Guidelines for CPAs Providing CSA STAR Attestation v4
# Table of Contents

- **Introduction** ........................................................................................................................................3
- **Part 1 – Professional Requirements** .....................................................................................................4
  - General ........................................................................................................................................4
  - Requirements for engagement performance ..............................................................................4
  - Competency requirements ..........................................................................................................5
  - Scope of Attestation ...................................................................................................................7
  - Criteria establishment and selection ...........................................................................................7
- **Part 2 – Additional CSA Guidelines** ......................................................................................................8
  - CSA Competency ........................................................................................................................8
  - Scope ..........................................................................................................................................8
  - Submitting materials to CSA .......................................................................................................9

Refer to the Terms, Conditions and Guidelines for AICPA SOC Logo use: [https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/soclogosinfo.html](https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/soclogosinfo.html)

© 2023 Cloud Security Alliance – All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance “Guidelines for CPAs Providing CSA STAR Attestation” at www.cloudsecurityalliance.org/star, subject to the following: (a) the Document may be used solely for your personal, informational, non-commercial use; (b) the Document may not be modified or altered in any way; (c) the Document may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Document as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance “Guidelines for CPAs Providing CSA STAR Attestation” (2023)
Introduction

This document provides guidance for CPAs in conducting a STAR Attestation. This document is not meant to replace any American Institute of Certified Professional Accountant (AICPA) Standards or AICPA System and Organization Controls (SOC) related guidance. Refer to http://www.aicpa.org/soc for information about SOC and how to obtain SOC related standards and guidance\(^1\).

\(^1\) SOC 2 Examination that Addresses Additional Subject Matters and Additional Criteria. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/soc2additionalsubjectmatter.html
Part 1 – Professional Requirements

1. General

1.1 STAR Attestation is a SOC 2® engagement2 in which the criteria include:

1.1.1 TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, or Privacy (TSC)3, and

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

2. Requirements for engagement4 performance

2.1 All firms wishing to perform CSA STAR attestation assessments must be corporate members of CSA.

2.2 A SOC 2® engagement is performed by a CPA in accordance with the AICPA Statements on Standards for Attestation Engagements (SSAEs) (i.e. AT-C section 105, Concepts Common to All Attestation Engagements and AT-C section 205, Examination Engagements) and the AICPA Guide SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2 Guide). A CPA performs the examination in accordance with either the AICPA SSAEs or the International Standard on Assurance Engagements 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information (ISAE 3000). If not precluded by regulations of the local jurisdiction, a non-CPA can perform the examination in accordance with ISAE 3000.

2.3 The SOC 2 Guide provides performance and reporting guidance, based on the SSAEs, for a Type 1 examination of a cloud service organization’s description of its system and the

---


suitability of the design. 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 TSC provides criteria for evaluating and reporting on controls related to security, availability, processing integrity, confidentiality, or 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 the service organization’s service commitments and system requirements being achieved based on the applicable trust services criteria; how controls address those risks; and complementary user-entity controls and how they interact with related controls at the service organization to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria.

2.4 The CCM control specifications (“CCM criteria”) include additional, prescriptive criteria for the security category in the TSC. The CCM criteria constitutes suitable criteria as defined by AT-C section 105, Concepts Common to All Attestation Engagements.

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 adopted the rules stated in the Code, and the AICPA Professional Ethics Executive Committee maintains it by issuing detailed guidance. The Code establishes behavioral and independence 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 attestation engagements such as audits of financial statements
- Be objective and have integrity, have no conflicts of interest, and neither knowingly misrepresent facts or subordinate auditor judgment to others
- Have professional competence
- Exercise due professional care
- Adequately plan and supervise professional services performed
- Obtain sufficient and appropriate audit evidence to support conclusions or recommendations in the audit report
- Comply with the relevant professional standards, such as the Statements on Standards in Tax Practice, Auditing and Accounting Standards
- Maintain confidentiality of client information
- Decline contingent fees for certain types of clients and engagements
- Not commit an act discreditable to the profession, such as failure to: file personal or firm returns, remit certain taxes collected or respond to requests for records
- Not engage in false, misleading, or deceptive advertising or coercive, overreaching, or harassing solicitation
- Decline commissions in certain types of engagements and disclose them in writing when acceptance is permitted
- Practice only in allowed 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 the firm and its personnel comply with applicable professional and legal and regulatory requirements and that the reports it issues are appropriate in the circumstances. The system of quality control is required to include policies and procedures addressing each of the following elements:

- Leadership responsibilities for quality within the firm, that is, the tone at the top
- Compliance with relevant ethical requirements
- Acceptance and continuance of client relationships and specific engagements
- Human resources that ensure necessary competence, capabilities, and commitment to ethical principles
- 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 external professionals. The examination, known as a peer review, determines whether quality control is effective and 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 deems SOC 2® engagements as must select engagements. This means that if a firm performs SOC 2® 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 mandatory CPEs 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® report, the CPA expresses an opinion on the following:

- Whether the description of the cloud service organization's system is presented in accordance with the description criteria and CCM criteria
- Whether the controls are suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and CCM criteria
- In type 2 examinations, whether the controls were operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and CCM criteria

5. Criteria establishment and selection

5.1 DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, contain the criteria for the description of a cloud service organization's system. TSC 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. CSA Competency

1.1 Individuals performing 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 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 TSC.

2.2 For a cloud system to qualify for STAR Attestation, the following must be satisfied:

- A STAR Level 1 Self-Assessment (CAIQ) must be completed and submitted by the audited organization.
- SOC 2 report scope must satisfy TSC Security category and CCM controls justified for inclusion.
- and the TSC Security category 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 categories of TSC 100’.

2.4 The version of the CCM (minimum version 4.X.X) and edition of the TSC 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 satisfies the control objective.

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:

- 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 Cloud service organization management shall authorize submission of completed STAR Attestation engagement information.

3.2 Organizations that are applying for their first STAR Attestation can provide a SOC 2 Type 1 report to the CSA to support their application. For subsequent applications for 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 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 application, the CSA will grant the applicant permission to use the CSA STAR logo and brand. Usage of the CSA STAR logo and brand is not permitted until explicitly granted by the CSA. The applicant organization will then be invoiced by CSA for applicable “Attestation Fees”. It is the responsibility of the assessment firm to inform clients that these fees will be directly invoiced in addition to the SOC attestation fees.

3.5 Because a SOC 2 Type 1 report addresses only the suitability of design of implemented controls while a SOC 2 Type 2 report also addresses the operating effectiveness of those controls, 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 based on a SOC 2 Type 2 report is valid for 12 months (1 year) from the end date of the reporting period. Attestation Fees are invoiced yearly as the updated attestations are submitted.

3.7 The validity period of a STAR Attestation is extended for a period of 3 months on top of the basic validity period to account for report generation and delivery (“maximum validity period”). This rule applies to STAR Attestations based either 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.
## Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Issue Date</th>
<th>Changes</th>
<th>Approved By</th>
</tr>
</thead>
<tbody>
<tr>
<td>v4</td>
<td>August 31, 2023</td>
<td>Added requirement for mandatory CAIQ Submission</td>
<td>JAD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added notice requirements to notify client of Assessment Fees</td>
<td></td>
</tr>
</tbody>
</table>