MOSSADAMS

Understanding How to Leverage SOC Audits

Financial Advisory Council for the State of Washington
June 28, 2018

Presenters

Chris Kradjan, Partner, CPA, CITP, CRISC, HITRUST CCSFP

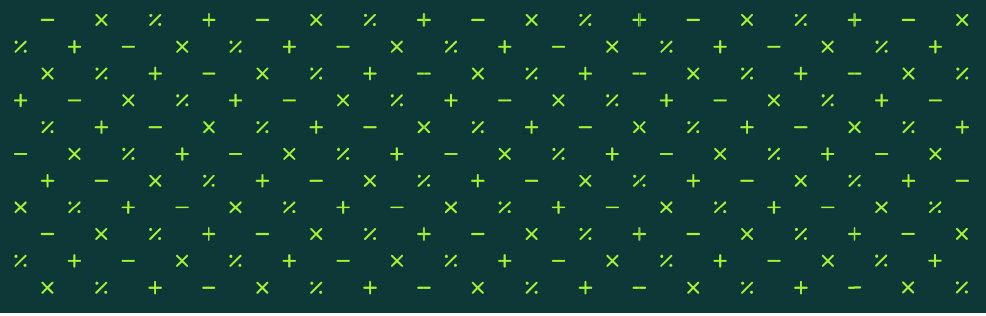
Chris has over 10 years of experience in the field of SOC, and oversees the IT Compliance Practice and is the National SOC Practice Leader for Moss Adams, including providing quality control for both SOC audit services and technology audits. Engagements include SOC 1, SOC 2, SOC 2+, SOC 3, and SOC for Cybersecurity. In addition to SOC auditing, Chris's practice areas include cybersecurity audits, PCI DSS services, HITRUST audits, security and privacy audits, internal controls reviews, Sarbanes-Oxley compliance services, and independent technology assessments. Chris is also regularly involved with technology and financial controls assessments based on the NIST, ISO 27002, CSA, ITIL, COBIT and COSO frameworks.

Chris recently served on the AICPA Assurance Services Executive Committee (AICPA ASEC), continues to be a member of the AICPA ASEC Trust/Information Integrity Task Force and the AICPA SOC 1 and SOC 2 Task Forces, and is working to review the current SOC guides and update the Trust Services Criteria. He has a Bachelor of Arts, Business Administration from Western Washington University

Agenda

- SOC Overview
- Type of SOC Reports
  - SOC 1
  - SOC 2
  - SOC 3
- SOC Report Comparison
- Reviewing SOC Reports
- Latest SOC Updates
- Question & Answers

SOC Overview



What is a SOC Report

- Service Organization Control (SOC) reports are internal control reports on the services provided by a service organization
- Used to assess and address the risks associated with an outsourced service
- Outsourced services can include any function of a business that is not performed in-house, such as payroll, cloud providers, infrastructure as a service, etc.

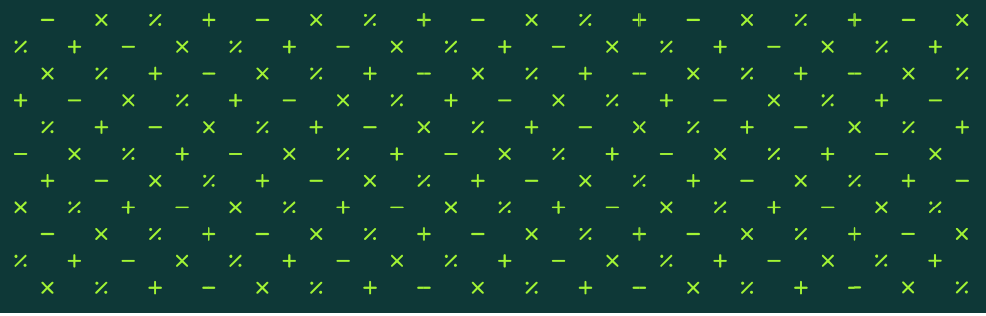
Risk of Outsourcing Processes

- Companies are increasingly outsourcing aspects of their business to service organizations
- While outsourcing can increase efficiency and reduce costs, it increases the overall risk the organization faces by no longer having complete control over a process
- These risks can impact financial statements, operations, and internal controls

Benefits of a SOC Audit

- Provides an independent examination of the internal controls at the service organization
- Reduces the cost and administrative burden of multiple audits over the same process
- Identifies potential opportunities to strengthen the business practices and operating environment
- Allows service organizations to communicate information about the company and their control environment

