We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

SOC Report Training

March 12, 2024

Presented by: Joel Eshleman, CPA, CISA, CIA

Principal, Specialized Advisory Services

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

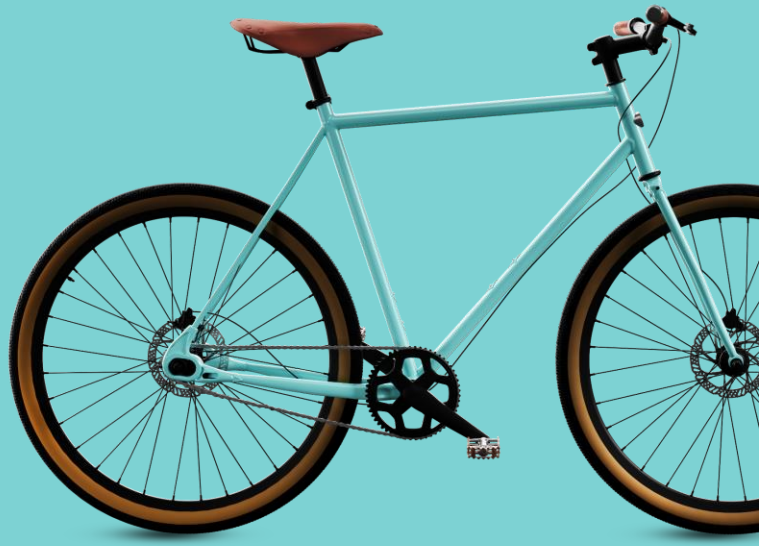
Learning Objectives

At the end of this session, you will be able to:

- Identify how to read an SOC Report
- Recognize the section of an SOC report
- Identify the purpose of the sections of SOC Report
- Discuss the details that are included in each section of the SOC Report
- Explain how the SOC auditors assesses each section of an SOC Report
- Recognize service organization responsibilities

Service Organization Controls (SOC) Engagements

Overview



Overview – What is a SOC report?

Service organization controls (SOC)/assurance engagements/service auditors' reports are intended to provide user entities with reasonable assurance that controls within the service organization are:

- Described accurately
- Suitably designed based on services provided, types of data processed/maintained and the overall operational environment of the service organization
- Operated effectively for a specified reporting period which is typically either 6, 9 or 12 months (Type 2)

What is a SOC Report?

SOC engagements are different than an IT audit or General (Computer) Controls Review (GCR)

SOC engagements are under the “umbrella” of Attestation (Assurance) services and require review by a designated SOC Principal and Quality Technical Reviewer prior to report issuance

SOC reports are intended to be distributed to user(s) of the service organizations’ operations or services

What is a SOC report?

Test(s) of controls must be supported by evidence that is documented based on standards defined by the AICPA and requirements of the independent firm performing the attestation.

SOC reports are signed by the firm and not an individual principal, director or manager.

Requires the firm to determine (and opine) if control descriptions are accurate (fairly presented).

What is an SOC report?

A service organization may choose to issue a letter that describes updates or changes in its controls since the previous report, typically referred to as a “gap” or “bridge” letter.

Management of the service organization is responsible for issuing as the audit firm does not opine or attest to the internal controls within the “gap” period.

SOC Business Driver(s)

Users of services organizations want to have trust and confidence in service provider relationships that comply with these standards (as applicable):

- Financial data has integrity (Reliable)
- Transactions or services are processed accurately/completely (Accuracy/Completeness)
- Systems are up when needed (Availability)
- Systems are secure (Security)
- Data has integrity (Processing Integrity)
- Data has protection (Confidentiality)
- Data sharing has protections (Privacy)
- Other

Additional SOC Business Driver(s)

- Sarbanes-Oxley (SOX)
- Model Audit Rule (MAR)
- Banking regulators
- HIPAA
- Marketing credentials
- Single audit (OMB)

Service Organization Controls (SOC) Engagements

Types of SOC engagements

Changes to Reporting/Standards

- Recodification into SSAE 21
  - Effective for reports issued **after June 15, 2022**
  - No substantive changes to the structure of the report or procedures
    - Required explicit statement of independence.
- Revised Points of Focus for Trust Service Criteria (SOC2)
- Revised Guidance for Description Criteria (SOC2)

SOC for Cybersecurity

Framework for entity to provide information on its cybersecurity risk management program

