AICPA

DC Section 300

Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report

Supplement A

2020 Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report

This supplement contains authoritative AICPA Assurance Services Executive Committee material.

The description criteria and related implementation guidance in this supplement have been extracted from DC section 300, *2020 Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report*,[1] issued in March 2020 by the AICPA's Assurance Services Executive Committee. The complete text may be found at https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html.

Description Criteria	*Implementation Guidance*
The description contains the following information applicable to the system and the trust services category or categories addressed by the description:	When making judgments about the nature and extent of disclosures to include, consider the following:
DC1: The types of goods produced, manufactured, or distributed by an entity	The description is expected to include disclosures about the types of products the entity produces, manufactures, or distributes and the system or systems that produce, manufacture, or distribute the products. Disclosures are made only to the extent that they relate to the trust services category or categories addressed by the description. A description can address a system and controls the entity uses to produce, manufacture, or distribute a physical product, such as an airplane engine, or an intangible product, such as commercial off-the-shelf (COTS) software; systems and controls the entity uses to operate a production line; or all systems and controls the entity uses to produce, manufacture, or distribute goods produced or manufactured within a specific facility or physical plant. The types of products addressed will depend on the nature of the entity: • *Producers.* Producers include entities that extract raw materials through operations that remove metals, minerals, and aggregates from the earth (such as oil and gas extraction, mining, dredging, and quarrying); produce food, feed, fiber, and other products by the cultivation of certain plants and the raising of domesticated animals (livestock); and develop software for on-site installation.

(continued)

[1] All DC sections can be found in AICPA *Description Criteria*.

Description Criteria	*Implementation Guidance*
	• *Manufacturers.* Manufacturers include entities that transform raw materials or components into other components or finished goods for use or sale using labor and machines, tools, chemical and biological processes, fabrication, or formulation. The components or finished goods may be sold to other manufacturers for the production of other products such as aircraft, computers or computer parts, household appliances, furniture, sports equipment, or automobiles. In other cases, the finished goods may be sold to wholesalers that, in turn, sell them to retailers that then sell them to end users and consumers. Manufacturers include contract manufacturers that outsource manufacturing for other entities. • *Commercial software developers.* Commercial software developers are entities that develop and sell commercial software. • *Distribution companies.* Distribution companies include entities that provide or manage all or a significant part of another entity's logistics, including one or a combination of the following: inbound freight; customs; warehousing; inventory management; order fulfillment, including picking and repackaging of items; distribution; or outbound freight. Such companies include third-party logistics (3PL or TPL) companies.
DC2: The principal product performance specifications, commitments, and requirements and production, manufacturing, or distribution commitments and requirements (principal system objectives)	For a specific production, manufacturing, or distribution system, entity management designs and implements processes and procedures to achieve certain specific objectives (referred to as *system objectives*) related to the goods produced or distributed and the system — including related controls — implemented and operated to mitigate risks that would prevent the entity from achieving those objectives. Entity management discloses the system objectives that it concludes are likely to influence the decision-making of intended users (referred to as *principal system objectives*) in the description to help users understand the objectives that drive the operation of the system and how the applicable trust services criteria were used to evaluate whether controls were effective. Depending on the trust services category or categories addressed by the description, the principal system objectives often relate primarily to the following: • Commitments regarding protection of the system from cybersecurity risks • The product meeting the product performance specifications that have been communicated to or agreed upon with customers • The product's conformity with other commitments made to customers • The product's conformity with product requirements established by the entity, law or regulation, industry standards, or customers' requirements • The product's availability in the quantities and at the times agreed upon with customers • The achievement of delivery commitments made to customers, including the timing of delivery, storage and transportation commitments, and the system requirements necessary to achieve those commitments

