DC Section 200

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

Prepared by the AICPA Assurance Services Executive Committee's SOC 2® Working Group

Introduction

.01 AICPA's Assurance Services Executive Committee (ASEC), through its Trust Information Integrity Task Force's SOC 2® Guide Working Group, has developed a set of benchmarks, known as *description criteria*. These description criteria are to be used when preparing and evaluating the description of the service organization's system (description) in an examination of a service organization's controls over security, availability, processing integrity, confidentiality, and privacy (SOC 2® examination). This document presents the description criteria for use in that examination. (The AICPA's trust services criteria are not addressed in this document. [fn 1] Those criteria are used in a SOC 2® examination to evaluate whether controls stated in the description 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.)

.02 Applying the description criteria requires judgment. Therefore, in addition to the description criteria, this document also presents implementation guidance for each criterion. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. This guidance does not address all possible situations; therefore, users should carefully consider the facts and circumstances of the service organization and its environment when applying the description criteria.

Applicability and Use of the Description Criteria

SOC 2® Examination

.03 The description criteria presented in this document were developed to be used in conjunction with the SOC 2® examination described in AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (guide). The SOC 2® examination is performed in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements* (AICPA, *Pro-*

[fn 1] The trust services criteria were issued in *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* and are codified in TSP section 100 (AICPA, *Trust Services Criteria*). Paragraphs .25–.26 of TSP section 100 provide transition guidance related to the use of those criteria in a service auditor's report.

fessional Standards). In that examination, the CPA (known as a *service auditor*) [fn 2] expresses an opinion about the following:

a. Whether the description is presented in accordance with the description criteria

b. Whether the controls were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved if controls operated effectively based on the applicable trust services criteria

c. In a type 2 examination, [fn 3] whether the controls 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. [fn 4]

.04 A SOC 2® examination is predicated on the concept that, because service organization management is ultimately responsible for developing, implementing, and operating the service organization's system, service organization management is also responsible for developing and presenting in the SOC 2® report a description of the service organization's system. Service organization management uses the description criteria in this document when preparing the description of the service organization's system; the service auditor uses the criteria when evaluating whether the description is presented in accordance with the description criteria.

Suitability and Availability of the Description Criteria

.05 According to the attestation standards, the attributes of suitable criteria are as follows: [fn 5]

- *Relevance.* Criteria are relevant to the subject matter.
- *Objectivity.* Criteria are free from bias.

[fn 2] In the attestation standards, a CPA performing an attestation engagement ordinarily is referred to as a *practitioner.* However, the AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* uses the term *service auditor*, rather than practitioner, to refer to a CPA reporting on controls at a service organization. Therefore, this document also uses the term *service auditor*.

[fn 3] There are two types of SOC 2® examinations (type 1 and type 2), and the subject matters vary depending on which type of examination the service auditor performs. The subject matters of a type 1 examination are (*a*) the description and (*b*) the suitability of the design of the controls to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The subject matters in a type 2 examination are (*a*) the description, (*b*) the suitability of design of the controls to provide reasonable that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria, and (*c*) the operating effectiveness of controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

[fn 4] This term refers to the trust services criteria in TSP section 100, *2017Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), that pertain to the category or categories included within the scope of the particular examination.

[fn 5] Paragraph .A42 of AT-C section 105, *Concepts Common to All Attestation Engagements* (AICPA, *Professional Standards*).

- *Measurability.* Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.

- *Completeness.* Criteria are complete when subject matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect users' decisions made on the basis of that subject matter.

.06 In addition to being suitable, AT-C section 105 [fn 6] indicates that the criteria used in an attestation engagement should be available to report users. The publication of the description criteria makes the criteria available to report users. Accordingly, ASEC has concluded that the description criteria presented in this document are suitable and available for use in a SOC 2® examination.

Preparing and Evaluating the Presentation of the Description of the Service Organization's System in Accordance With the Description Criteria

.07 Service organization management is responsible for the design, implementation, and operation of controls within the system used to provide services to user entities and business partners. In a SOC 2® examination, a description of the service organization's system presented in accordance with the description criteria is designed to enable user entities, business partners, and other intended users of the SOC 2® report (known collectively as *report users*) to understand the service organization's system, including the processing and flow of data and information through and from the system. The description describes the procedures and controls the service organization has implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. The description is prepared by service organization management from documentation supporting the system of internal control and system operations, as well as consideration of the policies, processes, and procedures within the system used to provide the services.

