We'll get you there.

SOC Reports

August 12, 2022

CPAs | CONSULTANTS | WEALTH ADVISORS

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.

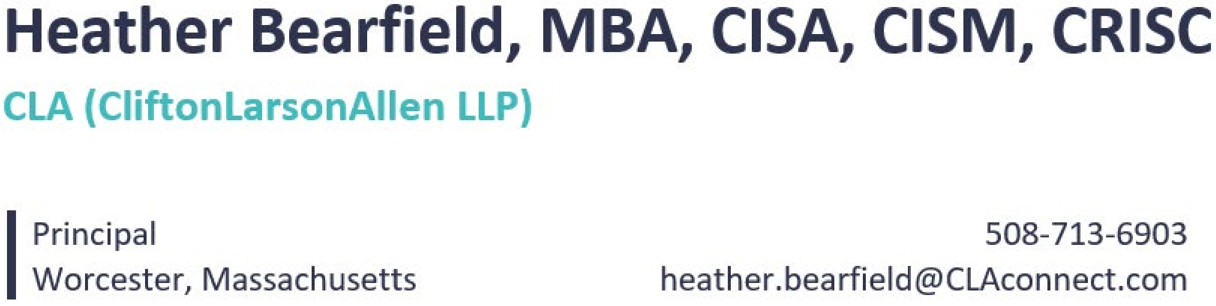
CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances 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 the different types of SOC reports available in the marketplace.
- Discuss what is driving SOC report demand and importance.
- Identify what SOC reports address and what they don’t address.
- Describe how to read and interpret SOC reports effectively – in laymen’s terms!
- Identify how an organization becomes SOC “certified”

Bio – Heather Bearfield



Heather Bearfield, MBA, CISA, CISM, CRISC

CLA (CliftonLarsonAllen LLP)

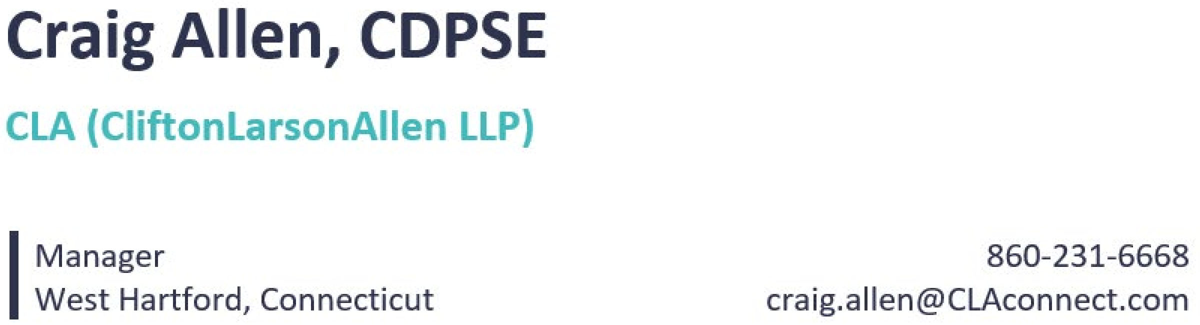
Principal
Worcester, Massachusetts

508-713-6903
heather.bearfield@CLAconnect.com

Heather is a Principal at CLA and has more than 20 years of experience serving clients in the following areas

- SOC 1 and 2 Examinations
- Sarbanes Oxley Compliance and Consulting
- PCI Examinations
- NIST CSF and 800-171 Compliance and Consulting

Bio – Craig Allen



Craig Allen, CDPSE

CLA (CliftonLarsonAllen LLP)

Manager
West Hartford, Connecticut

860-231-6668
craig.allen@CLAconnect.com

Craig is a Manager at CLA and has more than 10 years of experience serving clients in the following areas

- SOC 1 and 2 Examinations
- Sarbanes Oxley Compliance and Consulting
- HITRUST Compliance and Consulting
- NIST CSF and 800-171 Compliance and Consulting

Objective 1 - What is a SOC Report?

- SOC, an acronym, stands for “System and Organization Controls.”
- Simply put, a SOC report is an effective reporting option for entities (“service organizations”) to convey the effectiveness of their internal control environment for specific processes and/or service offerings.
- A SOC report’s scope can cover an entire organization or can be more limited:
  - A specific service line
  - A specific application
  - Scope flexibility is one of the main reasons for the SOC’s rising popularity

Objective 1 - What is a SOC Report?

- Important – SOC is first and foremost, an attestation report.
  - Ok – so what does that mean?

- It means that you can’t just say, “we have effective controls” in the SOC report and call it a day!

- SOC reports themselves must meet disclosure and examination requirements completed by an independent auditor (to be discussed later)

Objective 1 - What is a SOC Report?

- The compilation and assessment requirements are governed by standards issued by the American Institute of Certified Public Accountants (‘AICPA’)
- Overtime, SOC reporting requirements are becoming more stringent and auditor’s testing procedures becoming more detailed and robust.
- The specific standard as evolved over the years……
    - SAS 70 - original standard
    - SSAE 16 – adopted and superseded SAS 70 in 2011
    - SSAE 18 – adopted 2017
    - SSAE 21 – adopted 2022

Objective 1 – SOC Report Groups

- There 3 different buckets that SOC reports are grouped in, each are different and have their own unique traits:
  - SOC 1
  - SOC 2
  - SOC 3

- Within the SOC 1 and SOC 2 buckets, SOC reports are further categorized as either a Type 1 or Type 2.

- For example….
  - SOC 1 Type 1 or Type 2
  - SOC 2 Type 1 or Type 2
  - SOC 3 – This will always be a Type 2 report

Objective 1 - Key Players in the SOC World

- “Service Organization” – Company/Organization that is the one issuing the SOC report. Their processes and associated internal controls are in scope for the report.
- “Service Auditor” – Independent assessor engaged by the service organization to conduct an assessment on the service organization’s internal control. Their assessment results and audit opinion are included in the service organization’s SOC report.
- “User Entity” – The intended recipient(s) of the SOC report. The service organization is responsible for providing their SOC report to the user entity (not the auditor). They can be any stakeholder, such as customers, financial statement auditors, regulators, etc.
- “Subservice Organization” – A key vendor of a service organization for which certain procedures or internal controls has been outsourced to by the service organization.

Objective 1 - What is a SOC 1?

- Focus is on in-scope processes and services where key internal controls over financial reporting (IFCRs) are relevant

- Financial statement auditors are the primary user entities of a SOC 1

- We are not assessing the ICFRs relating to the service organizations' own financials!

- Controls in scope mostly involve ensuring the accuracy, completeness, and timeliness of financial data that is important to a service organization's user entities.

Objective 1 - What is a SOC 2?

- SOC 2 is considerably different from a SOC 1.
- Instead of the accuracy, completeness and timeliness of financial data, SOC 2 specifically addresses the internal controls over the security, availability, confidentiality, processing integrity, and privacy of data.
- Controls specific to IT/Cybersecurity are the main show here.
- The intended users of SOC 2s are broader than a SOC 1, more to follow on this…..

Objective 1 - What is a SOC 2?

- Focus is on key internal controls in place to meet defined criteria relating to the security, availability, confidentiality, processing integrity, and/or privacy of system data.

- IT/Cybersecurity internal controls are the main show here.

- The intended users of SOC 2s are broader than a SOC 1, more to follow on this….

Objective 1 – What is a SOC 2

Five “Categories” that can be in scope in a SOC 2:

- Security – Protection of a system against damage, unauthorized access, and unauthorized disclosure of information.
- Availability – Supports accessibility and use of information for operations, monitoring, and maintenance.
- Processing Integrity – Ensures that data processing is complete, accurate, timely, and authorized.
- Confidentiality – Ensures that all types of information deemed to be confidential is protected from unauthorized disclosure as well as retained and/or destroyed in accordance to specified requirements.
- Privacy – Ensure that personal information (PII and PHI) is collected, used, retained, disclosed , and disposed of in a valid manner.

Objective 1 – What is a SOC 2

- The service organization can choose which of the 5 categories will be in scope for their SOC 2.
- De facto though – Security will always be the baseline category in scope.
- Not many SOC 2s have all 5 in scope (but it depends on their industry)
- Privacy category has increasingly become more important over the past couple of years.

Objective 1 - What is a SOC 2

- Overtime, service organizations have come to appreciate the value of SOC 2s, as a result, their popularity has increased:
  - Current and prospective customers
  - Regulators
  - Management and Compliance

- With cybersecurity threats constantly emerging and evolving, our clients are under increasing pressure to show they have effective internal controls in place to mitigate these risks.

- Having effective internal controls in place is one of most cost-effective ways to help prevent, detect, and respond to cybersecurity incidents – SOC 2 offers our clients a means to identify and test for the effectiveness of these controls!

Objective 1 – What is a SOC 3?

- A SOC 3 is essentially a redacted SOC 2.
- Whereas a SOC 2 is a confidential document, a SOC 3 does not contain any sensitive information about a service organization and therefore, can be freely disseminated.
- Many service organizations will issue a SOC 3 in conjunction with an associated SOC 2. They will commonly publish the SOC 3 on their website.
- Commonly serves as a ‘teaser’ document for prospective customers and stakeholders.

Objective 1 – Type 1 vs. Type 2

- Type I report addresses the design effectiveness internal controls as of a specific date (ex. as of December 31, 2021)
- Type II report addresses the design <u>and</u> operating effectiveness of controls for a period of time (ex. from January 1, 2021 to December 2021)
- Type II report is more in demand as it covers a period of time.

Objective 1: Additional SOC Reports of Note

- SOC 2+ reporting options
    - Baseline SOC 2 criteria, with the incorporation of additional security frameworks:
        - HIPAA
        - ISO 27001
        - HITRUST
        - NIST
        - CSA (cloud security)
        - SOC 2+ reporting options
- SOC for Cybersecurity
- SOC for Supply Chain

Polling Question 1

Objective 2 – What is Driving SOC Demand?

- Company outsourcing of key services to third party service providers has rapidly increased over the past couple of decades, primarily due to cost and productivity considerations.
- At the same time, increase scrutiny over how to ensure effective financial reporting internal controls are in place at organizations (Sarbanes Oxley Act) – increased demand for SOC 1s.
- With cybersecurity related threats and regulations constantly emerging and evolving, Companies are under increasing pressure to show they have effective internal controls in place to mitigate these risks – increased demand for SOC 2s.

Objective 2 – Why is a SOC 1 Needed?

Illustrative example of a SOC 1:

- Payroll provider (for example ADP), circulates payroll reports to thousands of their customers on a bi-weekly or weekly basis containing financial reporting data, including:
  - Wage Expense
  - Payroll Taxes Withheld
  - Benefits Withheld
- Payroll provider is getting overwhelmed with requests by the F/S auditors of their customers (thousands), demanding that the provider provides evidence that they have effective internal controls over the accuracy, completeness, timeliness of the financial data in their payroll reports.
- The payroll provider cannot possibly accommodate thousands of separate audits of their internal controls. What is the solution??!!

Objective 2 – Why is a SOC 1 Needed?

- Illustrative example of a SOC 1:
  - SOC 1 is the answer!
  - The payroll provider can engage an independent auditor to conduct an assessment to determine whether they have effective internal controls and issue a SOC 1 report.
  - The SOC 1 report can then be circulated to all their customers' auditors. Potentially thousands of audits become one annual audit.
  - Talk about efficiency. Plus, they can brag to potential new clients that they have a SOC 1 report – an added competitive edge.
  - This is just one example. SOC 1 can be leveraged for many different industries and services. Remember, if there is financial data involved, SOC 1 is usually the way to go.

Objective 2 – Why is a SOC 2 Needed?

Illustrative example of a SOC 2:

- A technology company has an internally developed application that process' patient insurance claims. Various Insurance companies have outsourced this claim processing to this technology in order to save costs. The application will process, stored, and transmit PII and PHI information (highly sensitive)
- The technology company is getting overwhelmed with requests by their current and prospective Insurance company customers, demanding that the provider provides evidence that they have effective internal controls to ensure the security, availability, processing integrity, confidentiality, and privacy of the data received from the submitted insurance claims. (They are getting a ton of security questionnaires to fill out!!!)
- The Company is also subjected to the PII and PHI security, confidentiality, and privacy requirements stipulated within HIPAA and the California Data Privacy Law statutes.
- What is the solution to meet all these demands efficiently?

Objective 2 – Why is a SOC 2 Needed

- Illustrative example of a SOC 2:
  - SOC 2 is the answer!
  - The technology company can engage an independent auditor to conduct an assessment to determine whether they have effective internal controls and issue a SOC 2 report.
  - The SOC 1 report can then be circulated to all their Insurance company customers.
  - Talk about efficiency. In lieu of all the security questionnaires, a well-constructed SOC 2 can address most security questionnaires efficiently and effectively, as well as incorporate controls that satisfy certain security-related statutory requirements (such as HIPAA)

Objective 3 – What SOC Does and Won’t Do

- Let’s start with the SOC 1:
  - SOC 1 will cover controls that are only key for financial reporting related data and information of a service organization’s customers or stakeholders (remember the payroll company earlier?)
  - It will not address the service organization’s own internal financial reporting data and information.

Objective 3 – What SOC Does and Won't Do

- Now for the SOC 2:
  - Auditors will not, as part of their own testing procedures, conduct technical assessments such as IT vulnerability examinations or external penetration tests.
  - Instead, the auditors will assessment whether a vulnerability assessment or penetration test is periodically performed by the service organization and that findings were researched and resolved (control-based testing).
  - In other words, this is a control-based examination, not a technical assessment where the auditors are performing functions reserved by management. Auditors must maintain independence throughout the duration of the audit.

Polling Question 2

Objective 4 – Key SOC Report Sections

- Generally SOC 1 and 2 is divided into 5 sections:
    - Section 1: Auditor Opinion
    - Section 2: Assertion
    - Section 3: System Description
    - Section 4: Control Listing, Auditor Testing Procedures, and Testing Results
    - Section 5: Other Information Shared by the Service Organization (Optional)

Objective 4 – Auditor Opinion

- For all SOC reports, the service organization is required to engage an independent auditor to conduct an examination.
- The auditor's 'conclusion' for the examination procedures are summarized in an opinion, signed by the auditor firm and included within the SOC report.
- The opinion will include various required disclosures, but the key sections of the opinion include:
  - ○ General scope description and work performed by the auditor.
  - ○ What the auditor is responsible for and what the service organization is responsible for
  - ○ Auditor's opinion on whether the description in the report accurately reflects the system in scope for the SOC report whether the internal controls are designed and operating effectively.
- Remember, this is an opinion, which means <u>it does not provide absolute assurance</u> that everything is perfect at the service organization!

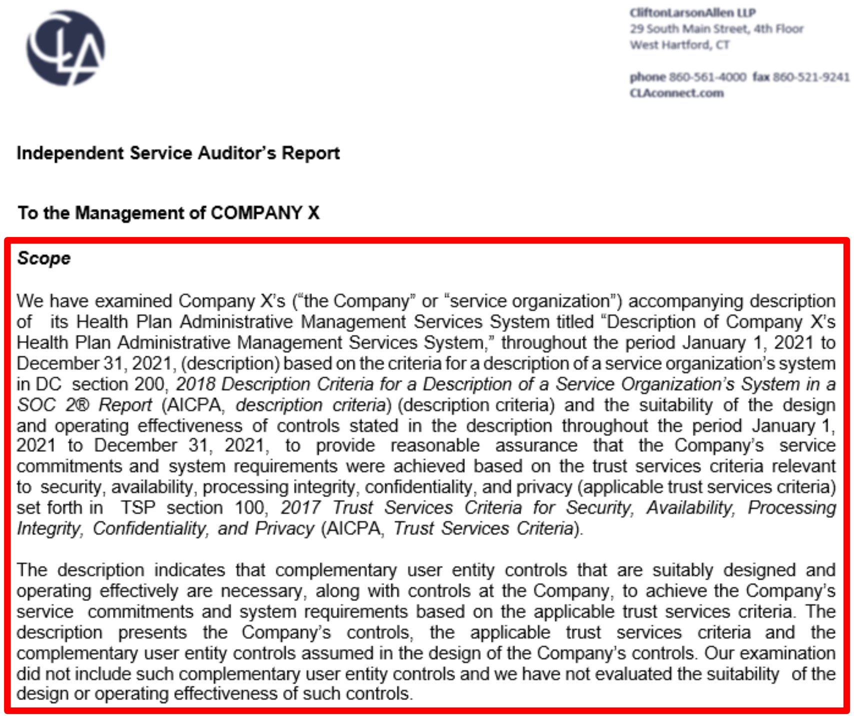
Objective 4 – Auditor Opinion

- An auditor's opinion can be group into 3 different buckets:
  - **Unqualified Opinion** – A 'clean' report. There are no material internal control testing deficiencies noted by the auditor that were significant enough for which entire control objectives (SOC 1) or criteria (SOC 2) were not met. <u>Important: There still can be testing exceptions noted in Section 4 but are not significant enough to be disclosed in the Auditor's opinion.</u>

  - **Qualified Opinion** – The standard opinion language will be modified because material testing exceptions were noted for specific control objectives or criteria in the report. It essentially means that there are effective internal controls in general at the service organization except for specific areas, which will be disclosed in the opinion.

  - **Adverse Opinion** – Horrible opinion. No service organization wants this. It essentially means that there were so many material internal control deficiencies that the auditor determined that there is no effective internal control environment in place at all. YUCK!!!!!

Objective 4 – Opinion Example



CliftonLarsonAllen LLP
29 South Main Street, 4th Floor
West Hartford, CT

phone 860-561-4000 **fax** 860-521-9241
CLAconnect.com

Independent Service Auditor's Report

To the Management of COMPANY X

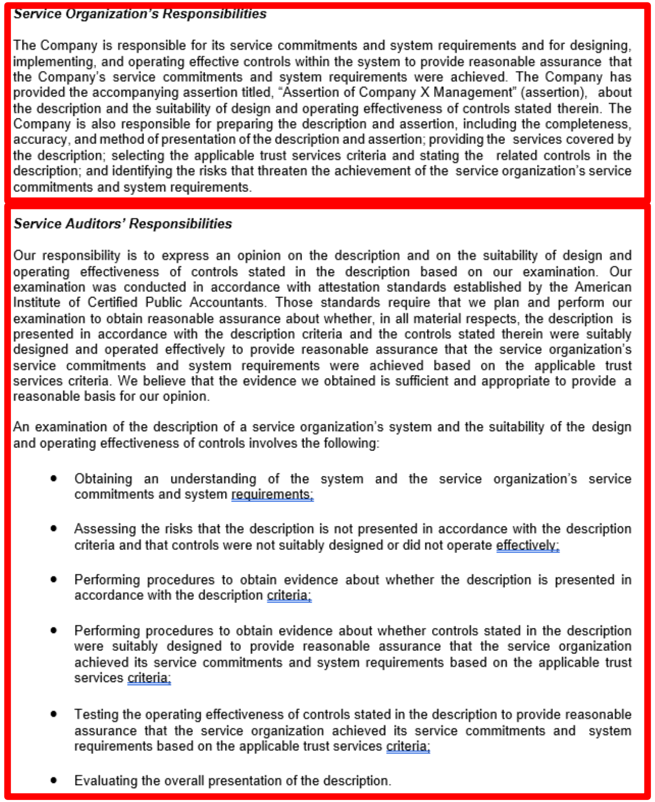
Scope

We have examined Company X's ("the Company" or "service organization") accompanying description of its Health Plan Administrative Management Services System titled "Description of Company X's Health Plan Administrative Management Services System," throughout the period January 1, 2021 to December 31, 2021, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *description criteria*) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of the Company's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

At the beginning of the opinion, the service auditor will include a description of the scope of the work that was performed. High level language is included here.

Objective 4 – Opinion Example



Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled, "Assertion of Company X Management" (assertion), about the description and the suitability of design and operating effectiveness of controls stated therein. The Company is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

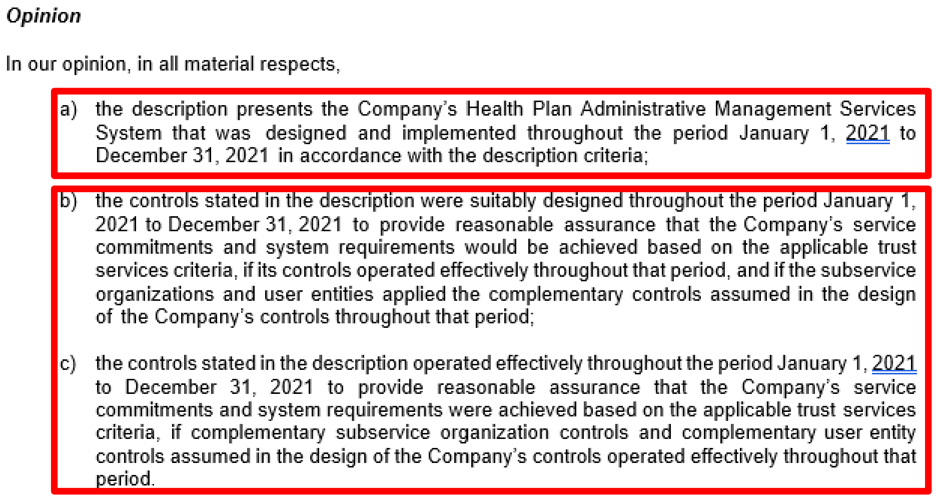
An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Evaluating the overall presentation of the description.

Description of the service organization's responsibilities.

Description of the service auditor's responsibilities.

Objective 4 – Opinion Example



Opinion

In our opinion, in all material respects,

a) the description presents the Company's Health Plan Administrative Management Services System that was designed and implemented throughout the period January 1, 2021 to December 31, 2021 in accordance with the description criteria;

b) the controls stated in the description were suitably designed throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout that period;

c) the controls stated in the description operated effectively throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of the Company's controls operated effectively throughout that period.

Opinion from the auditor indicating that the description in the SOC report presents the system in scope.

Opinion from the auditor indicating that the internal controls are designed and operating effectively.

Objective 4 – Qualified Opinion Example

Opinion

In our opinion, except for the matter referred to the preceding paragraph, in all material respects,

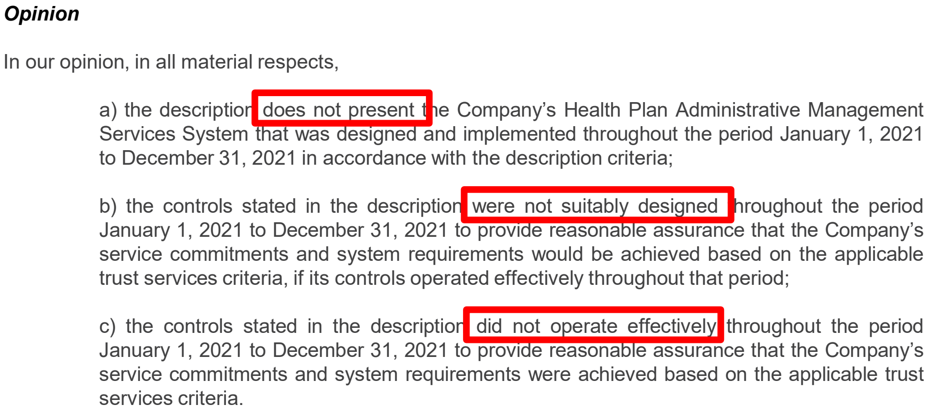
a) the description presents the Company’s Health Plan Administrative Management Services System that was designed and implemented throughout the period January 1, 2021 to December 31, 2021 in accordance with the description criteria;

b) the controls stated in the description were suitably designed throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that the Company’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period;

c) the controls stated in the description operated effectively throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the applicable trust services criteria.

For a qualified opinion, this additional language will be included in this section. An additional paragraph will also be included in the opinion describing the area(s) where internal controls were not effective.

Objective 4 – Adverse Opinion Example



Opinion

In our opinion, in all material respects,

a) the description does not present the Company's Health Plan Administrative Management Services System that was designed and implemented throughout the period January 1, 2021 to December 31, 2021 in accordance with the description criteria;

b) the controls stated in the description were not suitably designed throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period;

c) the controls stated in the description did not operate effectively throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria.

Sniffle….Sniffle

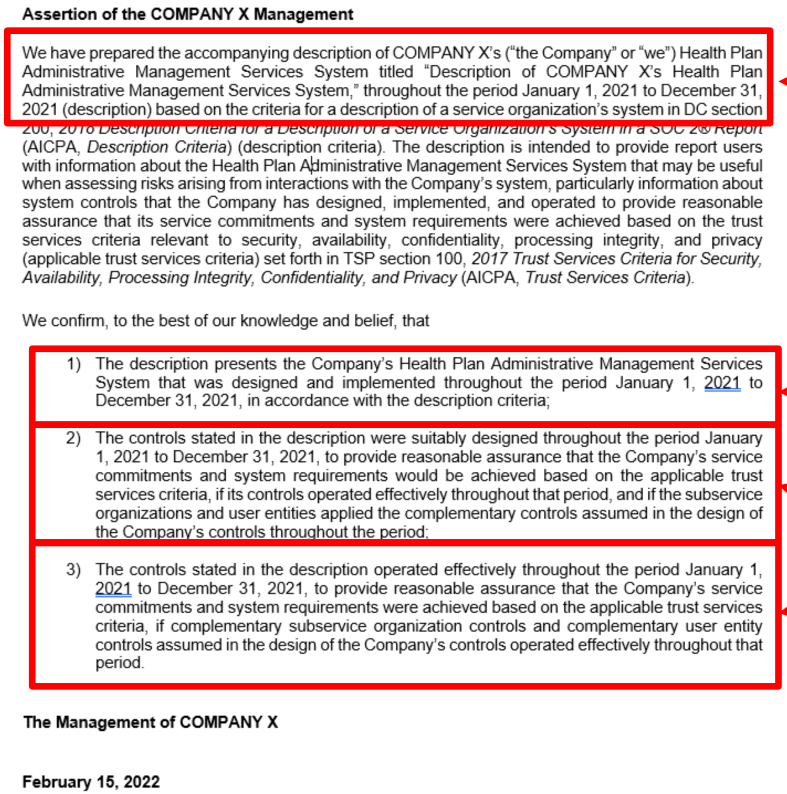
Objective 4 – Assertion Section

- Generally SOC 1 and 2 is divided into 5 sections:
    - Section 1: Auditor Opinion
    - Section 2: Assertion
    - Section 3: System Description
    - Section 4: Control Listing, Auditor Testing Procedures, and Testing Results
    - Section 5: Other Information Shared by the Service Organization (Optional)

Objective 4 – Assertion

- This is an official statement, that is signed and issued by the service organization's management, for which they declare that the system description included in the SOC report is accurate and complete.
- Management also declares in the assertion that the internal controls included in the report were designed and are operating effectively.
- Assertion statement <u>is required </u>to be included in all SOC reports.

Objective 4 – Assertion Example



Assertion of the COMPANY X Management

We have prepared the accompanying description of COMPANY X's ("the Company" or "we") Health Plan Administrative Management Services System titled "Description of COMPANY X's Health Plan Administrative Management Services System," throughout the period January 1, 2021 to December 31, 2021 (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Health Plan Administrative Management Services System that may be useful when assessing risks arising from interactions with the Company's system, particularly information about system controls that the Company has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

We confirm, to the best of our knowledge and belief, that

1) The description presents the Company's Health Plan Administrative Management Services System that was designed and implemented throughout the period January 1, 2021 to December 31, 2021, in accordance with the description criteria;

2) The controls stated in the description were suitably designed throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout the period;

3) The controls stated in the description operated effectively throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of the Company's controls operated effectively throughout that period.

The Management of COMPANY X

February 15, 2022

A general statement indicating that they have prepared the system description in scope for the SOC report.

A declaration from management indicating that the system description is essentially accurate and complete.

A declaration from management indicating that the internal controls are designed and operating effectively.

Objective 4 – System Description Section

- Generally SOC 1 and 2 is divided into 5 sections:
  - Section 1: Auditor Opinion
  - Section 2: Assertion
  - Section 3: System Description
  - Section 4: Control Listing, Auditor Testing Procedures, and Testing Results
  - Section 5: Other Information Shared by the Service Organization (Optional)

Objective 4 – System Description

- This section serves as the main body of the overall SOC report.

- It essentially describes all the internal controls and associated processes in paragraph format.

- The description needs to reference all the controls that were tested by the auditor. In other words, everything disclosed in the System Description needs to be assessed and scrutinized by the auditor before they issue their opinion.

Objective 4 – System Description

- System description will also, if applicable, include the following subsections:
  - **Complementary User Entity Controls (CUECs)** – these are general disclosures about the type of controls that the users of the SOC report should have in place in their own organizations. A combination of the user entity's controls and the controls managed by the service organization issuing the SOC report will constitute an effective control environment for the whole process.
  - **Complementary Subservice Organization Controls (CSOCs)** – Certain internal controls and associated responsibilities will commonly be outsourced to other organizations (for example, servers and infrastructure will be stored within Amazon Web Services' cloud environment). Like CUECs, this section will disclose the controls and responsibilities that have been 'outsourced' to these subservice organizations.

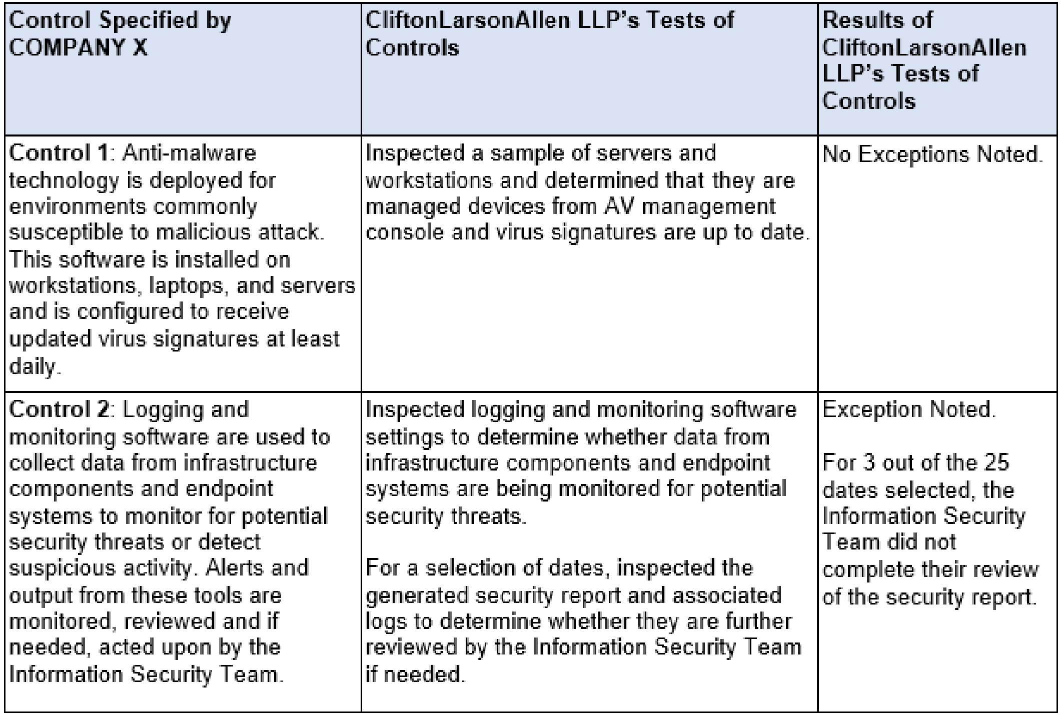
Objective 4 – Testing Procedures and Results Section

- Generally SOC 1 and 2 is divided into 5 sections:
  - Section 1: Auditor Opinion
  - Section 2: Assertion
  - Section 3: System Description
  - Section 4: Control Listing, Auditor Testing Procedures, and Testing Results
  - Section 5: Other Information Shared by the Service Organization (Optional)

Objective 4 – Testing Procedures and Results

- This section will disclose the following:
    - Mapping of all the key internal controls to the Control Objectives (SOC 1) or to the in-scope Trust Services Criteria (SOC 2)
    - Detail the specific testing procedures that the Auditor performed to assessing the design and operating effectiveness of the internal controls.
    - Test results of all the procedures that were performed (i.e. “No Exceptions Noted” or “Exception Noted”)

Objective 4 – Testing Procedures and Results



Control Specified by COMPANY X	CliftonLarsonAllen LLP's Tests of Controls	Results of CliftonLarsonAllen LLP's Tests of Controls
Control 1: Anti-malware technology is deployed for environments commonly susceptible to malicious attack. This software is installed on workstations, laptops, and servers and is configured to receive updated virus signatures at least daily.	Inspected a sample of servers and workstations and determined that they are managed devices from AV management console and virus signatures are up to date.	No Exceptions Noted.
Control 2: Logging and monitoring software are used to collect data from infrastructure components and endpoint systems to monitor for potential security threats or detect suspicious activity. Alerts and output from these tools are monitored, reviewed and if needed, acted upon by the Information Security Team.	Inspected logging and monitoring software settings to determine whether data from infrastructure components and endpoint systems are being monitored for potential security threats. For a selection of dates, inspected the generated security report and associated logs to determine whether they are further reviewed by the Information Security Team if needed.	Exception Noted. For 3 out of the 25 dates selected, the Information Security Team did not complete their review of the security report.

Objective 4 – Other Information Section

- Generally SOC 1 and 2 is divided into 5 sections:
  - Section 1: Auditor Opinion
  - Section 2: Assertion
  - Section 3: System Description
  - Section 4: Control Listing, Auditor Testing Procedures, and Testing Results
  - Section 5: Other Information Shared by the Service Organization (Optional)

Objective 4 – Other Information

- Entirely optional.

- Common disclosures contained here include the service organization management’s document response to any exceptions noted by the auditor.

- They can also disclose any other information they want about their organization but will not be subjected further testing by the auditor. The auditor will also include a disclosure in the opinion section indicating that it was not subjected to their examination.

- <u>However</u>, the service organization cannot put anything here that clearly contradicts what was disclosed in the previous sections of the report. For example, if the system description says there is 1 office location but in the Other Information section, it says there are 5 locations, there will be problems!

Objective 4 – SOC Report Review Tips

- SOC reports can be on average over 70 pages long – and a boring read to boot!
- When reviewing these monstrosities, focus on these questions:
  - Did the report contain an assertion provided by management?
  - What was opinion like? Did it contain qualified, unqualified, or adverse opinion language?
  - Did you, as the user entity, implement yourself the controls that were specified in the CUEC subsection?
  - Did you obtain and review the SOC reports issued (if they have one) by the subservice organizations mentioned in the CSOC subsection?
  - Did you review Section 4 for any noted deficiencies by the auditor?

Objective 5 – Becoming SOC "Certified"

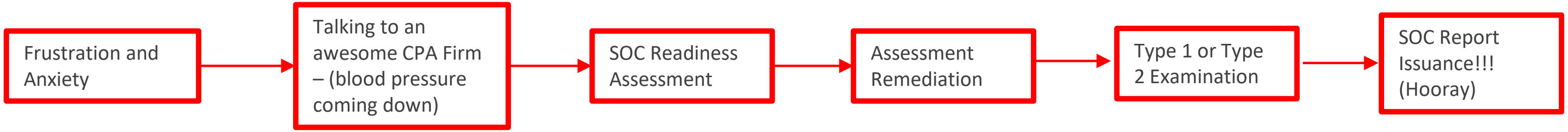
- We affix quotations to "certified" because contrary to popular belief, SOC certifications do not exist.

- Once you issue a SOC report, you don't get a formal certification from a governing body or association (like HITRUST or ISO) to hang up on your wall.

- Instead, you get a signed opinion from a CPA firm that is included in the report (discussed previously).

Objective 5 – The Road to Getting a Report

Traditional Path to Getting a SOC Report


Frustration and Anxiety
Talking to an awesome CPA Firm – (blood pressure coming down)
SOC Readiness Assessment
Assessment Remediation
Type 1 or Type 2 Examination
SOC Report Issuance!!! (Hooray)

Objective 5 – SOC Readiness – What is That??

- Serves as a ‘preassessment’ period prior to the actual SOC examination commencing.

- Service organization will engage the auditor to conduct a dry run of the audit in order to identify internal control gaps and to assist management to compile the system description.

- This is a vital part of the process (though not required) to ensure that the first SOC report does not have any deficiencies when the real audit begins.

- Gaps identified during the readiness assessment phase will be remediated by the service organization prior to the commencement of the audit (no required timeline to complete this phase)

Objective 5 – Examination Phase

- You’re completed the readiness assessment and have remediated the gaps, you’re ready the big leagues!
- The auditor will complete their examination, this can range from 2 to 3 months (Type 1) to up to 6 months (Type 2) on average.
- If done correctly by the auditor, the examination be an extensive process, requiring considerable effort to provide requested audit documentation.
- At the conclusion, the auditor will provide the final SOC report with their signed opinion to the service auditor.

Polling Question 3

We're Done!

Any Questions?