July 2018

AICPA

Reporting on a SOC 2® Examination

through the end of the transition period (Dec. 15, 2018)

Reporting on a SOC 2® Examination Through the End of the Transition Period (December 15, 2018)

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

The answers to these frequently asked questions (FAQs) are based on guidance developed by the SOC 2 Guide Working Group in response to questions raised about the transition guidance presented in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)* (2017 trust services criteria); DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (2018 description criteria); and the illustrative reports contained in the appendices of AICPA guide, *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (guide). These FAQs are not rules, regulations, or official statements of the Assurance Services Executive Committee or the Auditing Standards Board and, therefore, are not authoritative guidance.

1. Inquiry—Paragraph .25 of the 2017 trust services criteria includes the following transition guidance:

> The 2017 trust services criteria presented in this document will be codified as TSP section 100. The extant trust services criteria issued in 2016 will be available in TSP section 100A through December 15, 2018. After that date, the 2016 criteria will be considered superseded. During the transition period (April 15, 2017 through December 15, 2018), practitioners should distinguish in their reports whether the 2016 or 2017 trust services criteria have been used.

Does the *transition guidance* refer to the date on which the service auditor's report is issued or to the date of the subject matter presentation (for example, the "as of" date in a type 1 examination or the "period-end date" in a type 2 examination)?

Reply—The transition guidance refers to the date of the subject matter presentation. For example, assume the service auditor is engaged to perform a type 2 SOC 2 examination of the service organization's system for the nine months ended November 30, 2018. In that case, the practitioner should distinguish in the report (which would be issued in 2019) whether the 2017 trust services criteria (codified as TSP section 100) or the trust services criteria presented in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Criteria)* (2016 trust services criteria) were used to evaluate the suitability of design and operating effectiveness of the controls included in the description. In addition, the practitioner should also distinguish in the report whether the 2018 description criteria or the description criteria presented in DC section 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (2015 description criteria) were used to evaluate

the description, as discussed in the transition guidance provided in paragraphs .20-.22 of the 2018 description criteria.

2. Inquiry – Can a practitioner examine the description of the service organization's system prepared using the 2018 description criteria, when the suitability of design and operating effectiveness of controls stated within the description were evaluated using the 2016 trust services criteria?

Reply- No. As noted in footnotes 13 and 15 of Chapter 1 of the guide, the 2018 description criteria were designed to be used in conjunction with the 2017 trust services criteria. Similarly, the 2015 description criteria should be used in conjunction with the extant 2016 trust services criteria.

3. Inquiry—The new illustrative reports in the guide have been updated to comply with the reporting requirements of AT-C 205*, Examination Engagements* (which became effective in May 2017) and to reflect other revisions made to the SOC 2 guide. As a result, the illustrative reports contain language that is different from the illustrative reports presented in the 2015 AICPA guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 guide). During the transition period discussed above, should service auditors use the new language in an illustrative report on a SOC 2 examination in which the description was prepared in accordance with the 2015 description criteria and the suitability of design and operating effectiveness of controls stated in the description were evaluated using the 2016 trust services criteria?

Reply—No. The new illustrative SOC 2 reports in the guide contain language that may not apply to SOC 2 examinations performed in accordance with the extant criteria. For example, unlike the reports in the 2015 guide, management's assertion and the service auditor's opinion in the new illustrative reports state that controls provide reasonable assurance that the *service organization's service commitments and system requirements* would be achieved based on the trust services criteria.

Presented below is an illustrative management's assertion and service auditor's report for a type 2 SOC 2 examination that may be used when the SOC 2 examination uses the 2015 description criteria in DC 200A and the 2016 trust services criteria in TSC 100A. The illustrative service auditor's report meets the reporting requirements of AT-C 205; however, note this is just an example of language that may be used in this specific situation. A service auditor may use any language in the report, so long as the report meets the reporting requirements included in AT-C 205.

Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, and Confidentiality

In the following illustrative assertion and service auditor's report, XYZ Service Organization outsources certain aspects of its system to a subservice organization and elects to use the carve-out method for the subservice organization. In addition, complementary user entity and complementary subservice organization controls are required to meet certain trust services criteria. Changes to the assertion and report to reflect the use of the carve-out method and the need for complementary user entity and complementary subservice organization controls are shown in ***boldface italics***.

