Issued by the **AICPA Assurance Services Executive Committee (ASEC)**

Trust Services Criteria

AICPA®

Issued by the **AICPA Assurance Services Executive Committee (ASEC)**

Trust Services Criteria

22099-349

AICPA®

1 2 3 4 5 6 7 8 9 0 BRAAS 1 9 8 7
ISBN 978-1-94549-881-7

TABLE OF CONTENTS

Chapter	Paragraph
TSP Section 100—2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy	.01-.27
Notice to Readers	
Background	.01-.04
Organization of the Trust Services Criteria	.05-.10
Trust Services Categories	.09-.10
Application and Use of the Trust Services Criteria	.11-.19
Professional Standards Governing Engagements Using the Trust Services Criteria	.20-.23
Attestation Engagements	.20-.22
Consulting Engagements	.23
Trust Services Criteria	.24
Transition Guidance	.25-.26
Appendix A—Glossary	.27
TSP Section 100A—Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)	01.-.19
Introduction	.01-.07
Principles, Criteria, Controls, and Risks	.08-.12
Trust Services Principles	.13
Trust Services Criteria	.14
Trust Services Principles and Criteria	.15
Effective Date	.16
Appendix A—Definitions	.17
Appendix B—Illustration of Risks and Controls for a Sample Entity	.18
Appendix C—Mapping of the Trust Services Principles and Criteria to Extant Generally Accepted Privacy Principles	.19
TSP Section 100A-1—Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)	.01-.20
Introduction	.01-.12
Principles, Criteria, Controls, and Risks	.08-.12
Trust Services Principles	.13
Trust Services Criteria	.14
Trust Services Principles and Criteria	.15-.16
Privacy Principles and Criteria	.16
Effective Date	.17

Chapter Paragraph

TSP Section 100A-1—Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)—continued

Appendix A—Definitions ..... .18
Appendix B—Illustrative Risks and Controls ..... .19
Appendix C—Generally Accepted Privacy Principles ..... .20

TSP Section 100

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

(To supersede TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.)

Notice to Readers

The *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* presents control criteria established by the Assurance Services Executive Committee (ASEC) of the AICPA for use in attestation or consulting engagements to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy over information and systems (*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; or (*d*) for a particular type of information used by the entity. ASEC, in establishing and developing these criteria, followed due process procedures, including exposure of the proposed criteria for public comment. Under BL section 360, *Committees* (AICPA, *Professional Standards*), ASEC has been designated as a senior committee and has been given authority to make public statements and publish measurement criteria without clearance from AICPA Council or the board of directors.

Background

.01 The AICPA Assurance Services Executive Committee (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, or the confidentiality or privacy of the information processed by the systems 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 system(s) 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 meet the trust services criteria. Such risks 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

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 Applying the trust services criteria in actual situations requires judgment. Therefore, in addition to the trust services criteria, this document also presents points of focus for each criterion. The Committee of Sponsoring Organizations (COSO), in its *Internal Control—Integrated Framework* (COSO framework),[1] states that points of focus represent important characteristics of the criteria. Consistent with the COSO framework, the points of focus in this document may assist management when designing, implementing, and operating controls over security, availability, processing integrity, confidentiality, and privacy. In addition, the points of focus may assist both management and the practitioner when they are evaluating whether the controls were suitably designed and operated effectively to meet the trust services criteria.

.04 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. Use of the trust services criteria does not require an assessment of whether each point of focus is addressed. Users should carefully consider the facts and circumstances of the entity and its environment in actual situations when applying the trust services criteria.

Organization of the Trust Services Criteria

.05 The trust services criteria presented in this document have been aligned to the 17 criteria (known as *principles*) presented in *Internal Control—Integrated Framework,* which was revised in 2013 by COSO. 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 the 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 system(s) 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

[1] ©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

.06 In addition to the 17 principles in the COSO framework, certain of the supplemental criteria are shared amongst all the 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 service categories (common criteria) and
- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

.07 For the security category, the common criteria constitute the complete set of criteria. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of the common criteria and the criteria applicable to the specific trust services category or categories addressed by the engagement. The criteria for a trust services category addressed by the engagement are considered to be complete only if all the criteria associated with that category are addressed by the engagement.

.08 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 the criteria for that category should usually be addressed. However, in limited circumstances, such as when the scope of the engagement is to report on a system and a particular criterion is not relevant to services provided by a service organization, one or more criteria may not be applicable to the engagement. In such situations, the one or more criteria would not need to be addressed. 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 not applicable for a service organization that does not directly collect personal information from data subjects. Further, the common criteria should be applied regardless of which trust services category is included within the scope of the engagement.

Trust Services Categories

.09 The table in paragraph .24 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 meet 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.* 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.

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 to meet the entity's objectives.

Although the 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 meet its objectives related to privacy.

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

vii. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet 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.

.10 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.

Application and Use of the Trust Services Criteria

.11 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 matters 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 the cybersecurity risk management examination.[2]

- 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 meet 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.[3]
- 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.
- The suitability of the design of an entity's controls over security, availability, processing integrity, confidentiality, or privacy to meet the related trust services criteria.[4]

.12 Practitioners generally do not use the trust services criteria when engaged to report on an entity's compliance, or on an entity's internal control over compliance with laws, regulations, rules, contracts, or grant agreements. If the practitioner is engaged to report on compliance with laws, regulations, rules, contracts, or grant agreements in connection with an examination of the design and operating effectiveness of an entity's controls (for example, in a privacy engagement performed in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT- C section 205, *Examination*

---

[2] 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 cybersecurity risk management examination.

[3] AICPA Guide *Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*, issued in July 2015, contains performance and reporting guidance for SOC 2 examinations.

[4] 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" (AICPA, *Professional Standards*, AT-C sec. 9205 par. .04–.14). That document states that a practitioner may examine the suitability of the design of controls under AT-C section 205, *Examination Engagements*. Paragraph .10 of AT-C section 205 provides guidance on how a practitioner should report when the engagement is over controls that have not yet been implemented.

Engagements),[5] the compliance portion of the engagement would be performed in accordance with AT-C sections 105 and 315, *Compliance Attestation*.

.13 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 .11) in a variety of different types of engagements (see paragraphs .20–.23), 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.

.14 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 commitments to customers and system requirements. 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 meet the entity's commitments to customers, relevant laws and regulations, or guidelines of industry groups, such as trade or business associations.
- In an entity-wide cybersecurity risk management 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.[6]

---

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

[6] 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.

.15 As an example of how the different subject matters and engagement scopes 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, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

.16 In the SOC 2 engagement example discussed in paragraph .14, 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, back-up media storage, and other sensitive locations) to authorized personnel *to meet the service organization's commitments and system requirements.*

.17 In addition, criterion CC6.4 would only be applied as it relates to controls over the trust service category(ies) relevant to the system(s) included within the scope of the SOC 2 engagement.

