

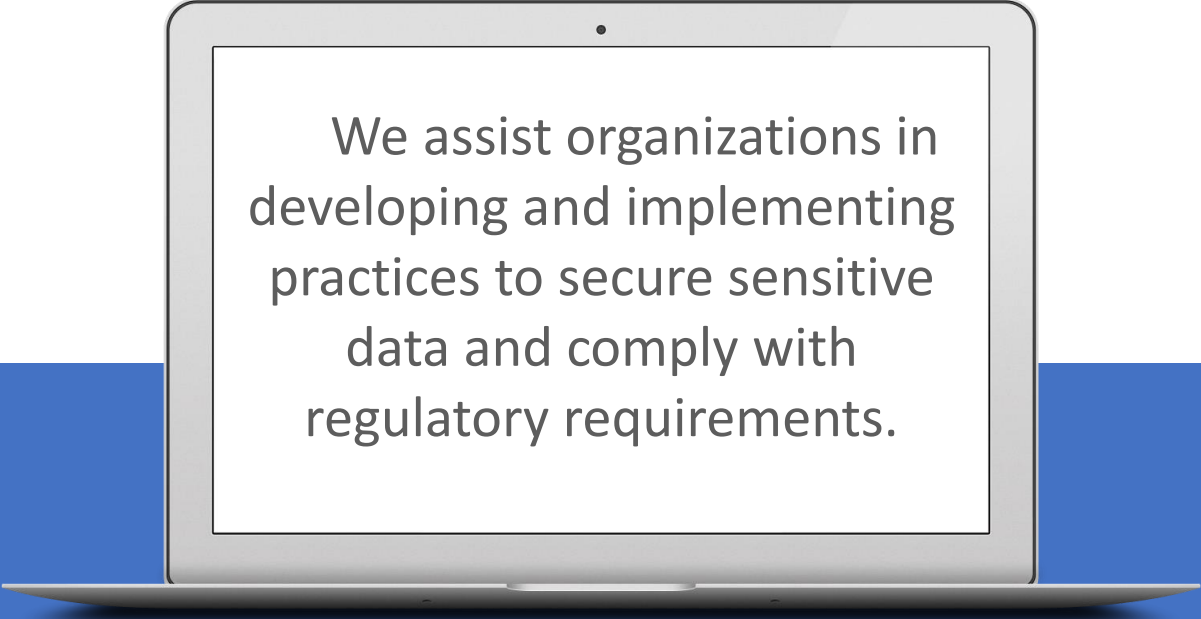
System and Organization Controls: SOC Suite of Certifications

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



databrackets
info@databrackets.com
866-276-8309

WHO WE ARE ...



We assist organizations in developing and implementing practices to secure sensitive data and comply with regulatory requirements.



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, CFE, CISA, CRISC, CISM

Ben Hunter Background

- Risk Advisory Manager at Bernard Robinson & Co.
- Specializes in Cybersecurity, SOC Reports and Information Technology Audits and Assessments.
- Obtained the AICPA Certified Information Technology Professional (CITP)
- Master of Science in Accounting
- Certified Public Accountant (CPA)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Security Manager (CISM)

AGENDA

1 What is a SOC Report?

2 SOC 1[®]—SOC for Service Organizations

3 Purpose & Applicability of SOC 2 Report

4 Why SOC2 different from an assessment?

5 Why else makes a SOC 2 different?

6 SOC Reports are flexible

7 SOC 3[®]—SOC for Service Organizations

8 SOC for Cybersecurity

9 Management's Assertion

10 Intended Users of a SOC 2 report

11 Examples of services provided

12 Type 1 and Type 2 SOC reports

13 NEXT STEPS

14 Q & A

What is a SOC for Service Organizations 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 for Service Organizations are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service.

What is a SOC for Service Organizations Report? ... Cont'd.

SOC examinations are not certifications. Therefore, the terms “certified,” “certificate,” or “certification” should not be used when referring to SOC examinations and reports. Similarly, a CPA firm providing its client with a certificate of completion inappropriately implies the SOC examination was a certification.

Correct: “Company announced that it recently completed its SOC 2 examination”

Incorrect: “Company completed a SOC2 compliance certification”

What are SOC for Service Organizations Report?

SOC for Service Organization reports are internal control reports, which independent CPAs provide, on the services a service organization provides.

- Useful for evaluating the effectiveness of controls related to the services performed by a service organization
- Appropriate for understanding how the service organization maintains oversight over third parties that provide services to customers
- Help reduce compliance burden by providing ONE report that addresses the shared needs of multiple users
- Enhances the ability to obtain and retain customers

What is a SOC Report?

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

Under Development: SOC for Supply Chains

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 for the customers of the Service Organizations will use the SOC 1 report

This meets the needs of user entities' managements and auditors as they evaluate the effect of a service organization's controls on a user entity's financial statement assertions.

These reports are important components of user entities' evaluation of their internal controls over financial reporting for purposes of compliance with laws and regulations and for when user entity auditors plan and perform financial statement audits.

