SOC 2® Reporting

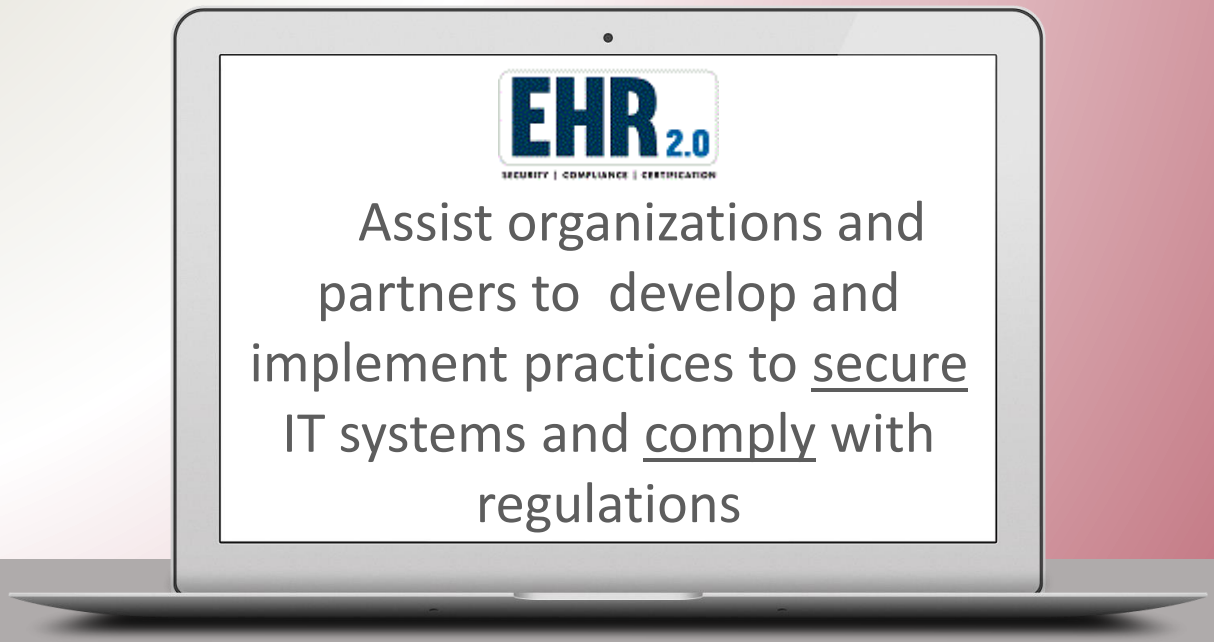
Ben Hunter III, CPA, CITP, CISA, CRISC, CFE

May 28, 2019

EHR20.COM
INFO@EHR20.COM
866-276-8309

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

WHO WE ARE …



DIY TOOLKIT
DIY assessment, training, customized policies & procedures and much more …

CONSULTING
Professional services to help you with your Compliance needs

MANAGED SERVICES
Managed compliance and security services to focus on your key business outcome.

DISCLAIMER

Consult your attorney

This webinar has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice.

Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

Ben Hunter III

CPA, CITP, CISA, CRISC, CFE

What is a SOC Report?

In 2017, the AICPA introduced the term *system and organization controls* (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization or system- or entity-level controls of other organizations. Formerly, SOC referred to *service organization controls*.

SOC 1®—SOC for Service Organizations: ICFR.

SOC 2®—SOC for Service Organizations: Trust Services Criteria.

SOC 3®—SOC for Service Organizations: Trust Services Criteria for General Use Report.

SOC for Cybersecurity.

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

SOC 1®—SOC for Service Organizations: ICFR.

Service organizations may provide services that are relevant to their customers' internal control over financial reporting (ICFR) and, therefore, to the audit of financial statements.

The CPAs performing the financial audit of the Service Organizations customers will use the SOC 1 report

brc

SERVING CLIENTS ACROSS THE SOUTHEAST

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

SOC 3®—SOC for Service Organizations: Trust Services Criteria for General Use Report.

Similar to a SOC 2® engagement, in a SOC 3® examination the practitioner reports on whether controls within the system were effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Although the requirements and guidance for performing a SOC 3® examination are similar to a SOC 2® examination, the reporting requirements are different.

Because of the different reporting requirements, a SOC 2® report is appropriate only for specified parties with sufficient knowledge and understanding of the service organization and the system, whereas a SOC 3® report is ordinarily appropriate for general use.

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

SOC for Cybersecurity.

As part of an entity's cybersecurity risk management program, an entity designs, implements, and operates cybersecurity controls. An engagement to examine and report on a description of the entity's cybersecurity risk management program and the effectiveness of controls within that program is a *cybersecurity risk management examination*.

For use by the Entity's management (oversight over IT), Board of Directors, analysts and investors, business partners, industry regulators

brc

SERVING CLIENTS ACROSS THE SOUTHEAST

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Purpose and Applicability of a SOC 2 Report

Examination and Reporting on a service organization's controls over one or more of the following:

- The security of a service organization's system
- The availability of a service organization's system
- The processing integrity of a service organization's system
- The confidentiality of the information that the service organization's system processes or maintains for user entities
- The privacy of personal information that the service organization collects, uses, retains, discloses, and disposes of for user entities

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Why is a SOC 2 different from an assessment?

A SOC 2® examination is an examination of a service organization's description of its system, the suitability of the design of its controls, and in a type 2 examination, the operating effectiveness of controls relevant to security, availability, processing integrity, confidentiality, or privacy.

The service auditor performs a SOC 2® examination in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements,* and AT-C section 205, *Examination Engagements*. Those standards establish performance and reporting requirements for the SOC 2® examination.