.18 In the cybersecurity risk management examination example in paragraph .14, 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, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's cybersecurity objectives.

.19 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 cybersecurity risk management examination.

Professional Standards Governing Engagements Using the Trust Services Criteria

Attestation Engagements

.20 Examination engagements and engagements to apply agreed-upon procedures performed in accordance with the AICPA *Statements on Standards for Attestation Engagements*[7] (SSAEs or *attestation standards*) may use the trust services criteria as the evaluation criteria. The attestation standards provide guidance on performing and reporting in connection with an examination, review,[8] and agreed-upon procedures engagements. Under the attestation standards, the CPA performing an attestation engagement is known as a *practitioner*. In an examination engagement, the practitioner provides a report in which he or she expresses an opinion on subject matter or an assertion

[7] Statement on Standards for Attestation Engagements No. 18, *Attestation Standards: Clarification and Recodification* (AICPA, *Professional Standards*), is effective for practitioners' reports dated on or after May 1, 2017.

[8] Paragraph .07 of AT-C section 305, *Prospective Financial Information*, 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.

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 are performed in accordance with AT-C sections 105 and 205; agreed-upon procedures engagements are performed in accordance with AT-C sections 105 and 215.

.21 According to the attestation standards, the criteria used in an attestation engagement should be suitable and available to report users. Attributes of suitable criteria are as follows:[9]

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

.22 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. Accordingly, ASEC has concluded that the trust services criteria are suitable criteria in accordance with the attestation standards.

Consulting Engagements

.23 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.[10] 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* (AICPA, *Professional Standards*).

Trust Services Criteria

.24 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[11] are presented using a normal font. In contrast, 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

---

[9] Paragraph .25*b* of AT-C section 105, *Concepts Common to All Attestation Engagements*.

[10] 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 (AICPA, *Professional Standards*, 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.

[11] ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

apply only when engagements using the trust services criteria are performed at a system level are presented in ***bold italics***.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	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:
	• 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 specifically related to all engagements 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.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• 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—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
	Additional point of focus specifically related to all engagements 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.
	• 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 specifically related to all engagements 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.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *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.*
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 point of focus specifically related to all engagements 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.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• 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.
	COMMUNICATION AND INFORMATION
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, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• 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.

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• 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.
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 specifically related to all engagements 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.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *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 to personnel.*
	• *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 points of focus that apply only when an engagement using the trust services criteria is performed 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.

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• 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 that applies only to an engagement using the trust services criteria for confidentiality:
	• *Communicates Objectives Related to Confidentiality and Changes to Objectives— The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.*
	Additional point of focus that applies only to an engagement using the trust services criteria for privacy:
	• *Communicates Objectives Related to Privacy and Changes to Objectives—The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.*
	Additional points of focus that apply only when an engagement using the trust services criteria is performed 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 communications about their responsibilities and have the information necessary to carry out those responsibilities.***

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• ***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 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 • 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 • 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.

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	External Nonfinancial Reporting Objectives
	• 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
	• 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
	• 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 specifically related to all engagements using the trust services criteria:
	• *Establishes Sub-objectives to Support Objectives—Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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 specifically related to all engagements using the trust services criteria:
	• *Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified 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 others with access to the entity's information systems.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Considers the Significance of the Risk—The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.*
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 specifically related to all engagements 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 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.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• 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 specifically related to all engagements using the trust services criteria:
	• *Assess 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.*
	• *Assess Changes in Vendor and Business Partner Relationships—The risk identification process considers changes in vendor and business partner relationships.*
	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.

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• 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 specifically related to all engagements using the trust services criteria:
	• *Considers Different Types of Ongoing and Separate Evaluations—Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit 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.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• 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.