Types of SOC Reports



Overview

Historical with SAS 70	New with SSAE 18 (Replaces SSAE 16)	New with AT101
• SAS 70 Reporting	• SOC 1 – Internal Controls Over Financial Reporting	• SOC 2 – Trust Services Principles (Detailed Reporting) • SOC 3 – Trust Services Principles (Summary Reporting)

SOC Comparison

SOC 1

1. Auditor's report
2. Management's assertion
3. Detail system description and Management controls
4. Auditor test of controls and results of those tests – **control objectives**

SOC 2

1. Auditor's report
2. Management's assertion
3. Detail system description and Management controls
4. Auditor test of controls and results of those tests – **criteria**

SOC 3

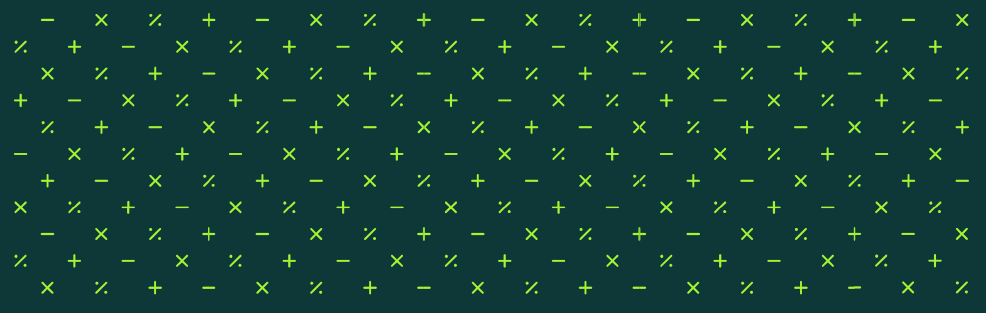
1. Auditor's report
2. Management's assertion
3. ~~**Detail** system description **and Management controls**~~
4. ~~**Auditor test of controls and results of those tests**~~

Source: AICPA

SOC Type 1 vs. SOC Type 2

- Type 1 Report
  - Design and implementation of internal controls
  - Point in time
  - “As of” date
- Type 2 Report
  - Operating effectiveness of internal controls
  - Period of time
  - Often 12-month period

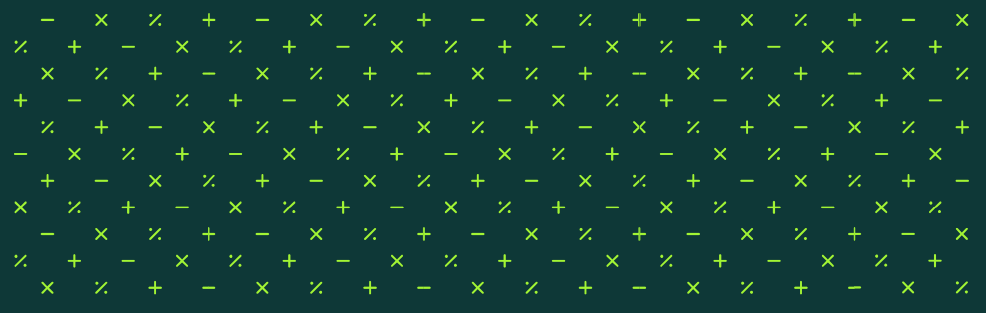
SOC 1



SOC 1

- Subject matter focuses on internal controls
  over financial reporting
- Auditor-to-auditor communication
- Restricted use and distribution of report
  - Auditor's of the user-entity's financial statements
  - Management of the user entities
  - Management of the service organization
- Type 1 or Type 2 report
  - Testing methods
  - Inquiry, observation, inspection, and reperformance
  - Carve-out and inclusive methods
  - Complementary user-entity controls

SOC 2 / SOC 2+



SOC 2

- Subject matter focuses on internal controls related to Trust Services Criteria:
  - Security *(Required)*
  - Availability *(Optional)*
  - Processing Integrity *(Optional)*
  - Confidentiality *(Optional)*
  - Privacy *(Optional)*
- Users of the report include:
  - Stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls
  - Restricted use, but intended for a broader range of users, including existing users, prospective users, and regulators

SOC 2

- Well suited for IT and cloud providers
  - SaaS / IaaS / PaaS
  - Application service provider
  - Data centers
- Virtualized environments
- Type 1 or Type 2 reports
- Report presentation similar to SOC 1 audit
- Expected to have limited carve outs and complementary user-entity controls

