



Information Systems Audit and Controls Association

Service Organization Control (SOC) Reports — Focus on SOC 2 Reporting Standard

February 4, 2014

**Tom Haberman,
Principal, Deloitte & Touche LLP**

**Reema Singh,
Senior Manager, Deloitte & Touche LLP**



Agenda

Overview of Service Organization Control (SOC) reports

Overview of SOC 2 reports

SOC 2 reports — industry application

Overview of a Service Organization Control (SOC) report

What is a Service Organization Control (SOC) report?

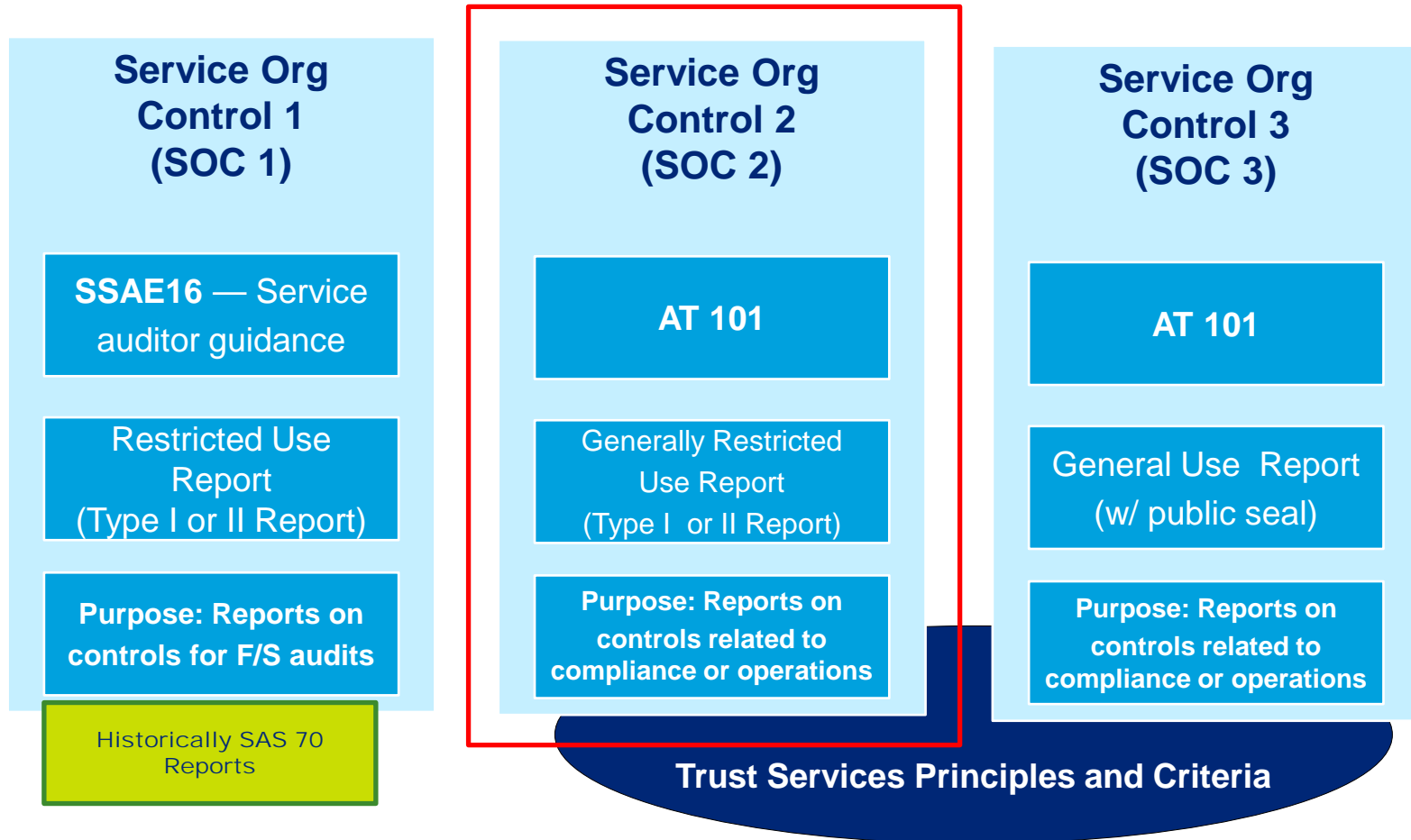
What is a SOC report?	“Service Organization Controls reports are designed to help service organizations, organizations that operate information systems and provide information system services to other entities, build trust and confidence in their service delivery processes and controls through a report by an independent certified public accountant.” ¹
So what does this mean?	SOC reports cover situations where one company outsources some portion of their business or technology to another company.
What is a SOC 2 report?	SOC 2 reports are an examination engagement to report on controls at a service organization intended to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy (trust services principles).
What are a few examples of SOC 2 reports?	Examples of service providers where a SOC 2 report might be relevant include cloud computing, customer call centers, enterprise IT outsourced services.