Description Criteria	*Implementation Guidance*
	• Distribution of the product in accordance with applicable laws and regulations regarding timing, storage, and transportation • The achievement of other objectives established by the entity for the manufacturing, production, or distribution system Certain commitments an entity makes to customers or business partners may not relate to security, availability, processing integrity, confidentiality, or privacy but may still be relevant to users. For example, dramatic price increases in the cost of raw materials may prevent the entity from delivering goods at contracted prices. The description of the system is not expected to address financial risks such as this this. Entity management is also responsible for designing, implementing, and operating controls to provide reasonable assurance that the entity achieves its principal system objectives. In determining the entity's principal system objectives, entity management may wish to consider the following potential categories of system objectives: *Product Performance Specifications* For a product, principal system objectives include producing or manufacturing a product that meets product performance specifications to the extent that those specifications relate to the trust services category or categories addressed by the description. Product performance specifications may address the physical characteristics or functionality of a product and are often published, specified in contracts, or otherwise communicated to customers. *Production, Manufacturing, or Distribution Specifications* For customers and business partners, it may be important to understand not only whether the product meets its specifications but also how production, manufacturing, or distribution occurs. For example, a business partner may establish specifications for the entity's use of the business partner's intellectual property during the production process; alternatively, a pharmaceutical entity may establish specifications for a product to be maintained at a specific temperature during the distribution process. To the extent that those specifications relate to the trust services category or categories addressed by the description, such production, manufacturing, or distribution specifications are likely to be objectives of the system. Often, for products to meet specifications, commitments, and requirements, electronics and onboard logic within the product need to meet certain requirements. When describing the system in this situation, entity management may need to consider specifications related to those portions of the system that create and implement executable logic embedded in the product (whether in software or hardware) as well as the hardware and software that produce and distribute the product.

(continued)

Description Criteria	*Implementation Guidance*
	Other Commitments In addition to meeting specific product, production, manufacturing, or distribution specifications, entities often make other commitments to customers and business partners. To the extent that those commitments relate to the trust services category or categories addressed by the description, the principal system objectives include those commitments. For example, an entity may make commitments about conforming with a variety of other standards and criteria, such as the risk management framework issued by the National Institute of Standards and Technology (NIST), cybersecurity standards issued by the International Organization for Standardization (ISO), or Food and Drug Administration (FDA) regulations on electronic records and electronic signatures included in Title 21 CFR Part 11. An entity may also make commitments on many different aspects of the product or its distribution, including commitments related to a product's performance specifications and availability. Additionally, an entity may make commitments related to one or more of the trust services categories addressed by the description. For example, if controls over privacy are addressed by the description, an entity may make commitments such as the following: • The entity will not process or transfer information without obtaining the data subject's consent. • The entity will provide a privacy notice to customers once every six months or when there is a change in its privacy policy. The commitments an entity makes to customers, business partners, and others are based on the needs of those entities. In identifying the commitments to be disclosed, entity management may begin by reviewing the specific commitments it has made to customers and business partners. Commitments may be communicated 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. As previously discussed, entity management may limit its disclosures to those commitments relevant to intended users (that is, the principal commitments). For example, entity management often makes the same product-availability commitment to its customers. Because information about the availability commitment is likely to be relevant to customers, entity management would describe that principal availability commitment in the description when the description addresses availability. If, however, entity management makes different commitments about product availability to an individual customer, that system objective ordinarily would not be disclosed in the description; this is because information about that specific customer commitment is unlikely to be relevant to other intended users. When the description addresses privacy, entity management discloses the commitments and system requirements identified in the entity's privacy notice or privacy policy that are relevant to the system being described. When making such disclosures, it may also be helpful to users if entity management describes the purposes, uses, and disclosures of personal information as permitted by agreements.

