AICPA

TSP Section 100

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus – 2022)

TSP Section 100

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)

Notice to Readers

The *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* (2017 TSC) presents control criteria established by the AICPA's Assurance Services Executive Committee (ASEC) for use in attestation or consulting engagements to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy of information and systems used to provide products or services (*a*) across an entire entity; (*b*) at a subsidiary, division, or operating unit level; (*c*) within a function relevant to the entity's operational, reporting, or compliance objectives; and (*d*) for a particular type of information used by the entity.

In developing and establishing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees*, [fn 1] designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA Council or the board of directors. Paragraph .A46 of AT-C section 105, *Concepts Common to All Attestation Engagements*, [fn 2] indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable.

Revisions in This Version

This version of the 2017 TSC has been modified to reflect new points of focus and edits to extant points of focus (collectively referred to as *revisions*) relevant to certain of the trust services criteria. As discussed in the "Background" section, points of focus represent important characteristics of the criteria. As such, they may assist both management and the practitioner when they are evaluating whether controls were suitably designed and operated effectively to achieve the entity's objectives based on the trust services criteria.

[fn 1] All BL sections can be found in AICPA *Professional Standards*.

[fn 2] All AT-C sections can be found in AICPA *Professional Standards*.

The changes to the points of focus in the 2022 revisions do not, in any way, alter the criteria in the 2017 TSC. Such criteria continue to be suitable criteria for use when evaluating controls in any trust services engagement.

Revisions to the points of focus were developed by ASEC's SOC 2® Working Group and ASEC's Data Privacy Working Group; these revisions were reviewed and approved by the chair of ASEC. The revised points of focus in this version are intended to better support application of the criteria in

- an environment of ever-changing technologies, threats and vulnerabilities, and other matters that may create additional risks to organizations.
- addressing changing legal and regulatory requirements and related cultural expectations regarding privacy.
- addressing data management (for example, data storage, backup, and retention), particularly when related to confidentiality.
- differentiating which points of focus related to privacy may apply only to an organization that is a data controller or only to an organization that is a data processor, as defined in the glossary. (Although this distinction is intended to assist management and the practitioner in identifying situations in which certain points of focus may be particularly relevant, the specific facts and circumstances of the organization's operations should be considered when identifying and applying points of focus in a trust services engagement.)

Background

.01 ASEC has developed a set of criteria (trust services criteria) to be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems used to provide products or services, or the confidentiality or privacy of information processed by the systems used to provide products or services at an entity, a division, or an operating unit of an entity. In addition, the trust services criteria may be used when evaluating the design and operating effectiveness of controls relevant to the security, availability, processing integrity, confidentiality or privacy of a particular type of information processed by one or more of an entity's systems or one or more systems used to support a particular function within the entity. This document presents the trust services criteria.

.02 As in any system of internal control, an entity faces risks that threaten its ability to achieve its objectives due to external and internal threats to the achievement of those objectives and the vulnerabilities of its systems, processes, and procedures. Such threats and vulnerabilities arise because of factors such as the following:

- The nature of the entity's operations
- The environment in which it operates

- The types of information generated, used, or stored by the entity
- The types of commitments made to customers and other third parties
- Responsibilities entailed in operating and maintaining the entity's systems and processes
- The technologies, connection types, and delivery channels used by the entity
- The use of third parties (such as service providers and suppliers), who have access to the entity's system, to provide the entity with critical raw materials or components or operate controls that are necessary, in combination with the entity's controls, to achieve the system's objectives
- Changes to the following:
  - — System operations and related controls
  - — Processing volume
  - — Key management personnel of a business unit, supporting IT, or related personnel
  - — Legal and regulatory requirements with which the entity needs to comply
- Introduction of new services, products, or technologies

An entity addresses these risks through the implementation of suitably designed controls that, if operating effectively, provide reasonable assurance of achieving the entity's objectives.

03 The trust services criteria set forth the outcomes that an entity's controls should ordinarily meet to achieve the entity's unique objectives. Therefore, the trust services criteria are intended to be used for evaluation and reporting, regardless of the specific controls implemented by management. This contrasts with the approach taken by process and controls frameworks, which mandate that the entity implement a specific set of controls. The trust services criteria recognize that there is no specific set of processes and controls that can effectively mitigate all the unique threats, vulnerabilities, and risks that entities face. Instead, each entity is responsible for establishing its own objectives, assessing the unique risks that threaten the achievement of those objectives, and implementing processes and controls to mitigate those risks to acceptable levels. Because each entity is unique, applying the trust services criteria in actual situations requires judgment.

.04 In addition to the trust services criteria, this document presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), in its *Internal Control — Integrated Framework* (the COSO framework), [fn 3] states that points of focus represent important

---

[fn 3]

characteristics of the criteria. Consistent with the COSO framework, the points of focus in this document may assist both management and the practitioner when they are evaluating whether controls were suitably designed and operated effectively to achieve the entity's objectives based on the trust services criteria.

.05 Some points of focus may not be suitable or relevant to the entity or to the engagement to be performed. In such situations, management may customize a particular point of focus or identify and consider other characteristics based on the specific circumstances of the entity.

.06 In some situations, management may consider additional points of focus based on the circumstances of the entity. For example, a service organization undergoing a SOC 2 examination may make a commitment about meeting the requirements of a process or control framework. In this case, the service organization would implement the set of controls detailed in the specific process or control framework. The evaluation of whether the service organization's controls were suitably designed and operated effectively based on the trust services criteria would include consideration of whether the implemented controls met the requirements of the process or control framework. In that situation, management and the practitioner are likely to consider the requirements of the process or control framework as additional points of focus.

.07 Use of the trust services criteria does not require an assessment of whether each point of focus is addressed. Users are advised to consider the facts and circumstances of the entity and its environment in actual situations in relation to the entity's objectives when evaluating the subject matter using the trust services criteria.

Organization of the Trust Services Criteria

.08 The trust services criteria presented in this document have been aligned to the 17 criteria (known as *principles*) presented in the COSO framework, which was revised in 2013. In addition to the 17 principles, the trust services criteria include additional criteria supplementing COSO principle 12: *The entity deploys control activities through policies that establish what is expected and procedures that put policies into action* (supplemental criteria). The supplemental criteria, which apply to the achievement of the entity's objectives relevant to a trust services engagement, are organized as follows:

- *Logical and physical access controls.* The criteria relevant to how an entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access
- *System operations.* The criteria relevant to how an entity manages the operation of a system and detects and mitigates processing deviations, including logical and physical security deviations
- *Change management.* The criteria relevant to how an entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made
- *Risk mitigation.* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners

.09 In addition to the 17 principles in the COSO framework, certain of the supplemental criteria are shared among all trust services categories (see the section "Trust Services Categories"). For example, the criteria related to logical access apply to the security, availability, processing integrity, confidentiality, and privacy categories. As a result, the trust services criteria consist of

- criteria common to all five of the trust services categories (common criteria) and
- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

.010 The common criteria provide specific criteria for addressing the following:

- The control environment (CC1 series)
- Information and communication (CC2 series)
- Risk assessment (CC3 series)
- Monitoring of controls (CC4 series)
- Control activities related to the design and implementation of controls (CC5 series)

The common criteria are suitable for evaluating the effectiveness of controls to achieve an entity's system objectives related to security; no additional control activity criteria are needed. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of (*a*) the common criteria and (*b*) the control activity criteria applicable to the specific trust services category or categories addressed by the engagement. The criteria for each trust services category addressed by the engagement are considered complete only if all the criteria associated with that category are addressed by the engagement.

Trust Services Category	***Common Criteria***	***Additional Category-Specific Criteria***
Security	X	N/A
Availability	X	X (A series)
Processing Integrity (Over the Provisioning of Services or the Production, Manufacturing, or Distribution of Goods)	X	X (PI series)
Confidentiality	X	X (C series)
Privacy	X	X (P series)

.11 The practitioner may report on any of the trust services categories of security, availability, processing integrity, confidentiality, or privacy, either individually or in combination with one or more of the other trust services categories. For each category addressed by the engagement, all criteria for that category are usually addressed. However, in limited circumstances, such as when the scope of the engagement is

to report on a system, a particular criterion may not be relevant to the services provided by a service organization and, consequently, is not applicable to the engagement. For example, when reporting on privacy for a service organization's system, criterion P3.1, *Personal information is collected consistent with the entity's objectives related to privacy*, is unlikely to be applicable for a service organization that does not directly collect personal information from data subjects.

Trust Services Categories

.12 The table in paragraph .29 presents the trust services criteria and the related points of focus. In that table, the trust services criteria are classified into the following categories:

a. *Security.* Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.

Security refers to the protection of

i. information during its collection or creation, use, processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

b. *Availability.* Information and systems are available for operation and use to meet the entity's objectives.

Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

c. *Processing integrity (over the provisioning of services or the production, manufacturing, or distribution of goods).* System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system

or functional level of an entity. In a SOC for Supply Chain examination, for example, processing integrity refers to whether processing is complete, valid, accurate, timely, and authorized to produce, manufacture, or distribute goods that meet the products' specifications.

d. *Confidentiality.* Information designated as confidential is protected to meet the entity's objectives.

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

e. *Privacy.* Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Although confidentiality applies to various types of sensitive information, *privacy* applies only to personal information.

The privacy criteria are organized as follows:

i. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.

ii. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

iii. *Collection.* The entity collects personal information to support the achievement of its objectives related to privacy.

iv. *Use, retention, and disposal.* The entity limits the use, retention, and disposal of personal information to support the achievement of its objectives related to privacy.

v. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to support the achievement of its objectives related to privacy.

vi. *Disclosure and notification.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to support the achievement of its objectives related to privacy.

vii. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to support the achievement of its objectives related to privacy.

viii. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

.13 As previously stated, the trust services criteria may be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the entity. As such, they may be used when evaluating whether the entity's controls were effective to meet the criteria relevant to any of those categories (security, availability, processing integrity, confidentiality, or privacy), either individually or in combination with controls in other categories.

