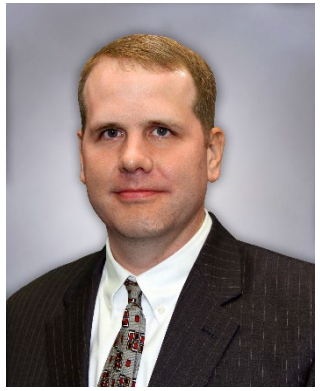
Reviewing SOC 2 Reports Efficiently and Effectively

McKonly & Asbury

CPAs & Business Advisors

INTRODUCTIONS



David Hammarberg, CPA, CFE, CISSP, CSEC, MCSE, CISA

- Partner of SOC and Cybersecurity

Lynnanne Bocchi, CPA, CIA, CISA, MBA

- Senior Manager
- Leader in the SOC Practice

McKonly & Asbury
CPAs & Business Advisors

FIRM OVERVIEW

McKonly & Asbury is a team of CPAs and Business Advisors serving clients from our offices in Camp Hill, Lancaster, and Bloomsburg.

We provide Advisory & Business Consulting, Audit & Assurance, Entrepreneurial Support & Client Accounting, Internal Audit, Professional Placement, and Tax services to a variety of industries including:


Affordable Housing


Construction


Employee Benefit Plans


Family-Owned Business


Healthcare


Manufacturing & Distribution


Nonprofits

McKONLY & ASBURY
CPAs & Business Advisors

WEBINAR OVERVIEW

- The SOC Suite of Services –
  - SOC 2 and SOC 3
- How to read a SOC report / What to look for
- 15 Minute Review – Can it be done?
- Why you should consider a SOC
  - Process Overview
- Vendors / Subservice Organization Considerations

SOC SUITE OF SERVICES

SOC Reporting – background and history

- SAS 70 *Service Organizations*
  - Released in 1992
  - Auditor-to-Auditor Communication
  - SAS = Statement on Auditing Standard
- Evolution to SSAE 16, now SSAE 18
  - Governed by Attestation Standards
  - Intended to report on control at a Service Organization

as they RELATE TO their users / customers

SOC SUITE OF SERVICES

SOC 2

- Report on internal controls, policies and procedures that relate to a service organizations system security unrelated to ICFR
  - Examples – Datacenter, Software Developer, Managed Services Provider, Insurance Companies
- Based on the AICPA's Trust Services Criteria – reports on a service organizations compliance with the principles of:
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy

SOC SUITE OF SERVICES

SOC 3

- Same base principles and approach as a SOC 2 (Trust Services Criteria)
  - SOC 2 –
    - Restricted use only to users / user auditors
    - Very descriptive of System
  - SOC 3 –
    - May be freely distributed
    - Limited description

HOW TO READ A SOC REPORT

Structure of a SOC 2 report

- Section I Service Auditors Report
- Section II Managements Assertion
- Section III Description of the System
- Section IV Description of Tests of Controls and Results of Testing
- Section V Other Information (Not Always Included)

Structure of SOC 3 report

- Section I Service Auditors Report
- Section II Managements Assertion
- Section III Description of the System (Limited)

HOW TO READ A SOC REPORT

What to Look For / What is Important

- Service Auditors Report
  - Type I vs Type II – not always explicitly identified
    - "As of XX/XX/XXXX" vs "The Period XX/XX/XXXX to YY/YY/YYYY"
    - Reference in Report to "Suitability of the design of controls" to achieve objectives vs. "Suitability of the design and operating effectiveness of controls" to achieve objectives.
  - System covered – is it the right one for you?
    - SOC 2/3 – what Trust Services Principles does it cover? Are they appropriate?
  - Opinion: Unmodified vs. Qualified (separate paragraph)
  - References to Subservice Organizations: Inclusive or Carve Out
  - References to User Control Considerations
    - Look to Section III if so

HOW TO READ A SOC REPORT

What to Look For / What is Important

- Description of the System
  - What is in-scope? Does it cover what you need it to cover?
  - What sub-service organizations are used?
    - Inclusive – How do they interplay? How does the entity monitor?
    - Carve-out – What monitoring does entity perform? Is the sub-service provider significant? If so, consider requesting sub-service organization's SOC report.
  - Obtain general understanding of how the entity manages transactions / controls / processes
  - USER CONTROL CONSIDERATIONS
    - Develop a checklist to ensure you are doing these things (if SOC is for your vendor)
    - Make sure list is comprehensive for your customers (if SOC is over your company)

