's control activities, and an opinion will be issued regarding whether controls are suitably designed, placed in operation, and operating effectively for a period of time. The testing required for a type 2 report is significantly more than a type 1 in order for the service organization to demonstrate the consistent operation over a period of time (e.g. January 1, 2013-December 31, 2013).

Contacts

Clarity over service providers' controls can go far to strengthen your brand and operations. PwC offers a full range of service organization control reports. By developing and delivering an independent and customized attestation, we pave the way so a service organization can approach both existing and prospective customers with confidence—and vigorously convey the trust and transparency that those customers need and expect. In providing those assurances, PwC frees organizations to focus on areas that serve to drive a business forward.

To have a deeper conversation on SOC reporting and on Trust Services Principles and Criteria, contact:

Todd Bialick
Third Party Assurance Leader
(973) 236 4902
todd.bialick@pwc.com

Kevin Knight
Partner, Third Party Assurance
(703) 918 3505
kevin.knight@pwc.com

Dave Benson
Director, Third Party Assurance
(267) 330 2269
david.benson@pwc.com

Steve Dobson
Director, Third Party Assurance
(704) 347 1627
steven.dobson@pwc.com

www.pwc.com

MW-15-1157