.14 Because organizations and their customers and business partners have an increased dependence on technology and concerns about cybersecurity risks and their impact on operational processes, security controls are generally a primary area of focus for system users. As a result, the security category is addressed in most trust services engagements. When the security category is included in a trust services examination, ASEC has determined that the common criteria are suitable for evaluating the effectiveness of controls to achieve an entity's objectives related to security; no additional control activity criteria are needed. When the additional categories of availability, processing integrity, confidentiality, or privacy are included in an examination using the trust services criteria, a complete set of criteria consists of (*a*) the common criteria and (*b*) the control activity criteria applicable to the specific category.

.15 Although uncommon, there may be circumstances in which the security category is not addressed by a trust services examination. In this situation, a complete set of criteria consists of (*a*) the common criteria; (*b*) the control activity criteria applicable to the specific category; and (*c*) the control activity criteria relevant to those aspects of the common criteria that may affect the specific category addressed in the examination. For example, in a trust services examination that addresses only the availability category, logical and physical access controls, systems operations, and change management controls would be evaluated based on their effect on the objectives related to availability.

Application and Use of the Trust Services Criteria

.16 The trust services criteria were designed to provide flexibility in application and use for a variety of different subject matters. The following are the types of subject matter a practitioner may be engaged to report on using the trust services criteria:

- The effectiveness of controls within an entity's cybersecurity risk management program to achieve the entity's cybersecurity objectives using the trust services criteria relevant to security, availability, and confidentiality as *control criteria* in a SOC for Cybersecurity examination. [fn 4]

- The suitability of design and operating effectiveness of controls included in management's description of a service organization's system relevant to one or more of the trust services criteria over security, availability, processing integrity, confidentiality, or privacy throughout a specified period to achieve the entity's objectives based on those criteria in a type 2 SOC 2 engagement. A type 2 SOC 2 engagement, which includes an opinion on the operating effectiveness of controls, also includes a detailed description of tests of controls performed by the service auditor and the results of those tests. A type 1 SOC 2 engagement addresses the same subject matter as a type 2 SOC 2 engagement; however, a type 1 SOC 2 report does not contain an opinion on the operating effectiveness of controls nor a detailed description of tests of controls performed by the service auditor and the results of those tests. [fn 5]

- The design and operating effectiveness of a service organization's controls over a system relevant to one or more of the trust services criteria over security, availability, processing integrity, confidentiality, and privacy in a SOC 3® engagement. A SOC 3 report contains an opinion on the operating effectiveness of controls but does not include a detailed description of tests of controls performed by the service auditor and the results of those tests.

- The suitability of design and operating effectiveness of controls of an entity, other than a service organization, over one or more systems relevant to one or more of the trust services categories of security, availability, processing integrity, confidentiality, or privacy (for example, a SOC for Supply Chain examination).

- The suitability of the design of an entity's controls over security, availability, processing integrity, confidentiality, or privacy to achieve the entity's objectives based on the related trust services criteria. [fn 6]

.17 A practitioner may be engaged to report on compliance with laws, regulations, rules, contracts, or grant agreements. If a practitioner is engaged to report on controls over compliance with laws, regulations,

---

[fn 4] AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* (the cybersecurity guide) provides practitioners with performance and reporting guidance for a SOC for Cybersecurity examination.

[fn 5] AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* contains performance and reporting guidance for SOC 2 examinations.

[fn 6] AT-C section 9205, *Examination Engagements: Attestation Interpretations of Section 205*, addresses an engagement such as this in Interpretation No. 2, "Reporting on the Design of Internal Control" (par. .04–.14 of AT-C sec. 9205). That document states that a practitioner may examine the suitability of the design of controls under AT-C section 205, *Assertion-Based Examination Engagements*. Paragraph .10 of AT-C section 9205 also provides guidance on how a practitioner should report when the engagement addresses controls that have not yet been implemented.

rules, contracts, or grant agreements, the practitioner may perform an engagement in accordance with AT-C section 105 and AT-C section 205, *Assertion-Based Examination Engagements*). In such a situation, the practitioner would consider whether the trust services criteria are suitable for the engagement. If a practitioner is engaged to report on whether an entity has complied with certain laws, regulations, rules, contracts or grant agreements, the practitioner may perform a compliance engagement in accordance with AT-C section 105, AT-C section 205, and AT-C section 315, *Compliance Attestation*.

.18 Internal control helps organizations achieve their operational, compliance, and reporting objectives. Because the effectiveness of controls cannot be separated from the objectives that they are intended to achieve, many of the trust services criteria include the phrase *to meet the entity's objectives.* Because the trust services criteria may be used to evaluate controls relevant to a variety of different subject matters (see paragraph .16) in a variety of different types of engagements (see paragraphs .25–.28), interpretation of that phrase depends upon the specific circumstances of the engagement. Therefore, when using the trust services criteria, consideration is given to how the *entity's objectives* referred to in the criteria are affected by the subject matter and scope of the particular engagement.

.19 For example, consider the following engagements:

- In a SOC 2 engagement to examine and report on a service organization's controls over the security, availability, processing integrity, confidentiality, or privacy of a *system*, management is responsible for meeting its commitments to customers. Therefore, the *objectives* in a SOC 2 engagement relate *to meeting its service commitments to customers and system requirements. Service commitments* are the declarations made by management to customers regarding the performance of one or more of the entity's systems. Such commitments generally are included in written contracts, service-level agreements, or public statements (for example, a privacy notice). Some commitments are applicable to all customers (baseline commitments), whereas others are designed to meet individual customer needs and result in the implementation of processes or controls, in addition to those required to meet the baseline commitments. *System requirements* refer to how the system should function to achieve the entity's commitments to customers, relevant laws and regulations, guidelines of industry groups such as trade or business associations, or other business objectives.

- In a SOC for Supply Chain engagement to examine and report on an entity's controls over the security, availability, processing integrity, confidentiality, or privacy of a system used to produce, manufacture, or distribute products, management is responsible for establishing principal system objectives. Such objectives are embodied in the product commitments the entity makes to customers, including producing or manufacturing a product that meets product performance specifications and other production, manufacturing, or distribution specifications. Commitments may also relate to other matters (for example, conforming with a variety of other standards and criteria such as the risk entity management framework issued by the National Institute of Standards and Technology, the cybersecurity standards issued by the International Organization for Standardization (ISO), or Food and Drug Administration regulations on electronic records and electronic signatures included in Code of Federal Regulations, *Electronic Records; Electronic Signatures*, Title 21, Part 11).

- In an entity-wide SOC for Cybersecurity examination, the entity establishes *cybersecurity objectives.* Cybersecurity objectives are those that could be affected by cybersecurity risk and,

therefore, affect the achievement of the entity's compliance, reporting, and operational objectives. The nature of an entity's cybersecurity objectives will vary depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, and other factors. For example, a telecommunication entity may have a cybersecurity objective related to the reliable functioning of those aspects of its operations that are deemed to be critical infrastructure, whereas an online dating entity is likely to regard the privacy of the personal information collected from customers to be a critical factor in achieving its operating objectives. [fn 7]

.20 As an example of how the subject matter and engagement scope can affect the use of the trust services criteria, consider trust services criterion CC6.4:

> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

.21 In the SOC 2 engagement example discussed in paragraph .20, the phrase *to meet the entity's objectives* in CC6.4 usually would be interpreted as follows:

> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel *to meet the service organization's commitments and system requirements.*

.22 In addition, criterion CC6.4 would only be applied as it relates to controls over the trust services categories relevant to the systems included within the scope of the SOC 2 engagement.

.23 In the SOC for Cybersecurity examination example in paragraph .19, the phrase *to meet the entity's objectives* in CC6.4 usually would be interpreted as follows:

> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel *to meet the entity's cybersecurity objectives*.

.24 In addition, criterion CC6.4 would be applied as it relates to controls within the cybersecurity risk management program (*a*) across an entire entity; (*b*) at a subsidiary, division, or operating unit level; (*c*) within a function relevant to the entity's operations, reporting, or compliance objectives; or (*d*) for a particular type of information used by the entity, depending on the scope of the SOC for Cybersecurity examination.

[fn 7] The practitioner's responsibility is similar to that in AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, which requires the service auditor in a SOC 1 engagement to determine whether the control objectives stated in management's description of the service organization's system are reasonable in the circumstances.

Professional Standards Governing Engagements Using the Trust Services Criteria

Attestation Engagements

.25 Examination engagements [fn 8] and engagements to apply agreed-upon procedures performed in accordance with Statements on Standards for Attestation Engagements (SSAEs) may use the trust services criteria as the evaluation criteria. The SSAEs provide guidance on performing and reporting in connection with examination, review, [fn 9] and agreed-upon procedures engagements. Under the SSAEs, the CPA performing an attestation engagement is known as a *practitioner*. [fn 10] In an examination engagement, the practitioner provides a report in which the practitioner expresses an opinion on subject matter or an assertion about the subject matter in relation to an identified set of criteria. In an agreed-upon procedures engagement, the practitioner does not express an opinion but, rather, performs procedures agreed upon by the specified parties and reports the results of those procedures. Examination engagements may be performed in accordance with AT-C sections 105 and 205 or AT-C section 105 and AT-C section 206, *Direct Examination Engagements*; [fn 11] agreed-upon procedures engagements are performed in accordance with AT-C section 105 and AT-C section 215, *Agreed-Upon Procedures Engagements*.

.26 According to the SSAEs, the criteria used in an attestation engagement should be suitable and available to report users. Attributes of suitable criteria are as follows: [fn 12]

- *Relevance*. Criteria are relevant to the system.
- *Objectivity*. Criteria are free from bias.
- *Measurability*. Criteria permit reasonably consistent measurements, qualitative or quantitative, of the system.
- *Completeness*. Criteria are complete when the description prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect decisions of the intended users made on the basis of that description.

