SOC 2 - Keeping Pace with Cybersecurity Risks

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Create Opportunities

Disclaimers

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623**.
- **Q&A session will be held at the end of the presentation.**
  - Your questions can be submitted via the **Questions Function at any time during the presentation.**
- The **PowerPoint presentation**, as well as the **webinar recording**, will be sent to you within the next 10 business days.
- For future webinar invitations, subscribe at CLAconnect.com/subscribe.
- Please complete our online survey.

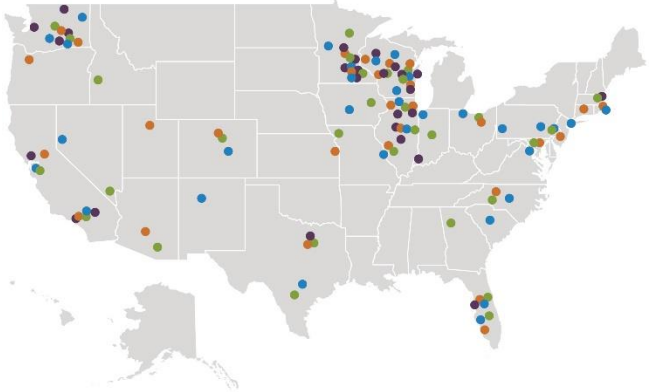
CPE Requirements

- Answer the polling questions
- Remain logged in for at least 50 minutes
- If you are participating in a group, complete the CPE sign-in sheet and return within two business days
  - Contact webmaster@CLAconnect.com
- Allow four weeks for receipt of your certificate; it will be sent to you via email from certificates@CLAconnect.com.

** This webinar, once recorded, has not been developed into a self study course. Therefore, watching the recording will not qualify for CPE credit.*

About CLA

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting
- More than 6,100 employees
- Offices coast to coast



Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.

SOC 2 Reporting

Learning Objectives

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

- Outline how the new framework allows for greater flexibility in how trust criteria are applied
- List ways to better prepare for your next examination
- Identify key elements to implement in order to meet the new SOC reporting requirements

Overview – What is a SOC report?

System and organization controls (SOC 2)/assurance engagements/service auditor's reports provide user organizations reasonable assurance that controls within the service organization meet the applicable Trust Service Criteria.

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*

Overview – What is a SOC 2 report?

SOC 2 engagements are different than an IT audit or IT General Controls Review (GCR)	
SOC 2 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 2 reports are intended to be distributed to user(s) of the service organizations' operations or services

Overview – What is a SOC 2 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 2 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].

SSAE 18

Effective Date: **REPORTS AFTER 5/1/2017** (Not periods)

- To address concerns over the clarity, length, and complexity
  - SSAE 10-17 > SSAE 18 (except SSAE 15 and 10)
- Sections applicable to SOC 2 report
  - AT-C Section 105: Concepts Common to All Attestation Engagements
    - ◊ SOC 1/2
  - AT-C Section 205: Examination Engagements
    - ◊ SOC 1/2

SOC 2

SOC 2 reports on ***suitably of control design to meet the selected Trust Service(s) Criteria*** relevant to:

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

Security (Common Criteria) – COSO Framework

- **Control Environment**
- **Communication and Information**
- **Risk Assessment**
- **Monitoring Activities**
- **Control Activities**

- Logical and Physical Access
- System Operations
- Change Management
- Risk Mitigation

Security New Criteria

- CC1.2 The **board of directors** demonstrates independence from management and exercises oversight of the development and performance of internal control.
- CC2.3 The entity **communicates with external parties** regarding matters affecting the functioning of internal control.
- CC3.3 The entity considers the potential for **fraud** in assessing risks to the achievement of objectives.
- CC9.2 The entity assesses and manages risks associated with **vendors and business partners**.

Availability

- A 1.3
  The entity **tests recovery plan** procedures supporting system recovery to meet its objectives.

Confidentiality

- C 1.2
  The entity **disposes of confidential information** to meet the entity's objectives related to confidentiality.