Description Criteria	*Implementation Guidance*
	Product Requirements In addition to specifications and commitments regarding products, the product itself may need to meet other requirements to meet those specifications or commitments. The product may also be subject to legal, regulatory, or other requirements. For example, COTS software may need to meet a specific set of requirements to function properly with a particular operating system; in the same way, food labeled as being organic may need to meet a specific set of requirements to be so labeled. *Production, Manufacturing, or Distribution Requirements* In addition to specifications and commitments, production, manufacturing, or distribution systems may be subject to requirements about how the system should function to accomplish the following: • Meet product performance specifications, commitments, or requirements • Meet the entity's production, manufacturing, or distribution commitments to customers and others (such as customers' customers) • Meet the entity's commitments to suppliers and business partners • Comply with applicable laws and regulations as well as guidelines of industry groups, such as business or trade associations • Achieve other objectives of the entity relevant to the trust services category or categories addressed by the description Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations. Examples of system requirements include the following: • Workforce member background checks established in government regulations for handling hazardous materials • Acceptable temperature ranges during product manufacturing • Software quality and security standards such as those issued by the Open Web Application Security Project, the Consortium for IT Software Quality, and the ISO • Labeling and tagging standards, including any associated metadata requirements, established by industry groups or other bodies • Business processing rules and standards established by regulators, such as the security requirements mandated by the Health Insurance Portability and Accountability Act System requirements may result from the entity's commitments relating to one or more of the trust services categories (for example, a commitment to programmatically enforce segregation of duties between production and quality control creates system requirements regarding user-access administration). The principal system requirements that need to be disclosed are those relevant to the trust services category or categories addressed by the description and likely to be relevant to users. In identifying which system requirements to disclose, entity management

(continued)

Description Criteria	*Implementation Guidance*
	may consider internal policies 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 profit margin for the products associated with the system ordinarily would not be relevant to users; therefore, they need not be disclosed.
DC3: For identified system incidents that were the result of controls that were not effective or otherwise resulted in a significant failure in the achievement of one or more of the entity's principal system objectives during the period addressed by the description,[10] the following information: *a.* Nature of each incident *b.* Timing surrounding the incident *c.* Extent (or effect) of the incident and its mitigation and remediation	Judgment is needed when determining whether to disclose a system incident. Consideration of the following matters as they relate to the system and the trust services category or categories being described may help make that determination: • Whether the incident resulted from one or more controls, including controls at a carved-out supplier, that did not provide reasonable assurance that the entity achieved one or more of its principal system objectives • Whether the incident resulted in a significant failure in the achievement of one or more of the entity's system objectives • Whether public disclosure of the incident was required (or is likely to be required) by laws or regulations • Whether the incident resulted in sanctions by any legal or regulatory agency Disclosures about identified system 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 and thereby compromise the entity's ability to achieve its system objectives. Rather, the disclosures are intended to enable users to understand the nature of the risks faced by the entity and the impact of the realization of those risks. For example, assume that an entity identified a security breach that resulted in its failure to achieve one or more of its system objectives. The breach occurred six months prior to the start of the period addressed by the description and had not been fully remediated during the period addressed by the description. In this example, entity management would likely need to disclose the incident in the description to enable users to understand the nature of the risks faced by the entity and the impact of the realization of those risks. Processes and controls related to mitigation and remediation of incidents are addressed by the requirements set forth in DC5.

[10] If the description addresses only implemented controls as of a point in time, this disclosure relates to identified system incidents that (*a*) were the result of controls that were not effective or (*b*) otherwise resulted in a significant failure in the achievement of one or more of the entity's principal system objectives as of the date of the description.

Description Criteria	*Implementation Guidance*
DC4: Risks that may have a significant effect on the entity's ability to achieve its principal system objectives	Disclosures about risks that may have a significant effect on the entity's ability to achieve its principal system objectives are limited to those that relate to the trust services category or categories addressed by the description. Such risks may include those arising from (1) characteristics of the production, manufacturing, or distribution system and underlying information systems, use of suppliers, and delivery channels used by the entity; (2) organizational and user characteristics; and (3) physical, environmental, technological, organizational, and other changes during the period addressed by the description. These categories of risks are discussed in further detail in the following paragraphs. *Characteristics of the production, manufacturing, or distribution system and underlying information systems, use of suppliers, and delivery channels used by the entity.* Disclosures about the risks related to these matters may include the following: • Nature and importance of key product and production specifications, commitments, and requirements • Use of supporting information systems such as overall architecture, code-to-control production machinery, cloud computing, and other IT-hosted services • The types and number of employee personnel (finance, administrative, operations, IT, sales and marketing, and so on) and third parties (contractors, supplier employees, business partners, and so on) with access to the entity's system • Use of suppliers (for example, raw materials or component suppliers such as subassemblies or embedded technology and logic) that produce, manufacture, or distribute products or software, including confidential intellectual property, service providers, and other third parties the entity depends on to achieve its system objectives • Types of physical and logical access of third parties to plants, locations, and information systems • Types of production, manufacturing, or distribution equipment, related technology and infrastructure used, and the source of such equipment, applications, and infrastructure (for example, whether software is internally developed or purchased without modification) • Nature of external-facing web applications and the nature of applications developed in-house • Dependency on strategically significant production, manufacturing, or distribution equipment and systems that are no longer made or supported or equipment and systems that would be difficult to repair or replace in the event of failure • Dependency on IT equipment and information systems critical to the production, manufacturing, or distribution processes and those based on emerging technologies