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Restricts Logical Access—Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.*
	• *Identifies and Authenticates Users—Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely.*
	• *Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.*
	• *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 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 supplement other measures used to protect data-at-rest, when such protections are deemed appropriate based on assessed risk.*
	• *Protects Encryption Keys—Processes are in place to protect encryption keys during generation, storage, use, and destruction.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Controls Access Credentials to Protected Assets—Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.*
	• *Removes Access to Protected Assets When Appropriate—Processes are in place to remove credential access when an individual no longer requires such access.*
	• *Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.*
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, specifically related to all engagements using the trust services criteria, 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 an individual no longer requires access.*
	• *Uses Role-Based Access Controls—Role-based access control is utilized to support segregation of incompatible functions.*
CC6.4	***The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Creates or Modifies Physical Access—Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.*
	• *Removes Physical Access—Processes are in place to remove access to physical resources when an individual no longer requires access.*
	• *Reviews Physical Access—Processes are in place to periodically review physical access to 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, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Identifies Data and Software for Disposal—Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.*
	• *Removes Data and Software From Entity Control—Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.*
CC6.6	***The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***
	The following points of focus, specifically related to all engagements using the trust services criteria, 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.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Implements Boundary Protection Systems—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.*
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, specifically related to all engagements using the trust services criteria, 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 back-up tapes), as appropriate.*
	• *Protects Mobile Devices—Processes are in place to protect mobile devices (such as laptops, smart phones and tablets) that serve as information assets.*
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, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts Application and Software Installation—The ability to install applications and software is restricted to authorized individuals.*
	• *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.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Uses Antivirus and Anti-Malware Software—Antivirus and anti-malware software is 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 and to remove any items detected prior to its implementation on the 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, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Uses Defined Configuration Standards—Management has defined configuration standards.*
	• *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 vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (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 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, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *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.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.*
	Additional points of focus that apply only in an engagement 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.*
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, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *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 Security Incidents—Procedures are in place to contain security incidents that actively threaten entity objectives.*
	• *Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.*
	• *Ends Threats Posed by Security Incidents—Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, 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 Protocols for Security Incidents—Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *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 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 that apply only in an engagement using the trust services criteria for privacy:
	• *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, specifically related to all engagements using the trust services criteria, 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, and changing configurations, as needed.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Communicates Information About the Event—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).*
	• *Determines Root Cause of the Event—The root cause of the event is determined.*
	• *Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.*
	• *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 continuity plans and systems 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, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software and procedures) is used to support system availability and processing integrity.*
	• *Authorizes Changes—A process is in place to authorize system changes prior to development.*
	• *Designs and Develops Changes—A process is in place to design and develop system changes.*
	• *Documents Changes—A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Tracks System Changes—A process is in place to track system changes prior to implementation.*
	• *Configures Software—A process is in place to select and implement the configuration parameters used to control the functionality of software.*
	• *Tests System Changes—A process is in place to test system changes prior to implementation.*
	• *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.*
	• *Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to meet 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 to continue to meet objectives 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 timeframe).*
	Additional points of focus that apply only in an engagement 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 meet the entity's objectives related to confidentiality.*
	Additional points of focus that apply only in an engagement 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 meet the entity's objectives related to privacy.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	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, specifically related to all engagements using the trust services criteria, 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 security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet 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 meet its objectives.*
CC9.2	***The entity assesses and manages risks associated with vendors and business partners.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Establishes Requirements for Vendor and Business Partner Engagements—The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.*
	• *Assesses Vendor and Business Partner Risks—The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.*
	• *Assigns Responsibility and Accountability for Managing Vendors and Business Partners—The entity assigns responsibility and accountability for the management of risks 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.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *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 periodically assesses the performance of vendors and business partners.*
	• *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.*
	Additional points of focus that apply only to an engagement 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 that apply only to an engagement 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.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	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 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 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 back-up 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 against environmental events.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *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 back-up 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 back-up failures, and initiating corrective action when such failures occur.*
	• *Addresses Offsite Storage—Back-up 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.*
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. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*
	• *Tests Integrity and Completeness of Back-Up Data—The integrity and completeness of back-up information is tested on a periodic basis.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	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:
	• *Identifies Confidential information—Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.*
	• *Protects Confidential Information from Destruction—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—Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.*
	ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY
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 Information Specifications—The entity identifies information specifications required to support the use of products and services.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *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 of the data is available to the users of the data* *(2) The definition of the data includes the following information:* *— The population of events or instances included in the data* *— The nature of each element (for example, field) of the 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)* *— Source(s) of the data* *— The unit(s) of measurement of data elements (for example, fields)* *— The accuracy/correctness/precision of measurement* *— The uncertainty or confidence interval inherent in each data element and in the population of those elements* *— The date the data was observed or the period of time during which the events relevant to the data occurred* *— The factors in addition to the date and period of time used to determine the inclusion and exclusion of items in the data elements and population* *(3) The definition 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 (meta-data) that has not been included within the data.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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 Production Errors—Errors in the production process 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.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	ADDITIONAL CRITERIA FOR PRIVACY
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—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—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 —An objective description of the entities and activities covered is included in the entity's privacy notice.*
	• *Uses Clear and Conspicuous Language—The entity's privacy notice is conspicuous and uses clear language.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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—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—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—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—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—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—Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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—The collection of personal information is limited to that necessary to meet the entity's objectives.*
	• *Collects Information by Fair and Lawful Means—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—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—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:
	• *Obtains Explicit Consent for Sensitive Information—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.*
	• *Documents Explicit Consent to Retain Information– Documentation of explicit consent for the collection, use, or disclosure of sensitive personal information is retained in accordance with objectives related to privacy.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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—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—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—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—Requests for deletion of personal information are captured, and information related to the requests is identified and flagged for destruction to meet the entity's objectives related to privacy.*
	• *Disposes of, Destroys, and Redacts Personal Information—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—Policies and procedures are implemented to erase or otherwise destroy personal information that has been identified for destruction.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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:
	• *Authenticates Data Subjects' Identity—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—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—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—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:
	• *Communicates Denial of Access Requests—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.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Permits Data Subjects to Update or Correct Personal Information—Data subjects are able to update or correct personal information held by the entity. The entity provides such updated or corrected information to third parties that were previously provided with the data subject's personal information consistent with the entity's objective related to privacy.*
	• *Communicates Denial of Correction Requests—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—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—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—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. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.*
	• *Discloses Information to Third Parties for New Purposes and Uses—Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of data subjects.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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—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—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:
	• *Discloses Personal Information Only to Appropriate Third Parties—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. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Remediates Misuse of Personal Information by a Third Party—The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such 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—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—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:
	• *Remediates Misuse of Personal Information by a Third Party—The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
	• *Provides Notice of Breaches and Incidents—The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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:
	• *Identifies Types of Personal Information and Handling Process—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—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 meet 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—Personal information is accurate and complete for the purposes for which it is to be used.*
	• *Ensures Relevance of Personal Information—Personal information is relevant to the purposes for which it is to be used.*

(continued)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
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—Data subjects are informed about how to contact the entity with inquiries, complaints, and disputes.*
	• *Addresses Inquiries, Complaints, and Disputes—A process is in place to address inquiries, complaints, and disputes.*
	• *Documents and Communicates Dispute Resolution and Recourse—Each complaint is addressed, and the resolution is documented and communicated to the individual.*
	• *Documents and Reports Compliance Review Results—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—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—Ongoing procedures are performed for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.*

Transition Guidance

.25 The 2017 trust services criteria presented in this document will be codified as TSP section 100. The extant trust services criteria issued in 2016 will be available in TSP section 100A through December 15, 2018. After that date, the 2016 criteria will be considered superseded. During the transition period (April 15, 2017 through December 15, 2018), practitioners should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used.

.26 In addition, the AICPA will continue to make available the 2014 trust services criteria in TSP section 100A-1 until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for practitioner reports for periods ended on or after December 15, 2016.

.27

Appendix A—Glossary

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 a computer, its operating system, a network, or other elements.

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, who 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 who supplies them 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. 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, including the following:

- Specification of the algorithm used in a calculation
- The hours a system will be available
- Published password standards
- Encryption standards used to encrypt stored customer data

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.

contractor. An individual, other than an employee, engaged to provide services to an entity in accordance with the terms of a contract.

control. A policy or procedure that is part of internal control. Controls exist within each of the five COSO internal control components: control environment, risk assessment, control activities, information and communication, and monitoring.

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" his or her 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.)

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).

cybersecurity risk management 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 cybersecurity risk management examination is performed in accordance with the attestation standards and the AICPA cybersecurity guide.

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.

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

disclosure. The release, transfer, provision of access to, 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.

environmental protections and safeguards. Controls and other activities implemented by the entity to detect, prevent, and manage the risk of casualty damage to the physical elements of the information system (for example, protections from fire, flood, wind, earthquake, power surge, or power outage).

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.

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.

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.

information assets. Data and the associated software and infrastructure used to process, transmit, and store information.

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

inherent limitations. Those limitations of all internal control systems. The limitations relate to the preconditions of internal control, external events beyond the entity's control, limits of human judgment, the reality that breakdowns can occur, and the possibility of management override and collusion.

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.

management override. Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status.

outsourced service providers. A service provider vendor 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 or can be about or 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 serves as the bases for procedures.

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, including the following:

- Types of information processed by the system
- Employees, third parties, and other persons that can access the information
- Conditions under which information can be processed without consent

Examples of privacy commitments include the following:

- The organization will not process or transfer information without obtaining the data subject's consent.
- The organization will provide a privacy notice to customers once in 6 months or when there is a change in the organization's business policies.
- The organization will respond to access requests within 10 working days of receiving the request from its customers.