SOC 2 + Additional Subject Matter

A service organization may engage the service auditor to examine and report on subject matters in addition to the TSC

Cybersecurity Examination

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

- Focuses on TSP 100: Security, Availability, and Confidentiality
- Also included additional cybersecurity description criteria
- General purpose report vs. restricted use (SOC2)
  - management

SOC Report Format

- **Section I**
  - Auditor's Opinion
- **Section II**
  - Management's Assertion Letter
- **Section III**
  - System Description of Controls
- **Section IV**
  - Test of Controls

Section 1 – Service Auditor's Report Highlights

Identifies products/services that are in scope

SOC 2 Example

We have examined the description in section III titled "Example Service Organization's Description of its **Transportation Management System** Throughout the **Period January 1, 20X1 to December 31, 20X1**" (description),

What is included and excluded from scope

Inclusive Example

- ABC Subservice Organization is a subservice organization that provides application maintenance and support services to XYZ Service Organization. XYZ Service Organization's description **includes a description of ABC Subservice Organization's application maintenance and support services** used by XYZ Service Organization to process transactions for user entities, including controls relevant to the control objectives stated in the description.

Carve-out Example

- Service Organization uses Computer Subservice Organization, a subservice organization, to provide hosting services. The description includes only the control objectives and related controls of Example Service Organization and **excludes the control objectives and related controls of the subservice organization.**

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

Section 1 – Service Auditor's Report Highlights

Opine on whether documentation controls satisfy the control objectives (SOC 1) or the trust services criteria (SOC 2)

SOC 2 Unqualified Example

- In our opinion, in all material respects, based on the description and the applicable trust services criteria

SOC 2 Qualified Example

- In our opinion, **except for the matter referred to in the preceding paragraph**, in all material respects, based on the description and the applicable trust services criteria

Section 2 – Management Assertion

Management's Assertion is a key component of a SOC report.

- Forms the foundation for managements confirmation of scope
- Should be amended with acknowledgement if any qualifications are noted
- Confirms managements 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

SOC 2 Example

We have prepared the description in section III titled "Example Service Organization's Description of its Transportation Management System Throughout the Period January 1, 20X1 to December 31, 20X1" (description),

Section 3 – Description of System Highlights

- The type of services provided:
  - Components of the system including Infrastructure, Software, People, Procedures, and Data
  - How the system captures and addresses significant events and conditions
- Relevant aspects of:
  - Control Environment
  - Risk Assessment Process
  - Monitoring Controls
  - Information and Communication
- **Security incidents that occurred**
- Complementary user entity controls
- Complementary subservice entity controls

Section 3 – SOC 2 New Description Criteria

DC 4: For identified system incidents that (*a*) were the result of controls that were not suitably designed or operating effectively or (*b*) otherwise resulted in a **significant failure** in the achievement of one or more of those service commitments and system requirements, as of the date of the description (for a type 1) or during the period of time covered by the description (for a type 2), as applicable, the following information:

a. Nature of each incident

b. Timing surrounding the incident

c. Extent (or effect) of the incident and its disposition

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's 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 Subservice Organization Controls

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

New for SSAE 18

- Disclosed in the second paragraph of the independent auditor' report in the scope section and in Section III (Description of System)
- Ensure these are included in the subservice organizations SOC 2 report
- Examples
  - Restricting physical access to data centers
  - Protecting their network and infrastructure

Section 4: Independent Service Auditor's Description of Tests of Controls and Results Highlights

Inquiry alone is never enough!

Test Type	Description
Inquiry	Made inquiries of appropriate XYZ personnel to obtain information or corroborating evidence of the control.
Observation	Observed that a specific control exists, is appropriate and operating as intended.
Inspection	Inspected documents and reports indicating performance of the control. This includes, among other things: • Inspection of reconciliations and management reports. • Examining documents or records of performance such as the existence of initials or signatures.
Re-performance	Re-performed the control or processing application of the control to ensure the accuracy of their operation.

Testing Exceptions

Some component of the control did not operate as described

- Less severe than a 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 Company	Test(s) of Controls Performed by Independent Auditor	Results Of Test(s)
1. **Monthly internal vulnerability scans of systems and applications are performed, and an assessment of the risks and remediation associated with the results is documented.**	Inspected the vulnerability scan reports for a sample of months during the period to determine that the scans were performed and that an assessment of the risks remediation plans were documented.	Exception noted. One (1) of 12 monthly vulnerability scan reports were not documented.

Summary Recap

Ensure the new TSC key changes are being met

Every section of the SOC 2 report has valuable information

Map your controls to CUECs

Look for any disclosed security incidents

CLAconnect.com

Thank you!

Jim Kreiser, CISA, CRMA, CFSA
Principal
Specialty Advisory Services
James.Kreiser@CLAConnect.com
717-857-2613

Phil Del Bello, CPA, CISA
Manager
Specialty Advisory Services
Phillip.DelBello@CLAConnect.com
410-308-8181