How to Bring SOC Reports into Your Classroom

Brenda Piazza, MBA, CISSP, CISA, CGEIT, CISM, CBP
Myles Stern, Ph.D., CMA

weARE webinar
October 8, 2021

Your presenters

Brenda Piazza, MBA, CISSP, CISA, CGEIT, CISM, CBP

National Director of IT Audit and Cybersecurity at MHM (Mayer Hoffman McCann)

Myles Stern, Ph.D., CMA

Associate Professor of Accounting, Mike Ilitch School of Business, Wayne State University

Lecturer, Lamden School of Accountancy, Fowler College of Business, San Diego State University

Acctg 670 – Seminar in Assurance Services

- Four-week unit on SOC (System and Organization Controls) reports
- San Diego State University, Spring Semester 2021
- Accounting master's students nearing degree completion
- Material is very modular.
  - Easy to adapt for a smaller amount of time

Motivation

- “CPA Evolution” identified SOC Reports as an important topic that hasn’t often been covered in accounting coursework.
- I knew only a little about SOC Reports but I’ve taught system and organization controls.

Unit on SOC Reports

Week	Topic	Deliverables
1	Introduction to SOC reports	None
2	SOC for Service Organizations	Brief individual student reports
3	Trust services criteria	Brief individual student reports Canvas discussion on SOC reports
4	SOC for Cybersecurity and SOC for Supply Chain	Brief individual student reports, Canvas discussion on SOC reports
5		Answers to 16 multiple-choice questions

Individual student reports

- 5-7 minute presentation using 3-5 PowerPoint slides
- Fill “gaps” in my lectures
- Very narrow topics
  - Describe the 2017 Equifax data breech.
  - What is Google Cloud Platform?
  - Why was COSO formed?
  - Explain and give examples for the “objectivity” attribute of criteria used in a CPA’s attestation engagement.

Canvas graded discussion

Controversy remains concerning whether CPAs should perform SOC examinations at all; which specific kinds of SOC examinations CPAs should conduct; and which SOC examinations, if any, a CPA firm should conduct or be permitted to conduct for an audit client. In your first post, take a position, either in favor or opposed, on a particular aspect of this general question. Use your subsequent postings to discuss the positions taken by other students.

16 multiple-choice questions

- “Treasure hunt” through lectures and readings
- Homework assignment: open book and no time limit
- Objective: Get students to review the material

Outcomes

- Students performed very well on homework assignments.
- Students reported
  - Learning a lot about SOC reports
  - Lectures and homework assignments contributed greatly to their understanding, readings less so.

Lecture: Introduction to SOC reports

Key topics

- What is the AICPA's SOC Suite of Services?
- Why are SOC reports needed?
- How have SOC reports evolved over time?
- Why CPA firms should provide these services.

AICPA's SOC Suite of Services

- SOC for Service Organizations
  - Internal control reports about outsourced services
- SOC for Cybersecurity
  - Effectiveness of an organization's cybersecurity risk management program
- SOC for Supply Chain
  - Cybersecurity risks in supply chains for producing or distributing goods

Lecture: SOC for Service Organizations

Key topics

- What are the different SOC reports for service organizations?
- How do those reports vary in contents and purpose?
- How can the service organization and the CPA decide which report fits best?

SOC for Service Organizations

- *Service auditor* provides assurance about the service organization's internal controls.
- *User auditor* audits a client who outsources some aspect of its accounting system to the service organization.

SOC for Service Organizations

- SOC 1® – SOC for Service Organizations: Internal Control over Financial Reporting
- SOC 2 ® – SOC for Service Organizations: Trust Services Criteria
- SOC 3 ® -- SOC for Service Organizations: Trust Services Criteria for General Use Report

Both SOC1 and SOC2 have type 1 and type 2 reports.

SOC for Service Organizations

SOC 1® – SOC for Service Organizations: Internal Control over Financial Reporting

SOC 2 ® – SOC for Service Organizations: Trust Services Criteria

- Type 1 report – As of a specified date:
  - Is the service organization's management's description of the system presented fairly?
  - Are the controls designed suitably?
- Type 2 report
  - Everything in type 1 plus:
  - Did the controls operate effectively throughout a specified period?

Which SOC report is the right fit?

Key question	Response	Required Report
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	SOC 1® Report
Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization's systems?	Yes	SOC 2® or SOC 3® Report
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	SOC 2® Report
Do you need to make the report generally available?	Yes	SOC 3® Report

Sources: 2014 AICPA SOC Reports "Flyer" and AICPA website

Lecture: AICPA Trust Services Criteria

Key topics

- What are the categories of trust services criteria?
- Why is security always investigated?
- What are the attributes of “suitable criteria”?
- What risk factors must be considered?
- What is COSO and what role does it play here?
- Why is the “control environment” criterion of paramount importance?