.08 A SOC 2® report is intended for use by those who have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide those services, among other matters. As a result, when drafting the description, service organization management can assume that users have such knowledge and understanding. Furthermore, if the users do not have such knowledge and understanding, they are likely to misunderstand the content of the SOC 2® report, the assertions made by management, and the service auditor's opinion, all of which are included in the report. For that reason, management and the service auditor should agree on the intended users of the report (referred to as *specified parties*). Specified parties of a SOC 2® report may include service organization personnel, user entities of the system throughout some or all of the period, business partners subject to risks arising from interactions with the system, practitioners providing services to user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of such matters.

.09 Though the description is generally narrative in nature, there is no prescribed format for the description. Flowcharts, matrixes, tables, graphics, context diagrams, or a combination thereof may be used to supplement the narratives contained within the description.

[fn 6] Paragraph .25*b* of AT-C section 105.

.10 Additionally, the description can be organized in a variety of ways. For example, the description may be organized by components of internal control (the control environment, risk assessment process, control activities, monitoring activities, and information and communications). Alternatively, it may be organized by components of the system (infrastructure, software, people, procedures, and data) and supplemented by disclosures of the aspects of the internal control components relevant to the identification and assessment of risks that would prevent the service organization from achieving its service commitments and system requirements and the design, implementation, and operation of controls to address them.

.11 The extent of disclosures included in the description may vary depending on the size and complexity of the service organization and its activities. In addition, the description need not address every aspect of the service organization's system or the services provided by the system, particularly if certain aspects of those services are not relevant to report users or are beyond the scope of the SOC 2® examination. For example, disclosures about a service organization's processes related to billing for the services provided to user entities are unlikely to be relevant to report users. Similarly, although the description includes procedures within both manual and automated systems by which services are provided, it need not necessarily disclose every step in the process.

.12 Ordinarily, a description of a service organization's system in a SOC 2® examination is presented in accordance with the description criteria when it (*a*) describes the system that the service organization has implemented (that is, placed in operation) to provide the services, (*b*) includes information about each description criterion, to the extent it is relevant to the system being described, and (*c*) does not inadvertently or intentionally omit or distort information that is likely to be relevant to report users' decisions. Although the description should include disclosures about each description criterion, such disclosures are not intended to be made at such a detailed level that they might increase the likelihood that a hostile party could exploit a security vulnerability, thereby compromising the service organization's ability to achieve its service commitments and system requirements. Instead, the disclosures are intended to enable report users to understand the nature of the risks faced by the service organization and the impact of the realization of those risks.

.13 A description is not presented in accordance with the description criteria if it (*a*) states or implies that certain IT components exist when they do not, (*b*) states or implies that certain processes and controls have been implemented when they are not being performed, or (*c*) contains statements that cannot be objectively evaluated (for example, advertising puffery).

- **.14** In certain circumstances, additional disclosures may be necessary to supplement the description. Management's decisions about whether such additional disclosures are necessary and the service auditor's evaluation of management's decisions involve consideration of whether the disclosures may affect information that is likely to be relevant to the decisions of report users. Additional disclosures may include the following, for example:Significant interpretations made in applying the description criteria in the specific circumstances of the SOC 2® examination (for example, what constitutes a security event or incident)

- Subsequent events, depending on their nature and significance

Materiality Considerations When Preparing and Evaluating Whether the Description Is Presented in Accordance With the Description Criteria

.15 As discussed in paragraph .02, applying the description criteria requires judgment. One of those judgments involves the informational needs of report users. Most SOC 2® reports have a broad range of

specified parties. Therefore, the description is intended to meet the common informational needs of the specified parties and does not ordinarily include information about every aspect of the system that may be considered important to each individual report user. However, an understanding of the perspectives and information needs of the broad range of intended SOC 2® report users is necessary to determine whether the description is presented in accordance with the description criteria and is sufficient to meet report users' needs.

.16 When evaluating whether the description is in accordance with the description criteria, management considers whether misstatements or omissions in the description, individually or in the aggregate, could reasonably be expected to influence decisions of specified parties to the SOC 2® report. For example, in a SOC 2® examination on controls relevant to privacy, management may discover that is has failed to describe a principal service commitment involving compliance with the European Union's General Data Protection Regulation. Because such information could reasonably be expected to influence the decisions of SOC 2® report users, management may conclude that the omission of such information may affect the decisions of such users. In that case, management would amend the description by including the relevant information. [fn 7]

.17 Because the description criteria call for disclosure of primarily nonfinancial information, most descriptions will be presented in narrative form. Therefore, materiality considerations are mainly qualitative in nature and center around whether there are misstatements in information that could reasonably be expected to influence report users' decisions, including the possibility that relevant information has been omitted. Qualitative factors to be considered include the following:

- Whether the description of the service organization's system includes the significant aspects of system processing
- Whether the description is prepared at a level of detail likely to be meaningful to report users
- Whether each of the relevant description criteria in paragraph .19 has been addressed without using language that omits or distorts the information
- Whether the characteristics of the presentation are appropriate, because the description criteria allow for variations in presentation

Description Criteria for a Description of a Service Organization's System in a SOC 2® Examination and Related Implementation Guidance

.18 To be presented in accordance with the description criteria, a description ordinarily needs to disclose information about each of the requirements (criteria) presented in the left column of the following table, to the extent that the criterion is applicable to the system and the trust services categories included within the scope of the examination. (Materiality considerations are discussed in the previous section beginning at paragraph .15.)