(continued)

Description Criteria	*Implementation Guidance*
	Organizational and customer characteristics. Disclosures about the risks related to organizational and customer characteristics may include the following: • The size and structure of the entity (for example, centralized versus decentralized, insourced or outsourced) • Types of business partners and other third parties, such as suppliers, significant to the operation of the system's products or services • Whether the entity's production, manufacturing, or distribution assets, employees, customers, suppliers, or business partners are in countries or regions deemed high risk by entity management as part of its risk assessment process • The distribution of responsibilities related to the production, manufacturing, or distribution risk management program between business functions (for example, operating units, risk management, production management, and legal) • Business units with production, manufacturing, or distribution systems administered under a separate management structure (for example, outside of a centralized production, manufacturing, or distribution function) *Physical, environmental, technological, organizational, and other changes.* Disclosures about the risks related to physical, environmental, technological, organizational, and other changes at the entity and in its environment during the period addressed by the description may include the following: • Changes to the entity's principal production, manufacturing, or distribution methods • Changes to business unit, production, manufacturing, or distribution, or to supporting IT and related personnel • Changes to risk assessment and controls monitoring processes that result from the failure of controls designed to achieve product performance specifications, commitments, and requirements • Significant changes to the entity's production, manufacturing, or distribution processes; supporting IT architecture and applications; and the processes and systems used by suppliers • Changes to legal and regulatory requirements that affect production, manufacturing, or distribution systems • Divestitures and other cessations of operations, particularly those (if any) that have ongoing service support obligations for production, manufacturing, or distribution related to those operations and the status of those activities

Description Criteria	*Implementation Guidance*
DC5: Relevant information about the system that produces, manufactures, or distributes the products, including the following: *a.* Components of the system, to include i. infrastructure, ii. software, iii. people, iv. procedures, and v. data *b.* Significant inputs used by the system (raw materials and other inputs) *c.* Boundaries of the system, when necessary to prevent users from misunderstanding the system being described	Disclosures about system components are made only to the extent that they relate to the trust services category or categories addressed by the description. *Infrastructure* Disclosures about the infrastructure component of a system (that is, production and distribution equipment, including IT equipment used to support production, manufacturing, or distribution) include matters such as the collection of physical or virtual resources that supports an overall production, manufacturing, or distribution environment, including the physical environment and related structures, production and manufacturing systems, 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 entity uses to produce, manufacture, or distribute the products. *Software* Disclosures about software used in the production, manufacturing, or distribution process include matters such as the application programs (including, if applicable, industrial control systems), programmable logic on devices used in production, the IT system software that supports those application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing 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, entity management, operation, security, and use of the system (business unit personnel, production line personnel, developers, operators, customer personnel, supplier personnel, and managers). *Procedures* Disclosures about the automated and manual procedures implemented by the entity primarily relate to those through which production, manufacturing, or distribution occur. These include, as appropriate, procedures through which production and manufacturing is initiated, authorized, and occurs; the procedures through which products are distributed; quality control procedures; and the processes by which reports and other information are prepared and distributed. A *process* consists of a series of linked procedures designed to accomplish a goal (for example, the process for assembling a product or managing third-party risks). *Procedures* are the specific actions undertaken to implement a process (for example, the procedure to assess and manage the requisition and engagement of suppliers). For that reason, entity management may find it easier to describe procedures in the context of the process of which they are a part. Procedures may include those necessary to design, create, or implement and maintain other components of the system, such as infrastructure, software, and data relevant to the trust services categories addressed in the description. They may also include procedures designed to measure whether raw materials and other inputs meet management-specified requirements for such inputs.

(continued)

Description Criteria	*Implementation Guidance*
	Policies Policies are entity management or board 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 entity deploys control activities through policies that establish what is expected and procedures that put policies into action. *Data* Disclosures about the data component include the types of data used by information systems, transaction streams, files, databases, tables, and output used or processed by such systems. 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 entity 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, entity management would address, at minimum, all system components as they relate to the information life cycle of the confidential and personal information used in producing, manufacturing, or distributing the products within well-defined processes and informal ad hoc procedures. System components may also be described using specific technical terms that help create a clearer understanding of the entity's system and system boundaries. The following paragraphs provide additional guidance on disclosures related to the components of the system or systems that may be included in the description. *Raw Materials and Other Inputs* Although not part of the system, raw materials are often necessary for a product to be produced or manufactured. For that reason, it is useful to describe significant raw materials or other inputs (for example, purchased components) used in the production or manufacturing process. Such disclosures help users better understand the production or manufacturing system addressed by the description. *Boundaries of the System* Not all activities performed at the entity are part of the system being described. Determining the functions or processes outside the boundaries of the system and describing them in the description may be necessary to prevent users from misunderstanding the boundaries of the system. Therefore, if there is a risk that 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.

Description Criteria	*Implementation Guidance*
	For example, because they are unlikely to be relevant to the achievement of the principal system objectives related to security, availability, processing integrity, confidentiality, and privacy, the following functions or processes at the entity may be outside the boundaries of the system being described: • The movement of materials between workstations on the production floor or the processes used to transport work-in-process inventory to the finished goods warehouse • Processes used to collect and report on sustainability matters that do not directly affect the finished product For entities that distribute products, the boundaries of the distribution system to be included in the description may include the following matters, as applicable: • The geographic region served • Transportation methods used • Types of products transported • Whether the entity repackages products produced or manufactured by others • Whether the entity provides special handling services
DC6: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the entity's principal system objectives were achieved	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*,[11] presents the criteria for each trust services category. A description is presented in accordance with this criterion when it includes information about each criterion related to the trust services category or categories addressed 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, entity 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.
DC7: If a customer's controls are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives would be achieved, those complementary customer controls	Customers often have a role in production, manufacturing, or distribution processes. Fulfilling those responsibilities is necessary for the customer to meet its goals in using an entity as a supplier or distributor. For example, the customer of a logistics company that provides fulfillment services is responsible for providing complete and accurate recipient information and communicating the items to be packaged and delivered. Such responsibilities are referred to as *customer responsibilities*. Because customer responsibilities can be voluminous, ordinarily they are not disclosed in the description; usually they are communicated through product documentation or user manuals. However, entity management would ordinarily disclose in the description the types of communications it makes to customers about their responsibilities.

(continued)

[11] All TSP sections can be found in AICPA *Trust Services Criteria*.

Description Criteria	*Implementation Guidance*
	In most cases, successful performance of customer responsibilities is not necessary for the entity to achieve its system objectives. In limited circumstances, however, a customer must have controls in place to provide reasonable assurance that its customer responsibilities are performed in a defined manner for the entity to achieve its system objectives. Such controls are referred to as *complementary customer controls* (CCCs). Consider, for example, a situation in which an entity installs a server at a customer's data center to enable customer access to the entity's production management system. The customer needs to implement physical access controls to protect the components of the entity's system installed at its data center for the entity to achieve its principal system objectives based on trust services criterion CC6.4. This criterion states, "The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to achieve the entity's objectives." When CCCs are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives are achieved, those CCCs are disclosed in the description along with the applicable trust services criteria to which they relate. Disclosures about CCCs are made only to the extent that they relate to the trust services category or categories addressed by the description. In some situations, a customer responsibility that appears to be a CCC is not. For example, a manufacturer may permit a customer's employees to access information systems and alter its production schedules. If a customer access administrator is responsible for issuing employee credentials and all actions performed by customer employees are the responsibility of the customer, then achievement of the entity's principal system objectives does not depend on the authorized and appropriate use of the customer employee credentials based on trust services criterion CC6.2. This criterion states the following: 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.
DC8: If a supplier's controls are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives are achieved and *a.* the entity is using the carve-out method (most common), the following: i. The nature of the products produced, manufactured, or distributed or the services provided by the supplier ii. Each applicable trust services criterion that is intended to be met by controls at the supplier	An entity that produces, manufactures, or distributes products obtains raw materials, components, or other goods (such as production equipment) from suppliers. It also may outsource various processing functions (such as the provision of IT networks) to service providers. A supplier may be a separate entity external to the entity or it may be a related entity, such as a subsidiary of the same company that owns the entity. In most situations, disclosure of the existence of suppliers is necessary to enable intended users to understand the system. In most cases, an entity is likely to have effective controls over the quality of raw materials, subassemblies, other goods, and system components (including services) obtained from suppliers to provide reasonable assurance of achieving its system objectives. Examples of situations in which an entity may have effective controls over a supplier's goods or services to achieve its principal system objectives include the following:

Description Criteria	*Implementation Guidance*
iii. The types of controls that entity management assumed, in the design of the entity's system, would be implemented by the supplier and are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives are achieved; such controls are commonly referred to as *complementary supplier controls* or *CSCs* *b.* the entity is using the inclusive method, the following: i. The nature of the products produced, manufactured, or distributed or the services provided by the supplier ii. The portions of the system that are attributable to the supplier iii. Relevant aspects of the supplier's infrastructure, software, people, procedures, and data iv. The controls at the supplier that are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives are achieved	• An entity has a robust quality inspection process for all inputs to the system that it executes on receipt of goods from the supplier. This process includes inspection of shipping containers and boxes for physical damage; statistical selection of sample inputs for measurement against input specifications and requirements; and visual inspection of inputs by production personnel. In this case, the entity's controls are sufficient to reduce the risk that inputs do not comply with specifications. • An entity has robust controls, including change-management controls, over the system a supplier uses to produce new software; the entity then uses the new software in its production process. In such cases, the entity's monitoring of the supplier's system and controls is sufficient for the entity to achieve its system objectives. • A supplier is responsible for performing quarterly maintenance on an entity's backup power system in an examination that addresses availability. If the entity implements its own monitoring controls over the supplier's controls, then the supplier's controls would not be necessary for the entity to achieve its system objectives. • An entity outsources its application development testing to a supplier and stipulates in its supplier contract that the supplier is responsible for performing certain controls that the entity deems necessary to address the risks related to doing business with the supplier. The entity designates an entity employee to oversee the outsourced services; that employee compares the supplier's test plans, test scripts, and test data to the entity's application change requests and detailed design documents. This entity employee also reviews the results of testing performed by the supplier before changes to the application are approved by the supplier and submitted to the entity for user-acceptance testing. The supplier's controls may not be necessary for the entity to assert that its controls provide reasonable assurance that the entity's availability commitments were achieved based on the applicable trust services criteria. In other situations, however, the entity may not have such controls. For example, an entity that sources subassemblies that contain embedded software may be unable to directly assess the quality and security of that software. In that case, the entity would delegate certain responsibilities to the supplier and expect the supplier to perform specific controls over the processes used to produce or deliver the subassemblies. As a result, effective supplier controls may be necessary for the entity to achieve its principal system objectives. *Carve-Out Method* When controls performed by the supplier are necessary, in combination with the entity's controls, to achieve the principal system objectives, such controls are referred to as *complementary supplier controls* (CSCs). Because CSCs are important to report users, they are disclosed in the description. The most common method for presenting CSCs is to include only those processes and controls whose performance is the responsibility of the entity and to identify the CSCs that the entity expects suppliers to implement. This method is known as the *carve-out method*.

