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*] (description), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide 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 the suitability of design and operating effectiveness of XYZ Service Organization's controls to meet the criteria related to security, availability, processing integrity, and confidentiality 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)**.**

XYZ Service Organization uses a subservice organization to **[identify the function or service provided by the subservice organization].** ***The description includes only the controls of XYZ Service Organization and excludes controls of the subservice organization. The description also indicates that certain trust services criteria specified therein can be met only if the subservice organization's controls contemplated in the design of XYZ Service Organization's controls are suitably designed and operating effectively along with related controls at the service organization. The description does not extend to controls of the subservice organization.***

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

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

a. the description fairly presents the [*type or name*] system throughout the period [*date*] to [*date*], based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

(2) The components of the system used to provide the services, which are as follows:

(a) *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).

(b) *Software*. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).

(c) *People*. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

(d) *Procedures*. The automated and manual procedures.

(e) *Data.* Transaction streams, files, databases, tables, and output used or processed by the system.

(3) The boundaries or aspects of the system covered by the description.

(4) For information provided to, or received from, subservice organizations or other parties,

(a) how such information is provided or received and the role of the subservice organization and other parties and

(b) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

(a) Complementary user entity controls contemplated in the design of the service organization's system.

(b) When the inclusive method is used to present a subservice organization, controls at the subservice organization

(6) If the service organization presents the subservice organization using the carve-out method,

(a) the nature of the services provided by the subservice organization and

(b) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

(7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons.

(8) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

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

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

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[1]

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*][2] (description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period [*date*] to [*date*] to meet the criteria for security, availability, processing integrity, and confidentiality 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).[3]

XYZ Service Organization uses a subservice organization to [identify the function or service provided by the subservice organization]. The description includes only the controls of XYZ Service Organization and excludes controls of the subservice organization. The description also indicates that certain trust services criteria can be met only if the subservice organization's controls, contemplated in the design of XYZ Service Organization's controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

---

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

[2] 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.

[3] 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.

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

XYZ Service Organization has provided the accompanying assertion titled, [insert the title of the attached management assertion] (assertion) about the fairness of the presentation of the description based on the description criteria and suitability of design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. XYZ Service Organization 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; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting controls that are suitably designed; and operating effectively to meet the applicable trust services criteria stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet 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:

- Performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria.

- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.

- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.

- Evaluating the overall presentation of the description.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section 4 of this report.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria:

a. The description fairly presents the [*name or type*] system that was designed and implemented throughout the period [*date*] *to* [*date*].

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

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

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of XYZ Service Organization, user entities of XYZ Service Organization's [*type* or *name*] system during some or all of the period [*date*] to [*date*], and prospective user entities, independent auditors, and practitioners providing services to such user entities, 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, subservice organizations, and other parties
- Internal control and its limitations
- User entity responsibilities, complementary user entity controls, and how they interact with related controls at the service organization to meet the applicable trust services criteria
- 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