- Focus on TSP 100: Security, Availability, and Confidentiality
- General purpose report vs. Restricted use (SOC2)
  - Management

SOC for Supply Chain

Framework for entity to provide information on its manufacturing or development risk management program

- Focus on TSP 100: Security, Availability and Confidentiality
- Restricted use (SOC2)
  - Management and user of the product

Service Organizations

- 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
  - *An Entity that accesses, processes or maintains data on behalf of another organization*
- What is the background and profile of the service organization?
  - Are there different business units or legal entities involved?
    - Confirm the locations, nature of processing (centralization and standardization) that occurs across divisions, departments, or locations
  - Assess "Tone at the Top"
    - Risk Assessment
    - Monitoring
    - Information and Communication

Vendor vs. Third Party Service Providers vs. Subcontractors

Vendor	Subcontractor	Third Party
• A business that sells a particular type of product	• A contract between a party to an original contract and a third party	• A person other than the principals

SOC Objective(s)

- Obtain **reasonable assurance** based on **suitable criteria** that **throughout the reporting period**:
  - Descriptions were fairly presented
  - Controls were suitably designed
  - SOC1 – Control objectives stated (**relevant to financial reporting**) were achieved
  - SOC2 – Trust principle(s) criteria were met
  - Controls operated effectively during the period (Type 2)
- Issue a report on the findings in a format prescribed

SOC1 (Formerly SAS70)

SOC1 reports on suitably of control design to satisfy the **control objectives defined by management** that are relevant to client user organization's financial reporting process.

The conclusion of the SOC1 engagement will be a **Report with Auditor's Opinion** providing reasonable assurance that controls placed in operation were suitably designed to satisfy the control objectives and operating effectively for the reporting period.

SOC1 reports are "Restricted Use" and are intended to go from one CPA Firm to another.

SOC 2

SOC2 reports on suitability of control design to meet the selected Trust Service(s) criteria relevant to:

- Security of Systems
- Availability of Systems
- Confidentiality of Data
- Privacy of Data
- Processing Integrity

The conclusion of the SOC2 – Type 2 engagement is a **Report with Auditor's Opinion** providing reasonable assurance that controls placed in operation were suitably designed to meet or exceed the criteria of each relevant Trust Principle and operated effectively for the reporting period. SOC2 Reports are "Limited Use".

SOC2 - Trust Service Criteria (TSC)

Security	Availability	Processing Integrity	Confidentiality	Privacy
Information and systems are protected against unauthorized access, disclosure of information	Information and systems are available for operation and use to meet entity's objectives	System processing is complete, valid, accurate, timely and authorized to meet the entity's objectives	Information designated as confidential is protected to meet the entity's objectives	Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives

SOC Engagement Reporting Period

Type 1

The Type 1 engagement provides assurance that controls were **suitably designed** and **described accurately** as of a specific date (i.e. December 31).

Or

Type 2

The Type 2 engagement provides assurance that controls were ***suitably designed, described accurately AND*** the controls placed in operation were ***operating effectively*** for the reporting period (*i.e. January 1 through June 30*).

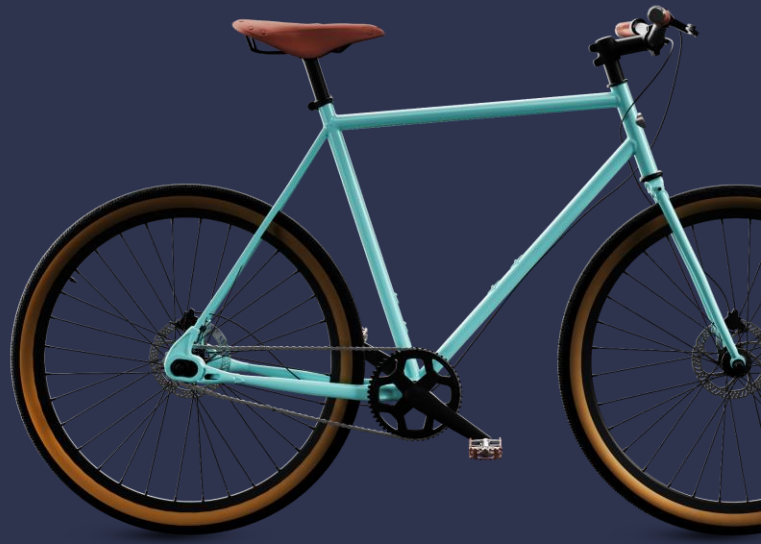
Determine if a Type 1 or Type 2 is most appropriate

SOC – Which One?