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.

report users. Intended users of the practitioner's report in accordance with AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*). 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.

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.

risk tolerance. The acceptable variation relative to performance to the achievement of objectives.

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

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

senior management. The chief executive officer or equivalent organizational leader and senior management team.

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

SOC 2 engagement. An examination engagement to report on the fairness of the presentation of management's description of the service organization's system, the suitability of the design of the controls included in the description, and, in a type 2 engagement, the operating effectiveness of those controls. This engagement is performed in accordance with the attestation standards and the AICPA Guide *Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*.

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.

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

system. Refers to the infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more 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 or provide a service. When the systems for multiple functions or services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each service's system will differ. In an engagement that addresses the confidentiality and privacy criteria, the system boundaries cover, at a minimum, all the system components as they

relate to the life cycle of the confidential and personal information within well-defined processes and informal ad hoc procedures.

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

system requirements. Specifications regarding how the system should function to meet the entity's commitments to customers and relevant laws, regulations, and guidelines of industry groups, such as business or trade associations. Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations. Examples of system requirements are as follows:

- Employee fingerprinting and background checks established in government banking regulations
- System edits that restrict the values accepted for system input, which are defined in application design documents
- Maximum acceptable intervals between periodic reviews of workforce member logical access as documented in the security policy manual
- Data definition and tagging standards, including any associated metadata requirements, established by industry groups or other bodies, such as the Simple Object Access Protocol
- Business processing rules and standards established by regulators, for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA)

System requirements may result from the 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, vendors, business partners, or others.

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

TSP Section 100A

Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)

(To amend TSP section 100 and supersede appendix C, "Generally Accepted Privacy Principles," of TSP section 100A-1, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. The criteria in TSP section 100A are effective for periods ending on or after December 15, 2016, with earlier implementation permitted. TSP section 100A-1 will retain the superseded material until March 31, 2018. The practitioner should identify which set of criteria was used for the report and assertion.)

Introduction

.01 The AICPA Assurance Services Executive Committee (ASEC) has developed a set of principles and criteria (trust services principles and criteria) to be used in evaluating controls relevant to the security, availability, or processing integrity of a system, or the confidentiality or privacy of the information processed by the system. In this document, a *system* is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements. System components can be classified into the following five categories:

- *Infrastructure.* The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
- *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- *Processes.* The automated and manual procedures.
- *Data.* Transaction streams, files, databases, tables, and output used or processed by a system.

.02 This document presents the trust services principles and criteria for assessing the effectiveness of an entity's controls over a system relevant to the security, availability, processing integrity, confidentiality, or privacy. Management of an entity may use the trust services principles and criteria to evaluate its controls over a system or may engage a CPA to report on or provide consulting services related to those controls.

.03 Attestation services, performed under the AICPA Statements on Standards for Attestation Engagements[1] (commonly known as the *attestation*

[1] At the time of publication, the AICPA's Auditing Standards Board (ASB), has completed clarifying Statements on Standards for Attestation Engagements (SSAEs or attestation standards) and will be issuing its clarified attestation standards as SSAE No. 18, *Attestation Standards: Clarification and Recodification*. The ASB expects SSAE No. 18 to be available in April 2016 and to be effective for practitioners' reports dated on or after May 1, 2017.

standards), include examination, review,[2] and agreed-upon procedures engagements. In the attestation standards, the CPA performing an attest engagement is known as a practitioner. In an examination engagement, the practitioner provides a report that expresses an opinion on subject matter or an assertion about the subject matter in relation to an identified set of criteria. For example, a practitioner may report on whether controls over a system were operating effectively to meet the trust services criteria for processing integrity and confidentiality. 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 are performed in accordance with AT section 101, *Attest Engagements*, of the attestation standards and agreed-upon procedures engagements are performed in accordance with AT section 201, *Agreed-Upon Procedures Engagements* (AICPA, *Professional Standards*).

.04 The following are the types of subject matter a practitioner may examine and report on using the trust services principles and criteria:

- The fairness of the presentation of a description of a service organization's system relevant to one or more of the trust services principles of security, availability, processing integrity, confidentiality, and privacy using the description criteria in paragraph 1.26 (and paragraph 1.27 for descriptions addressing controls over privacy) of the AICPA Guide *Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*, as of July 1, 2015; the suitability of the design of controls included in the description to meet the related trust services criteria; and the operating effectiveness of those controls throughout a specified period to meet those trust services criteria (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 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 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 results of those tests.
- The design and operating effectiveness of a service organization's controls over a system relevant to one or more of the trust services principles of security, availability, processing integrity, confidentiality, and privacy (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 results of those tests.

[2] Review engagements generally consist of the performance of inquiries and analytical procedures designed to provide a moderate level of assurance (that is, negative assurance). However, the Assurance Services Executive Committee believes that a practitioner ordinarily could not perform meaningful analytical procedures on an entity's controls or compliance with requirements of specified laws, regulations, rules, contracts, or grants to achieve this level of assurance, and it is uncertain what other procedures could be identified that, when combined with inquiry procedures, could form the basis for a review engagement. Also due to this uncertainty, users of a review report are at greater risk of misunderstanding the nature and extent of the practitioner's procedures. Accordingly, the feasibility of a review engagement related to trust services is uncertain.

- The design and operating effectiveness of the controls of an entity, other than a service organization, over a system relevant to one or more of the trust services principles of security, availability, processing integrity, confidentiality, and privacy.
- The suitability of the design of an entity's controls over a system relevant to one or more of the trust services principles of security, availability, processing integrity, confidentiality, and privacy to meet the related trust services criteria. (Interpretation No. 7, "Reporting on the Design of Internal Control," [AICPA, *Professional Standards*, AT sec. 9101 par. .59–.69] of AT section 101, *Attest Engagements*, explains the context for this type of engagement, which typically is performed prior to the system's implementation.)

.05 Details about the services an entity agrees to provide to its customers (for example, what, how and when they will be provided) generally are included in written contracts, service level agreements, or public statements (for example, a privacy notice). The trust services principles and criteria refer to such agreements as *commitments*. Some commitments are applicable to all customers (baseline commitments), while 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 specifications regarding how the system should function to meet the entity's commitments to customers, and relevant laws, regulations, or guidelines of industry groups, such as trade or business associations, are referred to as *system requirements* in the trust services principles and criteria. Many of the trust services criteria refer to commitments and system requirements, for example:

> **CC1.4**. The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].

Management is responsible for meeting its commitments and for maintaining and operating the system in a manner that enables it to meet the system requirements.