¹ — Definition from AICPA

<http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx>

Types of service organization control reports

New standards and options



Key terms relative to SOC reports

Service auditor	A practitioner who reports on controls at a service organization.
Service organization	An organization or segment of an organization that provides services to user entities, which are likely to be relevant to those user entities' internal control over financial reporting.
Subservice organization	A service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting.
User entity	An entity that uses a service organization.
Applicable trust services criteria	The criteria in Trust Services Principles (TSP) section 100, i.e., <i>Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids)</i> , that are applicable to the principle(s) being reported on. These are issued by the Assurance Services Executive Committee of the AICPA (the committee).
Boundaries of the system	The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services.

Key terms relative to SOC reports (cont.)

Engagement letter	A formal letter representing the written contract between the service auditor and the service organization to perform SOC services.
Management assertion	A written statement by management of the service organization regarding the description of the service organization's system; the suitability of the design of the controls; and in a Type 2 report, the operating effectiveness of the controls.
Management representation letter	A letter signed by management of the service organization that includes written statements of facts or representations that controls are suitably designed and implemented (Type 1) and operating effectively (Type 2).
Test of controls	A procedure designed to evaluate the operating effectiveness of controls in achieving the control objectives stated in management's description of the service organization's system.

Additional definitions are available in Appendix D of the AICPA Guide, "Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)"

Overview of SOC 2 reports

SOC 2 overview

Topic	SOC 2 guidance
Professional guidance	AICPA Attestation engagement under AT section 101 AICPA Guide, “Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy”
Effective date	As of May 2011
Scope	Controls at a service organization intended to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy (trust services principles)
Application of SOC 2	<ul style="list-style-type: none">• SOC 2 can be applied for regulatory or non-regulatory purposes to cover business areas outside of financial reporting.• The report can be distributed to customers and other stakeholders to demonstrate a focus on system and processing controls to meet their requirements.• SOC 2 can be applied to virtually every industry and business sector. SOC 2 will allow service organizations to provide assurance to customers and other stakeholders that effective internal controls are in place.

SOC 2 overview (cont.)

- SOC 2 is an AICPA report that allows service auditor to provide an opinion on the following principles:
 - Security
 - Availability
 - Processing integrity
 - Confidentiality
 - Privacy
- Can include one or more of the above trust services principles but may need to address entire principle scoped in unless it was deemed not applicable. That would need to be documented.
- In a SOC 2 report, the AICPA has supplied the criteria, where in a Statement on Standards for Attestation Engagements No. 16 (SSAE 16)/SOC 1, management specifies the objectives and controls. So, SOC 2 reports should be much more consistent across the marketplace.
 - Exception is for SOC 2 reports which cover privacy. These reports would also need to include the service organization's privacy policy, which could obviously vary from organization to organization.