Illustrative Assertion by Management of a Service Organization

[*XYZ Service Organization's Letterhead*]

Assertion of the Management of XYZ Service Organization

We have prepared the accompanying description of XYZ Service Organization's (XYZ) [*type or name*] system titled [*insert title of management's description*] throughout the period [*date*] to [*date*][1] (description), based on the criteria for a description of a service organization's system in DC section 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the [*type or name*] system that may be useful when assessing the risks arising from interactions with XYZ's [*type or name*] system, particularly information about system controls that XYZ has designed, implemented, and operated to provide reasonable assurance of meeting the criteria related to security, availability, processing integrity, and confidentiality set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Criteria*) (applicable trust services criteria)***.***

XYZ uses a subservice organization to **[identify the function or service provided by the subservice organization]*. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to meet the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of XYZ's***

[1] The title of the description of the service organization's system in the service auditor's report should be the same as the title used by management of the service organization in its description of the service organization's system.

controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ, to meet the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls.

We confirm, to the best of our knowledge and belief, that

a. the description presents XYZ's [*type or name*] system that was designed and implemented throughout the period [*date*] to [*date*], in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period [date] to [date] to provide reasonable assurance that the applicable trust services criteria would be met ***if the controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period*.**

c. the controls stated in the description operated effectively throughout the period [date] to [date] to meet the applicable trust services criteria ***if complementary subservice organization controls and complementary user entity controls assumed in the design of XYZ's controls, operated effectively throughout that period*.**

Illustrative Independent Service Auditor's Report on an Examination of a Service Organization's Description of its [*Type or Name*] System and the Suitability of Design and Operating Effectiveness of Controls Relevant to Security, Availability, Processing Integrity, and Confidentiality

Independent Service Auditor's Report[2]

To: XYZ Service Organization

Scope

We have examined XYZ Service Organization's accompanying description of its [*type or name*] system titled [*insert title of management's description*] throughout the period [*date*] to [*date*][3] (description) based on the criteria for a description of a service organization's system in DC

[2] The report may also be titled "Report of Independent Service Auditors."

[3] The title of the description of the service organization's system in the service auditor's report should be the same as the title used by management of the service organization in its description of the service organization's system.

section 200A, *2015 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 [*date*] to [*date*] to provide reasonable assurance of meeting the criteria for security, availability, processing integrity, and confidentiality set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Criteria*) (applicable trust services criteria).[4]

XYZ uses a subservice organization to [identify the function or service provided by the subservice organization]. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at XYZ to meet the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of XYZ's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at XYZ to meet the applicable trust services criteria. The description presents XYZ's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of XYZ's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

XYZ has provided the accompanying assertion titled, [insert the title of the attached management assertion] (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. XYZ is 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

---

[4] A statement such as the following is added to the service auditor's report when information that is not covered by the report is included in the description of the service organization's system.

> The information included in "Section X—Other Information Provided by XYZ Service Organization That is Not Covered by the Service Auditor's Report" is presented by management of XYZ Service Organization to provide additional information and is not a part of XYZ Service Organization's description. Information about XYZ Service Organization's [describe the nature of the information, for example, planned system changes] has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to meet the applicable trust services criteria, and accordingly, we express no opinion on it.

controls in the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and operating effective controls to provide reasonable assurance of meeting the applicable trust services criteria.

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 Certified Public Accountants. 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 of meeting the applicable trust services criteria throughout the period [*date*] to [*date*]. 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
- 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 to meet the applicable trust services criteria.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance of meeting the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the applicable trust services criteria were met.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances

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 of meeting 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 [*name or type*] system that was designed and implemented throughout the period [*date*] *to* [*date*], in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period [date] to [date] to provide reasonable assurance that the applicable trust services criteria would be met ***if the controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of XYZ's controls throughout that period.***

c. The controls stated in the description operated effectively throughout the period [date] to [date] to provide reasonable assurance that the applicable trust services criteria were met ***if complementary subservice organization controls and complementary user entity controls assumed in the design of XYZ's controls operated effectively throughout that period*.**

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 [*type* or *name*] system during some or all of the period [*date*] to [*date*], business partners of XYZ subject to risks arising from interactions with the 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 following:

- The nature of the service provided by the service organization

- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to meet the applicable trust services criteria
- 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 applicable trust services criteria 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

P: 919.402.4500 | F: 919.402.4505 | W: aicpa.org