ASEC has concluded that the trust services criteria are suitable criteria in accordance with the SSAEs.

[fn 9] Paragraph .07 of AT-C section 210, *Review Engagements*, prohibits a practitioner from performing a review of internal control; therefore, practitioners may not perform a review engagement in accordance with the attestation standards using the trust services criteria.

[fn 10] Statements on Standards for Attestation Engagements refer to a CPA who performs an attestation engagement as a *practitioner*. However, 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* to refer to the practitioner in a SOC 2 examination.

[fn 11] See footnote 8.

[fn 12] Paragraph .A24 of AT-C section 105, *Concepts Common to All Attestation Engagements*.

27 In addition to being suitable, AT-C section 105 indicates that the criteria used in an attestation engagement must be available to users. The publication of the trust services criteria makes the criteria available to report users.

Consulting Engagements

.28 Sometimes, the trust services criteria may be used in engagements that involve the performance of readiness services, in which a practitioner may assist management with the implementation of one or more new information systems within an organization. [fn 13] Such engagements typically are performed under the consulting standards. In a consulting engagement, the practitioner develops findings and makes recommendations for the consideration and use of management; the practitioner does not form a conclusion about or express an opinion on the subject matter of the engagement. Generally, consulting services are performed only for the use and benefit of the client. Practitioners providing such services follow CS section 100, *Consulting Services: Definitions and Standards*. [fn 14]

Trust Services Criteria

.29 The following table presents the trust services criteria and the related points of focus. In the table, criteria and related points of focus that come directly from the COSO framework are presented using a normal font. In contrast, supplemental criteria and points of focus that apply to engagements using the trust services criteria are presented in *italics.* Finally, criteria and points of focus that apply only when engagements using the trust services criteria are performed at a system level are presented in ***bold italics***.

	CONTROL ENVIRONMENT
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:

[fn 13] When a practitioner provides information systems design, implementation, or integration services to an attest client, threats to the practitioner's independence may exist. The "Information Systems Design, Implementation, or Integration" interpretation (ET sec. 1.295.145) of the AICPA Code of Professional Conduct provides guidance to practitioners on evaluating the effect of such threats to their independence.

All ET sections can be found in AICPA *Professional Standards*.

[fn 14] All CS sections can be found in AICPA *Professional Standards*.

	• Sets the Tone at the Top — The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.
	• Establishes Standards of Conduct — The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.
	• Evaluates Adherence to Standards of Conduct — Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
	• Addresses Deviations in a Timely Manner — Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.
	Additional point of focus when using the trust services criteria:
	• *Considers Contractors and Vendor Employees in Demonstrating Its Commitment — Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.*
CC1.2	**COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Establishes Oversight Responsibilities — The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.

	• Applies Relevant Expertise — The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.
	• Operates Independently [fn 15] — The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
	Additional point of focus when using the trust services criteria:
	• *Supplements Board Expertise — The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.*
CC1.3	**COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers All Structures of the Entity — Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.

[fn 15] The definition of *board of directors* in appendix A, "Glossary," recognizes that smaller, less complex businesses may meet the governance and oversight objectives of the entity with simplified organizational structures. With sufficient management oversight, a board of directors may be effective without retaining independent board members.

	• Establishes Reporting Lines — Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.
	• Defines, Assigns, and Limits Authorities and Responsibilities — Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.
	Additional points of focus when using the trust services criteria:
	• *Addresses Specific Requirements When Defining Authorities and Responsibilities — Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.*
	• *Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities — Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.*
	Additional point of focus when using the trust services criteria for privacy: • *Establishes Structures, Reporting Lines, and Authorities to Support Compliance With Legal and Contractual Privacy Requirements — When establishing structures, reporting lines, and authorities, management considers legal and contractual privacy requirements and objectives.*
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Establishes Policies and Practices — Policies and practices reflect expectations of competence necessary to support the achievement of objectives.

	• Evaluates Competence and Addresses Shortcomings — The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.
	• Attracts, Develops, and Retains Individuals — The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.
	• Plans and Prepares for Succession — Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.
	Additional points of focus when using the trust services criteria:
	• *Considers the Background of Individuals — The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Considers the Technical Competency of Individuals — The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Provides Training to Maintain Technical Competencies — The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.*
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:

	• Enforces Accountability Through Structures, Authorities, and Responsibilities — Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.
	• Establishes Performance Measures, Incentives, and Rewards — Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.
	• Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance — Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.
	• Considers Excessive Pressures — Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.
	• Evaluates Performance and Rewards or Disciplines Individuals — Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate.
	Additional point of focus when using the trust services criteria for privacy:
	• *Takes Disciplinary Actions — A sanctions process is defined, and applied as needed, when an employee violates the entity's privacy policies or when an employee's negligent behavior causes a privacy incident.*
	INFORMATION AND COMMUNICATION
CC2.1	**COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:

	• Identifies Information Requirements — A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.
	• Captures Internal and External Sources of Data — Information systems capture internal and external sources of data.
	• Processes Relevant Data Into Information — Information systems process and transform relevant data into information.
	• Maintains Quality Throughout Processing — Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.
	Additional points of focus when using the trust services criteria:
	• *Documents Data Flow — The entity documents and uses internal and external information and data flows to support the design and operation of controls.*
	• *Manages Assets — The entity identifies, documents, and maintains records of system components such as infrastructure, software, and other information assets. Information assets include physical endpoint devices and systems, virtual systems, data and data flows, external information systems, and organizational roles.*
	• *Classifies Information — The entity classifies information by its relevant characteristics (for example, personally identifiable information, confidential customer information, and intellectual property) to support identification of threats to the information and the design and operation of controls.*
	• *Uses Information That Is Complete and Accurate — The entity uses information and reports that are complete, accurate, current, and valid in the operation of controls.*
	• *Manages the Location of Assets — The entity identifies, documents, and maintains records of physical location and custody of information assets, particularly for those stored outside the physical security control of the entity (for example, software and data stored on vendor devices or employee mobile phones under a bring-your-own-device policy).*

CC2.2	**COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Communicates Internal Control Information — A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.
	• Communicates With the Board of Directors — Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.
	• Provides Separate Communication Lines — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the information.
	Additional points of focus when using the trust services criteria:
	• *Communicates Responsibilities — Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.*
	• *Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters — Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints.*

	• *Communicates Objectives and Changes to Objectives — The entity communicates its objectives and changes to those objectives to personnel in a timely manner.*
	• *Communicates Information to Improve Security Knowledge and Awareness — The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.*
	Additional point of focus when using the trust services criteria for privacy:
	• *Communicates Information to Improve Privacy Knowledge and Awareness — The entity communicates information to improve privacy knowledge and awareness and to model appropriate behaviors to personnel through a privacy awareness training program.*
	• *Communicates Incident Reporting Methods — The entity has communicated to employees and others within the entity the process used to report a suspected privacy incident.*
	Additional points of focus when using the trust services criteria at the system level:
	• ***Communicates Information About System Operation and Boundaries — The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.***
	• ***Communicates System Objectives — The entity communicates its objectives to personnel to enable them to carry out their responsibilities.***
	• ***Communicates System Changes — System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.***
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**

	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Communicates to External Parties — Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.
	• Enables Inbound Communications — Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.
	• Communicates With the Board of Directors — Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.
	• Provides Separate Communication Lines — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.
	Additional point of focus when using the trust services criteria for confidentiality:
	• *Communicates Objectives Related to Confidentiality and Changes to Those Objectives — The entity communicates, to external users, vendors, business partners, and others whose products or services, or both, are part of the system, the entity's objectives related to confidentiality and the protection of confidential information, as well as changes to those objectives.*
	Additional point of focus when using the trust services criteria for privacy:

	• *Communicates Objectives Related to Privacy and Changes to Those Objectives — The entity communicates, to external users, vendors, business partners, and others whose products or services, or both, are part of the system, the entity's objectives related to privacy and the protection of personal information, as well as changes to those objectives.*
	• *Communicates Incident Reporting Methods — The entity communicates to user entities, third parties, data subjects, and others the process used to report a suspected privacy incident.*
	Additional points of focus when using the trust services criteria at the system level:
	• ***Communicates Information About System Operation and Boundaries — The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.***
	• ***Communicates System Objectives — The entity communicates its system objectives to appropriate external users.***
	• ***Communicates System Responsibilities — External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive information about such responsibilities and have the information necessary to carry out such responsibilities.***
	• ***Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters — External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate entity personnel.***
	RISK ASSESSMENT
CC3.1	**COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:

	Operations Objectives [fn 16] • Reflects Management's Choices — Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.
	• Considers Tolerances for Risk — Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	• Includes Operations and Financial Performance Goals — The organization reflects the desired level of operations and financial performance for the entity within operations objectives.
	• Forms a Basis for Committing of Resources — Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.
	External Financial Reporting Objectives [fn 17] • Complies With Applicable Accounting Standards — Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.
	• Considers Materiality — Management considers materiality in financial statement presentation.
	• Reflects Entity Activities — External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.
	External Nonfinancial Reporting Objectives [fn 18]

[fn 16] Not all objectives may be necessary to support the achievement of the entity's objectives in a particular engagement. For example, financial reporting objectives may not be relevant to a SOC examination because the subject matter being evaluated by the criteria is not related to financial reporting.

[fn 17] See footnote 16.

[fn 18] See footnote 16.

	• Complies With Externally Established Frameworks — Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.
	• Considers the Required Level of Precision — Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.
	• Reflects Entity Activities — External reporting reflects the underlying transactions and events within a range of acceptable limits.
	Internal Reporting Objectives [fn 19] • Reflects Management's Choices — Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.
	• Considers the Required Level of Precision — Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.
	• Reflects Entity Activities — Internal reporting reflects the underlying transactions and events within a range of acceptable limits.
	Compliance Objectives [fn 20] • Reflects External Laws and Regulations — Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.
	• Considers Tolerances for Risk — Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	Additional point of focus when using the trust services criteria:

[fn 19] See footnote 16.