SOC 2 principles

Security

- IT security policy
- Security awareness and communication
- Risk assessment
- Logical access
- Physical access
- Environmental controls
- Security monitoring (breaches)
- User authentication
- Incident management
- Asset classification and management
- Systems development and maintenance
- Configuration management

Availability

- Availability policy
- Backup and restoration
- Disaster recovery

Confidentiality

- Confidentiality policy
- Confidentiality of inputs
- Confidentiality of data processing
- Confidentiality of outputs
- Information disclosures (including third parties)
- Confidentiality of Information in systems development

Processing integrity

- System processing integrity policies
- Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs
- Information tracing from source to disposition

Privacy

- Notice
- Choice
- On-ward transfer
- Access
- Security
- Data Integrity
- Training and awareness
- Enforcement and compliance

Security versus privacy

- These terms are often confused.
- *Security* relates to the authorization of transactions and protection of the integrity of those transactions throughout the system and also protecting personal and other information from unauthorized use or disclosure from the time it is collected until the time it is disposed of.
- *Security* may also relate to the protection of the system from interruptions in processing availability.
- *Privacy* encompasses a much broader set of activities beyond security that contribute to the effectiveness of a privacy program, including, for example, providing users with the following:
 - Notice of the service organization's privacy commitments and practices
 - Choice regarding the use and disclosure of their personal information (PII)
 - Access to their personal information for review and update
 - An inquiry, complaint, and dispute resolution process

Service Auditor's opinion on a SOC 2 engagement

In a SOC 2 report, the service auditor expresses an opinion on the following:

- Whether the description of the service organization's system is fairly presented
- Whether the controls are suitably designed to provide reasonable assurance that the applicable trust services criteria could be met if the controls operated effectively
- In Type 2 reports, whether the controls were operating effectively to meet the applicable trust services criteria
- In engagements to report on the privacy principle, whether the service organization complied with the commitments in its statement of privacy practices

Type 1 and Type 2 SOC 2 reports

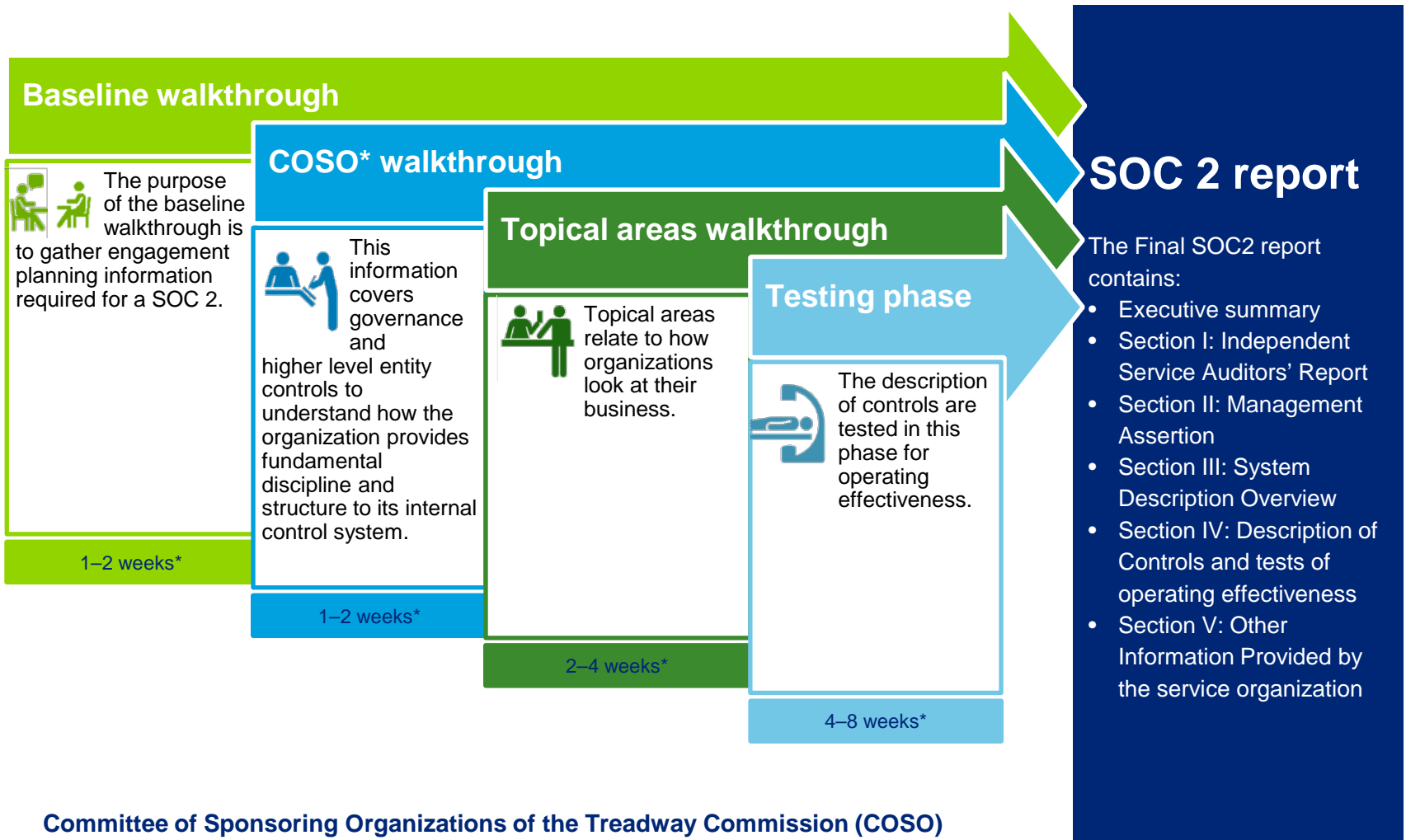
- Type 1
 - Reports on controls placed in operation (as of a point in time)
 - Looks at the design and implementation of controls; not operating effectiveness
 - Considered for information purposes only
 - Often performed only in the first year a client has a SOC report completed
- Type 2
 - Reports on the design, implementation and operating effectiveness over a period of time (generally not less than six months)
 - Includes tests of operating effectiveness and results
 - More comprehensive
 - Requires more internal and external effort
 - More emphasis on evidential matter