SOC 2 – System Boundary Components

- **Infrastructure** is comprising the physical structures, IT, and other hardware (facilities, computers, equipment, mobile devices and telecommunications networks)
- **Software** is the application programs and IT system software that supports application programs (operating systems, middleware, and utilities)
- **People** are the personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers)
- **Procedures** is the automated and manual procedures
- **Data** is the transaction streams, files, databases, and tables and output used or processed by a system

SOC 2 – Trust Services Criteria

- Trust Services Criteria updated in 2016 and again 2017
- Security criteria organized into seven common criteria
  1. Organization and management
  2. Communications
  3. Risk management and design and implementation of controls
  4. Monitoring of controls
  5. Logical and physical access controls
  6. System operations
  7. Change management
- New 2017 update on the horizon around mapping criteria to the COSO framework

Security	Availability	Confidentiality	Processing Integrity	Privacy
• IT security policy • Security awareness and communication • Logical access • Physical access • Environmental controls • Security monitoring • User authentication • Incident management • Asset classification / management • Systems development and maintenance • Personnel security • Configuration management • Change management • Monitoring / compliance	• Availability policy • Backup and restoration • Incident management • Disaster recovery • Business continuity management • Security • Change management • Monitoring / compliance	• Confidentiality policy • Confidentiality of inputs • Confidentiality of data processing • Confidentiality of outputs • Information disclosures (including third parties) • Confidentiality of Information in systems development • Incident management • Security • Change management • Monitoring / compliance	• System processing integrity policies • Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs • Information tracing from source to disposition • Incident management • Security • Change management • Availability • Monitoring	• Privacy policies • PII classification • Risk assessment • Incident & breach management • Provision of notice • Choice and consent • Collection • Use and retention • Disposal • Access • Disclosure to third parties • Security for privacy • Quality • Monitoring and enforcement

SOC 2+ (SOC 2 Plus)

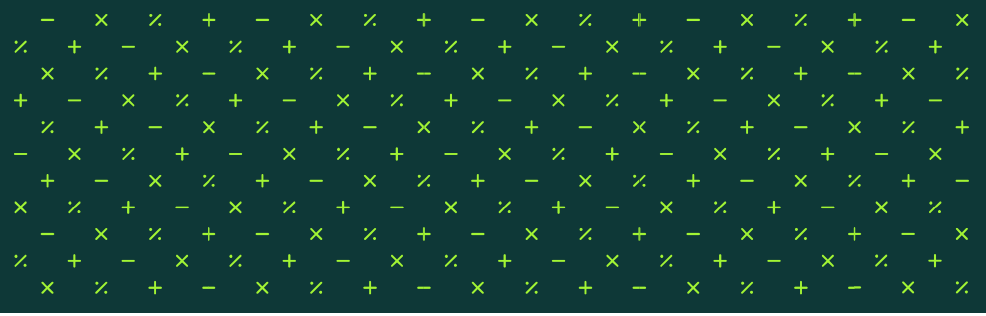
Used to address criteria in addition to the applicable trust services criteria or additional subject matter related to the service organization's services

Additional subject matter can include:

1. HIPAA
2. HITRUST
3. ISO 27001
4. Cloud Security Alliance

Existing SOC 2 controls are mapped to additional criteria or regulations and included in Section 5

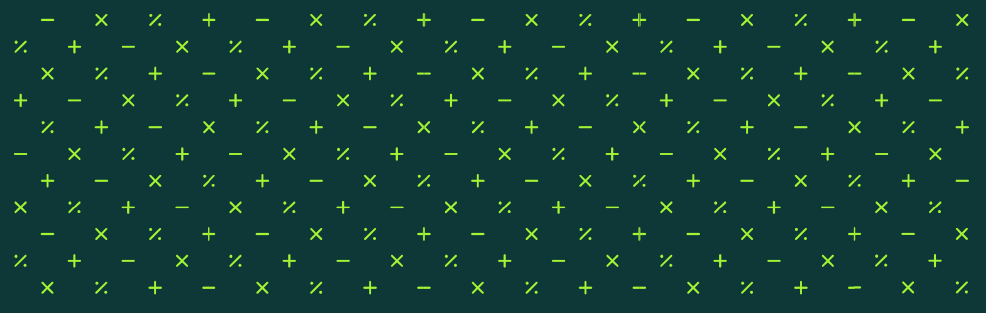
SOC 3



SOC 3

- Designed for users who want assurance on the controls at a service organization but do not have the need for or the knowledge necessary to make effective use of a SOC 2 report
- Can be issued concurrently with SOC 2 or separately (i.e., anytime after issuance of SOC 2)
- General use report
- Difference between SOC 2 and SOC 3 layout:
  - Abbreviated system description (section 3)
  - Excludes section 4 (tests of controls and results of tests)

