

The Importance of System Organization Control Reports and How to Effectively Interpret Them

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Jim Kreiser, CISA, CRMA, CFSA; Principal – Business Risk Services

Amanda Kemp, CISA; Director – Business Risk Services



We promise to *know you and help you.*



Learning Objectives

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

- Identify the different types of SOC reports
- Recognize implications and reporting impacts of SOC reports
 - *Identify management response to SOC reports*
- Identify how to effectively read SOC reports for exceptions, complimentary user entity controls (CUEC), etc.

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor



Service Organization Controls (SOC) Engagements

Overview

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Overview – What is a SOC report?

- Service organization controls (SOC)/assurance engagements/service auditor's reports are intended to provide user organizations reasonable assurance that controls within the service organization are:
 - ◇ Described accurately
 - ◇ Suitability 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)



Overview – 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



Overview – 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].



Overview – What is a 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)

- Client user organizations want to have trust and confidence in service provider relationships that (*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 Accuracy (Processing Integrity)
 - Data has Protection (Confidentiality)
 - Data Sharing has Protection (Privacy)
 - Other

SOC Business Driver(s)

- Other SOC 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

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

SSAE 18 Effective Date

- Effective for audit periods ending **on or after May 1, 2017**
- SSAE 18 is known as the System Organization Controls (SOC) Reporting Standard.
 - SOC 1 continues to be used, and there is relatively no impact to the SOC 1 as a result of SSAE 18 implementation
 - SOC 2 intended to be more focused on IT controls and security (most changes occurred with SOC 2) report



SOC for Cybersecurity

- Exposure Draft: 1/15/2018
- 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

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

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
- Issue a Report on the findings in a format prescribed by SSAE 18

SOC 1 (Formerly SAS70)

SOC 1 reports on suitability 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 SOC 1 engagement will be a ***Report with Auditors' 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

SOC 2 reports on *suitably 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 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 Principle and operated effectively for the reporting period. SOC2 Reports are “Limited Use”.

SOC 2 - Trust Service Criteria (TSC)

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



SOC Engagement Reporting Period

Another decision is determining if a Type 1 or Type 2 is most appropriate.....

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*).

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*).

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
	No	SOC3



Service Organization Controls (SOC) Engagements

Elements of Reporting

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

SOC Report Format

- Section I
 - Transmittal Letter – includes the auditor's opinion
- Section II
 - Management's Assertion Letter
- Section III
 - System Description of Controls
- Section IV
 - Test of Controls

Transmittal Letter

- Indicates what kind of report SOC 1, 2, SOC for Cybersecurity, if a SOC 2 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 (SOC 1) or Trust Service Criteria (SOC 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



Purpose of System Description

- Intended to provide user auditors and user entities with information about the service organization's system that may be relevant of the user entities' internal control
- SOC 1 – The AICPA standard states that the focus of the SOC 1 is on controls that are likely to be relevant to user entities' internal controls over financial reporting.
 - User entities
 - User entities' auditors

Purpose of System Description (cont.)

- SOC 2 – 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

- Control activity specified by the service organization
 - For SOC 1 these are controls related to the control objective
 - For SOC 2 these are controls related to the selected criteria (security, availability, confidentiality, privacy, processing integrity)
- Test of control performed by the independent auditor
- Results of testing which may include instances of non occurrence or any exceptions noted





Service Organization Controls (SOC) Engagements

Management Review Actions

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Complementary End User Controls

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

Complimentary User Entity Controls

- Complimentary 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 ensure 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' 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 operating 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 SO	Test(s) of Controls Performed by Independent Auditor	Results Of Test(s)
1. SO enters new plan participants upon receipt of completed.	Inspected participant documentation for a sample of new participants during the period to determine that new participants were processed completely and accurately.	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

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

SSAE 18

- Impacts
 - Risk Assessment
 - ◇ Enhance subject matter risk assessment
 - Vendor/Subservice Organizations
 - ◇ Enhanced vendor management program
 - ◇ Subservicer Control Considerations
 - Similar to Consideration End-User Control

Cybersecurity Examination

- Framework for an entity to provide information on its cybersecurity risk management program
 - Focuses on TSP 100: Security, Availability, and Confidentiality
 - General purpose report vs. restricted use (SOC2)
 - ◇ management
- Effective: 1/15/2018

Impact on Green Book

- Develop/maintain effective internal controls
- Identification of internal control deficiencies
- Report internal control deficiencies
- Developing and monitoring corrective action plans

Questions?





Thank you!

Jim Kreiser, CRMA, CISA, CFSA

Principal

**Business Risk and Specialty Advisory
Services**

James.Kreiser@CLAAconnect.com

215-643-3900

Amanda Kemp, CISA

Director

**Business Risk and Specialty Advisory
Services**

Amanda.Kemp@claconnect.com

215-643-3900