[fn 7] If the description has been prepared to meet the informational needs of a specific subset of SOC 2® report users (and the report is restricted to those specific users), management considers whether misstatements (including omissions) may affect the decisions of that specific subset of report users.

.19 The implementation guidance in the right column of the following table presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. The implementation guidance does not address all possible situations; therefore, service organization management is advised to carefully consider the specific facts and circumstances of the service organization and the nature of the services provided when applying the description criteria in a SOC 2® examination.

Description Criteria	***Implementation Guidance***
The description contains the following information:	When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
DC 1: The types of services provided	Examples of the types of services provided by service organizations are as follows: • *Customer support.* Providing customers of user entities with online or telephonic post-sales support and service management. Examples of these services are warranty inquiries and investigating and responding to customer complaints. • *Health care claims management and processing.* Providing medical providers, employers, third-party administrators, and insured parties of employers with systems that enable medical records and related health insurance claims to be processed accurately, securely, and confidentially. • *Enterprise IT outsourcing services.* Managing, operating, and maintaining user entities' IT data centers, infrastructure, and application systems and related functions that support IT activities, such as network, production, security, change management, hardware, and environmental control activities. • *Managed security.* Managing access to networks and computing systems for user entities (for example, granting access to a system and preventing, or detecting and mitigating, system intrusion). • *Financial technology (FinTech) services.* Providing financial services companies with information technology-based transaction processing services. Examples of such transactions are loan processing, peer-to-peer lending, payment processing, crowdfunding, big data analytics, and asset management.

Description Criteria	*Implementation Guidance*
DC 2: The principal service commitments and system requirements	A system of internal control is evaluated using the trust services criteria within the context of the entity's ability to achieve its business objectives and sub-objectives. When a service organization provides services to user entities, its objectives and sub-objectives relate primarily to the following: *a.* The achievement of the service commitments made to user entities related to the system used to provide the services and the system requirements necessary to achieve those commitments *b.* Compliance with laws and regulations regarding the provision of the services by the system *c.* The achievement of the other objectives the service organization has for the system These are referred to as the service organization's *service commitments* and *system requirements.* Although service organization management is responsible for designing, implementing, and operating controls to provide reasonable assurance that it achieves its system objectives, management is required to disclose in the description only its *principal* service commitments and system requirements, as discussed in the subsequent section. *Principal Service Commitments*. Disclosure of the principal service commitments and system requirements enables report users to understand the objectives that drive the operation of the system and how the applicable trust services criteria were used to evaluate whether controls were suitably designed and operated effectively. Service commitments include those made to user entities and others (such as customers of user entities), to the extent those commitments relate to the trust services category or categories addressed by the description. For example, service commitments could also include those made as part of the National Institute of Standards and Technology (NIST) risk management framework for government agencies and other parties. The service commitments a service organization makes to user entities and others are based on the needs of those entities. In identifying the service commitments to be disclosed, service organization management may begin by reviewing the commitments it made to user entities. Service commitments may be communicated to user entities in many ways, such as through contracts, service level agreements, and published policies (for example, a privacy policy). No specific form of communication is required. A service organization may make service commitments on

Description Criteria	*Implementation Guidance*
	many different aspects of the service being described, including the following: • Specification of the algorithm used in a calculation • The hours a system will be available • Published password standards • Encryption standards used to encrypt stored customer data Service commitments may also be made about one or more of the trust services categories addressed by the description. As an example, if controls over privacy are addressed by the description, a service organization may make commitments such as the following: • The organization will not process or transfer information without obtaining the data subject's consent. • The organization will provide a privacy notice to customers once every 6 months or when there is a change in the organization's business policies. • The organization will respond to access requests within 10 working days of receiving the request from its customers. Service organization management need not disclose every service commitment, but only those that are relevant to the broad range of SOC 2® report users (that is, the principal service commitments). For example, when the description addresses availability, a service organization may make the same system availability commitment to the majority of its user entities. Because information about the availability commitment common to most user entities is likely to be relevant to the broad range of SOC 2® report users, service organization management would describe that principal availability commitment in the description. In other cases, however, a service organization may make a different commitment about system availability to an individual user entity that requires greater system availability than most user entities. Service organization management ordinarily would not disclose that commitment because it is unlikely to be relevant to the broad range of SOC 2® report users. Because