.06 Trust services engagements do not entail reporting on an entity's compliance, or internal control over compliance, with laws, regulations, rules, contracts, or grant agreements, related to the principles being reported upon. If the practitioner is engaged to report on compliance with laws, regulations, rules, contracts, or grant agreements in conjunction with an engagement to report on the operating effectiveness of an entity's controls (for example, a privacy engagement in accordance with AT section 101), the compliance portion of the engagement would be performed in accordance with AT section 601, *Compliance Attestation* (AICPA, *Professional Standards*).

.07 Consulting services include developing findings and recommendations for the consideration and use of management of an entity when making decisions. In a consulting engagement, the practitioner does not express an opinion or form a conclusion about the subject matter. Generally, the work is performed only for the use and benefit of the client. Practitioners providing such services follow CS section 100, *Consulting Services: Definitions and Standards* (AICPA, *Professional Standards*).

Principles, Criteria, Controls, and Risks

.08 Trust services principles represent attributes of a system that support the achievement of management's objectives.

.09 For each of the principles there are detailed criteria that serve as benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. The attributes of suitable criteria are as follows:

- *Objectivity*. Criteria should be free from bias.
- *Measurability*. Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- *Completeness*. Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted.
- *Relevance*. Criteria should be relevant to the subject matter.

.10 ASEC has concluded that the trust services criteria for each individual principle, including the common criteria, have all of the attributes of suitable criteria. In addition to being suitable, AT section 101 indicates that the criteria must be available to users of the practitioner's report. The publication of the principles and criteria makes the criteria available to users.

.11 The trust services principles and criteria are designed to be flexible and to meet the business and assurance needs of users and management. Accordingly, a practitioner may be engaged to perform an engagement related to a single principle, multiple principles, or all of the principles.

.12 The environment in which the system operates, commitments made to customers and other third parties, responsibilities entailed in operating and maintaining a system, and the nature of the components of the system result in risks that the criteria will not be met. These risks are addressed through the implementation of suitably designed controls that, if operating effectively, provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, management of an entity needs to identify the specific risks that the criteria will not be met and the controls necessary to address those risks. Appendix B, "Illustration of Risks and Controls for a Sample Entity," provides examples of risks that may prevent the criteria from being met, as well as examples of controls that would address those risks. These illustrations are not intended to be applicable to any particular entity or to be all-inclusive of the risks to meeting the criteria or the controls necessary to address those risks.

Trust Services Principles

.13 The following are the trust services principles:

a. *Security.* The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.

The *security principle* refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system

requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

b. *Availability.* The system is available for operation and use to meet the entity's commitments and system requirements.

The *availability principle* refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The *availability principle* does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.

c. *Processing integrity.* System processing is complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements.

The *processing integrity principle* refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the system achieves its aim or the purpose for which it exists and whether it performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Processing integrity does not automatically imply that the information received and stored by the system is complete, valid, accurate, current, and authorized. The risk that data contains errors introduced prior to its input in the system often cannot be addressed by system controls, and detecting such errors is not usually the responsibility of the entity. Similarly, users outside the boundary of the system may be responsible for initiating processing. In these instances, the data may become invalid, inaccurate, or otherwise inappropriate even though the system is processing with integrity.

d. *Confidentiality.* Information designated as confidential is protected to meet the entity's commitments and system requirements.

The *confidentiality principle* addresses the system's ability to protect information designated as confidential, including, its final disposition and removal from the system in accordance with management's commitments and system requirements. 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 the boundaries of the system). Such requirements may be contained in laws or regulations, or commitments in user contracts. 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 the privacy applies only to personal information, while the confidentiality principle applies to various types of sensitive information. In addition, the privacy principle 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 to meet the entity's commitments and system requirements.

Although the confidentiality principle applies to various types of sensitive information, the privacy principle applies only to personal information. If the entity is directly responsible for providing services to data subjects covering all of the categories noted as follows, then the privacy principle may be appropriate. If the entity is not directly responsible for significant aspects of the following categories but retains responsibility for protecting personal information, the confidentiality principle may be more applicable.

The privacy criteria are organized into eight categories:

a. *Notice and communication of commitments and system requirements.* The entity provides notice to data subjects about its privacy practices its privacy commitments and system requirements.

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

c. *Collection.* The entity collects personal information to meet its privacy commitments and system requirements.

d. *Use, retention, and disposal.* The entity limits the use, retention, and disposal of personal information to meet its privacy commitments and system requirements.

e. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its privacy commitments and system requirements.

f. *Disclosure and notifications.* The entity discloses personal information, with the consent of the data subjects, to meet its privacy commitments and system requirements. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its privacy commitments and system requirements.

g. *Quality.* The entity collects and maintains accurate, up to date, complete, and relevant personal information to meet its privacy commitments and system requirements.

h. *Monitoring and enforcement.* The entity monitors compliance to meet its privacy commitments and system requirements including procedures to address privacy-related inquiries, complaints, and disputes.

Trust Services Criteria

.14 Many of the criteria used to evaluate a system are shared amongst all of the principles; for example, the criteria related to risk management apply to the security, availability, processing integrity, confidentiality, and privacy principles. As a result, the trust services criteria consist of (1) criteria common to all five principles (common criteria) and (2) additional principle specific criteria for the availability, processing integrity, confidentiality, and privacy principles. For the security principle, the common criteria constitute the complete set of criteria. For the principles of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of the common criteria and the criteria applicable to the principle(s) addressed by the engagement. The criteria for a principle addressed by the engagement are considered to be complete only if all of the criteria associated with that principle are addressed by the engagement. The common criteria are organized into seven categories:

a. *Organization and management.* The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units to meet the criteria for the principle(s) addressed by the engagement. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

b. *Communications.* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and system requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system to meet the criteria for the principle(s) addressed by the engagement.

c. *Risk management and design and implementation of controls.* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process to meet the criteria for the principle(s) addressed by the engagement.

d. *Monitoring of controls.* The criteria relevant to how the entity monitors the system, including the suitability of the design and operating effectiveness of the controls, and takes action to address deficiencies identified to meet the criteria for the principle(s) addressed by the engagement.

e. *Logical and physical access controls.* The criteria relevant to how the entity restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed by the engagement.

f. *System operations.* The criteria relevant to how the entity manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the criteria for the principle(s) addressed by the engagement.

g. *Change management.* The criteria relevant to how the entity identifies the need for changes to the system, makes the changes using a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed by the engagement.

Trust Services Principles and Criteria

.15 For each of the following trust services criteria, the wording presented in brackets needs to be tailored for the specific principle(s) addressed by the engagement. The trust services principles of security, availability, processing integrity, confidentiality, or privacy may be reported on individually or in combination with any or all of the other trust services principles. For each principle addressed by the engagement, all of the criteria for that principle should be addressed. Further, the common criteria should be applied regardless of the trust services principles being addressed by the engagement.