HOW TO READ A SOC REPORT

What to Look For / What is Important

- Description of Tests of Controls and Results of Testing (SOC 2 Type II only)
  - Understand the Control Objectives tested
    - Do they meet your need (as a user of a vendors SOC report)
    - Will they meet your customers needs (for your SOC report)
  - Review "Results of Tests" column
    - If ANY exceptions noted, document consideration of impact on achievement of objective
    - Exceptions will contain details – "2 of 37 tested failed" – understand magnitude of what occurred
    - Note – even with an unmodified opinion, you may identify control exceptions of concern to your use of the service organization even if the Service Auditor concluded the Control Objective / Trust Services Criteria was met

HOW TO READ A SOC REPORT

What to Look For / What is Important

- Other Information
  - Not required / often excluded, as such, read and understand what the entity is trying to convey. Often very important information in assessing the service provider.
  - May include managements responses to Control Testing Exceptions.

HOW TO READ A SOC REPORT IN 15 MINUTES

- P - Principles
- R - Response
- O - Opinion
- T - Time Period
- E - Exceptions
- C – Complementary User Entity Controls and Complementary Subservice Organization Controls
- T – Type
- S - Scope

McKonly & Asbury
CPAs & Business Advisors

PRINCIPLES

- AICPA Trust Services Criteria Framework
  - Security - Required
  - Availability
  - Confidentiality
  - Processing Integrity
  - Privacy

RESPONSE

McKonly & Asbury
CPAs & Business Advisors

OPINION

- Unqualified – Control designed and operating as stated
- Qualified – One of more controls (usually within a specific criteria) were not adequately designed or operating
- Adverse – More than one criterion was not met due to multiple controls being improperly designed or failing to operate effectively. DO NOT TRUST THIS ORGANIZATION!
- Disclaimer – The auditor is unable to provide an opinion due to lack of information from the SOC provider

TIME PERIOD

- Period covered by the report
- Necessity for a bridge letter
  - What is a bridge letter?
  - Time period covered by the bridge letter

EXCEPTIONS

- Instances where the control was not designed appropriately or did not operate as intended during the audit period
  - Found within the testing matrix

COMPLEMENTARY CONTROLS

- Complementary Entity User Controls
  - Controls the SOC provider's customers must have in place in order for the entity's controls to be reliable
- Complementary Subservice Organization Controls
  - Controls provided by the carved-out vendor

TYPE

- Type 1
  - Point in time
  - Opinion on the design of controls only
  - No test of operating effectiveness
- Type 2
  - Period of time
  - Tests of design and operating effectiveness

SCOPE

- The software applications or services offered to clients
- This includes
  - Data hosted within the application
  - Infrastructure used to provide the application
  - People and Processes that support the offering

WHY YOU SHOULD CONSIDER A SOC

External

- Environment surrounding Vendors / Service Organizations
  - Higher scrutiny from Users – their auditors, internal auditors, regulators, or THEIR customers are mandating all vendors have a SOC
  - Passing along your sub-service organization's SOC no longer accepted (i.e. your Data Center has a SOC, and you've provided that in the past)
  - More frequently becoming a condition of contract / renewal
  - Trend will continue – if you haven't been asked yet, you will be soon
- Positive indicator to prospective customers that you have taken this step – even if they aren't requiring it
- Timeline for SOC can be as long as a year – waiting until necessary may cost you business

WHY YOU SHOULD CONSIDER A SOC

Internal

- Identify and fill gaps in controls / processes or documentation
- Demonstrate to stakeholders that systems, processes and controls are well-defined and managed
- External validation of internal processes and controls (Fresh Eyes)

McKonly & Asbury
CPAs & Business Advisors

WHY YOU SHOULD CONSIDER A SOC

Process Overview

- Determine Need –SOC 2/3? Type 1 or 2?
- Internal evaluation – what system / services would be most relevant?
  - Determine Applicable Trust Services Principles and Criteria (SOC 2/3)
  - Perform a Risk assessment
  - Review of Service Level Agreements
  - What documentation is in place? Where is it stored?
  - What sub-service organizations do you use? What (specifically) does each do, and how are your systems reliant on that service?