Description Criteria	*Implementation Guidance*
	that service commitment is not disclosed in the description, the individual user entity understands that the evaluation of the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls was made based on the service organization's achievement of its principal service commitments and system requirements (that is, those common to the majority of user entities); therefore, the individual user entity may need to obtain additional information from the service organization regarding the achievement of its specific availability commitment. When the description addresses privacy, service organization management discloses the service commitments and system requirements identified in the service organization's privacy notice or in its privacy policy that are relevant to the system being described. When making such disclosures, it may also be helpful to report users if service organization management describes the purposes, uses, and disclosures of personal information as permitted by user entity agreements. *Principal System Requirements*. System requirements are the specifications about how the system should function to do the following: • Meet the service organization's service commitments to user entities and others (such as user entities' customers) • Meet the service organization's commitments to vendors and business partners • Comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations • Achieve other objectives of the service organization that are relevant to the trust services categories addressed by the description Requirements are often specified in the service organization's system policies and procedures, system design documentation, contracts with customers, and government regulations. The following are examples of system requirements: • Workforce member fingerprinting and background checks established in government banking regulations • System edits that restrict the values accepted for

Description Criteria	*Implementation Guidance*
	system input, which are defined in application design documents • Maximum acceptable intervals between periodic review of workforce member logical access as documented in the security policy manual • Data definition and tagging standards, including any associated metadata requirements, established by industry groups or other bodies, such as the Simple Object Access Protocol (SOAP) • Business processing rules and standards established by regulators, for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA) System requirements may result from the service organization's commitments relating to one or more of the trust services categories (for example, a commitment to programmatically enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration). The principal system requirements that need to be disclosed are those that are relevant to the trust services category or categories addressed by the description and that are likely to be relevant to the broad range of SOC 2® report users. In identifying which system requirements to disclose, service organization management may consider internal policies that are relevant to the system being described, key decisions made in the design and operation of the system, and other business requirements for the system. For example, internal requirements related to the operating margin for the services associated with the system are not relevant to the broad range of SOC 2® report users and, therefore, need not be disclosed.
DC 3: The components of the system used to provide the services, including the following: *a. Infrastructure* *b. Software* *c. People* *d. Procedures* *e. Data*	*Infrastructure.* Disclosures about the infrastructure component include matters such as the collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and related hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services. *Software.* Disclosures about the software component include matters such as the application programs, the IT system soft-

Description Criteria	*Implementation Guidance*
	ware that supports those application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop and laptop applications. *People.* Disclosures about the people component include the personnel involved in the governance, management, operation, security, and use of the system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers). *Procedures.* Disclosures about the automated and manual procedures implemented by the service organization primarily relate to those through which services are provided. These include, as appropriate, procedures through which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared. A process consists of a series of linked procedures designed to accomplish a particular goal (for example, the process for managing third party risks). Procedures are the specific actions undertaken to implement a process (for example, the procedure in place to assess and manage the requisition and engagement of vendors). For that reason, service organization management may find it easier to describe procedures in the context of the process of which they are a part. Policies are management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. The service organization deploys control activities through policies that establish what is expected and procedures that put policies into action. Reports and other information prepared by the service organization may also be included in the description to enable report users to better understand the order of activities performed by the service organization. System components may also be described using specific technical terms that will help create a clearer understanding of the service organization's system and system boundaries. Technical terms can also aid report users in understanding the service organization's physical and logical components when considering a service organization's impact on the user entities. It may be helpful for service organizations to enhance their system descriptions using open systems interconnect (OSI) seven-layer model concepts. An organization could describe how and

Description Criteria	*Implementation Guidance*
	on which layer specific components of the system are operated, for example, with a statement such as this: Encrypted connections are made to the service organization using client virtual private network (VPN) hardware that connects system users via secure shell (SSH) to secure file transfer protocol (SFTP) servers that operate following transport layer security (TLS) standards and protocols. *Data.* Disclosures about the data component include types of data used by the system, transaction streams, files, databases, tables, and output used or processed by the system. When the description addresses the confidentiality or privacy categories, other matters that may be considered for disclosure about the data component include the following: • The principal types of data created, collected, processed, transmitted, used, or stored by the service organization and the methods used to collect, retain, disclose, dispose of, or anonymize the data • Personal information that warrants security, data protection, or breach disclosures based on laws or commitments (for example, personally identifiable information, protected health information, and payment card data) • Third-party entity information (for example, information subject to confidentiality requirements in contracts) that warrants security, data protection, or breach disclosures based on laws or commitments When the description addresses controls over confidentiality and privacy, management would address, at a minimum, all the system components as they relate to the information life cycle of the confidential and personal information used in providing the service within well-defined processes and informal ad hoc procedures. *Boundaries of the system.* Not all activities performed at the service organization are part of the system being described. Determining the functions or processes that are outside the boundaries of the system and describing them in the description may be necessary to prevent report users from misunderstanding the boundaries of the system. Therefore, if there is a risk that report