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
CC1.0	***Common Criteria Related to Organization and Management***
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy or any combination thereof*].
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] and provides resources necessary for personnel to fulfill their responsibilities.

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].
CC2.0	***Common Criteria Related to Communications***
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.
CC2.2	The entity's [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] of the system, is provided to personnel to carry out their responsibilities.
CC2.5	Internal and external users have been provided with information on how to report [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] failures, incidents, concerns, and other complaints to appropriate personnel.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] are communicated to those users in a timely manner.

(continued)

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
CC3.0	***Common Criteria Related to Risk Management and Design and Implementation of Controls***
CC3.1	The entity (1) identifies potential threats that could impair system [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.
CC4.0	***Common Criteria Related to Monitoring of Controls***
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*], and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*]. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].
CC5.6	Logical access security measures have been implemented to protect against [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].

(continued)

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].
CC6.0	***Common Criteria Related to System Operations***
CC6.1	Vulnerabilities of system components to [*insert the principle(s)addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].
CC6.2	[*Insert the principle(s)addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.
CC7.0	***Common Criteria Related to Change Management***
CC7.1	The entity's commitments and system requirements, as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*], are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] commitments and system requirements.
Additional Criteria for Availability	
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.
Additional Criteria for Processing Integrity	
PI1.1	Procedures exist to prevent, or detect and correct, processing errors to meet the entity's processing integrity commitments and system requirements.
PI1.2	System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.
PI1.3	Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.
PI1.4	Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the entity's processing integrity commitments and system requirements.
PI1.5	System output is complete, accurate, distributed, and retained to meet the entity's processing integrity commitments and system requirements.
PI1.6	Modification of data, other than routine transaction processing, is authorized and processed to meet the entity's processing integrity commitments and system requirements.

(continued)

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
Additional Criteria for Confidentiality	
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.
C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.
C1.6	Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.
C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.
C1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.
Additional Criteria for Privacy	
P1.0	***Privacy Criteria Related to Notice and Communication of Commitments and System Requirements***
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's privacy commitments and system requirements. 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 privacy commitments and system requirements.
P1.2	The entity's privacy commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
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 the data subject or other authorized person, if required, and such consent is obtained only for the purpose for which the information is intended consistent with the entity's privacy commitments and system requirements. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.
P3.0	***Privacy Criteria Related to Collection***
P3.1	Personal information is collected consistent with the entity's privacy commitments and system requirements.
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 consistent with the entity's privacy commitments and system requirements.
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 privacy commitments and system requirements.
P4.2	The entity retains personal information consistent with the entity's privacy commitments and system requirements.
P4.3	The entity securely disposes of personal information consistent with the entity's privacy commitments and system requirements.
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 the data subject consistent with the entity's privacy commitments and system requirements. If access is denied, the data subject is informed of the denial and reason for such denial, as required, consistent with the entity's privacy commitments and system requirements.

(continued)

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
P5.2	The entity corrects, amends, or appends personal information based on information provided by the data subjects and communicates such information to third parties, as committed or required, consistent with the entity's privacy commitments and system requirements. If a request for correction is denied, the data subject is informed of the denial and reason for such denial consistent with the entity's privacy commitments and system requirements.
P6.0	***Privacy Criteria Related to Disclosure and Notification***
P6.1	The entity discloses personal information to third parties with the explicit consent of the data subject to meet the entity's privacy commitments and system requirements, and such consent is obtained prior to disclosure.
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information consistent with the entity's privacy commitments and system requirements.
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures of personal information, including breaches, consistent with the entity's privacy commitments and system requirements.
P6.4	The entity obtains privacy commitments from vendors and other third parties whose products and services are part of the system and who have access to personal information processed by the system that are consistent with the entity's privacy commitments and system requirements.
P6.5	Compliance with the entity's privacy commitments and system requirements by vendors and others third parties whose products and services are part of the system and who have access to personal information processed by the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.
P6.6	The entity obtains commitments from vendors and other third parties that may have access to personal information processed by the system, 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 to meet the entity's established incident response procedures, privacy commitments, and system requirements.
P6.7	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others consistent with the entity's privacy commitments and system requirements.
P6.8	The entity provides to the data subjects an accounting of the personal information held and disclosure of a data subject's personal information, upon the data subject's request, consistent with the entity's privacy commitments and system requirements.

Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles	
P7.0	***Privacy Criteria Related to Quality***
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information consistent with the entity's privacy commitments and system requirements.
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 with the entity's privacy commitments and system requirements; corrections and other necessary actions related to identify deficiencies are taken in a timely manner.

Effective Date

.16 The trust services principles and criteria are effective for periods ending on or after December 15, 2016. Early implementation is permitted.

.17

Appendix A—Definitions

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 must be able to find out what personal information an entity has on file about them and how the information is being used. Individuals must be able to correct erroneous information in such records.

authorized access. Access to system components that (*a*) has been approved by a person designated to do so by management and (*b*) does not compromise segregation of duties, confidentiality commitments, or otherwise increase risk to the system beyond the levels approved by management (that is, access is appropriate).

boundary of the system. The specific aspects of an entity's infrastructure, software, people, procedures, and data necessary to perform a function or provide a service. When the systems for multiple functions or services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each service's system will differ. In an engagement that addresses the confidentiality and privacy principles, the system boundaries cover, at a minimum, all the system components as they relate to the life cycle of the confidential and personal information within well-defined processes and informal ad hoc procedures.

collection. The process of obtaining personal information from either the individual directly, such as a Web 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 a system. 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 principles. The practitioner need only consider commitments related to the principles addressed by the engagement. Commitments may be made on many different aspects of the service being provided, including the following:

- Specification of the algorithm used in a calculation
- The hours a system will be available
- Published password standards
- Encryption standards used to encrypt stored customer data

consent. This privacy requirement is one of the fair information practice principles. 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" his or her agreement with a data controller by some active communication between the parties. According to the EU Data Protection Directive, explicit consent is required for processing of sensitive information. Further, data controllers cannot infer consent from nonresponse to a communication.
- **implied consent.** When consent may reasonably be inferred from the action or inaction of the individual.

data subjects. The individual to whom personal information is collected.

disclosure. The release, transfer, provision of access to, 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 lifecycle that pertains to how an entity removes or destroys an individual's personal information.

environmental protections. Measures implemented by the entity to detect, prevent, and manage the risk of casualty damage to the physical parts of the system (for example, protections from fire, flood, wind, earthquake, power surge, or power outage).

external users. Individuals that are non-workforce members or personnel who are authorized by customers, entity management, or other authorized persons to interact with the system.

internal users. Workforce members or personnel whose job function causes them to be members of the people component of the system.