SOC Report Comparison



SOC Comparison – Reporting Options

	Internal Controls Over Financial Reporting	Operational Controls	
	SOC 1	**SOC 2**	**SOC 3**
Summary	• Detailed reports for users and auditors	• Detailed report for users, auditors and specified parties	• Summary report that can be more generally distributed
Applicability	• Focused on financial reporting risks and controls specified by the service provider • Most applicable when the service provider performs financial transactions processing or supports transaction processing systems	• Focused on the Trust Services Principles: o Security o Availability o Confidentiality o Processing Integrity o Privacy • Applicable to a broad variety of systems	

SOC Comparison – Scope

	SOC 1	SOC 2/SOC 3
Required Focus	• Internal control over financial reporting	• Operational controls
Define Scope and Systems	• Classes of transactions • Procedures for processing and reporting transactions • Accounting records of the systems • Handling of significant events and conditions other than transactions • Report preparation for users • Other aspects relevant to processing and reporting user transactions	• Infrastructure • Software • Procedures • People • Data
Control Domains Covered	• Transaction processing controls • Supporting information technology general controls	• Security • Availability • Confidentiality • Processing Integrity • Privacy
Level of Standardization	• Control objectives are defined by the service provider and may vary depending on the type of service provided.	• Principles are selected by the service provider • Specific predefined criteria are used rather than control objectives

SOC Comparison – Report Structure

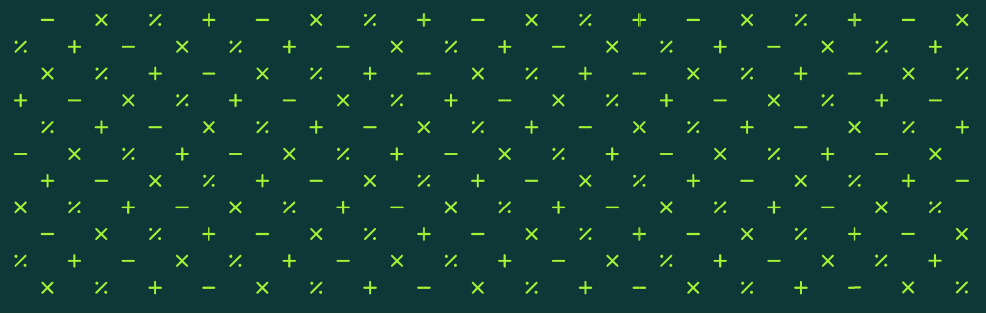
SOC 1	SOC 2	SOC 3
• Auditor's Opinion	• Auditor's Opinion	• Auditor's Opinion
• Management Assertion	• Management Assertion	• Management Assertion
• Assertion System Description (including Controls)	• Assertion System Description (including Controls)	• Assertion System Description • (Summary)
• Control Objectives	• Criteria	• Criteria (Referenced)
• Control Activities	• Control Activities	—
• Test of Operating Effectiveness*	• Test of Operating Effectiveness*	—
• Results of Tests*	• Results of Tests*	—
• Other Information (if applicable)	• Other Information (if applicable)	—

*Note: Only applicable for Type 2 reports.

SOC Comparison – Report Types

	Type 1	Type 2
SOC Reports	• SOC 1 • SOC 2	• SOC 1 • SOC 2
Coverage	• Point in time	• Period of time
Assessment	• Design	• Design • Operating Effectiveness • Results of Tests

Reviewing SOC Reports



Common Issues

- Reliance on service organizations was not identified or not properly documented.
- Sub-service organizations that were scoped out of the report were not addressed.
- Complementary-entity user controls were not sufficiently tested or not properly linked to the test of controls.
- Update procedures were not properly performed or documented when the auditor’s report did not sufficiently cover the entire audit period.
- Control exceptions identified by the service provider were not evaluated to determine the sufficiency of audit procedures.