Financial Statement Assertions

Occurrence

Classification

Completeness

Existence

Accuracy

Rights & Obligations

Cut-off

Valuation

Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)

For those who need to understand internal control at a service organization as it relates to:

security, availability, processing integrity, confidentiality or privacy

Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)

These reports can play an important role in oversight of the organization, vendor management programs, internal corporate governance and risk management processes, and regulatory oversight.

Stakeholders who may use these reports include management or those charged with governance of the user entities and of the service organization, customers, regulators, business partners and suppliers, among others.

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.

Why is 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.

Why else makes a SOC 2 different?

2017 Trust Services Criteria (TSC) Mappings to Various Frameworks

- 2017 TSC mapping to ISO 27001
- 2017 TSC mapping to NIST CSF
- 2017 TSC mapping to COBIT5
- 2017 TSC mapping to 2016 Trust Services Principles & Criteria
- 2017 TSC mapping to NIST 800-53

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 and privacy requirements of HIPAA

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

Information about how controls at a service organization comply with the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers

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.

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.

SOC Report Comparison

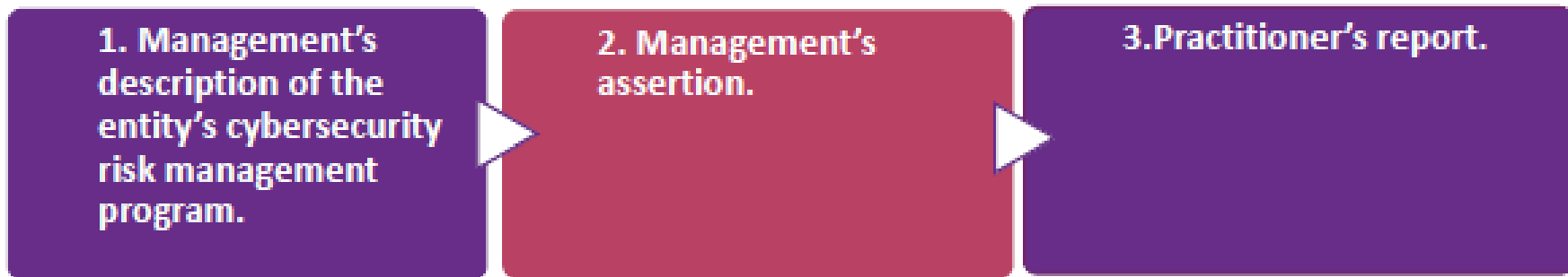
	Who Are the Users	Why	What
SOC 1*	Users' controller's office and user auditors	Audits of f/s	Controls relevant to user financial reporting
SOC 2*	Management Regulators Others	GRC programs Oversight Due diligence	Concerns regarding security, availability, processing integrity, confidentiality or privacy
SOC 3*	Any users with need for confidence in service organization's controls	Marketing purposes; detail not needed	Easy-to-read report on controls

Which SOC Report is Right for You?

Will report be used by your customers and their auditors to plan/perform an audit of their financial statements?	Yes	SOC 1 [®] Report
Will report be used by customers/stakeholders to gain confidence and place trust in a service organization's system?	Yes	SOC 2 [®] or SOC 3 [®] Report
Do you need to make report generally available?	Yes	SOC 3 [®] Report

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



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.

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.

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

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.

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

Why CPA Firms?

- **1970's** – CPAs are required to consider the effects of electronic data processing on the evaluation of internal control in financial statement audits
- **1990's** – CPAs begin performing SAS 70 audits (Statements on Auditing Standards) to report on effectiveness of internal control over financial reporting
- **2000s** – CPAs begin using the trust services criteria for evaluating controls
- **2017** – Introduction of SOC for Cybersecurity attestation services
- **2020** – Continue to develop and evolve SOC reports to enable users to better understand and manage risks arising from their business relationships with the service organization.

Why CPA Firms?

- **Understanding of IT processes and controls, security principles and concepts and Information Risk Management**
- Experience with common security frameworks
- Expertise in evaluating processes, control effectiveness and providing advisory and assurance services relating to these matters
- Multidisciplinary teams that include CISAs, CITPs, CISSPs,
- Proficiency in measuring performance against established criteria
- **Strict adherence to professional standards, professional code of conduct and quality control requirements**
- Holistic understanding of an entity's industry and business
- Objectivity, credibility and integrity
- **Independence, professional skepticism and commitment to quality**

Next Steps

Contact us for free no-obligation evaluation and quote

866-276 8309 or info@databrackets.com

UPCOMING EVENTS

☐ Security Hardening of AWS Cloud Hosting – March 26, 2020

Register now >> <https://databrackets.com/events/>

FIND US



CALL US
866-276 8309



SERVICE
info@databrackets.com



LOCATION
150, Cornerstone Dr.
Cary, NC



SOCIALIZE
Facebook
Twitter

Twitter: [@databrackets](https://twitter.com/databrackets)

Facebook: [databrackets](https://facebook.com/databrackets)

Questions

Please don't hesitate to ask

Thank You

for your attention!

To purchase reprints of this document, please
email info@databrackets.com.

Thank you for joining us today

05 March 2020