Description Criteria	*Implementation Guidance*
	users might be confused about whether a specific function or process is part of the system being described, the description needs to clarify which processes or functions are included in the examination. For example, the following functions or processes at the service organization may be outside the boundaries of the system being described: • The process used to invoice user entities for the services provided by the service organization. • The conversion of new user entities to the service organization's systems. For some service organizations, such conversions are handled by an entirely different system than the one being described. • The receipt of data from sources outside the system being described. An example is a payroll processing system that receives information inputs from an employer in a ready-to-process state, which limits the responsibility of the service organization's system to processing the inputs provided by the employer to produce direct bank deposits to specified bank accounts. *Third Party Access.* Vendors, business partners, and others (third parties) often store, process, and transmit sensitive data or otherwise access a service organization's system. These third parties may provide components of the system. Service organization management may need to describe the components of the system provided by such third parties. Such disclosures may include, for example, the nature of the third parties' access and connectivity to the service organization's system.
DC 4: For identified system incidents that (*a*) were the result of controls that were not suitably designed or operating effectively or (*b*) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements, as of the date of the description (for a type 1) or during the period of time covered by the description (for a type 2), as appli-	Judgment is needed when determining whether to disclose an incident. However, consideration of the following matters as they relate to the system being described may help make that determination: • Whether the incident resulted from one or more controls that were not suitably designed or operating effectively • Whether the incident resulted in a significant failure in the achievement of one or more of the

Description Criteria	*Implementation Guidance*
cable, the following information: *a.* Nature of each incident *b.* Timing surrounding the incident *c.* Extent (or effect) of the incident and its disposition	service organization's service commitments and system requirements • Whether public disclosure of the incident was required (or is likely to be required) by cybersecurity laws or regulations • Whether the incident had a material effect on the service organization's financial position or results of operations and required disclosure in a financial statement filing • Whether the incident resulted in sanctions by any legal or regulatory agency • Whether the incident resulted in the service organization's withdrawal from material markets or cancellation of material contracts Disclosures about identified security incidents are not intended to be made at a detailed level, which might increase the likelihood that a hostile party could exploit a security vulnerability, thereby compromising the service organization's ability to achieve its service commitments and system requirements. Rather, the disclosures are intended to enable report users to understand the nature of the risks faced by the service organization and the impact of the realization of those risks. Assume that the service organization identified a security breach that resulted in the service organization's failure to achieve one or more of its service commitments and system requirements. The breach, which occurred six months prior to the start of the period covered by the description, had not been fully remediated during the period covered by the description. In this example, management would likely need to disclose the incident in the description to enable report users to understand the nature of the risks faced by the service organization and the impact of the realization of those risks. In addition, service organization management should consider whether to disclose known incidents at a subservice organization, regardless of whether management has elected to use the inclusive or carve-out method.
DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), presents the criteria for each of the trust services categories. A description is presented in accordance with this criterion when it includes information about each of the criteria related to the trust services category

Description Criteria	*Implementation Guidance*
achieved	or categories covered by the description (applicable trust services criteria), including controls related to the control environment, risk assessment process, information and communication, monitoring activities, and control activities. For example, if the description addresses availability, management would provide information about the controls it has implemented to address the common criteria in the trust services criteria and the additional trust services criteria for availability.
DC 6: If service organization management assumed, in the design of the service organization's system, that certain controls would be implemented by user entities, and those controls are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved, those complementary user entity controls (CUECs)	*Complementary User Entity Controls.* CUECs are those controls that service organization management assumed, in the design of the system, would be implemented by user entities and are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved. Usually, a service organization can achieve its service commitments and system requirements without depending on the implementation of CUECs at user entities because the service organization restricts its service commitments and system requirements to those matters that are its responsibility and that it can reasonably perform. Consider trust services criterion (CC) 6.2: > Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. CC 6.2 limits the service organization's responsibilities because the criterion requires only that the system register a user (identified by the user entity as an authorized user) and issue system credentials to that user after the user entity supplies the service organization with a list of authorized users. The user entity is responsible for identifying the users and supplying the service organization with a list of authorized users. If the user entity provides a list that inadvertently includes employees who are not authorized, the service organization has still met the criterion. Accordingly, identifying the authorized users and communicating that information to the service organization are not considered CUECs. The description is presented in accordance with this criterion if the CUECs are complete, accurately described, and relevant to the service organization's achievement of its service commitments and system requirements.