[fn 20] See footnote 16.

	• *Establishes Sub-Objectives for Risk Assessment — Management identifies sub-objectives for use in risk assessment related to security, availability, processing integrity, confidentiality, or privacy to support the achievement of the entity's objectives.*
CC3.2	**COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels — The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.
	• Analyzes Internal and External Factors — Risk identification considers both internal and external factors and their impact on the achievement of objectives.
	• Involves Appropriate Levels of Management — The entity puts into place effective risk assessment mechanisms that involve appropriate levels of management.
	• Estimates Significance of Risks Identified — Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
	• Determines How to Respond to Risks — Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.
	Additional points of focus when using the trust services criteria:
	• *Identifies Threats to Objectives —The entity identifies threats to the achievement of its objectives from intentional (including malicious) and unintentional acts and environmental events.*

	• *Identifies Vulnerability of System Components — The entity identifies the vulnerabilities of system components, including system processes, infrastructure, software, and other information assets.*
	• *Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties — The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and other third parties with access to the entity's information systems.*
	• *Assesses the Significance of the Risks — The entity assesses the significance of the identified risks, including (1) determining the criticality of system components, including information assets, in achieving the objectives; (2) assessing the susceptibility of the identified vulnerabilities to the identified threats (3) assessing the likelihood of the identified risks (4) assessing the magnitude of the effect of potential risks to the achievement of the objectives; (5) considering the potential effects of unidentified threats and vulnerabilities on the assessed risks; (6) developing risk mitigation strategies to address the assessed risks; and (7) evaluating the appropriateness of residual risk (including whether to accept, reduce, or share such risks).*
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers Various Types of Fraud — The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
	• Assesses Incentives and Pressures — The assessment of fraud risks considers incentives and pressures.
	• Assesses Opportunities — The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.

	• Assesses Attitudes and Rationalizations — The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.
	Additional point of focus when using the trust services criteria:
	• *Considers the Risks Related to the Use of IT and Access to Information — The assessment of fraud risks includes consideration of internal and external threats and vulnerabilities that arise specifically from the use of IT and access to information.*
CC3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Assesses Changes in the External Environment — The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.
	• Assesses Changes in the Business Model — The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
	• Assesses Changes in Leadership — The entity considers changes in management and respective attitudes and philosophies on the system of internal control.
	Additional point of focus when using the trust services criteria:

	• *Assesses Changes in Systems and Technology — The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.*
	• *Assesses Changes in Vendor and Business Partner Relationships — The risk identification process considers changes in vendor and business partner relationships.*
	• *Assesses Changes in Threats and Vulnerabilities — The risk identification process assesses changes in (1) internal and external threats to and vulnerabilities of the components of the entity's systems and (2) the likelihood and magnitude of the resultant risks to the achievement of the entity's objectives.*
	MONITORING ACTIVITIES
CC4.1	**COSO Principle 16*:* The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers a Mix of Ongoing and Separate Evaluations — Management includes a balance of ongoing and separate evaluations.
	• Considers Rate of Change — Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.
	• Establishes Baseline Understanding — The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.
	• Uses Knowledgeable Personnel — Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.
	• Integrates With Business Processes — Ongoing evaluations are built into the business processes and adjust to changing conditions.

	• Adjusts Scope and Frequency — Management varies the scope and frequency of separate evaluations depending on risk.
	• Objectively Evaluates — Separate evaluations are performed periodically to provide objective feedback.
	Additional point of focus when using the trust services criteria:
	• *Considers Different Types of Ongoing and Separate Evaluations — Management uses a variety of ongoing and separate risk and control evaluations to determine whether internal controls are present and functioning. Depending on the entity's objectives, such risk and control evaluations may include first- and second-line monitoring and control testing, internal audit assessments, compliance assessments, resilience assessments, vulnerability scans, security assessment, penetration testing, and third-party assessments.*
CC4.2	**COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Assesses Results — Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
	• Communicates Deficiencies — Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.
	• Monitors Corrective Action — Management tracks whether deficiencies are remedied on a timely basis.
	CONTROL ACTIVITIES
CC5.1	**COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**

	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Integrates With Risk Assessment — Control activities help ensure that risk responses that address and mitigate risks are carried out.
	• Considers Entity-Specific Factors — Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
	• Determines Relevant Business Processes — Management determines which relevant business processes require control activities.
	• Evaluates a Mix of Control Activity Types — Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.
	• Considers at What Level Activities Are Applied — Management considers control activities at various levels in the entity.
	• Addresses Segregation of Duties — Management segregates incompatible duties and, where such segregation is not practical, management selects and develops alternative control activities.
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls — Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
	• Establishes Relevant Technology Infrastructure Control Activities — Management selects and develops control activities over the technology infrastructure, which are

	designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
	• Establishes Relevant Security Management Process Controls Activities — Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.
	• Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities — Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.
CC5.3	**COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Establishes Policies and Procedures to Support Deployment of Management's Directives — Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
	• Establishes Responsibility and Accountability for Executing Policies and Procedures — Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.
	• Performs in a Timely Manner — Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.
	• Takes Corrective Action — Responsible personnel investigate and act on matters identified as a result of executing control activities.
	• Performs Using Competent Personnel — Competent personnel with sufficient authority perform control activities with diligence and continuing focus.

	• Reassesses Policies and Procedures — Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.
	Logical and Physical Access Controls
CC6.1	***The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.***
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus when using the trust services criteria for all engagements:
	• *Identifies and Manages the Inventory of Information Assets — The entity identifies, inventories, classifies, and manages information assets (for example, infrastructure, software, and data).*
	• *Assesses New Architectures — The entity identifies new system architectures and assesses their security prior to implementation into the system environment.*
	• *Restricts Logical Access — The entity restricts logical access to information assets, including infrastructure (for example, server, storage, network elements, APIs, and endpoint devices), software, and data (at rest, during processing, or in transmission) through the use of access control software, rule sets, and standard configuration hardening processes.*
	• *Identifies and Authenticates Users — The entity identifies and authenticates persons, infrastructure, and software prior to accessing information assets, whether locally or remotely. The entity uses more complex or advanced user authentication techniques such as multifactor authentication when such protections are deemed appropriate based on its risk mitigation strategy.*
	• *Considers Network Segmentation — The entity uses network segmentation, zero trust architectures, and other techniques to isolate unrelated portions of the entity's information technology from each other based on the entity's risk mitigation strategy.*
	• *Manages Points of Access — Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed.*

	The types of individuals and systems using each point of access are identified, documented, and managed.
	• *Restricts Access to Information Assets — Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules and configuration standards for information assets.*
	• *Manages Identification and Authentication — Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.*
	• *Manages Credentials for Infrastructure and Software — New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.*
	• *Uses Encryption to Protect Data — The entity uses encryption to protect data (at rest, during processing, or in transmission), when such protections are deemed appropriate based on the entity's risk mitigation strategy.*
	• *Protects Cryptographic Keys — The entity protects cryptographic keys during generation, storage, use, and destruction. Cryptographic modules, algorithms, key lengths, and architectures are appropriate based on the entity's risk mitigation strategy.*
	Additional point of focus when using the trust services criteria for confidentiality:
	• *Restricts Access to and Use of Confidential Information for Identified Purposes — Logical access to and use of confidential information is restricted to identified purposes.*
	Additional point of focus when using the trust services criteria for privacy:
	• *Restricts Access to and the Use of Personal Information — Logical access to and use of personal information is restricted to authorized personnel who require such*

	access to fulfill the identified purposes to support the achievement of the entity's objectives related to privacy.
CC6.2	***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.***
	The following points of focus highlight important characteristics relating to this criterion:
	• *Creates Access Credentials to Protected Information Assets —The entity creates credentials for accessing protected information assets based on an authorization from the system's asset owner or authorized custodian. Authorization is required for the creation of all types of credentials of individuals (for example, employees, contractors, vendors, and business partner personnel), systems, and software.*
	• *Reviews Validity of Access Credentials — The entity reviews access credentials on a periodic basis for validity (for example, employees, contractors, vendors, and business partner personnel) and inappropriate system or service accounts.*
	• *Prevents the Use of Credentials When No Longer Valid — Processes are in place to disable, destroy, or otherwise prevent the use of access credentials when no longer valid.*
CC6.3	***The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.***
	The following points of focus highlight important characteristics relating to this criterion:
	• *Creates or Modifies Access to Protected Information Assets — Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.*
	• *Removes Access to Protected Information Assets — Processes are in place to remove access to protected information assets when no longer required.*

	• *Uses Access Control Structures — The entity uses access control structures, such as role-based access controls, to restrict access to protected information assets, limit privileges, and support segregation of incompatible functions.*
	• *Reviews Access Roles and Rules — The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals (for example, employees, contractors, vendors, business partner personnel) and inappropriate system or service accounts. Access roles and rules are modified, as appropriate.*
CC6.4	***The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***
	The following points of focus highlight important characteristics relating to this criterion:
	• *Creates or Modifies Physical Access — Processes are in place to create or modify physical access by employees, contractors, vendors, and business partner personnel to facilities such as data centers, office spaces, and work areas, based on appropriate authorization.*
	• *Removes Physical Access — Processes are in place to remove physical access to facilities and protected information assets when an employee, contractor, vendor, or business partner no longer requires access.*
	• *Recovers Physical Devices — Processes are in place to recover entity devices (for example, badges, laptops, and mobile devices) when an employee, contractor, vendor, or business partner no longer requires access.*
	• *Reviews Physical Access — Processes are in place to periodically review physical access to help ensure consistency with job responsibilities.*
CC6.5	***The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.***
	The following points of focus highlight important characteristics relating to this criterion:

	• *Removes Data and Software for Disposal — Procedures are in place to remove, delete, or otherwise render data and software inaccessible from physical assets and other devices owned by the entity, its vendors, and employees when the data and software are no longer required on the asset or the asset will no longer be under the control of the entity.*
CC6.6	***The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***
	The following points of focus highlight important characteristics relating to this criterion:
	• *Restricts Access — The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.*
	• *Protects Identification and Authentication Credentials — Identification and authentication credentials are protected during transmission outside its system boundaries.*
	• *Requires Additional Authentication or Credentials — Additional authentication information or credentials are required when accessing the system from outside its boundaries.*
	• *Implements Boundary Protection Systems — Boundary protection systems (for example, firewalls, demilitarized zones, intrusion detection or prevention systems, and endpoint detection and response systems) are configured, implemented, and maintained to protect external access points.*
CC6.7	***The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.***
	The following points of focus highlight important characteristics relating to this criterion:

	• *Restricts the Ability to Perform Transmission — Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information.*
	• *Uses Encryption Technologies or Secure Communication Channels to Protect Data — Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.*
	• *Protects Removal Media — Encryption technologies and physical asset protections are used for removable media (such as USB drives and backup tapes), as appropriate.*
	• *Protects Endpoint Devices — Processes and controls are in place to protect endpoint devices (such as mobile devices, laptops, desktops, and sensors).*
CC6.8	***The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.***
	The following points of focus highlight important characteristics relating to this criterion:
	• *Restricts Installation and Modification of Application and Software — The ability to install and modify applications and software is restricted to authorized individuals. Utility software capable of bypassing normal operating or security procedures is limited to use by authorized individuals and is monitored regularly.*
	• *Detects Unauthorized Changes to Software and Configuration Parameters — Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.*
	• *Uses a Defined Change Control Process — A management-defined change control process is used for the implementation of software.*
	• *Uses Antivirus and Anti-Malware Software — Antivirus and anti-malware software on servers and endpoint devices is configured, implemented, and maintained to provide for the interception or detection and remediation of malware.*

	• *Scans Information Assets From Outside the Entity for Malware and Other Unauthorized Software — Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software. Detected malware or other software is removed prior to connection to the entity's network.*
	System Operations
CC7.1	***To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.***
	The following points of focus highlight important characteristics relating to this criterion:
	• *Uses Defined Configuration Standards — The entity has defined configuration standards to be used for hardening systems.*
	• *Monitors Infrastructure and Software — The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.*
	• *Implements Change-Detection Mechanisms — The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.*
	• *Detects Unknown or Unauthorized Components — Procedures are in place to detect the introduction of unknown or unauthorized components.*
	• *Conducts Vulnerability Scans — The entity conducts infrastructure and software vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after significant changes are made to the environment. Action is taken to remediate identified deficiencies in a timely manner to support the achievement of the entity's objectives.*
CC7.2	***The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.***

	The following points of focus highlight important characteristics relating to this criterion:
	• *Implements Detection Policies, Procedures, and Tools — Detection policies, procedures, and tools are defined and implemented on infrastructure and software to identify potential intrusions, inappropriate access, and anomalies in the operation of or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.*
	• *Designs Detection Measures — Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.*
	• *Implements Filters to Analyze Anomalies — Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.*
	• *Monitors Detection Tools for Effective Operation — Management has implemented processes to monitor and maintain the effectiveness of detection tools.*
CC7.3	***The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.***
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus when using the trust services criteria for all engagements:
	• *Responds to Security Incidents — Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.*
	• *Communicates and Reviews Detected Security Events — Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program, and actions are taken, if necessary.*

	• *Develops and Implements Procedures to Analyze Security Incidents — Procedures are in place to analyze security incidents and determine system impact.*
	Additional points of focus when using the trust services criteria for confidentiality:
	• *Assesses the Impact on Confidential Information — Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of confidential information.*
	• *Determines Confidential Information Used or Disclosed — When an unauthorized use or disclosure of confidential information has occurred, the affected information is identified and actions are taken to help prevent future recurrence and address control failures to support the achievement of entity objectives.*
	Additional points of focus when using the trust services criteria for privacy:
	• *Assesses the Impact on Personal Information — Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.*
	• *Determines Personal Information Used or Disclosed — When an unauthorized use or disclosure of personal information has occurred, the affected information is identified and actions are taken to help prevent future recurrence and address control failures to support the achievement of entity objectives.*
CC7.4	***The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.***
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus when using the trust services criteria for all engagements:

	• *Assigns Roles and Responsibilities — Roles and responsibilities for the design, implementation, maintenance, and execution of the incident-response program are assigned, including the use of external resources when necessary.*
	• *Contains and Responds to Security Incidents — Procedures are in place to respond to and contain security incidents that actively threaten entity objectives.*
	• *Mitigates Ongoing Security Incidents — Procedures are in place to mitigate the effects of ongoing security incidents.*
	• *Resolves Security Incidents — Procedures are in place to resolve security incidents through closure of vulnerabilities, removal of unauthorized access, and other remediation actions.*
	• *Restores Operations — Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.*
	• *Develops and Implements Communication of Security Incidents — Protocols for communicating, in a timely manner, information regarding security incidents and actions taken to affected parties are developed and implemented to support the achievement of the entity's objectives.*
	• *Obtains Understanding of Nature of Incident and Determines Containment Strategy — An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate response and containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.*
	• *Remediates Identified Vulnerabilities — Identified vulnerabilities are remediated through the development and execution of remediation activities.*
	• *Communicates Remediation Activities — Remediation activities are documented and communicated in accordance with the incident-response program.*
	• *Evaluates the Effectiveness of Incident Response — The design of incident-response activities is evaluated for effectiveness on a periodic basis.*

	• *Periodically Evaluates Incidents — Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.*
	Additional points of focus when using the trust services criteria for privacy:
	• *Applies Breach Response Procedures — Breach response procedures are defined and applied in the event of a confirmed privacy incident.*
	• *Communicates Unauthorized Use and Disclosure — Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.*
	• *Application of Sanctions — The conduct of individuals and organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.*
CC7.5	***The entity identifies, develops, and implements activities to recover from identified security incidents.***
	The following points of focus highlight important characteristics relating to this criterion:
	• *Restores the Affected Environment — The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, modifying access controls, and changing configurations, as needed.*
	• *Communicates Information About the Incident — Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security incidents are made to management and others as appropriate (internal and external).*
	• *Determines Root Cause of the Incident — The root cause of the incident is determined.*

	• *Implements Changes to Prevent and Detect Recurrences — Additional architecture or changes to preventive and detective controls are implemented to prevent and detect incident recurrences in a timely manner.*
	• *Improves Response and Recovery Procedures — Lessons learned are analyzed and the incident-response plan and recovery procedures are improved.*
	• *Implements Incident-Recovery Plan Testing — Incident-recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of resilience posture and continuity plans based on test results.*
	Change Management
CC8.1	***The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.***
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus when using the trust services criteria for all engagements:
	• *Manages Changes Throughout the System Life Cycle — A process for managing system changes throughout the life cycle of the system and its components (infrastructure, data, software, and manual and automated procedures) is used to support the achievement of entity objectives.*
	• *Authorizes Changes — A process is in place to authorize system and architecture changes prior to design, development, or acquisition and configuration.*
	• *Designs and Develops Changes — A process is in place to design and develop system changes in a secure manner to support the achievement of entity objectives.*
	• *Documents Changes — A process is in place to document system changes to support ongoing maintenance of the system and to support internal and external users in performing their responsibilities.*

	• *Tracks System Changes — A process is in place to track system changes prior to implementation.*
	• *Configures Software — A process is in place to select, implement, maintain, and monitor configuration parameters used to control the functionality of developed and acquired software.*
	• *Tests System Changes — A process is in place to test internally developed and acquired system changes prior to implementation into the production environment. Examples of testing may include unit, integration, regression, static and dynamic application source code, quality assurance, or automated testing (whether point in time or continuous).*
	• *Approves System Changes — A process is in place to approve system changes prior to implementation.*
	• *Deploys System Changes — A process is in place to implement system changes with consideration of segregation of responsibilities (for example, restricting unilateral code development or testing and implementation by a single user) to prevent or detect unauthorized changes.*
	• *Identifies and Evaluates System Changes — Objectives affected by system changes are identified, and the ability of the modified system to support the achievement of the objectives is evaluated throughout the system development life cycle.*
	• *Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents — Changes in infrastructure, data, software, and procedures required to remediate incidents are identified and the change process is initiated upon identification.*
	• *Creates Baseline Configuration of IT Technology — A baseline configuration of IT and control systems is created and maintained.*
	• *Provides for Changes Necessary in Emergency Situations — A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent time frame).*

	• *Manages Patch Changes — A process is in place to identify, evaluate, test, approve, and implement patches in a timely manner on infrastructure and software.*
	Additional points of focus when using the trust services criteria for availability:
	• *Considers System Resilience — The entity considers system resilience when designing its systems and tests resilience during development to help ensure the entity's ability to respond to, recover from, and resume operations through significant disruptions.*
	Additional points of focus when using the trust services criteria for confidentiality:
	• *Protects Confidential Information — The entity protects confidential information during system design, development, testing, implementation, and change processes to support the achievement of the entity's objectives related to confidentiality.*
	Additional points of focus when using the trust services criteria for privacy:
	• *Protects Personal Information — The entity protects personal information during system design, development, testing, implementation, and change processes to support the achievement of the entity's objectives related to privacy.*
	• *Privacy by Design — The entity considers privacy requirements in the design of its systems and processes and limits the collection and processing of personal information to what is necessary for the identified purpose.*
	Risk Mitigation
CC9.1	***The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.***
	The following points of focus highlight important characteristics relating to this criterion:

	• *Considers Mitigation of Risks of Business Disruption — Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from incidents that disrupt business operations. Those resilience policies and procedures include monitoring processes, information, and communications to support the achievement of the entity's objectives during response, mitigation, and recovery efforts.*
	• *Considers the Use of Insurance to Mitigate Financial Impact Risks — The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to support the achievement of its objectives.*
CC9.2	***The entity assesses and manages risks associated with vendors and business partners.***
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus when using the trust services criteria for all engagements:
	• *Establishes Requirements for Vendor and Business Partner Engagements — The entity establishes specific requirements for vendor and business partner engagements that include (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.*
	• *Identifies Vulnerabilities — The entity evaluates vulnerabilities arising from vendor and business partner relationships, including third-party access to the entity's IT systems and connections with third-party networks.*
	• *Assesses Vendor and Business Partner Risks — The entity inventories, tiers, and assesses, on a periodic basis, threats arising from relationships with vendors and business partners (and those entities' vendors and business partners) and the vulnerability of the entity's objectives to those threats. Examples of threats arising from relationships with vendors and business partners include those arising from their (1) financial failure, (2) security vulnerabilities, (3) operational disruption, and (4) failure to meet business or regulatory requirements.*
	• *Assigns Responsibility and Accountability for Managing Vendors and Business Partners — The entity assigns responsibility and accountability for the management of risks and changes to services associated with vendors and business partners.*

	• *Establishes Communication Protocols for Vendors and Business Partners — The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.*
	• *Establishes Exception Handling Procedures From Vendors and Business Partners — The entity establishes exception handling procedures for service or product issues related to vendors and business partners.*
	• *Assesses Vendor and Business Partner Performance — The entity assesses the performance of vendors and business partners, as frequently as warranted, based on the risk associated with the vendor or business partner.*
	• *Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments — The entity implements procedures for addressing issues identified with vendor and business partner relationships.*
	• *Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships based on predefined considerations. Those procedures may include safe return of data and its removal from the vendor or business partner system.*
	Additional points of focus when using the trust services criteria for confidentiality:
	• *Obtains Confidentiality Commitments From Vendors and Business Partners — The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.*
	• *Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.*
	Additional points of focus when using the trust services criteria for privacy:
	• *Obtains Privacy Commitments From Vendors and Business Partners — The entity obtains privacy commitments, consistent with the entity's privacy commitments and*

	requirements, from vendors and business partners who have access to personal information.
	• *Assesses Compliance With Privacy Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.*
	ADDITIONAL CRITERIA FOR AVAILABILITY
A1.1	***The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Measures Current Usage — The use of the system components is measured to establish a baseline for capacity management and to use when monitoring and evaluating the risk of impaired availability due to capacity constraints.*
	• *Forecasts Capacity — The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers system resilience and capacity in the event of the failure of system components that constrain capacity.*
	• *Makes Changes Based on Forecasts — The system change management process is initiated when forecasted usage exceeds capacity tolerances.*
A1.2	***The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services availability criteria, highlight important characteristics relating to this criterion:
	• *Identifies Environmental Threats — As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.*

	• *Designs Detection Measures — Detection measures are implemented to identify anomalies that could result from environmental threat events.*
	• *Implements and Maintains Environmental Protection Mechanisms — Management implements and maintains environmental protection mechanisms to prevent and mitigate environmental events.*
	• *Implements Alerts to Analyze Anomalies — Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.*
	• *Responds to Environmental Threat Events — Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator backup subsystem).*
	• *Communicates and Reviews Detected Environmental Threat Events — Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system, and actions are taken, if necessary.*
	• *Determines Data Requiring Backup — Data is evaluated to determine whether backup is required.*
	• *Performs Data Backup — Procedures are in place for backing up data, monitoring to detect backup failures, and initiating corrective action when such failures occur.*
	• *Addresses Offsite Storage — Backup data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.*
	• *Implements Alternate Processing Infrastructure — Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable. Measures may include geographic separation, redundancy, and failover capabilities for components.*
	• *Considers Data Recoverability — Management identifies threats to data recoverability (for example, ransomware attacks) that could impair the availability of the system and related data and implements mitigation procedures.*

A1.3	***The entity tests recovery plan procedures supporting system recovery to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Implements Business Continuity Plan Testing — Business continuity plan testing is performed on a periodic basis to test the entity's ability to respond to, recover from, and resume operations through significant disruptions. Testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity and vendors that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel or vendors; and (4) revision of continuity plans and systems based on test results.*
	• *Tests Integrity and Completeness of Backup Data — The integrity and completeness of backup information is tested on a periodic basis.*
	ADDITIONAL CRITERIA FOR CONFIDENTIALITY
C1.1	***The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.***
	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Defines and Identifies Confidential information — Procedures are in place to define, identify, and designate confidential information when it is received or created.*
	• *Retains Confidential Information — Confidential information is retained for no longer than necessary to fulfill the identified purpose, unless a law or regulation specifically requires otherwise.*
	• *Protects Confidential Information From Destruction — Policies and procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.*
C1.2	***The entity disposes of confidential information to meet the entity's objectives related to confidentiality.***

	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Identifies Confidential Information for Destruction — Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.*
	• *Destroys Confidential Information — Policies and procedures are in place to automatically or manually erase or otherwise destroy confidential information that has been identified for destruction.*
	ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY (OVER THE PROVISION OF SERVICES OR THE PRODUCTION, MANUFACTURING, OR DISTRIBUTION OF GOODS)
PI1.1	***The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Identifies Functional and Nonfunctional Requirements and Information Specifications — The entity identifies and communicates functional and nonfunctional requirements related to system processing and information specifications required to support the use of products and services.*
	• *Defines Data Necessary to Support a Product or Service — When data is provided as part of a service or product or as part of a reporting obligation related to a product or service:* 1. *The definition and purpose of the data is available to the users of the data.* 2. *The definition of the data includes the following information:* a. *The population of events or instances included in the set of data* b. *The nature of each element (for example, field) of the set of data (that is, the event or instance to which the data element relates, for example, transaction price of a sale of XYZ Corporation stock for the last trade in that stock on a given day)* c. *The sources of the data within the set* d. *The units of measurement of data elements (for example, fields)* e. *The accuracy, correctness, or precision of measurement*

	f. The uncertainty or confidence interval inherent in each data element and in the population of those elements *g. The time periods over which the set of data was measured or the period of time during which the events the data relates to occurred* *h. In addition to the date or period of time, the factors that determined the inclusion and exclusion of items in the data elements and population* 3. *The definition of the data is complete and accurate.* 4. *The description of the data identifies any information that is necessary to understand each data element and the population in a manner consistent with its definition and intended purpose (metadata) that has not been included within the data.*
	The following point of focus, which applies only to an engagement using the trust services criteria for processing integrity for a system that produces, manufactures, or distributes products, highlights important characteristics relating to this criterion:
	• *Defines Information Necessary to Support the Use of a Good or Product — When information provided by the entity is needed to use the good or product in accordance with its specifications:* 1. *The required information is available to the user of the good or product.* 2. *The required information is clearly identifiable.* 3. *The required information is validated for completeness and accuracy.*
PI1.2	***The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Defines Characteristics of Processing Inputs — The characteristics of processing inputs that are necessary to meet requirements are defined.*
	• *Evaluates Processing Inputs — Processing inputs are evaluated for compliance with defined input requirements.*
	• *Creates and Maintains Records of System Inputs — Records of system input activities are created and maintained completely and accurately in a timely manner.*
PI1.3	***The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.***

	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Defines Processing Specifications — The processing specifications that are necessary to meet product or service requirements are defined.*
	• *Defines Processing Activities — Processing activities are defined to result in products or services that meet specifications.*
	• *Detects and Corrects Processing or Production Activity Errors — Errors encountered in processing or production activities are detected and corrected in a timely manner.*
	• *Records System Processing Activities — System processing activities are recorded completely and accurately in a timely manner.*
	• *Processes Inputs — Inputs are processed completely, accurately, and timely as authorized in accordance with defined processing activities.*
PI1.4	***The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Protects Output — Output is protected when stored or delivered, or both, to prevent theft, destruction, corruption, or deterioration that would prevent output from meeting specifications.*
	• *Distributes Output Only to Intended Parties — Output is distributed or made available only to intended parties.*
	• *Distributes Output Completely and Accurately — Procedures are in place to provide for the completeness, accuracy, and timeliness of distributed output.*

	• *Creates and Maintains Records of System Output Activities — Records of system output activities are created and maintained completely and accurately in a timely manner.*
PI1.5	***The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Protects Stored Items — Stored items are protected to prevent theft, corruption, destruction, or deterioration that would prevent output from meeting specifications.*
	• *Archives and Protects System Records — System records are archived, and archives are protected against theft, corruption, destruction, or deterioration that would prevent them from being used.*
	• *Stores Data Completely and Accurately — Procedures are in place to provide for the complete, accurate, and timely storage of data.*
	• *Creates and Maintains Records of System Storage Activities — Records of system storage activities are created and maintained completely and accurately in a timely manner.*
	ADDITIONAL CRITERIA FOR PRIVACY [fn 21]

[fn 21] The privacy points of focus assume that the service organization is a *data processor* or *data controller*, or both, as defined in appendix A, "Glossary." In many cases, a service organization may function as a data processor for its business-to-business (B2B) customers (user entities), which may in turn function as data controllers. In other cases, a service organization may function as a data controller. Practitioners have a responsibility to understand whether the service organization functions as a data processor, data controller, or both, and to evaluate all the points of focus to determine which are applicable based on the service organization's responsibilities. The following references indicate a typical allocation of responsibility.

[P] = This point of focus is likely to be relevant to a data processor.

[C] = This point of focus is likely to be relevant to a data controller.

P1.0	**Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy**
P1.1	***The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates to Data Subjects [C] — Notice is provided to data subjects regarding the following:* — *Purpose for collecting personal information* — *Choice and consent* — *Types of personal information collected* — *Methods of collection (for example, use of cookies or other tracking techniques)* — *Use, retention, and disposal* — *Access* — *Disclosure to third parties* — *Security for privacy* — *Quality, including data subjects' responsibilities for quality* — *Monitoring and enforcement* *If personal information is collected from sources other than the individual, such sources are described in the privacy notice.*
	• *Provides Notice to Data Subjects [C] — Notice is provided to data subjects (1) at or before the time personal information is collected or as soon as practical thereafter, (2) at or before the entity changes its privacy notice or as soon as practical*

	thereafter, or (3) before personal information is used for new purposes not previously identified.
	• *Covers Entities and Activities in Notice [C] — An objective description of the entities and activities covered is included in the entity's privacy notice.*
	• *Uses Clear Language and Presents a Current Privacy Notice in a Location Easily Found by Data Subjects [C] — The entity's privacy notice is current, dated, uses clear language, and is in a location that can be easily found by data subjects.*
	• *Reviews the Privacy Notice [C] — A process is defined to periodically review the content of the privacy notice and to implement any identified updates.*
	• *Communicates Changes to Notice [C] — Data subjects are informed when changes are made to the privacy notice and the nature of such changes.*
	• *Retains Prior Notices [C] — Prior versions of the privacy notice are retained in accordance with internal requirements to document prior communications.*
P2.0	**Privacy Criteria Related to Choice and Consent**
P2.1	***The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates to Data Subjects [C] — Data subjects are informed (a) about the choices available to them with respect to the collection, use, and disclosure of personal information and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.*
	• *Communicates Consequences of Denying or Withdrawing Consent [C] — When personal information is collected, data subjects are informed of the consequences of*

	refusing to provide personal information or denying or withdrawing consent to use personal information for purposes identified in the notice.
	• *Obtains Implicit or Explicit Consent [C] — Implicit or explicit consent is obtained from data subjects at or before the time personal information is collected or soon thereafter. The individual's preferences expressed in his or her consent are confirmed and implemented.*
	• *Documents and Obtains Consent for New Purposes and Uses [C] — If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the data subject is notified, and implicit or explicit consent is obtained prior to such new use or purpose.*
	• *Obtains Explicit Consent for Sensitive Information [C] — Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.*
	• *Obtains Consent for Data Transfers [C] — Consent is obtained before personal information is transferred to or from an individual's endpoint device.*
P3.0	**Privacy Criteria Related to Collection**
P3.1	***Personal information is collected consistent with the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Limits the Collection of Personal Information [P][C] — The collection of personal information is limited to that necessary to support the achievement of the entity's objectives.*
	• *Collects Information by Fair and Lawful Means [P][C] — Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.*

	• *Collects Information From Reliable Sources [P][C] — Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.*
	• *Informs Data Subjects When Additional Information Is Acquired [P][C] — Data subjects are informed if the entity develops or acquires additional information about them for its use.*
P3.2	***For information requiring explicit consent, the entity communicates the need for such consent as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Informs Data Subjects of Consequences of Failure to Provide Consent [C] — Data subjects are informed of the consequences of failing to provide the entity with explicit consent.*
	• *Documents Explicit Consent to Retain Information [C] — Documentation of explicit consent for the collection, use, or disclosure of sensitive personal information is retained to support the achievement of entity objectives related to privacy.*
P4.0	**Privacy Criteria Related to Use, Retention, and Disposal**
P4.1	***The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Uses Personal Information for Intended Purposes [P][C] — Personal information is used only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained, unless a law or regulation specifically requires otherwise.*
P4.2	***The entity retains personal information consistent with the entity's objectives related to privacy.***

	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Retains Personal Information [P][C] — Personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.*
	• *Protects Personal Information [P][C] — Policies and procedures have been implemented to protect personal information from erasure or destruction during the specified retention period of the information.*
P4.3	***The entity securely disposes of personal information to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Captures, Identifies, and Flags Requests for Deletion [P][C] — Requests for deletion of personal information are captured and information related to the requests is identified and flagged for destruction to support the achievement of the entity's objectives related to privacy.*
	• *Disposes of, Destroys, and Redacts Personal Information [P][C] — Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.*
	• *Destroys Personal Information [P][C] — Policies and procedures are implemented to erase or otherwise destroy personal information that has been identified for destruction.*
P5.0	**Privacy Criteria Related to Access**
P5.1	***The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:

	• *Responds to Data Controller Requests [P] — The entity has a process to respond to data subject requests received from data controllers in accordance with service agreements and privacy objectives. Such process may include authentication of the request, permitting access where appropriate, responding within a reasonable time, and notification if the request is denied.*
	• *Authenticates Data Subjects' Identity [P][C] — The identity of data subjects who request access to their personal information is authenticated before they are given access to that information.*
	• *Permits Data Subjects Access to Their Personal Information [P][C] — Data subjects are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.*
	• *Provides Understandable Personal Information Within Reasonable Time [P][C] — Personal information is provided to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any.*
	• *Informs Data Subjects If Access Is Denied [P][C] — When data subjects are denied access to their personal information, the entity informs them of the denial and the reason for the denial in a timely manner, unless prohibited by law or regulation.*
P5.2	***The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Responds to Data Controller Requests [P] — The entity has a process to respond to data controllers' update requests, including updates to personal information and denial of requests, in accordance with service agreements to support the achievement of the entity's objectives related to privacy.*
	• *Communicates Denial of Access Requests [P][C] — Data subjects are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the*

	individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.
	• *Permits Data Subjects to Update or Correct Personal Information [P][C] — Data subjects are able to update or correct personal information held by the entity. The entity communicates updates, corrections, and deletion requests to third parties that were previously provided with the data subject's personal information consistent with the entity's objectives related to privacy.*
	• *Communicates Denial of Correction Requests [P][C] — Data subjects are informed, in writing, about the reason a request for correction of personal information was denied and how they may appeal.*
P6.0	**Privacy Criteria Related to Disclosure and Notification**
P6.1	***The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates Privacy Policies to Third Parties [P][C] — Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.*
	• *Discloses Personal Information Only When Appropriate [P][C] — Personal information is disclosed to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject, unless a law or regulation specifically requires otherwise.*
	• *Discloses Personal Information Only to Appropriate Third Parties [P][C] — Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements.*
	• *Discloses Information to Third Parties for New Purposes and Uses [P][C] — Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of data subjects.*
P6.2	***The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.***

	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:
	• *Creates and Retains Record of Authorized Disclosures [P][C] — The entity creates and maintains a record of authorized disclosures of personal information that is complete, accurate, and timely.*
P6.3	***The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:
	• *Creates and Retains Record of Detected or Reported Unauthorized Disclosures [P][C] — The entity creates and maintains a record of detected or reported unauthorized disclosures of personal information that is complete, accurate, and timely.*
P6.4	***The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Evaluates Third-Party Compliance With Privacy Commitments [P][C] — The entity has procedures in place to evaluate whether third parties have effective controls to meet the terms of the agreement, instructions, or requirements.*
	• *Remediates Misuse of Personal Information by a Third Party [P][C] — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
	• *Obtains Commitments to Report Unauthorized Disclosures [P][C] — A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of personal information.*

P6.5	***The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Remediates Misuse of Personal Information by a Third Party [P][C] — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
	• *Reports Actual or Suspected Unauthorized Disclosures [P][C] — A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of personal information.*
P6.6	***The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Identifies Reporting Requirements [P][C] — The entity has a process for determining whether notification of a privacy breach is required, including the method to be used, the timeline, and the identification of recipients of such notifications.*
	• *Provides Notice of Breaches and Incidents [P][C] — The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators, and others to support the achievement of the entity's objectives related to privacy.*
P6.7	***The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:

	• *Responds to Data Controller Requests [P] — The entity has a process to respond to data controller requests for an accounting of personal information held in accordance with service agreements and privacy objectives.*
	• *Identifies Types of Personal Information and Handling Process [P][C] — The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified.*
	• *Captures, Identifies, and Communicates Requests for Information [P][C] — Requests for an accounting of personal information held and disclosures of the data subjects' personal information are captured and information related to the requests is identified and communicated to data subjects to support the achievement of the entity's objectives related to privacy.*
P7.0	**Privacy Criteria Related to Quality**
P7.1	***The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Ensures Accuracy and Completeness of Personal Information [P][C] — Personal information is accurate and complete for the purposes for which it is to be used.*
	• *Ensures Relevance of Personal Information [P][C] — Personal information is relevant to the purposes for which it is to be used.*
P8.0	**Privacy Criteria Related to Monitoring and Enforcement**
P8.1	***The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:

	• *Communicates to Data Subjects or Data Controllers [P][C] — Data subjects or data controllers are informed about how to contact the entity with inquiries, complaints, and disputes.*
	• *Addresses Inquiries, Complaints, and Disputes [P][C] — A process is in place to address inquiries, complaints, and disputes.*
	• *Documents and Communicates Dispute Resolution and Recourse [P][C] — Each complaint is addressed and the resolution is documented and communicated to the individual.*
	• *Documents and Reports Compliance Review Results [P][C] — Compliance with objectives related to privacy are reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.*
	• *Documents and Reports Instances of Noncompliance [P][C] — Instances of noncompliance with objectives related to privacy are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.*
	• *Performs Ongoing Monitoring [P][C] — Ongoing procedures are performed for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.*

Appendix A — Glossary

.30

access to personal information. The ability to view personal information held by an organization. This ability may be complemented by an ability to update or correct the information. Access defines the intersection of identity and data, that is, who can do what to which data. Access is one of the fair information practice principles. Individuals need to be able to find out what personal information an entity has on file about them and how the information is being used. Individuals need to be able to correct erroneous information in such records.

architecture. The design of the structure of a system, including logical components, and the logical interrelationships of computers, operating systems, networks, or other elements, whether internally or externally hosted.

authentication. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data.

authorization. The process of granting access privileges to a user, program, or process by a person that has the authority to grant such access.

board or **board of directors.** Individuals with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. Depending on the nature of the entity, 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 entity, a board of governors or commissioners for a government entity, general partners for a partnership, or an owner for a small business.

