AICPA

Performing and reporting on a SOC 2® examination

in accordance with International Standards on Assurance Engagements (ISAEs) or in accordance with both the AICPA's attestation standards and the ISAEs

This document is nonauthoritative and is included for informational purposes only.

Performing and reporting on a SOC 2® examination

in accordance with International Standards on Assurance Engagements (ISAEs) or in accordance with both the AICPA's attestation standards and the ISAEs

The advent of technology has led to the evolution of businesses that are often globally interconnected and interdependent. This has resulted in questions related to the use of SOC 2® reports internationally. For example, a service organization located in the United States might provide services to a user entity located in a foreign country (foreign user entity), or a non-U.S. CPA might be asked to perform a SOC 2® examination for a service organization located outside of the United States (foreign service organization). The purpose of this document is to answer some of the more commonly asked questions on this topic.

1. Inquiry — A foreign user entity of a U.S. service organization may wish to obtain a SOC 2® report from the U.S. service organization. In the United States, a SOC 2® examination is performed in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*[1], and AT-C section 205, Examination Engagements[2], of the attestation standards the American Institute of CPAs (AICPA) established, and in accordance with the AICPA Guide SOC 2® *Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.* However, the foreign user entity may request a service auditor's report indicating that the SOC 2® examination was performed in accordance with International Standard on *Assurance Engagements (ISAE) 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, which the International Audit and Assurance Standards Board (IAASB) issues. The ISAEs are the international equivalent of the AICPA's attestation standards. May a U.S. CPA perform a SOC 2® examination and report in accordance with ISAE 3000 (Revised), rather than in accordance with AT-C section 205 of the attestation standards established by the AICPA?

   Reply — No. A U.S. CPA may not perform a SOC 2® examination and report only in accordance with ISAE 3000 (Revised). Such reporting is not permitted under the "Compliance With Standards Rule" (ET sec. 1.310.001)[3] of the AICPA Code of Professional Conduct, which states that "a member who performs auditing, review, compilation, management consulting, tax or other professional services shall comply with standards promulgated by bodies designated by Council." When a member is engaged to perform a professional service that is covered by established standards, the member must perform the service using such established standards.

Council has designated the Auditing Standards Board as the body with responsibility for promulgating Statements on Standards for Attestation Engagements, which govern the performance of SOC 2® examinations. Therefore, a U.S. CPA engaged to perform a SOC 2® examination must perform the examination in accordance with the attestation standards issued by the AICPA (AT-C section 205) and report accordingly.

2. Inquiry — May the U.S. CPA perform a SOC 2® examination in accordance with both AT-C section 205 of the attestation standards issued by the AICPA and ISAE 3000 (Revised) of the assurance standards issued by the IAASB?

   Reply — Yes. A frequently asked question titled "Use of standards that have not been established by a body designated by AICPA Council,"[4] clarifies that a member is permitted to apply any relevant alternative standards in an attestation examination. Therefore, a U.S. CPA who performs a SOC 2® examination in accordance with AT-C section 205 may also perform the examination in accordance with ISAE 3000 (Revised) and issue one report that states that the examination was performed in accordance with the attestation standards established by the AICPA and ISAE 3000 (Revised) issued by the IAASB, provided the U.S. CPA complies with the requirements of both sets of standards and there are no conflicts between AT-C section 205 and IASE 3000 (Revised) that would lead the U.S. CPA to reach a different conclusion with respect to the opinion.

Although many of the requirements of AT-C section 205 and ISAE 3000 (Revised) are similar, there are certain differences. For example, under the requirements of ISAE 3000 (Revised), a practitioner may issue an examination report without obtaining a written assertion from the responsible party; under AT-C section 205, a practitioner is not permitted to issue an examination report if the practitioner has not obtained such an assertion from the responsible party, except when the responsible party is not the engaging party. A SOC 2® examination performed in accordance with both the attestation standards and ISAEs is expected to be similar in scope and approach to a SOC 2® examination performed in accordance with only the attestation standards.

To make it easier for CPAs engaged to examine and report under both sets of standards, the ASB has published "Substantive Differences Between International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, and AT-C sections 105, *Concepts Common to All Attestation Engagements*, and 205, Examination Engagements, of Statements on Standards for Attestation Engagements," which identifies the substantive differences between the requirements of the attestation standards (AT-C sections 105 and 205) and ISAE 3000 (Revised). The document is available at aicpa.org/content/dam/aicpa/interestareas/frc/auditattest/downloadabledocuments/attest-clarity/differences-between-isae-3000-at-c-105-and-205.pdf.

When the U.S. CPA has performed a SOC 2® examination in accordance with the attestation standards and the ISAEs, the U.S. CPA would indicate in the report that the examination was also conducted in accordance with *ISAE 3000* (Revised). In addition, the U.S. CPA's report would need to include the elements of the auditor's report included in paragraphs .63–.66 of AT-C section 205 and paragraph .69 of ISAE 3000 (Revised).

The following is an illustrative report that meets the requirements in AT-C section 205 and ISAE 3000 (Revised) related to the contents of the report, when the U.S. CPA is reporting under both standards. The illustrative SOC 2® report is prepared in accordance with AT-C section 205; additions included to meet the requirements of ISAE 3000 (Revised) are shown in ***boldface italics***.

