


PREPARING FOR SOC CHANGES

AN ARMANINO WHITE PAPER

By Liam Collins, Partner-In-Charge, SOC Audit Practice







On May 1, 2017, SSAE 18 went into effect and superseded SSAE 16. The following information is here to help guide organizations through this change, as well as the change to SOC 2 reports beginning December 15, 2018.

CONTENTS

1	Overview of SSAE 18
3	SSAE 18: Changes to SOC 1 Reporting
5	SOC 2 Changes
10	SOC 2 + Additional Subject Matter
11	Cybersecurity
12	Conclusion



OVERVIEW OF SSAE 18

The American Institute of Certified Public Accountants (AICPA) issued its Statement on Standards for Attestation Engagements No. 18, Attestation Standards: Clarification and Recodification (SSAE 18) in April 2016 to address concerns with the standards regarding clarity, length, and complexity.

To assist firms with a process to provide assurance services related to the increasingly important cybersecurity state of entities, the AICPA released two proposals for Statements on Standards for Attestation Engagements. The first pertains to an entity's cybersecurity risk program, by providing criteria to provide a framework to ensure the entity has the necessary controls. The second provides further updates to TSP Section 100, Trust Services Principles and Criteria for

Security, Availability, Processing Integrity, Confidentiality, and Privacy used in SOC 2 engagements, providing revised and updated criteria for assessing the effectiveness of cybersecurity program controls.

In the following sections, we provide insight on important changes entities should be aware of as these new standards come into effect.



KEY ITEMS

May 1, 2017 – Reports issued after this date must be completed in compliance with SSAE 18

December 15, 2018 – Reports issued after this date must be completed in compliance with the updated 2017 Trust Services Criteria

SSAE 18 redrafts all previous SSAEs except for:

AT 701 Chapter 7, “Management’s Discussion and Analysis” of SSAE 10, Attestation Standards: Revision and Recodification, which will now be codified as AT-C 395

SSAE 15, An Examination of an Entity’s Internal Control Over Financial Reporting That is Integrated With Audit of Its Financial Statements (AT Section 501). This standard is being moved to the Auditing Standards AU-C 940



SSAE 18: CHANGES TO SOC 1 REPORTING

All SOC 1 attestations issued after May 1, 2017, must be performed in accordance with SSAE 18, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (AT-C section 320). SSAE 18 changes to SOC 1 requirements include the following topics:

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

When using the carve-out method to report on subservice organizations, management will be required to identify controls that management assumes will be implemented by those subservice organizations and that are necessary to achieve the control objectives stated in management's description. This is in addition to the requirement to monitor the effectiveness of controls at carved-out subservice organizations.

Service Organization Responsibilities:

- Identify the types of controls that management assumes will be implemented at each carved-out subservice organization and that are necessary to achieve the control objectives
- Evaluate and rationalize the existing list of subservice organizations presented in the report and identify the impacted control objectives
- Link to the relevant control objectives that are impacted and include in the description

SOC Report Comparison			
	THE USERS	WHY	WHY
SOC 1	Users' controller's office and user's 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

Completeness and Accuracy of Information Produced by the Service Organization

Reinforcement of the service auditor's requirement to evaluate evidence around the completeness and accuracy of information produced by the service organization and ability to include the procedures performed in the description of the tests of the controls

Service Organization Responsibilities:

- Provide the service auditor with an understanding of how information is produced and provide additional documentation as needed

RISK ASSESSMENT

Additional risk assessment context is provided for the service auditor around understanding the service organization's system, understanding the risks and assessment of material misstatements, and understanding the internal audit function to enable the service auditor to design and perform further appropriate audit procedures.

Service Organization Responsibilities:

Ensure that risk assessment documentation is available to the service auditor and management has ensured the relevant issues identified are addressed in a timely manner

DESIGN OF CONTROLS

The service auditor will now review management's assessment of the design of controls through:

- Understanding management's process for identifying and evaluating the risks that threaten the achievement of the control objectives and assessing the completeness and accuracy of management's risk identification process
- Evaluating the linkage of the controls with those risks
- Determining that the controls have been implemented

Service Organization Responsibilities:

- Ensure management is prepared to provide and discuss its assessment of controls with the service auditor

SOC 2 CHANGES

Beginning December 15, 2018, all practitioners will be required to use the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (trust services criteria) when providing attestation or consulting services to evaluate these controls.

SOC 2 audits are performed under Concepts Common to All Attestation Engagements (AT-C section 105) and Examination Engagements (AT-C section 205). The most significant changes to the existing trust services criteria are:

- Renames "Trust Services Principles and Criteria" as simply "Trust Services Criteria" or "TSC"
- Restructures and aligns the trust services criteria with the COSO 2013 framework to facilitate their use in an entity-wide engagement
- Adds supplemental criteria to address cybersecurity risks in engagements performed using the trust services criteria

TSC Criteria Sections

Control Environment

Communication and Information

Risk Assessment

Monitoring Activities

Logical and Physical Access Controls

System Operations

Change Management

Risk Mitigation

Additional Criteria for Availability

Additional Criteria for Confidentiality

Additional Criteria for Processing Integrity

Additional Criteria for Privacy

In the restructuring of the controls, the AICPA has provided a mapping to assist in the transition. With the move to closer align with the COSO 2013 framework, it has provided additional criteria that have not been required in prior iterations. The table below highlights some of the larger areas that have been added:

SOC Report Comparison	
CRITERIA	POINT OF FOCUS
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Establishes Oversight Responsibilities – The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
	Applies Relevant Expertise – The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.
	Operates Independently – The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
	Supplements Board Expertise – The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality and privacy, as needed, through the use of a subcommittee or consultants.
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Identifies Information Requirements – A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.
	Captures Internal and External Sources of Data – Information systems capture internal and external sources of data.
	Processes Relevant Data Into Information – Information systems process and transform relevant data into information.
	Maintains Quality Throughout Processing – Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable and retained. Information is reviewed to assess its relevance in supporting the internal control components.

CRITERIA	POINT OF FOCUS
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	OPERATIONS OBJECTIVES
	Reflects Management's Choices – Operations objectives reflect management's choices about structure, industry considerations and performance of the entity.
	Considers Tolerances for Risk – Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	Includes Operations and Financial Performance Goals – The organization reflects the desired level of operations and financial performance for the entity within operations objectives.
	Forms a Basis for Committing of Resources – Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.
	EXTERNAL FINANCIAL REPORTING OBJECTIVES
	Complies With Applicable Accounting Standards – Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.
	Considers Materiality – Management considers materiality in financial statement presentation.
	Reflects Entity Activities – External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.
	EXTERNAL NONFINANCIAL REPORTING OBJECTIVES
	Complies With Externally Established Frameworks – Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.
	Considers the Required Level of Precision – Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting objectives.
	Reflects Entity Activities – External reporting reflects the underlying transactions and events within a range of acceptable limits.
	INTERNAL REPORTING OBJECTIVES
	Reflects Management's Choices – Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.
	Considers the Required Level of Precision – Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.
	Reflects Entity Activities – Internal reporting reflects the underlying transactions and events within a range of acceptable limits.
	COMPLIANCE OBJECTIVES
	Reflects External Laws and Regulations – Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.
	Considers Tolerances for Risk – Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	Establishes Sub-objectives to Support Objectives – Management identifies sub-objectives related to security, availability, processing integrity, confidentiality and privacy to support the achievement of the entity's objectives related to reporting, operations and compliance.

CRITERIA	POINT OF FOCUS
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Assesses Changes in the External Environment – The risk identification process considers changes to the regulatory, economic and physical environment in which the entity operates.
	Assesses Changes in the Business Model – The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
	Assesses Changes in Leadership – The entity considers changes in management and respective attitudes and philosophies on the system of internal control.
	Assess Changes in Systems and Technology – The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.
	Assess Changes in Vendor and Business Partner Relationships – The risk identification process considers changes in vendor and business partner relationships.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Establishes Policies and Procedures to Support Deployment of Management's Directives – Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
	Establishes Responsibility and Accountability for Executing Policies and Procedures – Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.
	Performs in a Timely Manner – Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.
	Takes Corrective Action – Responsible personnel investigate and act on matters identified as a result of executing control activities.
	Performs Using Competent Personnel – Competent personnel with sufficient authority perform control activities with diligence and continuing focus.
	Reassesses Policies and Procedures – Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Uses Defined Configuration Standards – Management has defined configuration standards.
	Monitors Infrastructure and Software – The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.
	Implements Change-Detection Mechanisms – The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files or content files.
	Detects Unknown or Unauthorized Components – Procedures are in place to detect the introduction of unknown or unauthorized components.
	Conducts Vulnerability Scans – The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment, and takes action to remediate identified deficiencies on a timely basis.

CRITERIA	POINT OF FOCUS
<p>CC9.1 The entity identifies, selects and develops risk mitigation activities for risks arising from potential business disruptions.</p>	<p>Considers Mitigation of Risks of Business Disruption – Risk mitigation activities include the development of planned policies, procedures, communications and alternative processing solutions to respond to, mitigate and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during response, mitigation and recovery efforts.</p>
	<p>Considers the Use of Insurance to Mitigate Financial Impact Risks – The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.</p>
<p>PI1.1 The entity obtains or generates, uses and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.</p>	<p>Identifies Information Specifications – The entity identifies information specifications required to support the use of products and services.</p>
	<p>Defines Data Necessary to Support a Product or Service – When data is provided as part of a service or product or as part of a reporting obligation related to a product or service:</p> <ol style="list-style-type: none"> 1. The definition of the data is available to the users of the data. 2. The definition of the data includes the following information. 3. The definition is complete and accurate. 4. The description of the data identifies any information that is necessary to understand each data element and the population in a manner consistent with its definition and intended purpose (meta-data) that has not been included within the data.

SOC 2 + ADDITIONAL SUBJECT MATTER

A service organization may request that the service auditor's report address either criteria in addition to the applicable trust services criteria or additional subject matter related to the service organization's services using additional suitable criteria related to that subject matter, or both.

Additional Subject Matter and Criteria		
SUBJECT MATTER	CRITERIA	EXAMPLE OF THE ENGAGEMENT
Description of the physical characteristics of a service organization's facilities	<ul style="list-style-type: none">• Completeness• Accuracy• Criteria specified by an outside party	Reporting on a detailed description of the physical characteristics of a service organization's facilities (for example, square footage) in addition to reporting on controls at the service organization relevant to the security of the system based on the trust services criteria for security
Historical data related to the availability of computing resources	<ul style="list-style-type: none">• Completeness• Accuracy	Reporting on historical data regarding the availability of computing resources at a service organization in addition to reporting on controls at the service organization relevant to the availability of the system based on the trust services criteria for availability
Compliance with a statement of privacy practices	Statement of privacy practices	Reporting on a service organization's compliance with a statement of privacy practices in addition to reporting on controls at the service organization relevant to the privacy of the system based on the trust services criteria for privacy
N/A	Requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Administrative Simplification 45 CFR Sections 164.308-316	Reporting on privacy at a service organization based on regulatory requirements (for example, the security requirements under HIPAA), in addition to reporting on controls at the service organization relevant to the privacy of the system based on the trust services criteria for privacy
N/A	Statement of privacy practices	Reporting on security at a service organization based on criteria established by an industry group (such as the Cloud Security Alliance's Cloud Control Matrix), in addition to reporting on controls at a service organization relevant to the security of a system based on the trust services criteria for security



CYBERSECURITY

In addition to these, the AICPA has released an additional option by releasing its cybersecurity risk management framework in response to the growing number of frameworks and confusion about what frameworks are applicable to an organization. This framework is designed so that organizations can communicate their cybersecurity risk management efforts while providing information about the systems, processes and controls they have in place to detect, prevent and respond to breaches. The reporting framework, including the related criteria, are used to perform an examination-level attestation engagement, known as a cybersecurity risk management examination. Based upon this, the AICPA has created three levels of reporting:

This framework is designed so that organizations can communicate their cybersecurity risk management efforts while providing information about the systems, processes and controls they have in place to detect, prevent and respond to breaches. The reporting framework, including the related criteria, are used to perform an examination-level attestation engagement, known as a cybersecurity risk management examination. Based upon this, the AICPA has created three levels of reporting:

1 Entity

Areas Included:

Description, Opinion, Assertion

Intended Audience:

- Board/audit committee
- Management
- Investors
- Regulators
- Analysis

Benefit (Entity and Recipient)

- Provides transparency to key elements of the entity's cybersecurity risk management program
- Improves communications
- Enhances confidence in the integrity of the information presented

2 Service Provider

Areas Included:

Testing, Description, Opinion, Assertion

Intended Audience:

- Business unit management
- Vendor risk management
- Accounting/internal audit
- CISO
- BCP

Benefit (Entity and Recipient)

- In addition to entity-level benefits, provides sufficient, detailed information to address the user vendor risk management needs

3 Supply Chain

Areas Included:

Testing, Description, Opinion, Assertion

Intended Audience:

- Business unit management
- Vendor risk management
- CISO
- BCP

Benefit (Entity and Recipient)

- In addition to entity-level benefits, provides sufficient, detailed information to address the user's supply chain risk management tools

The AICPA developed two sets of different but complementary criteria to be used in a cybersecurity engagement for implementation of the above reporting framework:

1. Description criteria used by management when preparing a description of its cybersecurity risk management program and by the CPA when evaluating the presentation.
2. Control criteria management uses when assessing the effectiveness of controls within that program to achieve the entity's cybersecurity objectives. Management may select the criteria to use in the examination, as long as it is suitable in the circumstances.

In addition, the AICPA is developing vendor management criteria for SOC 2 +.

CONCLUSION

The AICPA has implemented a variety of changes to better enable CPAs to provide assurance services to organizations to address the different governance, risk and compliance issues that have arisen. Armanino is equipped to assist organizations in discovering the correct path to fit their current and long-term compliance goals.

STRATEGIC INSIGHTS PRACTICAL ACTION

Armanino provides an integrated set of accounting services—audit, tax, consulting, business management and IT solutions—to a wide range of organizations operating both in the U.S. and globally.

You can count on Armanino to think strategically and provide the sound insights that lead to positive action. We address not just your compliance issues, but your underlying business challenges, as well—assessing opportunities, weighing risks, and exploring the practical implications of both your short- and long-term decisions.

When you work with us, we give you options that are fully aligned with your business strategy. If you need to do more with less, we will implement the technology to automate

your business processes. If the issue is financial, we can show you proven benchmarks and best practices that can add value companywide. If it's operational, we'll consult with your people about workflow efficiencies. If it is compliance, we'll ensure that you meet the requirements and proactively plan to take full advantage of the changes at hand. At every stage in your company's lifecycle, we'll help you find the right balance of people, processes and technology.

For additional information on the upcoming SOC changes, contact:



Liam Collins
Partner-In-Charge, SOC Audit Practice
Liam.Collins@armaninoLLP.com
415 710 4705

armanino 