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

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

- Types of information processed by the system
- Employees, third parties, and other persons that can access the information
- Conditions under which information can be processed without consent

Some examples include the following:

- The organization will not process or transfer information without obtaining the data subject's consent.
- The organization will provide a notice to customers once in 6 months or when there is a change in the organization's business policies.
- The organization will respond to access requests within 10 working days of receiving the request from its customers.

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.

report users. Intended users of the practitioner's report in accordance with AT section 101, *Attest Engagements* (AICPA, *Professional Standards*). Report users may be the general public or may be restricted to specified parties in accordance with paragraph .78 of AT section 101.

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

system requirements. Specifications regarding how the system should function to meet the entity's commitments to customers and relevant laws, regulations, and guidelines of industry groups, such as business or trade associations. Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations. Examples of system requirements are

- workforce member fingerprinting and background checks established in government banking regulations.
- system edits that restrict the values accepted for system input, which are defined in application design documents.
- maximum acceptable intervals between periodic review of workforce member logical access as documented in the security policy manual.
- data definition and tagging standards, including any associated metadata requirements, established by industry groups or other bodies, such as the Simple Object Access Protocol.
- business processing rules and standards established by regulators, for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA).

System requirements may result from the 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.

SOC 2 engagement. An examination engagement to report on the fairness of the presentation of management's description of the

service organization's system, the suitability of the design of the controls included in the description, and, in a type 2 engagement, the operating effectiveness of those controls. This engagement is performed in accordance with the attestation standards and the AICPA Guide *Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*.

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 principles.

third party. An entity that is not a party to the contract between the entity and the contractual user of the system but has an involvement with the system.

trust services. A set of professional attestation and advisory services based on a core set of principles and criteria that address the operation and protection of a system and related data.

workforce member. Employees, contractors, and others (personnel) engaged by company to perform activities as part of the system.

.18

Appendix B—Illustration of Risks and Controls for a Sample Entity

In evaluating whether controls are suitably designed to meet each of the trust services criteria, management needs to evaluate the risks that would prevent the criteria from being met for the system being assessed. In identifying these risks, management needs to consider the

- products and services provided by the system.
- components of the system used to provide the products and services.
- environment in which the system operates.
- commitments the entity has made to system users and parties affected by the system.
- system requirements that derive from
  - — laws and regulations affecting how the system functions and products and services are provided,
  - — commitments made to system users and parties affected by the system, and
  - — business objectives of the entity.

The illustration that follows is an example of the risks that a hypothetical mid-sized entity might identify during its risk evaluation and the controls that it could implement to address those risks. It is provided to assist practitioners with an understanding of the types of risks an entity might identify and controls to mitigate the risks to meet the criteria. It is not intended to be an all-inclusive listing of possible risks and controls. Each entity needs to consider other risks and controls to address those risks to meet the criteria. Also, the types of controls are presented at a high level and do not include the details that would be necessary for a suitably designed control, for example, the position of the person performing the control, the frequency with which the control is performed, and how the control is performed, documented, and monitored.

Criteria		Illustrative Risks	Illustrative Types of Controls
Criteria Common to All [Security, Availability, Processing Integrity, Confidentiality, and Privacy] Principles			
CC1.0	***Common Criteria Related to Organization and Management***		
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	The entity's organizational structure does not provide the necessary structure, resources, and information flow to manage [*security, availability, processing integrity, confidentiality, or privacy*] activities.	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and system requirements.
		The roles and responsibilities of key managers are not sufficiently defined to permit proper oversight, management, and monitoring of [*security, availability, processing integrity, confidentiality, or privacy*] activities.	Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.
			Job descriptions are reviewed by entity management on an annual basis for needed changes and, when job duty changes are required necessary, changes to these job descriptions are also made.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Reporting relationships and organizational structure do not permit effective senior management oversight of [*security, availability, processing integrity, confidentiality, or privacy*] activities.	Reporting relationships and organizational structures are reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.
		Personnel have not been assigned responsibility or have not been delegated insufficient authority to meet [*security, availability, processing integrity, confidentiality, or privacy*] commitments and system requirements.	Roles and responsibilities are defined in written job descriptions.
		Responsibility and accountability for privacy and data protection are not assigned to personnel with sufficient authority within the entity to manage risk and compliance.	Roles and responsibilities for privacy and data governance are defined and communicated to personnel as well as to third parties. The entity has assigned a chief privacy officer (CPO) who reports to the general counsel and audit committee. The CPO oversees the privacy staff responsible for implementation and monitoring of privacy controls. In addition, designated privacy advocates are assigned in each business unit and report indirectly to privacy staff.

Criteria		Illustrative Risks	Illustrative Types of Controls
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	Personnel have not been assigned responsibility or have been delegated insufficient authority to meet [*security, availability, processing integrity, confidentiality, or privacy*] commitments and system requirements.	Roles and responsibilities are defined in written job descriptions.
			Job descriptions are reviewed on a periodic basis for needed changes and updated if such changes are identified.
		Responsibility and accountability for privacy and data protection controls are not assigned to personnel with sufficient authority within the entity to manage risk and compliance.	The CPO oversees a privacy staff responsible for the implementation and monitoring of privacy controls. In addition, designated privacy advocates, who indirectly report to the CPO and privacy staff, are assigned in each business unit. Privacy advocates are responsible for helping to ensure the implementation of privacy controls and monitoring activities.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] and provides resources necessary for personnel to fulfill their responsibilities.	Newly hired, newly assigned, or transferred personnel do not have sufficient knowledge and experience to perform their responsibilities.	Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring, performance review, and transfer evaluation processes.
			The experience and training of candidates for employment or assignment are evaluated before they assume the responsibilities of their position.
		Personnel do not have sufficient periodic training to perform their responsibilities.	Management establishes requisite skillsets for personnel and provides continued training about its commitments and requirements for personnel.
			Management monitors compliance with training requirements.
		Technical tools and knowledge resources are insufficient to perform assigned tasks.	During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.

