CSA cloud security alliance®

Guidelines for CPAs Providing CSA STAR Attestation v2

May 2017

STAR™ ATTESTATION

Introduction

This document provides guidance for CPAs in conducting a STAR Attestation. This document is not meant to replace any American Institute of Certified Public Accountant (AICPA) Standards or AICPA Service Organization Control® (SOC) related guidance. Refer to http://www.aicpa.org/soc for information about SOC and how to obtain SOC related standards and guidance.

Part 1 – Professional Requirements

1 General

1.1 STAR Attestation is a SOC 2^{SM} engagement in which the criteria include:

1.1.1 the applicable criteria in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (TSPC), and

1.1.2 the control specifications included in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

2 Requirements for engagement performance

2.1 A SOC 2^{SM} engagement is performed by a CPA in accordance with the AICPA Statements on Standards for Attestation Engagements or ISAE 3000s (the "Attestation Standard"), the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2^{SM} Guide).

2.2 The Attestation Standard provides a framework for performing and reporting on all attestation engagements. The SOC 2^{SM} Guide provides performance and reporting guidance based on the Attestation Standard for an examination of a cloud service organization's description of its system and the suitability of the design, and in type 2 engagements, the operating effectiveness of controls that are likely to be relevant to the security, availability, or processing integrity of a cloud service organization's system or the confidentiality or privacy of the information processed by the system. The TSPC provides criteria for evaluating and reporting on controls related to security, availability, processing integrity, confidentiality, and privacy. SOC 2 reports are generally restricted use reports as they are intended for specified parties who are knowledgeable about the nature of the service provided by the service organization; how the service organization’s system interacts with user entities, subservice organizations, and other parties; internal control and its limitations; the applicable trust services criteria, the risks that may prevent those criteria from being met, and how those controls address those risks; and complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.

2.3 The CCM control specifications constitute suitable criteria as defined by the Attestation Standard (“CCM criteria”) and includes criteria equivalent to the criteria for the security principle in the TSPC plus certain additional criteria related to security.

3 Competency requirements

3.1 CPA services are subject to specific professional standards. Adherence to these standards is incumbent on CPAs under rules of the AICPA and individual state laws that have adopted these standards.

3.1.1 **State or Country Accountancy Laws.** CPAs are licensed by the states or by countries . Because licensure is required to provide certain CPA services, state/national governments have regulatory authority over CPA activities. As a result, some CPA standards are imposed not only by the profession, but by force of law. Violation of accountancy laws can lead to substantial fines and license suspension or revocation.

3.1.2 **Ethics Code.** The AICPA Code of Professional Conduct (Code) applies to all CPA services. CPAs have to adhere to the Code regardless of the type of service provided or the subject matter involved. The membership of the AICPA approved the rules stated in the Code, and the AICPA Professional Ethics Executive Committee maintains it by issuing detailed guidance. The Code establishes behavioral standards and is supplemented by rules specific to individual services established elsewhere in professional standards. The rules are supplemented by interpretations and rulings that provide guidance relevant to applying them. The following summarizes the general rules in the Code; the rules require the CPA to:

- Be independent when providing financial statement services or attestation services
- Be objective and have integrity, have no conflicts of interest, and neither knowingly misrepresent facts or subordinate his or her judgment to others
- Have professional competence
- Exercise due professional care
- Adequately plan and supervise professional services performed
- Obtain sufficient relevant data for conclusions or recommendations
- Comply with the relevant professional standards
- Maintain confidentiality of client information

- Decline contingent fees for certain types of clients
- Not commit an act discreditable to the profession
- Not engage in false, misleading, or deceptive advertising or coercive, over-reaching, or harassing solicitation
- Decline commissions in certain types of engagements and disclose them when acceptance is permitted
- Practice only in certain organizational forms and use a firm name that is not misleading.

3.1.3 **Quality Control.** CPAs are required to apply quality control policies and procedures over their financial statement and attestation services. The objective of a system of quality control is to provide the CPA firm with reasonable assurance that that firm and its personnel comply with applicable professional and legal and regulatory requirements and that the reports it issues are appropriate in the circumstances. There are six required elements to a system of quality control:

- Leadership responsibilities, that is, the tone at the top
- Compliance with relevant ethical requirements
- Acceptance and continuance of client relationships and engagements to perform engagements only when the CPA is competent and capable of doing so, can comply with relevant requirements, and has considered the client's integrity
- Human resources that ensure necessary competence, capabilities, and commitment
- Engagement performance, which involves consistent quality, supervision, and review, including when necessary, consultation
- Monitoring to ensure the system's continued effectiveness.

CPA firms' quality control practices are periodically examined by independent outside professionals. The examination determines whether quality control is effective and the examination results in a formal report. The report is typically available to the public, allowing potential clients and information users the opportunity to determine a CPA firm's adherence to quality control standards. The AICPA Peer Review Board recently approved SOC 2^{SM} engagements as must select engagements. This means that if a firm performs SOC 2^{SM} engagements, at least one such engagement should be selected during its peer review.