Report Usage	Response	Report Type
Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer's financial statements?	Yes	SOC1
Will the report be used by your customers as part of their compliance with the Sarbanes-Oxley Act or similar law or regulation?	Yes	SOC1
Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization's systems?	Yes	SOC2 or SOC3
Do you need to make the report generally available or seal?	Yes	SOC3
Do your customers have the need for and ability to understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests?	Yes	SOC2

Service Organization Controls (SOC) Engagements

Elements of Reporting



SOC Report Format

Section I
Independent auditor's report

Section II
Management's assertion letter

Section III
System description of controls

Section IV
Test of controls

Section V
Other information provided by the service organization
(not audited)

Independent Auditor's Report – Service Auditor Response

- Indicates what kind of report SOC1, 2, SOC for Cybersecurity, if a SOC2 will include relevant criteria (security, availability, confidentiality, privacy, processing integrity)
- Indicates use of subservice organization(s)
- Opines on the effectiveness of the design, description and operating effectiveness (if a Type 2) of the controls relative to either the control objectives (SOC1) or Trust Service Criteria (SOC2)

Management Assertion (User Organization Responsibility)

- Management's assertion is a key component of a SOC report
  - Forms the foundation for management's confirmation of scope
  - Confirms management's responsibility for the scope, description, and control environment
  - The auditor's opinion, in part, is based on validation of the reasonableness of management's assertion
  - Should be amended with acknowledgement if any qualifications are noted

Purpose of System Description (User Organization Responsibility)

- Intended to provide user entities and their auditors with information about the service organization's system that may be relevant of the user entity's internal control
- SOC1 – The AICPA standard states that the focus of the SOC1 is on controls that are likely to be relevant to user entities' internal controls over financial reporting
  - User entities
  - User entity's auditors
- User Organization Responsibility
  - Fair presentation

Purpose of System Description (cont.)

- SOC2 – Controls that affect the security, availability, or processing integrity of the systems used or the confidentiality or privacy of the information processed
  - Management of user entities
  - Assist management
- Extent of the description may vary depending on the size and complexity of the service organization and the system
- Description does not need to address every aspect of the service organization's processing or the services provided to user entities

Purpose of System Description (cont.)

Subservice Organization:
Purpose of the description of the services provided

Inclusive Method:
Service Organization
Subservice Organization

Carve Out Method:
Service Organization
Subservice Organization

Complementary User Controls

Test of Controls (both responsible)

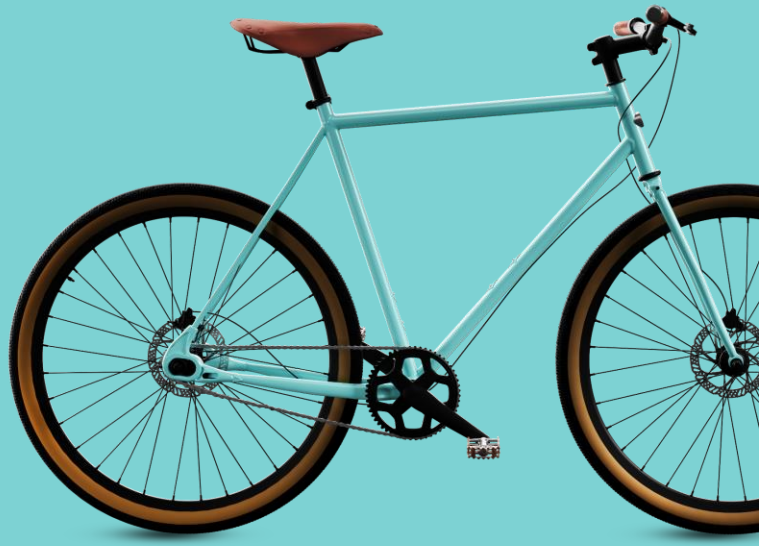
- Control activity specified by the service organization
  - For SOC1 these are controls related to the control objective
  - For SOC2 these are controls related to the selected criteria (security, availability, confidentiality, privacy, or processing integrity)
- Test of control performed by the independent auditor
- Results of testing which may include instances of nonoccurrence or any exceptions noted