Description Criteria	*Implementation Guidance*
	User Entity Responsibilities. In addition to CUECs, user entities may have other responsibilities when using the system. Those responsibilities are necessary for the user entity to derive the intended benefits of using the services of the service organization. For example, the user of an express delivery service is responsible for providing complete and accurate recipient information and for using appropriate packaging materials. Such responsibilities are referred to as user entity responsibilities. Trust services criterion CC 2.3 states *[t]he entity communicates with external parties regarding matters affecting the functioning of internal control*. This would include communication of user responsibilities. However, because user entity responsibilities can be voluminous, they are often communicated through other methods (for example, by describing them in user manuals). Consequently, disclosure of user entity responsibilities in the description is usually not practical. Instead, management ordinarily identifies in the description the types of communications it makes to external users about user entity responsibilities. The form and content of such communication is the responsibility of service organization management. When service organization management communicates user entity responsibilities only to specific parties (such as in contracts with user entities), management considers whether other intended users of the SOC 2® report are likely to misunderstand it; in that case, management should limit the use of the report to those specific parties. If service organization management does not want to limit the use of the report, management would include the significant user entity responsibilities in the description of the service organization's system to prevent users from misunderstanding the system and the service auditor's report. In that case, the report would be appropriate for the broad range of SOC 2® users. When service organization management includes significant user entity responsibilities in the description, management evaluates those disclosures as part of its evaluation about whether the description is presented in accordance with the description criteria.
DC 7: If the service organization uses a subservice organization and the controls at the subservice organization are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are	*Inclusive method.* When service organization management elects the inclusive method, the relevant aspects of the subservice organization's infrastructure, software, people, procedures and data are considered part of the service organization's system and are included in the description of the service organization's system. Although the relevant aspects are considered a part of the service organization's system, the portions of the system that are attributable to the subservice organization would be separately identified in the description. Such disclo-

Description Criteria	*Implementation Guidance*
achieved, the following: *a.* When service organization management elects to use the inclusive method: i. The nature of the service provided by the subservice organization ii. The controls at the subservice organization that are necessary, in combination with controls at the service organization to provide reasonable assurance that the service organization's service commitments and system requirements are achieved iii. Relevant aspects of the subservice organization's infrastructure, software, people, procedures, and data	sures include the aspects of the internal control components relevant to identification and assessment of risks that would prevent the service organization from achieving its service commitments and system requirements and the design, implementation, and operation of controls to address them. The description would separately identify controls at the service organization and controls at the subservice organization. However, there is no prescribed format for differentiating between the two. *Carve-out method.* When service organization management elects the carve-out method, consideration may be given to disclosure of the identity of the subservice organization when such information may be useful to user entities or business partners who want to obtain information about and perform procedures related to the services provided by the subservice organization. Complementary subservice organization controls (CSOCs) are controls that service organization management assumed, in the design of the system, would be implemented by subservice organizations and are necessary, in combination with controls at the service organization to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. When using the carve-out method, the description would identify the types of CSOCs that the subservice organization is assumed to have implemented. It is important that the description also includes the subservice organization's responsibilities for implementing those CSOCs and indicates that the related service commitments and system requirements can be achieved only if the CSOCs are suitably designed and operating effectively during the period addressed by the description. To be meaningful to report users, management includes only CSOCs that are specific to the services provided by the system being described. CSOCs may be presented as broad categories of controls or types of controls rather than as individual controls. Service organization management may wish to include in the description a table that identifies those instances in which service commitments and system requirements are achieved solely by the service organization's controls and those in which a combination of controls at the service organization and CSOCs are needed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. Examples of CSOCs include the following:

Description Criteria	*Implementation Guidance*
iv. The portions of the system that are attributable to the subservice organization *b.* When service organization management decides to use the carve-out method: i. The nature of the service provided by the subservice organization ii. Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization iii. The types of controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization	• Controls relevant to the completeness and accuracy of transaction processing on behalf of the service organization • Controls relevant to the completeness and accuracy of specified reports provided to and used by the service organization • General IT controls relevant to the processing performed for the service organization • Data centers are protected against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). The description is presented in accordance with this criterion if the CSOCs are complete, accurately described, and relevant to the service organization's achievement of the service commitments and system requirements related to the system being described. *Other matters.* A service organization that uses multiple subservice organizations may prepare its description using the carve-out method for one or more subservice organizations and the inclusive method for others. Regardless of the method service organization management selects, the description needs to disclose controls designed to provide reasonable assurance that the service organization's service commitments and system requirements are achieved, which include controls that the service organization uses to monitor the services provided by the subservice organization. Such monitoring controls may include, but are not limited to, a combination of the following: • Testing of controls at the subservice organization by members of the service organization's internal audit function • Reviewing and reconciling output reports • Holding periodic discussions with the subservice organization personnel and evaluating subservice organization performance against established service level objectives and agreements • Making site visits to the subservice organization • Inspecting type 2 SOC 2® reports on the sub-