Neither a Type 1 or Type 2 SOC 2 report can be used for reliance purposes by financial auditors.

SOC 2 reports — summary of benefits

- Reports can be referenced by boards as part of their oversight responsibility of service providers
- Reduces questions and site visits from clients, prospective clients to the service provider
- Often requested by prospective clients during the due diligence process
- Can act as a differentiator from competitors during new business negotiation process
- Certain organizations are requiring the issuance of SOC 2 reports as a part of the service contracts and agreements
- Demonstrate compliance with regulatory and legal requirements (such as Federal Information Security Management Act (FISMA))

Components of a SOC 2 report



How does SOC 2 differ from SSAE 16/SOC 1?

- Similar in structure and general approach to SOC 1:
 - An option for a Type 1 or Type 2 report.
 - An opinion
 - An assertion
 - A section describing the processing environment
 - Description of control objectives, control activities, and tests
 - Management representation letter
- A SOC 2 report does not need to cover processing related to financial reporting, nor is it intended to support financial reporting for your users.
- SOC 2 can be supplied to a wider audience.
 - Intended users are management of the service organization, user entities, and other “specified parties.”
 - Specified parties can be anyone who understands the nature of the services being provided by the service organization, how the service organization operates, and internal controls.

How does SOC 2 differ from SSAE 16/SOC 1?

- Many practitioners who have looked at SOC 2 feel it will provide more technical detail throughout the report; narrative section, control activities, tests, etc. than the existing SOC 1 reports.

Is SOC 2 the right report for your purpose?

	SOC 1 report	SOC 2 report	SOC 3 report
Professional standard used	AT 801	AT 101	AT 101
Used by auditors to plan and perform financial audits	Yes	No	No
Used by user entities to gain confidence and place trust in service organization systems	No	Yes	Yes
Obtain details of the processing performed and related controls, the tests performed by the service auditor and results of those tests	Yes	Yes	No
Report generally available — can be freely distributed or posted on a website as a “SysTrust for Service Organizations” seal	No	No	Yes

Is SOC 2 the right report for your purpose?