WHY YOU SHOULD CONSIDER A SOC

Process Overview

- Map existing controls to identified Objectives / TSC
  - Have you covered all aspects of the Objective? All relevant Trust Services Criteria (consider Points of Focus)?
  - Are you using an appropriate mix of preventative and detective controls?
  - Are controls a reasonable mix of system controls and manual controls?
  - In the individual responsible for such controls at an appropriate level with appropriate training/background?
  - Are controls designed with sufficient precision that they can clearly cover the objective and be tested, but also broadly enough to be utilized to link to multiple Objectives or TSC?
  - Perform a gap assessment and remediate where gaps identified!

WHY YOU SHOULD CONSIDER A SOC

Process Overview

- Consider the controls identified
  - Do you have sufficient, competent evidence of the performance of control activities and results of the identified controls?
    - If not – remediate and design appropriate, comprehensive documentation standards
  - How will you archive and organize evidence of control performance?
  - Can Internal Audit assist in the testing or documentation process? How?
- Perform Control Walkthroughs
  - Walk through an identified process, ensuring that all controls identified are functioning the way you anticipate they are, and ample evidence exists of their functioning.

WHY YOU SHOULD CONSIDER A SOC

Process Overview

- AFTER all of controls are identified and you are comfortable with the ‘mapping’ – THEN begin drafting Management’s Description of the System
- Develop a plan for regular monitoring and updating of controls
  - Risk Assessment and Environmental Assessment
  - Feedback from Users
  - Evaluation of Strategic Plans
  - Refine Documentation Strategies

WHY YOU SHOULD CONSIDER A SOC

Process Overview

- Considerations for Year 2 and beyond
  - Any relevant control changed during testing period must have both pre- and post-change included in SOC report so users can understand system changes
  - OK to refine / adjust Control Objectives or add additional Trust Services Principals in subsequent years
  - Consider if service level continues to be appropriate
    - Type I vs Type II
    - Potential need for SOC 2 for certain services or customers

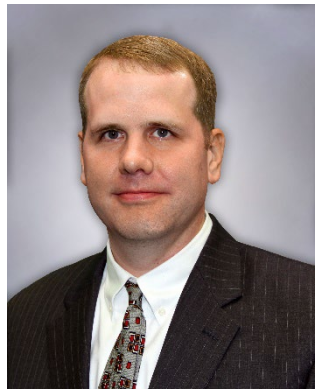
VENDOR / SUBSERVICE ORGANIZATIONS

- Considerations when using Service Organizations
  - What to do with it
    - Read it, being particularly focused on areas covered in “What to Look For”
    - Understand **User Control Considerations** – DOCUMENT your compliance!
    - Don’t hesitate to call the Vendor and ask questions for clarity
    - If qualified opinion or significant control exceptions, determine next steps with vendor
  - What NOT to do with it
    - Just file it away and check the box that you received it

UNDERSTAND THAT THERE IS VALUE IN THE SOC REPORT

You just need to know how to read it

CONTACT US



David Hammarberg, CPA, CFE, CISSP, CSEC, MCSE, CISA

- dhammarberg@macpas.com

Lynnanne Bocchi, CPA, CIA, CISA, MBA

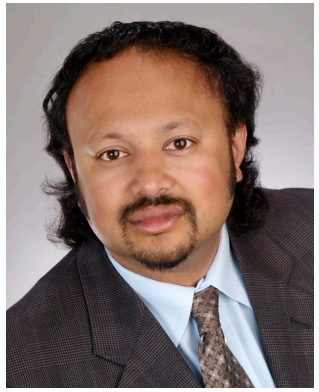
- lbocchi@macpas.com

REGISTRATION IS OPEN!

Thursday, May 18, 2023
Penn Harris Hotel
1150 Camp Hill Bypass
Camp Hill, PA 17011

COLLABORATE! 2023
Annual Leadership Conference

Keynote Speaker: Lee Rubin
5 Components of Extraordinary Teams



Featured Speaker: Dr. Anirban Basu
Show Me the Money

Visit us online at **www.macpas.com** for more information.

McKonly & Asbury
CPAs & Business Advisors

APRIL 27 WEBINAR

SOC Versus SOX

- Our team will provide the opportunity to attain a greater understanding of the differences between Service Organization Controls Reports (SOC) and the Sarbanes-Oxley Act of 2002 SEC requirements.

Register Today!

Visit us online at **www.macpas.com** for more information.

McKonly & Asbury
CPAs & Business Advisors