(continued)

Description Criteria	*Implementation Guidance*
	When the carve-out method is used, the description identifies the types of CSCs that the supplier is expected to implement and the trust services criteria the CSCs affect. Consideration also may be given to disclosing the supplier's identity when such information might be useful to customers or business partners. CSCs are usually presented in tabular format toward the end of the description along with the trust services criteria to which each CSC relates. Entity management may request the practitioner's assistance when determining how to present the CSCs in the description. The practitioner can provide examples of CSC disclosures made by other entities and recommend improvements to the entity's presentation of the CSCs in the description. *Inclusive Method* In some situations, entity management might wish to present the relevant processes and controls of the supplier in its description either to meet the common information needs of users or because of the significance of the supplier's role in the process. This method of presentation is known as the *inclusive method*. Under the inclusive method, the relevant aspects of the supplier's infrastructure, software, people, procedures, and data are considered part of the entity's system; therefore, they are disclosed in the description and subject to the practitioner's examination procedures. The description separately identifies entity controls and supplier controls. However, there is no prescribed format for differentiating the two. When the inclusive method is used, supplier management is also a responsible party in the examination. Because of the additional complexities involved with the use of the inclusive method, entity and supplier management usually agree on the use of the inclusive method during engagement acceptance. *Other Matters* An entity that uses multiple suppliers may prepare its description using the carve-out method for one or more suppliers and the inclusive method for others. Regardless of the method entity management selects, the description needs to disclose controls designed to provide reasonable assurance that the entity's principal system objectives are achieved; these include controls the entity uses to monitor the services provided by the supplier. Such monitoring controls might include a combination of the following: • Quality control testing of inputs received • Testing of supplier controls by members of the entity's internal audit function • Reviewing and reconciling output reports • Holding periodic discussions with supplier personnel and evaluating supplier performance against established service-level objectives and agreements • Visiting the supplier site • Inspecting attestation reports on the supplier's system • Monitoring external communications, such as customer complaints, relevant to the products or services provided by the supplier

Description Criteria	*Implementation Guidance*
DC9: Any specific applicable trust services criterion that is not relevant to the system and the reasons why it is not relevant	If one or more applicable trust services criteria are not relevant to the system being described, entity management includes in the description an explanation why such criteria are not relevant. An applicable trust services criterion may not be relevant if it does not apply to the production, manufacturing, or distribution services provided by the entity. For example, a seller of an implantable medical device uses an entity to implement the specific software configuration of electronic medical devices for each patient. In this case, it is the customers — not the entity — that collect personal information from the customers' patients. Medical information for each patient is provided by the patient's physician to the seller, who then forwards the information to the entity for the configuration data to be created and implemented on the device. When the description addresses controls over privacy, entity management would not disclose in its description the customers' controls over collection; however, the reasons for that omission would be disclosed. 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 entity management to omit from the description disclosures of personal information to third parties based only on the fact that the entity's policies forbid such disclosures. Instead, the description would describe the policies and related controls for preventing or detecting such disclosures.
DC10: Significant changes during the period addressed by the description[12] to the entity's system and controls that are relevant to the achievement of the entity's principal system objectives	Significant changes to be disclosed are those that are likely to be relevant to a broad range of 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. Significant changes to a system include the following examples: • Changes to production processes, including those that result from changes to product performance specifications • Changes to IT and security personnel • Changes to IT processes, IT architecture and applications, and the processes and system used by suppliers • 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, change from centralized to decentralized control or from insourced to outsourced control) • Changes to the risk assessment and controls monitoring processes that result from the failure of controls designed to achieve product performance specifications, commitments, and requirements Disclosures about significant changes to the system are made only to the extent that they relate to the trust services category or categories addressed by the description.

[12] When the description addresses only the suitability of design of implemented controls as of a point in time, this criterion is not applicable.

P: 000.000.000 | F: 000.000.000 | W: urlhere.org