Lecture: SOC for Cybersecurity and SOC for Supply Chain

Key topics

- What are the contents and purpose of SOC for Cybersecurity reports?
- What are the risks from cybersecurity breaches and why will these risks continue?
- What are the contents and objectives of SOC for Supply Chain reports?
- Why are SOC for Supply Chain reports likely to evolve?

Teaching suggestions

- Have a practitioner be a guest speaker
- Material can be very dry: kick it up!
  - Russian 2020 cyber attack included in lecture on SOC Suite of Services
  - Short individual student reports over three weeks
  - Students find cybersecurity topics very interesting.
- Combine “Intro to SOC Reports” and “SOC for Service Organizations” for one-class overview.

Practitioners' Use of SOC Reports

Using a SOC Report in a Financial Statement Audit

Gain an Understanding of Internal Controls

An auditor is required to obtain an understanding of an user entity's internal controls as part of the financial statement audit in order to assess the risk of material misstatement, including an understanding of the services provided by the service organization. This includes:

- The nature of the services provided by the service organization and the significance of those services to the user entity, including their effect on the user entity's internal control
  - ADP for Payroll
- The nature and materiality of the transactions processed, GL accounts, and / or financial reporting processes affected by the service organization
  - Salary Payable, Accrued Payroll, Tax Liability
- The relevant contractual terms for the activities undertaken by the service organization for the user entity

Reviewing a SOC Report

Once it is determined that the SOC 1 or SOC 2 report will be used to support the auditor's understanding of the design and implementation of controls at the service organization, the user auditor should:

- Evaluate the reporting period (type 1 as of date; type 2 reporting period)
- Determine whether the complementary user entity controls (CEUCs) are relevant in addressing the risks of material misstatement relating to the relevant assertions in the user entity's financial statements and, if so, obtain an understanding of whether the user entity has designed and implemented such controls
  - Example: User entity management is responsible for reviewing the employee changes and any errors presented during the payroll preview to determine if any corrections are needed
- Evaluate the service auditor's professional competence and independence from the service organization
  - Must be a CPA firm
- Opinion and exceptions

Difficulties in SOC Examinations

User Entity Auditor - Evaluating a SOC 1 report

Common user entity auditor issues with a SOC report

- SOC 1 report does not address all of the services or locations provided by the service organization to the user entity
- Type 1 report only is available (cannot reduce control risk)
- Too few controls or control objectives are included in the SOC 1 report
- Period covered by the SOC 1 is not sufficient
  - Different period end from financial statements
    - Bridge letter provided by service organization
    - Length of time that can be addressed by bridge letter
- Deviations/exceptions identified in tests of controls
- Qualified opinion regarding the design or operating effectiveness of controls

SOC 1 Report Deviations:

- How does a report modification impact the user entity's financial statement audit?
  - Consider the relevance of the qualification on the user entity financial statements. For example:
    - If a debt collection agency posted your money into someone else's account, that would be of great concern.
  - The control objective that is qualified may not be relevant to the user entity. For example:
    - An investment company SOC report may include a qualification for the control objective over investment valuation. A user entity may have controls in place, such as independent pricing service, that address this assertion.
    - A record keeper with a SOC report qualification relating to investments, where the user entity audit is a limited scope Employee Benefit Plan audit.

SOC Report Not Available

- How does the lack of a SOC 1 report for a service organization, or a conclusion that the SOC 1 report provided is insufficient, impact the user entity's financial statement audit?
  - One of the primary needs to obtain a SOC 1 report is to gain an understanding of internal controls in order to assess the risk of material misstatement
  - SOC 1 reports are also used to gain evidence that the internal controls at the service organization are:
    - Designed and implemented throughout a 6 or 12 month period
    - Operating effectively to reduce the control risk and the extent of substantive testing
  - Ability to rely on Information Produced by the Entity (IPE)
  - Only SOC 2 available

SOC Report Not Available (Cont'd)

- If a sufficient understanding about the effects of the service organization on the client's internal control cannot be obtained a SOC report, the auditor should obtain this understanding by:
  - Contacting the service organization, through the client, to obtain the specific information
  - Visiting the service organization and performing procedures that will provide the necessary information about the relevant controls at the service organization
  - Performing detailed testing of the reports provided by the service organization against data provided by the client to the service organization
  - Using another auditor to perform procedures that will provide the necessary information about the relevant controls at the service organization

Personal Experience of Issues When Reviewing Other SOC Reports

- Qualification in change management control objective for cloud-based accounting system
- SOC report prepared by a non-CPA
- Incomplete SOC report
  - Control objectives are missing
- Incomplete description of the system in SOC 2
- Trust services principle missing from the SOC 2 relevant to the System

How to Bring SOC reports into your classroom

Your questions, please.