SOC Comparison – Report Types

	Description
Inventory	• Inventory existing outsourced vendor relationships to determine whether third-party assurance may be required
Assess	• Assess the key financial reporting risks associated with significant outsourced vendors • Identify in-scope service organizations
Identify	• Identify relevant reports that have been obtained and determine appropriateness • Identify any additional reports or documents needed to complete the assessment (e.g., bridge letter, Management's discussion with the service provider, etc.)
Test and Conclude	• Assess the adequacy of the SOC report scope • Perform review procedures to evaluate the operational effectiveness of controls relied upon at the service organization

Structure and Contents

- The structure and contents of SOC 1 and SOC 2 reports generally follows the below list:
  - Independent service auditor’s report (opinion)
  - Management’s written assertion
  - Service organization’s description of the system
  - Complementary user entity controls
  - Control objectives (SOC 1)/Criteria (SOC 2), control activities and control tests performed (Type 2 reports)
  - Supplemental information from the service organization
- When performing an evaluation of an SOC report, management should identify and evaluate each section of the report

Independent Service Auditor's Report

- This section describes the scope of the examination and provides the service auditor's opinion on:
  - Management's presentation of its system of internal control.
  - The suitability of the design of the system.
  - Opinion on the operating effectiveness of the controls
    (Type 2 reports only).

- It generally includes the following sections:
  - Scope
  - Service Organization's Responsibilities
  - Service Auditor's Responsibilities
  - Inherent Limitations
  - Opinion
  - Description of Test of Controls
  - Restricted Use

Reviewing Service Auditor's Report

- Verify that the report coverage is adequate. If the coverage is insufficient and/or the report date does not coincide with the client's year-end, verify how Management was able to gain acceptance of the coverage exceptions.
- Verify the type of report issued and determine whether it is appropriate for use (e.g., SOC 1 vs. SOC 2, and Type 1 vs. Type 2).
- Verify whether service providers are being used by the service organization and determine whether the service auditor's evaluation included sub-service providers.
- Determine the type of opinion issued (i.e., qualified vs. unqualified).

Management's Written Assertion

- Management's assertions may be in a separate section of the report or included in the section containing the description of the system.
- Management's written assertions cover the following:
  - The fair presentation of the description of the system
  - The suitability of the design of controls and verification that they were implemented as of a specific date (Type 1) or throughout the period (Type 2)
  - The operating effectiveness of the controls throughout the period (Type 2)
  - The relevant changes to the system throughout the period (Type 2)

Reviewing Management's Assertion

- Verify that Management's written assertions in this section mirror the service auditor's opinion.
- Verify that there are no qualifications in the assertions/modifications in the language (i.e., use of "except for" or other exclusionary language).
- Verify that there are no omissions in description criteria outlined by the AICPA relative to the services provided.

Service Organization's Description

- This section includes the service organization's explanation of the system and generally includes a description of the following:
  - Services provided
  - Description of entity-level controls relating to the control environment, risk assessment processes, monitoring activities and information and communication processes
  - Procedures by which services are provided and transactions are accounted for, and related accounting records
  - Significant events other than transactions
  - Report preparation processes
  - Control objectives and related control activities
  - Complementary user entity controls
  - Description of sub-service provider controls

Reviewing Description of the System

- Verify that the services provided are consistent with the services received.
- Understand if there are any significant events that impact the services relied upon.

Complementary User Entity Controls

- Complementary user entity controls (CUECs) are controls which the service organization assumes will be in place at user entities.
- Identifies the roles, responsibilities and obligations of the user entity to ensure achievement of the control objectives identified in the report.
- Also known as “user organization control,” “complementary customer controls,” or other similar names or phrases.

Reviewing CUECs

- Identify and evaluate all CUECs that are relevant (i.e., those which directly impact financial reporting risk[s]).
- For IT-related CUECs, communicate with the IT team and consider the Company's responsibilities in areas of change management, security and operations.
- For all in-scope CUECs, ensure that the CUEC is appropriately mapped to key controls and that the design and operating effectiveness of those controls have been tested.

Objectives, Activities, and Tests

- Presents the control objectives and related control activities performed by the service organization
- Presents the test procedures performed and the results of control testing performed by the service auditors
- Shows the exceptions or deviations noted by the service auditors
- Shows Management’s response to the exceptions noted

Evaluating Control Exceptions

- Consider performing a self-assessment of the service auditors' test adequacy of the test procedures performed.
- Review the responses provided by the service organization and determine whether the responses are satisfactory. Management may also consider discussing the nature of the exceptions with the service auditors.
- Evaluate all relevant exceptions, which include:
  - Exceptions relevant to control objectives that mitigate the financial reporting risks.
  - Exceptions related to Information Technology General Controls (ITGCs) supporting relevant applications that mitigate the financial reporting risks.

Sub-Service Organizations

- A third-party provider used by the primary service providers to outsource processes and controls.
- They can be part of transaction processing (e.g., claims processing) or the IT environment (e.g., data center hosting).
- They are identified by the service organization in their assertion and by the service auditor in their opinion.

Reviewing Sub-Service Organizations

- Evaluation of internal controls should include the impact of all identified sub-service providers.
- Assess the impact of sub-service providers to the Company's internal control over financial reporting.
- Identify and evaluate all sub-service providers used by in-scope service organizations as part of the SOC review procedures.
- For in-scope sub-service providers, formally document the review of the sub-service providers' SOC report, if applicable.

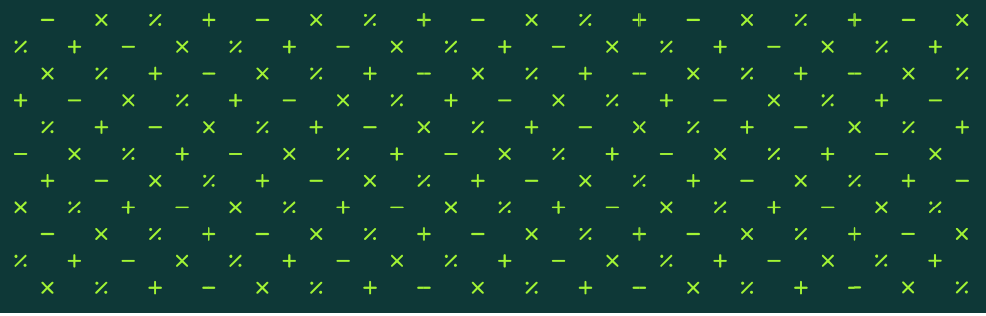
Reviewing Coverage

- To rely on SOC reports for SOX 404, the report must generally cover at least the first nine months of the audit period.
- Obtain a bridge letter if there is a gap between the SOC report date and the Company's year-end date.
- Review the bridge letters and evaluate the impact of changes in the service organizations' controls, if any.
- If the report coverage is less than nine months and/or there is a gap larger than three months, Management must document how it became comfortable with the small coverage period and/or gap in the reporting period.

SOC Analyzer Tool

- Based on the most recent SOC Audit Guides
- Organized to efficiently capture needed information
  - Vendor and report profile
  - Control Reliance
  - Complement user entity controls and subservices controls
  - Conclusions
- Available upon request

Latest SOC Updates



Reasons for SOC 2 TSC Changes

- Allows enhanced SOC 2 reporting
- Streamlines criteria and helps reduce presentation redundancies
- Integrates the 2013 COSO framework
- Facilitates greater coverage of IT governance and cybersecurity
- Expands link to other IT reporting frameworks

Key Reporting Changes

- The Trust Services Principles renamed as Trust Services Criteria (TSC)
- TSC now aligns with the 17 principles under the COSO 2013 framework
- Previous principles—Security, Availability, Processing Integrity, Confidentiality, and Privacy—renamed as the Trust Services Categories
- Points of Focus added for all Trust Services Criteria
- Plus new SOC 2 Guide introduces System Description Criteria and more reporting appendices
- Required for SOC 2 audits with periods ending ***after December 15, 2018***

Common Gaps

- Independent oversight by board of directors or similar governance group
- Use of quality information and identification of controls based on the identification and assessment of risks
- Consideration of fraud in assessing risks
- Completion of logical and physical access review
- Logical and physical protections over the destruction of assets
- Detection/monitoring associated with system and integrity checks
- Risk mitigation associated with business disruption and recovery

Impact to Audit

- Revised scope of controls
- Refined system description
- Written management assertion now required
- Other core elements of the audit remain the same:
  - Engagement management
  - Report management
  - Document request
  - Interviews, inspection and observation test procedures
  - Written representations and issuance

Additional Resources

AICPA SOC Website

aicpa.org/soc4so

Questions?

Chris Kradjan

(206) 302-6511

chris.kradjan@mossadams.com

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory offered through Moss Adams Wealth Advisors LLC. Investment banking offered through Moss Adams Capital LLC.

THANK YOU