Challenges

- Deciding on the right principle(s) to include in scope
 - We recommend inventorying customers' requests
 - Align with overall departmental/company strategies
- Drawing report boundaries
 - Few organizations had a previous need to look at their systems in the manner needed for a SOC 2
 - Example — tracing PII through the environment
 - Smaller, non-public organizations selling to SEC Filers
 - Extent of policies and procedures needed seen as extensive
- Level of precision to meet principles and criteria

SOC 2 reports — industry application

SOC 2 reports — industry application

Market feedback

Marketplace appears to be embracing the product:

- Security principal is being used extensively
- Software as a Service (SAAS) providers are taking advantage of “full” reports by covering all 5 areas
- Smaller service organizations are issuing SOC 2 reports
- Jury is still out on standalone Privacy reports

Service providers appreciate the “closed” nature of SOC 2 Guidance:

- Trust Principles draw some “bright lines” around definitions of sound security, privacy, etc.
- Guidance seen as proscriptive
- Can be provided to both current users as well as prospective users

Still to come:

- SOC 2 to replace individual on-site audits and questionnaires
- SOC 2 to replace aspects of regulatory exams

SOC 2 illustrative applications

Illustrative applications of SOC 2 reports

SOC 2 reports provide a way to build trust with customers and demonstrate compliance in controls with various industry regulations and standards.

Consolidation SOC 2

Multiple surveys or questionnaires from user entities can be encompassed under a consolidated SOC 2 report.



ISO

ISO 27001, 27002 regulations can be reported under the SOC 2 reporting framework.



Career College Initiative

For-profit colleges can provide assurance that they meet a voluntary set of operating standards.



FISMA

Agencies with federal contracts can demonstrate that controls meet the FISMA requirements.



Smart Grid

Smart grid companies can demonstrate compliance with various regulatory body requirements, industry frameworks, and standards.



Cloud Computing

Cloud service providers can give their customers assurance of effective controls across the SOC 2 Trust Principles.

SOC 2 illustrative applications

Call centers

Call center services

- SOC 1 may not be a good fit because while call center services are important from a business perspective, the processes executed may not be financially significant for customers of a service provider.
- User organizations may be concerned about handling of end-customer information and a SOC 2 report may demonstrate that there are controls encompassing the security, confidentiality, and privacy of information.

SOC 2 illustrative applications

Medical claims processing

Medical claims processing service provider

- A SOC 2 report focused on processing integrity (completeness, accuracy, timelines, etc.) could provide customers with comfort regarding the controls over transactions in claims processing. This may be prepared in addition to a SOC 1 report leveraging existing controls and testing.

SOC 2 illustrative applications

Information technology services

Data center hosting

- SOC 1 or SOC 2 may be a good fit for these types of services. Hosting does have relevance to Internal Controls over Financial Reporting (ICFR), however there could be security and availability concerns that may be addressed with a SOC 2 report.

Cloud service providers

- Cloud service providers need to provide their customers assurance of effective controls across the SOC 2 trust principles in order for those customers to comfortably entrust the cloud provider with their sensitive data and critical computing needs. SOC 2 reports provide a way to build trust with customers and demonstrate compliance in controls with various industry regulations and standards (e.g., The Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH), Gramm-Leach-Bliley Act (GLBA), FISMA).

SOC 2 illustrative applications

Financial services

Credit card processing

- A SOC 1 or SOC 2 are both alternatives. Payment card processing may have relevance to a user's ICFR, thus fitting the SOC 1 criteria. From a SOC 2 perspective the report may cover a number of principles of interest including security, confidentiality, availability, integrity of processing, and privacy of the credit card holders personal information.

SOC 2 illustrative applications

Power and utility companies

Power and utility compliance

- Power and utilities companies can leverage SOC 2 to demonstrate compliance with various regulatory body requirements, industry frameworks, and standards such as *Natural Environment Research Council (NERC) Critical Infrastructure Protection (NERC CIP)*, *Smart Grid: National Institute of Standards and Technology (NIST) IR 7628 — Guidelines for Smart Grid Cyber Security*, *Advanced Metering Infrastructure (AMI) — Securities and Exchange Commission (SEC) System Security Requirements*, and state privacy requirements.

Questions?



Official Professional Services Sponsor

Professional Services means audit, tax, consulting and financial advisory services.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2014 Deloitte Development LLC. All rights reserved.

36 USC 220506

Member of Deloitte Touche Tohmatsu Limited