Documentation Requirements for Test

- Maintain policies/procedure
  - Procedures to review
- Collect population of transactions
  - Ensure that a central point exist for transactions
    - Book of Record (financial transactions, HR activities)
    - Central log (change tickets)
- Maintain control documentation
  - Central locations (network file, ticket system, application)
  - Decentralize (email, local)
  - Who/when documents is reviewed (reconciliations)
- Ongoing monitoring for compliance

Service Organization Controls (SOC) Engagements

Management Review Actions



Periodic Vendor Risk Assessments

Size of contract – dollar and scope

Impact on your organization

Data involved

Personnel involved

Compliance

What risk factors are your organization most concerned about?

Complementary End User Controls (Auditor's Report)

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Example Trust Organization's controls are suitably designed and operating effectively, along with related controls at the service organization.

We have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

Complementary End User Controls

Controls that the service organization expects user organizations to have in place

- Disclosed in the third paragraph of the independent auditor report in the scope section and in Section III (Description of System)
- Management needs to evaluate the impact of the controls and determine if appropriate controls have been implemented
- Examples
  - Communicating or processing user changes
  - Reviewing processing reports and communicating errors
  - Validating data entry

Complementary User Entity Controls

Complementary User Entity Controls (CUEC) are a key component of the report for user organizations to fully understand and assess

Listing of controls conveyed from the service organization and service auditor highlighting key controls that users should implement to enhance the overall control environment and functions of the service organization operate as intended and are effective.

Without established or effective CUECs, minimal basis for reliance on SOC report from service organization (as opinion is based on contemplation of CUECs being implemented).

Carve Out

Services/Processes excluded from the scope of the report

- Typically disclosed in the second paragraph of the independent auditor's report under scope
- Management needs to determine the impact to the service
  - If impact is deemed significant, then a requests should be made for the sub-servicer SOC report
- Examples
  - Data center co-location
  - Statement printing
  - Pharmacy benefit manager

Carve Out

Example Trust Organization uses various subservice organizations including:

- Depository Trust Company (DTC), the Federal Reserve Bank (FED), and XYZ Bank as depositories and DEF Bank and JKL Bank as custodians to settle and safe-keep customer assets.
- ABC Company, BLB Inc, xTRA, and RTR to obtain market data and to price securities.
- BRD Inc., NR Trust, and DEF Bank to obtain corporate action services.

Example Trust Organization's control objectives and related controls, which are listed in Section IV of this report, include only the control objectives and related controls of Example Trust Organization and exclude the control objectives and related controls of these subservice organizations. Our examination did not extend to controls at the subservice organizations.

Qualifications

Service organization was unable to meeting the control objective/criteria:

- Disclosed in the opinion section of the independent auditor's report
  - Fair presentation
  - Suitably designed
  - Operating effectively
- Management needs to evaluate the impact of the qualification and work with the service organization to identify corrective actions

Qualifications

The service organization states in its description that it has controls in place to reconcile securities account master files to subsidiary ledgers, to follow up on reconciling items, to perform surprise annual physical counts, and to independently review its reconciliation procedures. However, as noted at page [mn] of the description of test of controls and results, controls related to the reconciliations and annual physical counts were not performed during the period April 1, 20X1, to December 31, 20X1.

As a result, controls were not operating effectively to achieve the control objective, “Controls provide reasonable assurance that securities account master files are properly reconciled to subsidiary ledgers and surprise annual physical counts are performed.”

In our opinion, **except for the matters referenced in the preceding paragraphs**, in all material respects, based on the criteria described in XYZ Service Organization's assertion on page [aa].

Testing Exceptions

Some component of the control did not operate as described

- Less severe than an operating effectiveness qualification
- Management needs to evaluate the impact of the testing exception and may need to work with the service organization to identify corrective actions

Testing Exceptions

Control Activity Specified by SO

- SO enters new plan participants upon receipt of completed application.

Test(s) of Controls Performed by Independent Auditor

- Inspected participant documentation for a sample of new participants during the period to determine that new participants were processed completely and accurately.

Results of Test(s)

- Exception noted.
- One (1) of 25 new member/participant forms was missing second witness' signature.

Service Organization Controls (SOC) Engagements

Recent Updates and Key Considerations

Questions?

Joel Eshleman, CPA, CISA, CIA
Principal, Specialized Advisory Services
joel.eshleman@CLAconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS