AICPA Updates for Attestation Engagements

Understanding the AICPA's Updates for SOC 1 and SOC 2 Reports and the New Cybersecurity Attestation

Contents

Acknowledgments

Lead Author

David Barton, Managing Director, UHY LLP

Contributors

Chad Creasman, Senior Consultant, UHY LLP
David Hartley, Principal, UHY LLP
Dave King, Senior Manager, UHY LLP
Veronica Kovach, Senior Manager, UHY LLP

1.0 Introduction

In April 2016, the American Institute of Certified Public Accountants (AICPA) issued Statement on Standards for Attestation Engagements No. 18, *Attestation Standards: Clarification and Recodification* (SSAE 18). The purpose of SSAE 18 is to consolidate the AICPA attestation standards in an effort to eliminate potential confusion regarding the type of assurance services that a CPA in the practice of public accounting (practitioner) can perform.

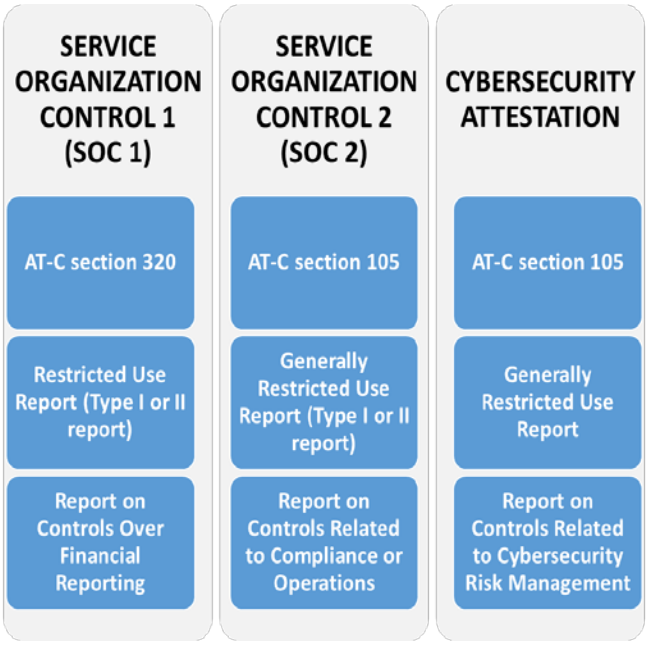

Figure 1 - Overview of SSAE 18 Reporting Options

For additional information: See the link below in "Additional Resources"

In September 2016, the AICPA released two proposals for Statements on Standards for Attestation Engagements, which recommend adopting a widely accepted approach to cybersecurity reporting. The first proposal provides criteria used to describe an entity's cybersecurity risk management program. The second proposal is an update to the current TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* that would allow the criteria to be used in assessing the effectiveness of cybersecurity program controls.

UHY LLP drafted this document to educate users of attestation reports and provide guidance on selecting the appropriate reporting option.

2.0 The New Standard for SOC 1: SSAE 18

Beginning May 1, 2017, all SOC 1[SM] attestations 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). As with all attestation standards, SSAE 18 is meant for use by practitioners when issuing an examination, review, agreed-upon procedures, or an assertion on subject matter that is the responsibility of another party.

The issuance of SSAE 18 resulted in two significant changes to SOC 1 requirements:

- Requirement for implementing controls to monitor the effectiveness of internal controls at all subservice organizations.
- The practitioner is required to obtain an understanding of the subject matter and to identify and assess the risk of material misstatement *and perform procedures in response to risks*.

SSAE 18 was the last step in the process to address concerns over the clarity, length, and complexity of the AICPA standards. SSAE 18 supersedes all existing attestation standards (SSAEs 10-17, except for SSAE 15 and Chapter 7, "Management's Discussion and Analysis," of SSAE 10). SSAE 18 is an attestation standard and not a

certification or report type. Therefore all requests for SOC 1 attestations, including language within contracts, should be specified as a "SOC 1" report, not "SSAE 18."

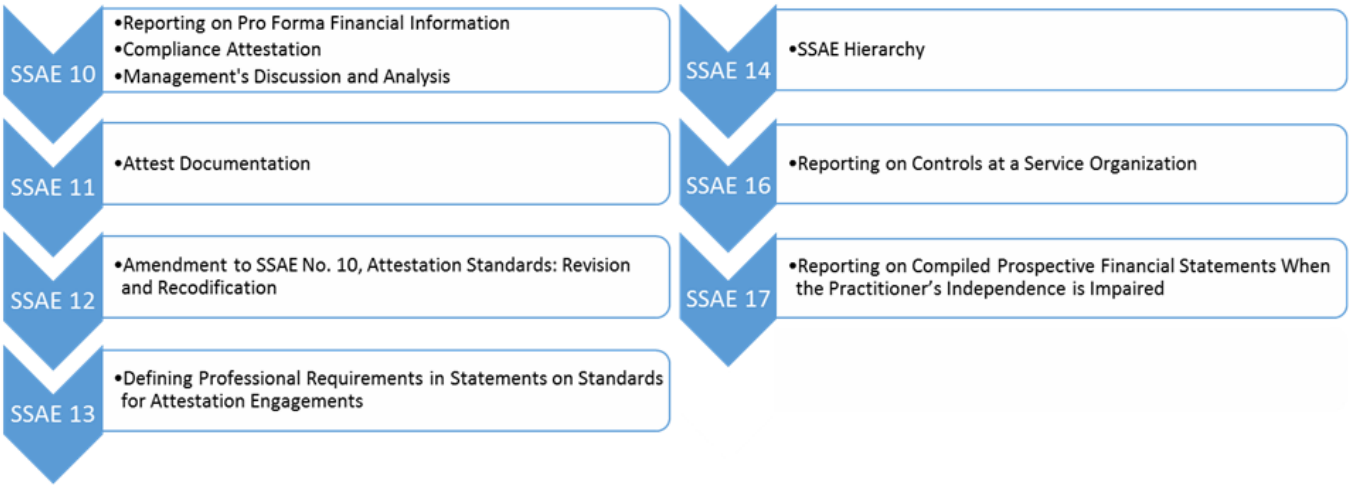

Figure 2 - Overview of Superseded Statements on Standards for Attestation Engagements
For additional information: See the link below in "Additional Resources"

3.0 Updated Trust Services Criteria for SOC 2

Beginning June 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 controls relevant to the security, availability, or processing integrity of an entity's system(s), or the confidentiality or privacy of information processed by an entity's system(s).

Unlike a SOC 1 attestation, a SOC 2^{SM} is not performed in accordance AT-C section 320 of SSAE 18; rather, it is 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:

1. Renames *Trust Services Principles and Criteria* as simply *Trust Services Criteria* to avoid confusion with COSO 2013 framework *principles*
2. Restructures and aligns the trust services criteria with the COSO 2013 framework to facilitate their use in an entity-wide engagement
3. Adds supplemental criteria to address cybersecurity risks in engagements performed using the trust services criteria

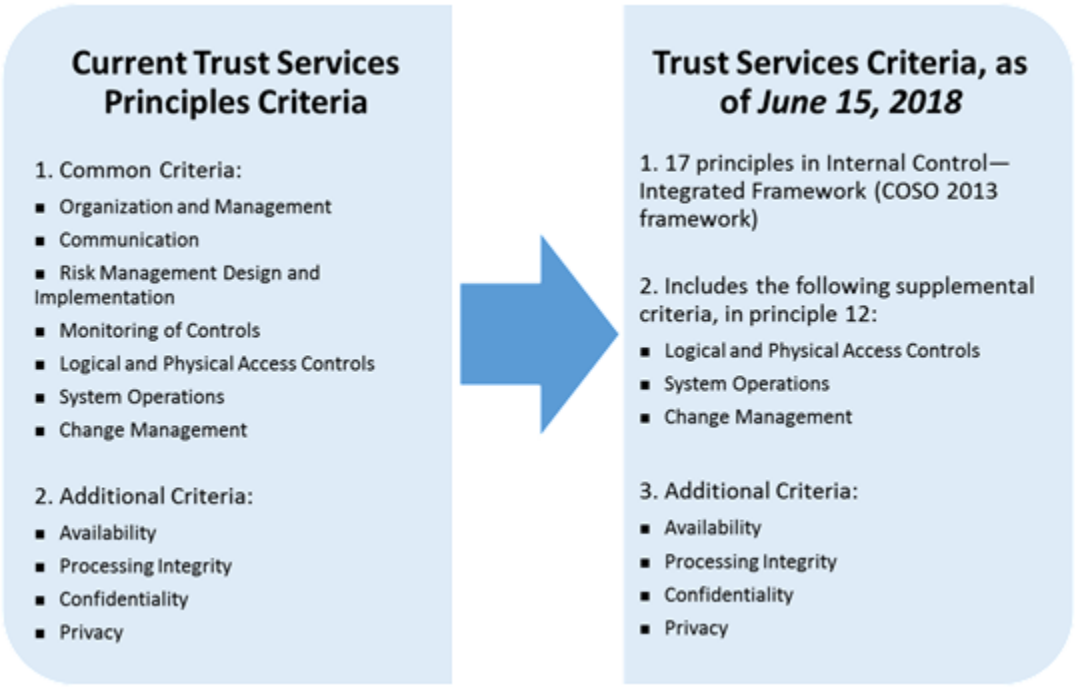

Figure 3 - Summary of Proposed Updates to Trust Services Criteria

For additional information: See the link below in "Additional Resources"

4.0 Proposed Cybersecurity Standards – A New Option

As a result of the need for management, boards of directors, and interested stakeholders to obtain information on an entity's cybersecurity risk management efforts, the AICPA has proposed a reporting framework that organizations can use to communicate information about their cybersecurity risk management program in a way that is useful for decision making.

Description Criteria for Cybersecurity Reporting

The proposed description criteria is intended for use in developing management's description of an entity's cybersecurity risk management program and for practitioners to express an opinion on management's description. To date, no widely accepted approach or professional standard for assessing a cybersecurity risk management program exists. This absence led to the development of disparate frameworks and assurance programs, which creates a burden for organizations that attempt to design and implement a cybersecurity program.

After careful consideration of the nature, type, and extent of cybersecurity information needed to meet reporting needs of a broad range of users, the AICPA determined that no single source alone addressed the required elements. Therefore, the proposed description criteria took a variety of frameworks into account, including the following:

- NIST Special Publication 800 series
- ISO/IEC 27001/27002 and related standards
- COBIT 5
- COSO's Internal Control—Integrated Framework (COSO 2013 framework)
- PCI DSS 3.2

Control Criteria for Cybersecurity Reporting

Currently, the AICPA is not requiring the use of a specific criteria to evaluate the design and operating effectiveness of cybersecurity program controls. While the updated trust services criteria has been recommended, management and practitioners may use any suitable control framework for evaluating the design and operating effectiveness of cybersecurity program controls.

In addition to the proposed description criteria and control criteria, the AICPA is now developing a cybersecurity attestation guide that will provide guidance to practitioners on performing a cybersecurity engagement in accordance with attestation standards.

Cybersecurity Attestation vs. Cybersecurity Risk Assessment – Which One Do I Need?

A common question that arises from reading the exposure draft for the proposed cybersecurity standards is "How is an attestation different from a cybersecurity risk assessment?"

Cybersecurity Attestation

An entity seeking a means to communicate information on their cybersecurity risk management program to entity investors, customers, business partners and regulators will need a cybersecurity attestation. A cybersecurity attestation provides a practitioner's assessment of an entity's cybersecurity program and a report that is appropriate for general use to address the reporting needs of a broad range of users. A cybersecurity attestation report contains the following:

- Management's description of the cybersecurity risk management program
- Management's written assertion
- Practitioner's opinion expressed on whether, in all material respects:
  a) the description is presented in accordance with the description criteria; and
  b) the suitability of the design and operating effectiveness of the controls meet the control criteria

Cybersecurity Risk Assessment

A cybersecurity risk assessment would be the better choice for an entity that is in the process of designing and implementing a cybersecurity risk management program, or is looking to improve their existing program by identifying gaps and areas for improvement. A risk assessment is a review of an entity's technology management and business processes by an independent third party in order to identify any gaps or areas for improvement. All findings from a risk assessment are presented in an internal facing report that includes recommendations for remediation to business process managers, IT management, and executive leadership.

In many cases, the answer to the question may be "both". The two efforts derive from two different needs. Many entities will benefit from starting with a risk assessment in order to identify gaps, which could impact their ability to meet the cybersecurity criteria. Performing a risk assessment first gives an organization the opportunity to remediate any gaps and implement a more robust cybersecurity program that is capable of meeting all of the criteria specified for the cybersecurity attestation. Once the risk assessment and remediation efforts are completed and the cybersecurity program is in place and operating effectively, a cybersecurity attestation engagement can be performed to generate a report that provide comfort to internal and external parties.

5.0 Conclusion

The introduction of SSAE 18 and the resulting recodification of attestation standards will once again create some level of confusion and uncertainty in the marketplace for assurance services. Entities and their customers should engage the services of competent practitioners who understand the changes and can assist the organization with navigating through these updated standards.

6.0 Additional Resources

Superseded Statements on Standards for Attestation Engagements:

http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx

Proposed Updates to TS Criteria:

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/exposuredrafts/asec_ed_rev_trust_services.pdf

Proposed Description Criteria for Cybersecurity Risk Management Program:

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/exposuredrafts/asec_ed_criteria_cyber_engagement.pdf