Description Criteria	*Implementation Guidance*
that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved (commonly referred to as complementary subservice organization controls or CSOCs)	service organization's system • Monitoring external communications, such as complaints from user entities relevant to the services performed by the subservice organization
DC 8: Any specific criterion of the applicable trust services criteria that is not relevant to the system and the reasons it is not relevant	If one or more applicable trust services criteria are not relevant to the system being described, service organization management includes in the description an explanation of why such criteria are not relevant. For example, an applicable trust services criterion may not be relevant if it does not apply to the services provided by the service organization. Assume user entities—not the service organization—collect personal information from the user entities' customers. When the description addresses controls over privacy, service organization management would not disclose in its description the user entities' controls over collection; however, the reason for that omission would be disclosed. In contrast, the existence of a policy prohibiting certain activities is not sufficient to render a criterion not applicable. For example, when the description addresses controls over privacy, it would be inappropriate for service organization management to omit from the description disclosures of personal information to third parties based only on the fact that the service organization's policies forbid such disclosures. Instead, the description would describe the policies

Description Criteria	*Implementation Guidance*
	and related controls for preventing or detecting such disclosures.
DC 9: In a description that covers a period of time (type 2 examination), the relevant details of significant changes to the service organization's system and controls during that period that are relevant to the service organization's service commitments and system requirements	Significant changes to be disclosed consist of those that are likely to be relevant to the broad range of report users. Disclosure of such changes is expected to include an appropriate level of detail, such as the date the changes occurred and how the system differed before and after the changes. Examples of significant changes to a system include the following: • Changes to the services provided • Significant changes to IT and security personnel • Significant changes to system processes, IT architecture and applications, and the processes and system used by subservice organizations • Changes to legal and regulatory requirements that could affect system requirements • Changes to organizational structure resulting in a change to internal control over the system (for example, a change to the legal entity)

Transition Guidance

.20 The description criteria presented in this document (2018 description criteria) have been designed to be used in conjunction with the use of the 2017 trust services criteria set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in a SOC 2® report. The 2018 description criteria will be codified as DC section 200 in AICPA, *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) will be codified as DC section 200A.

.21 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), either the 2018 description criteria or the 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

.22 When preparing 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 should be used.

Appendix — Glossary

.23

For purposes of this document, the following terms have the meanings attributed as follows:

applicable trust services criteria. The criteria codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, and TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), used to evaluate controls relevant to the trust services category or categories included within the scope of a particular examination.

board or board of directors. Individuals with responsibility for overseeing the strategic direction of the service organization and the obligations related to the accountability of the service organization. Depending on the nature of the service organization, such responsibilities may be held by a board of directors or supervisory board for a corporation, a board of trustees for a not-for-profit service organization, a board of governors or commissioners for a government service organization, general partners for a partnership, or an owner for a small business.

boundaries of the system (or system boundaries). The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. When systems for multiple services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each system will differ. In a SOC 2® engagement that addresses the confidentiality and privacy criteria, the system boundaries cover, at a minimum, all the system components as they relate to the life cycle of the confidential and personal information within well-defined processes and informal ad hoc procedures.

business partner. An individual or business (and its employees), other than a vendor, who has some degree of involvement with the service organization's business dealings or agrees to cooperate, to any degree, with the service organization (for example, a computer manufacturer who works with another company who supplies it with parts).

carve-out method. Method of addressing the services provided by a subservice organization in which the components of the subservice organization's system used to provide the services to the service organization are excluded from the description of the service organization's system and from the scope of the examination. However, the description identifies (1) the nature of the services performed by the subservice organization; (2) the types of controls expected to be performed at the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and (3) the controls at the service organization used to monitor the effectiveness of the subservice organization's controls.

complementary subservice organization controls. Controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

complementary user entity controls. Controls that service organization management assumed, in the design of the service organization's system, would be implemented by user entities and are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved.

controls at a service organization. The policies and procedures at a service organization that are part of the service organization's system of internal control. Controls exist within each of the five COSO internal control components: control environment, risk assessment, control activities, information and communication, and monitoring. The objective of a service organization's system of internal control is to provide reasonable assurance that its service commitments and system requirements are achieved.

