McKonly & Asbury

# SOC VS. SOX

## APRIL 27, 2023

# PRESENTER PROFILES

## Elaine Nissley, Principal, CISA, PMP, CRMA, CRISC

- Over 30 Years of Internal Audit and Internal Controls Experience
- Leads the Internal Audit Practice
- Provides Internal Audit Outsourcing services
- Sarbanes Oxley and OMB Circular A-123 Compliance

## Lynnanne Bocchi, Senior Manager, CPA, CIA, CISA, MBA

- Over 10 years of Internal Controls Experience
- Leader in the SOC Practice
- Provide SOC 1, SOC 2, SOC 3, HITRUST, HIPAA, and Cybersecurity IT Assessment services

McKonly & Asbury

# 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

# LEARNING OBJECTIVES

- Understand Processes and Purpose
  - Service Organization Control Reports
  - Sarbanes Oxley Internal Control Assessments
- Learn Strategies To:
  - Gain SOX Efficiencies Using SOC
  - Gain SOC Efficiencies Using SOX

McKonly & Asbury

McKonly & Asbury

# SYSTEM AND ORGANIZATION CONTROLS (SOC)

# PURPOSE

- Who gets a SOC examination?
  - Service Organizations
- Why do they need a SOC examination?
  - To provide comfort to user organizations about the processes and controls at the service organization
- Who is going to be using the report?
  - User organization management
  - User organization auditors

McKonly & Asbury

# SOC 1

- SOC 1 Examinations are focused on service organizations reporting on controls relevant to internal control over financial reporting (ICFR) or a specific financial statement assertion
- Service organizations determine control objectives and controls to meet the appropriate objectives

# SOC 2

- SOC 2 examinations ensure service organizations maintain controls to securely manage customer data and protect them and their privacy.
- SOC 2 service organization controls must meet the specified Trust Services Principles defined by the AICPA
- Trust Services Principles include Security, Availability, Processing Integrity, Confidentiality and Privacy

# SOC 2 (CONTINUED)

- AICPA Trust Services Principles
  - Provide control objectives for SOC 2 and SOC 3 engagements.
  - Prescribed control objectives for the 5 trust services principles
    - Security
    - Availability
    - Processing Integrity
    - Confidentiality
    - Privacy

# SOC 2 (CONTINUED)

- Service Organizations receiving a SOC 2 select the trust services principles to be including in the examination
  - Security is the common control baseline and is required to be in every SOC 2 report
  - Service Organization can exclude specific trust services criteria as long as it is disclosed in the report along with the reason it is not applicable

# SOC 3

- SOC 3 was established as a general use report alternative to the SOC 2 Report
  - SOC 3 examinations are examinations on controls relevant to the applicable Trust Services Principles
  - The report includes only the auditor's opinion and limited description of controls (narrative)
- SOC 3 examination covers both design and operating effectiveness of controls relevant to applicable Trust Services Principles

# SOC REPORTS

- Components of SOC 1 and SOC 2 Reports
  - Auditor's Opinion
  - Management's Assertion
  - Description of Controls (Narrative)
  - Complementary Entity User Controls
  - Controls and Test of Controls
  - Other information

McKonly & Asbury

# SOC REPORTS (CONTINUED)

- Two Types of SOC Reports
  - Type I
  - Type II
- Type I
  - Opinion on design effectiveness of controls
  - At a specific date
- Type II
  - Opinion on design and operating effectiveness of controls
  - Covers a period of time (minimum of 6 months)

McKonly & Asbury

# DESCRIPTION OF CONTROLS NARRATIVE

- Prepared by the service organization
  - Provides narrative of the controls for service organization
  - Key components for SOC Reports
    - Overview
    - Control Environment
    - Information and Communication
    - Risk Assessment
    - Control Activities
    - Monitoring
    - Logical and Physical Access
    - System Operations
    - Change Management
    - Risk Mitigation

McKonly & Asbury

# COMPLEMENTARY USER ENTITY CONTROLS

- Controls identified by the Service Organization that should be in place at the user organization for the controls to work effectively.
- Identifies the responsibilities of user organization and limits the responsibilities of service organizations.

