DC Section 200A

2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report

The description criteria in this document (2015 description criteria) are a reproduction of paragraphs 1.26–.27 of the 2015 edition of AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* and are designed to be used in conjunction with the 2016 trust services criteria set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Principles*), in a SOC 2® report.

The 2015 description criteria may be used when preparing a description of the service organization's system as of December 15, 2018, or prior to that date (type 1 examination) or a description for periods ending as of December 15, 2018, or prior to that date (type 2 examination). However, for a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria [fn 1] should be used. During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

1.26 The criteria for determining whether the description of the service organization's system is fairly presented are as follows:

a. The description contains the following information:

i. The types of services provided

ii. The components of the system used to provide the services, which are as follows:

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

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

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

[fn 1] The 2018 description criteria are codified in DC section 200, *Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*.

(4) *Procedures*. The automated and manual procedures. [fn 4]

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

iii. The boundaries or aspects of the system covered by the description

iv. For information provided to, or received from, subservice organizations and other parties

(1) how the information is provided or received and the role of the subservice organizations and other parties

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

v. The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

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

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

vi. If the service organization presents the subservice organization using the carve-out method

(1) the nature of the services provided by the subservice organization

(2) 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

vii. Any applicable trust services criteria that are not addressed by a control and the reasons

viii. 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

b. 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 report users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs

---

[fn 4] The description of the procedures of the system includes those by which services are provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, delivered, and reports and other information prepared.

1.27 If the description addresses controls over privacy, in addition to the criteria in paragraph 1.26 for determining whether the description of the service organization's system is fairly presented, the description should also include the following information:

a. The types of personal information collected from individuals or obtained from user entities or other parties [fn 5] and how such information is collected and, if collected by user entities, how it is obtained by the service organization

b. The process for

i. identifying specific requirements in agreements with user entities and in laws and regulations applicable to the personal information and

ii. implementing controls to meet those requirements

c. If the service organization presents the subservice organization using the carve-out method

i. any aspect of the personal information life cycle for which responsibility has been delegated to the subservice organization

ii. the types of activities the subservice organization would need to perform to comply with the service organization's privacy commitments

d. If the service organization provides a privacy notice to individuals about whom personal information is collected, used, retained, disclosed, and disposed of or anonymized in delivering its services, the privacy notice prepared in accordance with the relevant criteria for a privacy notice set forth in TSP section 100 or a description of how the privacy notice may be obtained

e. If the service organization does not provide and is not required by law, regulation, or commitments to provide the privacy notice to individuals, a statement that the service organization is not responsible for providing a privacy notice and describes how it communicates its privacy-related commitments and practices to user entities, which includes the following information:

i. A summary of the significant privacy-related commitments common to most agreements between the service organization and its user entities and any requirements in a particular user entity's agreement that the service organization meets for all or most user entities

ii. A summary of the significant privacy-related requirements mandated by law, regulation, an industry, or a market that are not included in user entity agreements but the service organization meets for all or most user entities

iii. The purposes, uses, and disclosures of personal information as permitted by user entity agreements and beyond those permitted by such agreements but not prohibited by such agreements and the service organization's commitments regarding the purpose, use, and disclosure of personal information that are prohibited by such agreements

---

[fn 5] An example of an entity that collects personal information from user entities is a credit reporting bureau that maintains information about the creditworthiness of individuals.

iv. A description of the service organization's practices regarding the retention of personal information

v. A description of the service organization's practices for disposing of personal information

vi. If applicable, how the service organization supports any process permitted by user entities for individuals to obtain access to their information to review, update, or correct it

vii. If applicable, a description of the process to determine that personal information is accurate and complete and how the service organization implements correction processes permitted by user entities

viii. If applicable, how inquiries, complaints, and disputes from individuals (whether directly from the individual or indirectly through user entities) regarding their personal information are handled by the service organization

ix. A statement regarding the existence of a written security program and what industry or other standards it is based on

x. Other relevant information related to privacy practices deemed appropriate for user entities by the service organization