3.1.4 **Continuing Professional Education.** CPAs must adhere to the continuing education requirements set forth by the State Board of Accountancy of the state/s where a CPA license is held. The requirements for continuing professional education vary from state to state. The AICPA requires certain CPE for maintaining membership. There are also special CPE requirements for those performing work related to the Government Accountability Office (GAO).

4 Scope of Attestation

4.1 In a SOC 2^{SM} report, the CPA expresses an opinion on the following:

- Whether the description of the cloud service organization's system is fairly presented, based on the description criteria
- Whether the controls are suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively
- In type 2 reports, whether the controls were operating effectively to meet the applicable trust services criteria and CCM criteria
- In engagements to report on the privacy principle, whether the service organization complied with the commitments in its statement of privacy practices.

5 Criteria establishment and selection

5.1 Paragraphs 1.26–.27 of the current[1] SOC 2^{SM} Guide contain the criteria for the description of a cloud service organization's system. TSP section 100 contains the criteria for evaluating the design and operating effectiveness of controls. CSA CCM contains the control specifications which constitute additional suitable criteria related to security.

[1] The July 1, 2015, SOC 2 Guide was the current version at the time of this document release.

Part 2 Additional CSA Guidelines

1 CSA Competency

1.1 Individuals carrying out STAR Attestation engagements (in the case of an engagement team, the engagement team lead) must hold the CSA's Certificate in Cloud Security Knowledge (CCSK) in addition to, the requirements posed in Part 1, paragraph 3.1.4 above by the State Boards of Accountancy and AICPA.

2 Scope

2.1 The STAR Attestation program is based on the combined requirements of the CCM and the TSPC.

2.2 For a cloud system to qualify for STAR Attestation, its SOC 2 report scope must cover and the system must satisfy all CCM controls and the TSPC Security principle, and must be evaluated to ensure it includes all activities related to the reported cloud system.

2.3 This scope of the reported system must be specified in the SOC 2 report under the Management Assertion section that, the cloud system 'has implemented and satisfies all controls in the CCM and the selected principles of TSP 100'.

2.4 The version of the CCM (minimum version 3.0.1) and edition of the TSPC used in the report must be specified in the SOC 2 report under the Management Assertion section.

2.5 If certain CCM controls are deemed not applicable to the cloud system, the applicant is required to offer an alternative implemented control that is able to provide equal protection to the control intention.

2.6 For each excluded control, the applicant is required to specify the following information in the Management Assertion section or description of the systems of the SOC 2 report:

2.6.1 control name, control ID, rationale on exclusion, how the cloud system's alternative control implementation meets or exceeds the original control intention.

3 Submitting materials to CSA

3.1 Determination of submitting information to the completion of a STAR Attestation engagement will be determined by management of the cloud service organization.

3.2 Organizations that are applying for their first STAR Attestation over a cloud system, can provide a SOC 2 Type 1 report to the CSA to support their application. For subsequent applications of the same cloud system, only a SOC 2 Type 2 report will be accepted. A system can only gain STAR attestation once based on a SOC 2 Type 1 report. If an organization has more than one system, each system can gain attestation once, using a SOC 2 Type 1 report.

3.3 Because STAR Attestation does not require mandatory follow-up engagements, the "point in time" date for SOC 2 Type 1 reports or the "period of time" covered by SOC 2 Type 2 reports will be denoted on the STAR Registry along with the scope covered.

3.4 Upon receipt of the CSA STAR Attestation submission, CSA will grant the submitter permission and usage guidelines for the CSA STAR logo and brand. Usage of the CSA STAR logo and brand is not permitted until explicitly granted by CSA. Further information about CSA guidelines regarding STAR Attestation is available at www.cloudsecurityalliance.org/star/attestation/.

3.5 Due to the different level of assurance provided by the SOC 2 Type 1 versus the SOC 2 Type 2 reports, the period of validity of the resulting STAR Attestation ("basic validity period") differs. A STAR Attestation obtained based on a SOC 2 Type 1 report is only valid for 6 months from the as-of date, i.e., an organization that received their STAR Attestation based on a SOC 2 Type 1 report is required to submit a SOC 2 Type 2 report to maintain uninterrupted STAR Attestation status.

3.6 A STAR Attestation achieved based on a SOC 2 Type 2 report is valid for 12 months (1 year) from the end date of the reporting period.

3.7 The validity period of a STAR Attestation is extended by grace period of 3 months on top of the basic validity period for report generation and delivery ("maximum validity period"). This rule applies to STAR Attestations based on both SOC 2 Type 1 and SOC 2 Type 2 reports. For clarity, the maximum validity period of a STAR Attestation based on a SOC 2 Type 1 report and a SOC 2 Type 2 report is 9 (6 + 3) months and 15 (12 + 3) months respectively.