# CONTROL ACTIVITIES AND TESTS OF CONTROLS

- Control Objectives (SOC 1) or Trust Services Criteria (SOC 2)
  - Key Controls to meet to the objective or criteria
  - Test of controls performed by the auditor
  - Results of the test of controls performed by the auditor
    - Exceptions
    - Control Objectives not being met
    - Controls not operating during the period

# EXCEPTIONS AND CONTROL FAILURES

- Exceptions identified during controls testing
  - ANY exceptions identified during testing are required to be reported in test of controls
    - The size of the sample along with number of items with exceptions MUST be disclosed in the exception
    - In the event of substantial exceptions if the service organization does not have sufficient mitigating controls the auditor's opinion may need to be modified

# SOC CONTROLS TESTING

- Three methods for testing controls
  - Inquiry (cannot be performed alone)
  - Observation
  - Examination
- Walkthroughs of controls are performed for all control areas (Inquiry)
- Sampling is based upon frequency of control activity and reporting period (Observation or Examination)

# USER CONSIDERATIONS FOR SOC REPORTS

- Reviewing a SOC report
  - Evaluate the specific area or process that the SOC report is being provided to ensure it matches the area you are auditing
  - Review the auditor's opinion for any modifications or qualification of the report
  - Review the controls, test of controls and results of tests for
    - Control objectives directly related to the financial statement assertions you will be auditing
    - Exceptions

# USER CONSIDERATIONS FOR SOC REPORTS

- Review the Complementary Entity User Controls to determine if they apply to the service you receive, and if they are in place

McKonly & Asbury

# SARBANES OXLEY (SOX)

# PURPOSE

- Regulatory Compliance
- Internal Control Over Financial Reporting
  - Improved Accuracy of Financial Reports
  - Improve the Reliability of Financial Reports
  - Complete and Accurate Disclosures
  - Protect Investors From Fraudulent Reporting
  - Protect Employees from Corporate Scandals

# REGULATORY

- Section 302
  - Quarterly Certification
- Section 401
  - GAAP Compliance
  - Off-balance Sheet transactions
- Section 409
  - Disclosures
- Section 802
  - Penalties

McKonly & Asbury

# REGULATORY

- Section 806
  - Whistleblower Protection
- Section 902
  - Executive Penalties
- Section 906
  - CEO & CFO Certification
  - False or Misleading Report Penalties

# REGULATORY

- Section 404
  - Internal Control Over Financial Reporting (ICFR)
  - Statements from Management
    - Responsibility for Internal Controls
    - How Effectiveness of Internal Controls Evaluated
    - Assessment of the effectiveness of the internal controls
  - External auditor attest to management's assessment

# COSO FRAMEWORK

- Recommended for SOX ICFR
- Basis for SOC
  - SOC 1 ICFR
  - SOC 2 Trust Services

# COSO FRAMEWORK

- Committee of Sponsoring Organizations (COSO) framework
- SEC - COSO is an acceptable framework for ICFR Assessment
- Framework
  - Five Components
  - Seventeen Principles
  - Rule of Judgement
  - Business/Financial Processes
  - Information Technology General Controls

# COSO FRAMEWORK

**Control Environment**

1. Commitment to integrity and ethical values
2. Board of directors
    - Independence from management, and
    - Oversight of the development and performance of internal control
3. Management establishes, with board oversight,
    - Structures, reporting lines, and
    - Appropriate authorities and responsibilities in the pursuit of objectives
4. Commitment to attract, develop, and retain competent individuals
5. Holds individuals accountable for their internal control responsibilities

# COSO FRAMEWORK

## Risk Assessment

6. Specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. Identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. Considers the potential for fraud in assessing risks to the achievement of objectives.
9. Identifies and assesses changes that could significantly impact the system of internal control.

# COSO FRAMEWORK

## Control Activities

10. Selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. Selects and develops general control activities over technology to support the achievement of objectives.
12. Deploys control activities through policies that establish what is expected and procedures that put policies into action.

# COSO FRAMEWORK

## Information and Communication

13. Obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. Internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. Communicates with external parties regarding matters affecting the functioning of internal control.

# COSO FRAMEWORK

## Monitoring Activities

16. Selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. Evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

# ICFR

## Control Activities and Financial Statement Assertions

- Business Process Controls
  - Accuracy of information fed into financial reporting
  - Impact in part or whole is material
  - Risk based