controls at a subservice organization. The policies and procedures at a subservice organization that are relevant to the service organization's achievement of its service commitments and system requirements.

criteria. The benchmarks used to measure or evaluate the subject matter.

external users. Users, other than entity personnel, who are authorized by entity management, customers, or other authorized persons to interact with the entity's information system.

inclusive method. Method of addressing the services provided by a subservice organization in which the description of the service organization's system includes a description of the (*a*) the nature of the services provided by the subservice organization and (*b*) the components of the subservice organization's system used to provide services to the service organization, including the subservice organization's controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. (When using the inclusive method, controls at the subservice organization are subject to the service auditor's examination procedures. Because the subservice organization's system components are included in the description, those components are included in the scope of the examination.)

information life cycle. The collection, use, retention, disclosure, disposal, or anonymization of confidential or personal information within well-defined processes and informal ad hoc procedures.

intended users. Individuals or entities that the service organization intends will be report users.

internal control. A process, effected by a service organization's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

operating effectiveness (or controls that are operating effectively). Controls that operated effectively provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria.

personal information. Information that is about, or can be related to, an identifiable individual.

policies. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures.

privacy notice. A written communication by entities that collect personal information to the individuals about whom personal information is collected that explains the entity's (*a*) policies regarding the nature of the information that they will collect and how that information will be used, retained, disclosed, and disposed of or anonymized and (*b*) commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information, the choices that individuals have related to their personal information, the security of such information, and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

report users (specified users or specified parties) of a SOC 2® report. In this document, the term refers to users of a SOC 2® report. The service auditor's report included in a SOC 2® report ordinarily includes an alert restricting the use of the report to specified parties who possess sufficient knowledge and understanding of the service organization and the system to understand the report. The expected knowledge is likely to include an understanding of the following matters:

- 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 achieve the service organization's service commitments and system requirements
- 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

Users likely to possess such knowledge include user entities and their personnel, business partners and their personnel, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who understand how the service organization's system may be used to provide the services.

service auditor. As used in this document, a CPA who performs a SOC 2® examination of controls within a service organization's system relevant to security, availability, processing integrity, confidentiality, or privacy.

service commitments. Declarations made by service organization management to user entities and others (such as user entities' customers) about the system used to provide the service. Service

commitments can be communicated in written individualized agreements, standardized contracts, service-level agreements, or published statements (for example, in a security practices statement).

service organization. An organization, or segment of an organization, that provides services to user entities.

SOC 2® examination. An examination engagement to report on whether (*a*) the description of the service organization's system is in accordance with the description criteria, (*b*) the controls were 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 (*c*) in a type 2 report, the controls 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. The SOC 2® examination is performed in accordance with the attestation standards 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*.

subsequent events. Events or transactions that occur after the specified period covered by the engagement, but prior to the date of the service auditor's report, which could have a significant effect on the evaluation of the presentation of the description of the service organization's system or the evaluation of the suitability of design and operating effectiveness of controls.

subservice organization. A vendor used by a service organization that performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

suitability of design (or suitably designed controls). Controls are suitably designed if they have the potential to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved. Suitably designed controls are operated as designed by persons who have the necessary authority and competence to perform the control.

system. Refers to the infrastructure, software, procedures, and data that are designed, implemented, and operated by people to achieve one or more of the organization's specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements.

system components. Refers to the individual elements of a system, which may be classified into the following five categories: infrastructure, software, people, procedures, and data.

system event. An occurrence that could lead to the loss of, or disruption to, operations, services, or functions and result in a service organization's failure to achieve its service commitments or system requirements. Such an occurrence may arise from actual or attempted unauthorized access or use by internal or external parties and (*a*) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems, (*b*) result in unauthorized disclosure or theft of information or other assets or the destruction or corruption of data, or (*c*) cause damage to systems. Such occurrences also may arise from the failure of the system to process data as designed or from the loss, corruption, or destruction of data used by the system.

system incident. A system event that requires action on the part of service organization management to prevent or reduce the impact of the event on the service organization's achievement of its service commitments and system requirements.

system requirements. Specifications about how the system should function to (*a*) meet the service organization's service commitments to user entities and others (such as user entities' customers); (*b*) meet the service organization's commitments to vendors and business partners; (*c*) to comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (*d*) achieve other objectives of the service organization that are relevant to the trust services categories addressed by the description. Requirements are often specified in the service organization's system policies and procedures, system design documentation, contracts with customers, and government regulations.

user entity. An entity that uses the services provided by a service organization.

vendor. An individual or business (and its employees) engaged to provide services to the service organization. Depending on the services a vendor provides (for example, if it operates certain controls on behalf of the service organization that are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved), a vendor might also be a subservice organization.