Independent service auditor's report

To: XYZ Service Organization

Scope

We have examined XYZ Service Organization's (XYZ's) accompanying description of its medical claims processing system titled "XYZ Service Organization's Description of Its Medical Claims Processing System" throughout the period Jan. 1, 20XX, to Dec. 31, 20XX, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period Jan. 1, 20XX, to Dec. 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria for security, availability, processing integrity, confidentiality and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Service organization's responsibilities

XYZ is responsible for its service commitments and system requirements and for designing, implementing and operating effective controls within the system to provide reasonable assurance that XYZ's service commitments and system requirements were achieved. XYZ has provided the accompanying assertion titled "Assertion of XYZ Service Organization Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. XYZ is also responsible for preparing the description and assertion, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of CPAs **(AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board.** Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and XYZ's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether the controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Testing the operating effectiveness of the controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Service auditor's independence and quality control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of tests of controls

The specific controls we tested and the nature, timing and results of those tests are listed in section XX.

Opinion

In our opinion, in all material respects,

a. the description presents XYZ's medical claims processing system that was designed and implemented throughout the period Jan. 1, 20XX, to Dec. 31, 20XX, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period Jan. 1, 20XX, to Dec. 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period; and

c. the controls stated in the description operated effectively throughout the period Jan. 1, 20XX, to Dec. 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted use

This report, including the description of tests of controls and results thereof in section XX, is intended solely for the information and use of XYZ, user entities of XYZ's medical claims processing system during some or all of the period Jan. 1, 20XX, to Dec. 31, 20XX, business partners of XYZ subject to risks arising from interactions with the medical claims processing system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of:

- The nature of the service the service organization provided
- How the service organization's system interacts with user entities, business partners, subservice organizations and other parties
- Internal control and its limitations
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[Service auditor's signature]

[Service auditor's city and state]

[Date of the service auditor's report]

3. Inquiry — Given the same fact pattern as in the previous inquiry, may a non-U.S. CPA (or equivalent, such as a Chartered Accountant) perform a SOC 2® examination in accordance with ISAE 3000 (Revised)?

Reply — Yes. If not precluded by regulations of the local jurisdiction, a non-U.S. CPA may perform a SOC 2® examination in accordance with ISAE 3000 (Revised) and report accordingly. The non-U.S. CPA may find the guidance in AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* helpful when performing such an examination.

The following is an illustrative service auditor's report that may be appropriate when reporting on a SOC 2® examination performed in accordance with ISAE 3000 (Revised). The illustrative report is based on the reporting requirements of ISAE 3000 (Revised). However, it has also been modeled after the reports in ISAE 3402, *Assurance Reports on Controls at a Service Organization*. Although the subject matter of the reports in ISAE 3402 is "controls at a service organization that provides a service to user entities that is likely to be relevant to user entities' internal control as it relates to financial reporting" rather than controls at the service organization relevant to security, availability, processing integrity, confidentiality or privacy, which is the subject matter of a SOC 2® examination, there are certain aspects of the language in the illustrative report in ISAE 3402 that more closely parallel a SOC 2® examination.

Independent service auditor's assurance report

on description of controls and their design and operating effectiveness

To: XYZ Service Organization

Scope

We have been engaged to report on XYZ Service Organization's (XYZ's) description at pages [bb–cc] of its medical claims processing system throughout the period Jan. 1, 20XX, to Dec. 31, 20XX, (the description) based on the criteria for a description of a service organization's system in D.C. section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, (description criteria) and on the design and operation of controls stated in the description to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)* (applicable trust services criteria).

Service organization's responsibilities

XYZ is responsible for: preparing the description and accompanying statement at page [aa], including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; selecting the applicable trust services category or categories and stating the related controls in the description; identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and designing, implementing, and operating controls that are suitably designed and operating effectively to provide reasonable assurance that its service commitments and system requirements were achieved.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Control I[5] and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the description and on the design and operation of controls related to the service commitments and system requirements stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented in accordance with the description criteria and the controls are suitably designed and 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.

An assurance engagement to report on the description and the design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not presented in accordance with the description criteria and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to obtain reasonable assurance that the service commitments and system requirements stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a service organization

The description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own environment. Also, because of their nature, service organization controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection of any evaluation of the suitability of design or operating effectiveness of controls to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed because of the matters outlined in this report. In our opinion, in all material respects,

a. the description presents the medical claims processing system as designed and implemented throughout the period from Jan. 1, 20XX, to Dec. 31, 20XX, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period from Jan. 1, 20XX, to Dec. 31, 20XX, to provide reasonable assurance that XYZ's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period; and

c. the controls, which were those necessary to provide reasonable assurance that XYZ's service commitments and system requirements were achieved based on the applicable trust services criteria, operated effectively throughout the period from Jan. 1, 20XX, to Dec. 31, 20XX.

Description of tests of controls

The specific controls tested and the nature, timing and results of those tests are listed on pages [yy–zz].

Intended users and purpose

This report and the description of tests of controls on pages [yy–zz] are intended only for customers who have used XYZ's medical claims processing system and their auditors, who have a sufficient understanding to consider it, along with other information, including information about controls operated by customers themselves, when assessing the risks arising from interactions with the medical claims processing system of XYZ Service Organization.

[Service auditor's signature]

[Date of the service auditor's assurance report]

[Service auditor's address]

Endnotes

[1] All AT-C sections can be found in AICPA *Professional Standards*.

[2] A SOC 2® examination may also be performed in accordance with AT Section 101, *Attest Engagements*, of the PCAOB's interim attestation standards.

[3] All ET sections can be found in AICPA *Professional Standards*.

[4] *Frequently Asked Questions: General ethics* questions issued by the AICPA Professional Ethics Division as of May 1, 2017. aicpa.org/InterestAreas/ProfessionalEthics/Resources/Tools/DownloadableDocuments/Ethics-General-FAQs.pdf

[5] *ISQC I , Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements*

P: 888.777.7077 | F: 800.362.5066 | W: aicpa-cima.com