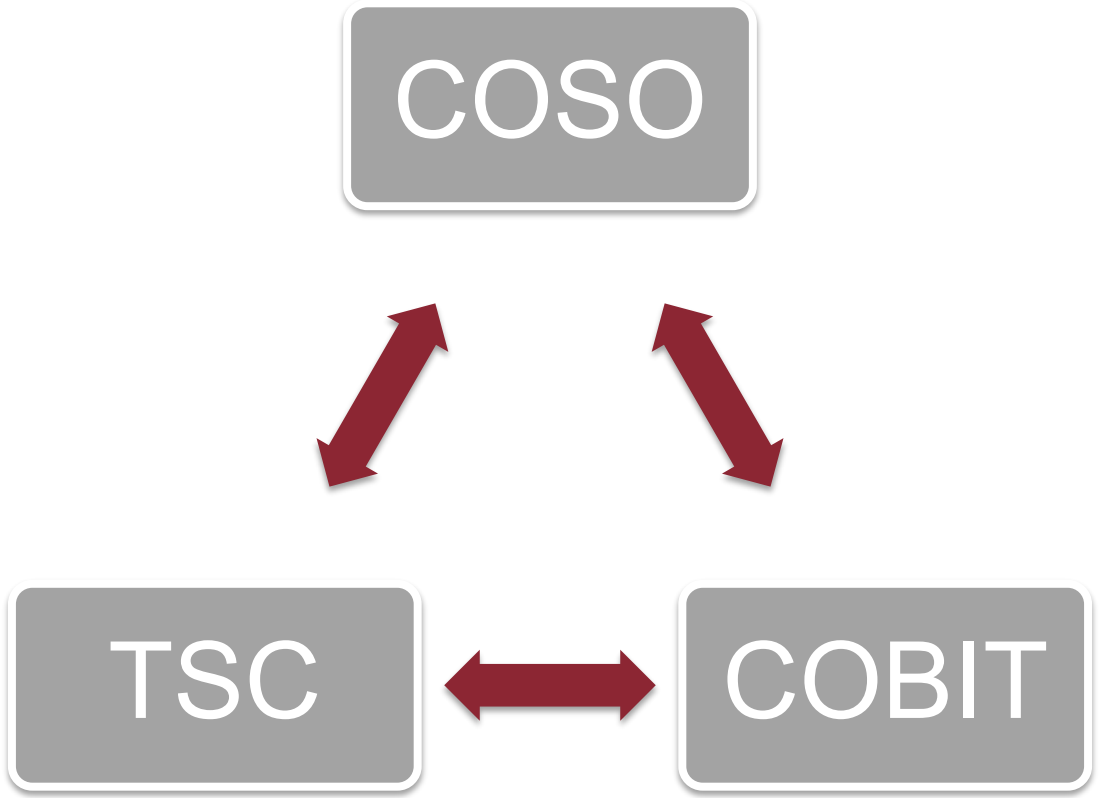
# INFORMATION TECHNOLOGY

- ICFR Relies on Information Technology
- IT Controls - ensure the systems are accurate, complete, and free from error since that would impact the financial reporting
- SOX IT Systems - Identify which IT processes and systems impact financial reporting
- IT Applications Controls
- IT General Controls

# INFORMATION TECHNOLOGY

- Control Objectives for Information and Related Technology (COBIT) Domains
  - Evaluate, Direct, and Monitor (EDM)
  - Align, Plan, and Organize (APO)
  - Build, Acquire, and Implement (BAI)
  - Deliver, Service, and Support (DSS)
  - Monitor, Evaluate, and Assess (MEA)

# CONTROL OBJECTIVE MAPPING



McKonly & Asbury

# SOC & SOX COMMONALITIES

# DIFFERENCES

## SOC

- Complementary Entity User Controls
- Not Regulatory, Customer Contract Requirements
- AICPA
- Auditor Opinion
- Period-of-Time
- Testing
  - Inquiry
  - Observation
  - Examination

## SOX

- No Complementary Entity User Controls
- SEC Requirement for Publicly Traded Companies
- AICPA & PCAOB
- Management Assessment
- At End of Fiscal Period
- Testing
  - Inquiry
  - Observation
  - Examination
  - Re-performance

McKonly & Asbury

# SIMILARITIES

- COSO Framework (SOC only First 5 Trust Service Criteria)
- Control Walkthroughs
- Test of Design Effectiveness
- Test of Operating Effectiveness (SOC Type II only)
- Sample Based on Frequency of Control
- Can Rely on the Work of Internal Audit & Use Similar Assessment Criteria
- Control Objectives Map COSO/TSC/COBIT

McKonly & Asbury

# CONTACT US

**Elaine Nissley, Principal, CISA, PMP, CRMA, CRISC**

- enissley@macpas.com

**Lynnanne Bocchi, CPA, CIA, CISA, MBA**

- lbocchi@macpas.com

McKonly & Asbury

# 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***

**Did you know *COLLABORATE!* 2023 offers…**

– 6.5 Continuing Professional Education credits
– 6.00S maximum credits from the PACLE Board
– 6.5 SHRM credits

SHRM SHRM-CP | SHRM-SCP RECERTIFICATION PROVIDER

McKonly & Asbury is recognized by SHRM to offer Professional Development Credits (PDCs) for SHRM-CP® or SHRM-SCP® recertification activities.

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

McKONLY & ASBURY