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

collection. The process of obtaining personal information from the individual directly (for example, through the individual's submission of an internet form or a registration form) or from another party, such as a business partner.

commitments. Declarations made by management to customers regarding the performance of one or more systems that provide services or products. Commitments can be communicated in written individualized agreements, standardized contracts, service-level agreements, or published statements (for example, a security practices statement). A commitment may relate to one or more trust services categories. Commitments may be made on many different aspects of the service being provided or the product, production, manufacturing, or distribution specifications.

component. One of five elements of internal control, including the control environment, risk assessment, control activities, information and communication, and monitoring activities.

compromise. Refers to a loss of confidentiality, integrity, or availability of information, including any resultant impairment of (1) processing integrity or availability of systems or (2) the integrity or availability of system inputs or outputs.

controls. Policies and procedures that are part of the entity's system of internal control. The objective of an entity's system of internal control is to provide reasonable assurance that principal system objectives are achieved.

control activity. An action established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

consent. This privacy requirement is one of the fair information practice objectives. Individuals must be able to prevent the collection of their personal data, unless legally required. If an

individual has a choice about the use or disclosure of his or her information, consent is the individual's way of giving permission for the use or disclosure. Consent may be affirmative (for example, opting in) or implied (for example, not opting out). There are two types of consent:

- **explicit consent.** A requirement that an individual "signifies" agreement with a data controller by some active communication between the parties.

- **implied consent.** When consent may reasonably be inferred from the action or inaction of the individual.

COSO. The Committee of Sponsoring Organizations of the Treadway Commission. COSO is a joint initiative of five private-sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. (See www.coso.org.)

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

cybersecurity objectives. Objectives that address the cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting, and operational objectives).

data controller. An organization that (alone or jointly with others) determines the purposes for and the means by which personal data is processed.

data processor. An organization that processes personal data at the direction of a data controller. In many cases, a service organization may process personal data for its business-to-business (B2B) customers (user entities), which in turn may function as data controllers. In other cases, a service organization may function as a data controller, depending on the facts and circumstances.

data subject. The individual about whom personal information is collected.

design. As used in the COSO definition of internal control, the internal control system design is intended to provide reasonable assurance of the achievement of an entity's objectives.

disclosure. The provision of access to or the release, transfer, or divulging in any other manner of information outside the entity holding the information. Disclosure is often used interchangeably with the terms *sharing* and *onward transfer*.

disposal. A phase of the data life cycle that pertains to how an entity removes or destroys data or information.

effectiveness (of controls). Encompasses both the suitability of the design of controls and the operating effectiveness of controls to provide reasonable assurance that the entity's principal system objectives are achieved.

endpoint devices. Connected hardware or virtual devices that communicate across a network, such as mobile devices, laptops, desktops, and sensors.

entity. A legal entity or management operating model of any size established for a particular purpose. A legal entity may, for example, be a business enterprise, a not-for-profit organization, a government body, or an academic institution. The management operating model may follow product or service lines, divisions, or operating units, with geographic markets providing for further subdivisions or aggregations of performance.

entity-wide. Activities that apply across the entity — most commonly in relation to entity-wide controls.

environmental. Of or having to do with the matters that can damage the physical elements of information systems (for example, fire, flood, wind, earthquake, power surges, or power outages). An entity implements controls and other activities to detect, prevent, and manage the risk of casualty damage to the physical elements of the information system from environmental elements.

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.

functional requirements. Requirements that must be met for the system to correctly fulfill its designed purpose.

information and systems. Refers to information in electronic form (electronic information) during its use, processing, transmission, and storage and systems that use, process, transmit or transfer, and store information or that produce, manufacture, or distribute products.

information assets. Data and the associated software and infrastructure used to process, transmit, and store information or to produce, manufacture, or distribute products.

infrastructure. The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, network elements, and endpoint devices.

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

nonfunctional requirements. System attributes such as security, reliability, performance, maintainability, scalability, and usability that define how well a system will operate.

outsourced service providers. A service provider that performs business processes, operations, or controls on behalf of the entity when such business processes, operations, or controls are necessary to achieve the entity's objectives.

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.

practitioner. As used in this document, a CPA who performs an examination of controls within an entity's system relevant to security, availability, processing integrity, confidentiality, or privacy.

principal system objectives. System objectives that relate to the trust services category or categories addressed by the examination and that could reasonably be expected to influence the relevant decisions of intended users. (See **system objectives**.)

privacy commitments. Declarations made by management regarding the performance of a system processing personal information. Such commitments can be communicated in written agreements, standardized contracts, service-level agreements, or published statements (for example, a privacy practices statement). In addition, privacy commitments may be made on many different aspects of the service being provided.

privacy notice. A written communication by entities that collect personal information, to the individuals about whom personal information is collected, about 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.

process or control framework. A framework that contains a set of processes or controls, established by another party, that organizations are expected to implement in support of establishing an effective system of internal control. These frameworks are usually developed by an industry group, regulator, governmental entity, standard-setting body, or other organization (collectively referred to as *sponsoring organizations*) to obtain information from organizations with which they do business about their processes and controls. The most common types of process or control frameworks relate to security and privacy.

products. Tangible or intangible goods manufactured or produced by an entity. Throughout this document, the term is used interchangeably with *goods.*

report users. Intended users of the practitioner's report in accordance with AT-C section 205, *Assertion-Based Examination Engagements*. [fn 1] There may be a broad range of report users for a general-purpose report but only a limited number of specified parties for a report that is restricted in accordance with paragraph .64 of AT-C section 205.

[fn 1] All AT-C sections can be found in AICPA *Professional Standards*.

residual risk. The risk to the achievement of objectives that remains after management's response has been designed and implemented.

retention. A phase of the data life cycle that pertains to how long an entity stores information for future use or reference.

risk. The possibility that an event will occur and adversely affect the achievement of objectives.

risk response. The decision to accept, avoid, reduce, or share a risk.

security event. An occurrence, arising from actual or attempted unauthorized access or use by internal or external parties, that impairs or could impair the availability, integrity, or confidentiality of information or systems: result in unauthorized disclosure or theft of information or other assets; or cause damage to systems.

security incident. A security event that requires action on the part of an entity to protect information assets and resources.

senior management. The CEO or equivalent organizational leader and senior management team.

service provider. A supplier (such as a service organization) engaged to provide services to the entity. Service providers include outsourced service providers as well as suppliers that provide services not associated with business functions, such as janitorial, legal, and audit services.

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 AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*.

SOC 3® engagement. An examination engagement to report on the suitability of design and the operating effectiveness of an entity's controls over a system relevant to one or more of the trust services categories.

SOC for Cybersecurity examination. An examination engagement to report on whether (*a*) management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (*b*) the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria. A SOC for Cybersecurity examination is performed in accordance with the attestation standards and AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*.

SOC for Supply Chain examination. An examination engagement to report on whether (*a*) the description of the entity's system is presented in accordance with the description criteria and (*b*) the

controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria. Such an examination is based on guidance contained in AICPA Guide *Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System* (SOC for Supply Chain guide).

software. A collection of instructions that tell a computer how to operate. Software may be both internally developed and purchased from vendors and can include both application software (for example, user applications and database management systems) and system software (for example, operating systems, drivers, utilities, programming software, and interfaces).

stakeholders. Parties that are affected by the entity, such as shareholders, the communities in which an entity operates, employees, customers, and suppliers.

subsequent events. Events or transactions that occur after the specified period addressed by the description but prior to the date of the practitioner's report. Such events or transactions could have a significant effect on the evaluation of whether the description is presented in accordance with the description criteria or whether controls were effective to provide reasonable assurance that the entity's principal system objectives were achieved based on the applicable trust services criteria.

supplier. See **vendor**.

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

system boundaries. The specific aspects of an entity's infrastructure, software, people, procedures, and data necessary to perform a function (such as producing, manufacturing, or distributing a product) or provide a service. When systems for multiple functions or services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each system will differ.

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

system event. An occurrence that could lead to the loss of, or disruption to, operations, services, or functions and could result in an entity's failure to achieve its system objectives. 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 entity management to prevent or reduce the impact of the event on the entity's achievement of its system objectives.

system objectives. The entity's objectives, established by entity management, that are embodied in the product commitments it makes to customers, including producing or manufacturing a product that meets product performance specifications and other production, manufacturing, or distribution specifications. The system objectives also include the requirements established for the functioning of the system to meet production, manufacturing, or distribution commitments.

system requirements. Specifications regarding how the system should function to (*a*) meet the entity's commitments to customers and others (such as customers' customers); (*b*) meet the entity's commitments to suppliers and business partners; (*c*) comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (*d*) achieve other entity objectives that are 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.

System requirements may result from the entity's commitments relating to security, availability, processing integrity, confidentiality, or privacy. For example, a commitment to programmatically enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration.

third party. An individual or organization other than the entity and its employees. Third parties may be customers, suppliers, business partners, or others.

threat. Any circumstance or event, arising from human actions or natural events, that could potentially impair (*a*) the achievement of an entity's objectives, its assets, or activities of its personnel, or (*b*) other entities through unauthorized access, destruction, disclosure, modification of data, or denial of service.

trust services. A set of professional attestation and advisory services based on a core set of criteria related to security, availability, processing integrity, confidentiality, or privacy.

unauthorized access. Access to information or system components that (*a*) has not been approved by a person designated to do so by management and (*b*) compromises segregation of duties, confidentiality commitments, or otherwise increases risks to the information or system components beyond the levels approved by management (that is, access is inappropriate).

vendor (or supplier). An individual or business (and its employees) that is engaged to provide goods or services to the entity. Depending on the services provided (for example, if the vendor operates certain controls on behalf of the entity that are necessary to achieve the entity's objectives), it also might be a service provider.

vulnerability. Weakness in a component of a system, particularly information assets, system security procedures, internal controls, or implementation, that could be exploited or triggered by human action or natural events.