According to those standards, an attestation examination is predicated on the concept that a party other than the practitioner (the responsible party) makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria.

brc

Management's Assertion

Management's written assertion addresses whether

(a) the description of the service organization's system is presented in accordance with the description criteria,
(b) the controls stated in the description were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and
(c) in a type 2 examination, those controls were operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Intended Users of a SOC 2 report

A SOC 2® report is intended for use by those who have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide those services, among other matters.

The expected knowledge of specified parties ordinarily includes the following:

- Nature of the service provided
- How the service organization's system interacts with the user entities
- Internal control and its limitations
- Complementary user entity controls
- User entity responsibilities
- Applicable trust services criteria
- Risk that may threaten the achievement of the service organization's service commitments and system requirements.

Examples of services provided

Customer Support

Health care claims management and processing

Enterprise IT outsourcing services

Managed security

Financial technology (FinTech) Services

Almost any type of service where another company has your company's data and your customer's information.

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Two types of SOC reports

Type 1 and Type 2

A type 1 examination is an examination of whether:

1. a service organization's description presents the system that was designed and implemented as of a point in time in accordance with the description criteria and
2. controls were suitably designed as of a point in time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, if controls operated effectively

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Two types of SOC reports

Type 1 and Type 2

A type 2 examination also addresses the description of the system and the suitability of design of controls, but it also includes an additional subject matter:

whether controls operated effectively throughout the period of time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

A type 2 examination also includes a detailed description of the service auditor's tests of controls and the results of those tests.

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Contents of a SOC 2 type 2 Report

1. Description of the system throughout a period of time in accordance with the description criteria
2. Management assertion
3. Service auditor's opinion about whether
    1. The description of the service organizations system throughout a period of time is presented in accordance with the description criteria
    2. The controls stated in the description were suitably designed
    3. The controls stated in the description operated effectively
4. Description of the service auditor's tests of controls and results

brc

Description Criteria

DC1: The types of services provided

DC 2: The principal service commitments and system requirements

DC 3: The components of the system used to provide the services, including the following:

a. *Infrastructure*
b. *Software*
c. *People*
d. *Procedures*
e. *Data*

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

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

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Description Criteria

DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved

DC 6: If service organization management assumed, in the design of the service organization's system, that certain controls would be implemented by user entities, and those controls are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved, those complementary user entity controls (CUECs)

Description Criteria

DC 7: If the service organization uses a subservice organization and the controls at the subservice organization are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved, the following:

a. When service organization management elects to use the inclusive method:
   i. The nature of the service provided by the subservice organization
   ii. The controls at the subservice organization that are necessary, in combination with controls at the service organization to provide reasonable assurance that the service organization's service commitments and system requirements are achieved
   iii. Relevant aspects of the subservice organization's infrastructure, software, people, procedures, and data
   iv. The portions of the system that are attributable to the subservice organization

b. When service organization management decides to use the carve-out method:
   i. The nature of the service provided by the subservice organization
   ii. Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization
   iii. The types of controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved (commonly referred to as complementary subservice organization controls or CSOCs)

Description Criteria

DC 8: Any specific criterion of the applicable trust services criteria that is not relevant to the system and the reasons it is not relevant

DC 9: In a description that covers a period of time (type 2 examination), the relevant details of significant changes to the service organization's system and controls during that period that are relevant to the service organization's service commitments and system requirements

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Trust Services Criteria

The trust services criteria in TSP section 100 are used to evaluate the suitability of design and operating effectiveness of controls related to one or more of the trust services categories:

security, availability, processing integrity, confidentiality, and privacy

The engaging party, typically service organization management, may choose to engage the service auditor to report on controls related to one or more of these categories.

The Trust Services Criteria are aligned with the The Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control—Integrated Framework* (COSO framework)

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Trust Services Criteria

a. Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

b. Availability. Information and systems are available for operation and use to meet the entity's objectives.

c. Processing integrity. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

d. Confidentiality. Information designated as confidential is protected to meet the entity's objectives.

e. Privacy. Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Difference between Privacy and Confidentiality

Privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information.

Trust services privacy criteria encompasses the service organization's specific processes that address each of the following, as applicable:

- Notice of the service organization's privacy commitments and practices
- Data subjects' choices regarding the use and disclosure of their personal information
- Data subjects' rights to access their personal information for review and update
- An inquiry, complaint, and dispute resolution process

Trust Services Criteria

Depending on which category or categories are included within the scope of the examination, the applicable trust services criteria consist of
criteria common to all five of the trust service categories (common criteria) and

additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

For example, if the SOC 2® examination is only on availability, the controls should address all the common criteria and the additional specific criteria for availability.

Common Criteria

a. Control environnent

b. Communication and information

c. Risk assessment

d. Monitoring activities

e. Control activities (Control activities are further broken out into the following sub-classifications:

- logical and physical access controls,
- system operations,
- change management, and
- risk mitigation

SOC Reports are flexible

A SOC 2 report can have additional Information

Information on the physical characteristics of a service organization's facilities (for example, square footage)

Information about historical data regarding the availability of computing resources at a service organization

Information about how controls at a service organization help meet the organization's responsibilities related to the security requirements of HIPAA

Information about how controls at a service organization address the Cloud Security Alliance's Cloud Controls Matrix

Upcoming Events

- ❑ Financial Health Check-up for Medical Practices – 6/12
- ❑ How to Comply with California Consumer Privacy Act -6/26
- ❑ FDA CFR Part 11 Compliance – 7/23

Next Steps/Action Items

- ❑ Contact AHS for free no-obligation evaluation on your EMR needs

Jit Chawla – (919) 228-8744 or info@acehealthsolutions.com

- ❑ Download Open EMR or try online demo
- ❑ https://www.open-emr.org/demo/

Questions?