Criteria		Illustrative Risks	Illustrative Types of Controls
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	Personnel did not comply with the entity's requirements for conduct.	Management monitors personnel compliance with the code of conduct through monitoring of customer and workforce member complaints and the use of an anonymous third-party administered ethics hotline. The entity's code of conduct includes a sanctions policy for personnel who violate the code of conduct. The sanctions policy is applied to personnel who violate the code of conduct.
			Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and to formally reaffirm them annually thereafter.
		A candidate with a background considered to be unacceptable by management of the entity is hired by the entity.	Senior management develops a list of characteristics that would preclude a candidate from being hired based on sensitivity or skill requirements for the given position. That list is provided to the individuals within the organization who make final hiring decisions, and those characteristics are considered when evaluating all candidates.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Before a third party is engaged by the entity, the third-party personnel undergo background screening. A background check includes, at a minimum, credit, criminal, drug, and employment checks.
			Agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors.
			Prior to employment, personnel are verified against regulatory screening databases.
			The entity has established standards and guidelines for personnel ethical behavior.
CC2.0	***Common Criteria Related to Communications***		
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	External users misuse the system due to their failure to understand its scope, purpose, and design.	System descriptions are made available to authorized external users that delineate the boundaries of the system and describe relevant system components as well as the purpose and design of the system. Documentation of the system description is made available to authorized external users via the entity's customer-facing website.

Criteria		Illustrative Risks	Illustrative Types of Controls
			A description of the system is posted on the entity's intranet and is available to the entity's internal users. This description delineates the boundaries of the system and key aspects of processing.
		Internal users are unaware of key organization and system support functions, processes, roles, and responsibilities.	A description of the entity organization structure, system support functions, processes, and organizational roles and responsibilities is posted on the entity's intranet and made available to entity internal users. The description delineates the parties responsible, accountable, consented, and informed of changes in design and operation of key system components.
		External users fail to address risks for which they are responsible that arise outside the boundaries of the system.	System descriptions are made available to authorized external users that delineate the boundaries of the system and describe significant system components as well as the purpose and design of the system. The system description is made available to external users via ongoing communications with customers or via the customer website.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
CC2.2	The entity's [*insert the principle(s) addressed by the engagement: security, availability, processing integrity confidentiality, or privacy, or any combination thereof*] commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Internal and external users misunderstand the capabilities of the system in providing for [*security, availability, processing integrity, confidentiality, or privacy*] and take actions based on the misunderstanding.	The entity's [*security, availability, processing integrity, confidentiality, or privacy*] commitments regarding the system are included in the master services agreement and customer-specific service level agreements. In addition, a summary of these commitments is made available on the entity's customer-facing website. A privacy notice is posted on all of the entity's publicly available websites and software. The privacy notice describes the entity's privacy commitments.
			Policy and procedures documents for significant processes that address system requirements are available on the intranet.
		The entity fails to meet its commitments due to lack of understanding on the part of personnel responsible for providing the service.	Policy and procedures documents for significant processes are made available on the entity's intranet.
			Personnel are required to attend annual security, confidentiality, and privacy training.
			Personnel are required to read and accept the entity's code of conduct and the statement of security, confidentiality, and privacy practices upon hire and annually thereafter.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Processes are monitored monthly through service level management procedures that monitor compliance with service level commitments and agreements. Results are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties, including customers, when such commitments and agreements are not met.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	The system fails to function as designed due to internal users' failure to meet with their responsibilities.	Policy and procedures documents for significant processes that address system requirements are available on the intranet.
			Personnel are required to attend annual security, confidentiality, and privacy training.
			Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon hire and annually thereafter.
			Processes are monitored through service level management procedures that monitor compliance with commitments and requirements. Results are shared with applicable personnel and customers.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		The system fails to function as designed due to external users' failure to meet their responsibilities.	Customer responsibilities are described on the customer-facing website and in system documentation.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] of the system, is provided to personnel to carry out their responsibilities.	Controls fail to function as designed or operate effectively due to misunderstanding on the part of personnel responsible for implementing and performing those controls resulting in failure to achieve [*security, availability, processing integrity, confidentiality, or privacy*] commitments and system requirements.	Policy and procedures documents for significant processes are available on the intranet.
			Processes are monitored following service level management procedures that monitor compliance with commitments and requirements. Results are shared according to policies.
			Customer responsibilities are described on the customer-facing website and in system documentation.

Criteria		Illustrative Risks	Illustrative Types of Controls
CC2.5	Internal and external users have been provided with information on how to report [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] failures, incidents, concerns, and other complaints to appropriate personnel.	System anomalies are detected by internal or external users but the failures are not reported to appropriate personnel resulting in the system failing to achieve its [*security, availability, processing integrity, confidentiality, or privacy*] commitments and system requirements.	Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and made available on the intranet.
			Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns, and complaints, and the process for doing so, are described on the customer-facing website and in system documentation.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] are communicated to those users in a timely manner.	Internal and external users misunderstand changes in system capabilities or their responsibilities in providing for [*security, availability, processing integrity, confidentiality, or privacy*] due to system changes and take actions based on the misunderstanding.	Proposed system changes affecting customers are published on the customer-facing website XX days before their implementation. Internal and external users are given the chance to participate in user acceptance testing for major changes XX days prior to implementation. Changes made to systems are communicated and confirmed with customers through ongoing communications mechanisms such as customer care meetings and via the customer-facing website.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Management of the business unit must confirm understanding of changes by authorizing them.
		Internal and external users are not aware of system changes.	The system change calendar that describes changes to be implemented is posted on the entity intranet.
			Updated system documentation is published on the customer website and intranet 30 days prior to implementation.
			System changes that result from incidents are communicated to internal and external users through email as part of the implementation process.
		Changes in roles and responsibilities and changes to key personnel are not communicated to internal and external users in a timely manner.	Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal and external users via email as part of the change management process.
CC3.0	***Common Criteria Related to Risk Management and Design and Implementation of Controls***		
CC3.1	The entity (1) identifies potential threats that could impair system [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] commitments and system requirements	Not all system components are included in the risk management process resulting in a failure to identify and mitigate or accept risks.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.

Criteria		Illustrative Risks	Illustrative Types of Controls
	(including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises as necessary, risk assessments and mitigation strategies based on the identified changes.		

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Not all changes that significantly affect the system are identified resulting in a failure to correctly reassess related risks.	During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives. In response to the identification of such risks, management updates its policies, procedures, processes, and controls, as needed.
		Personnel involved in the risk management process do not have sufficient information to evaluate risks and the tolerance of the entity for those risks.	The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
		One or more internal or external risks that are significant threaten the achievement of [*security, availability, processing integrity, confidentiality, or privacy*] commitments, and system requirements that can be addressed by security controls, are not identified.	During the risk assessment and management process, risk management office personnel identify changes to business objectives, commitments and system requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Identified risks are rated using a risk evaluation process and ratings are reviewed by management.
			The entity preforms a privacy impact assessment (PIA) to identify privacy specific risks or compliance obligations and assesses the likelihood and potential magnitude of those risks. A PIA entails assessing the impact when new processes involving personal information are developed and when changes are made to such processes.
			The risk and controls group evaluates the effectiveness of controls and mitigation strategies in meeting identified risks and recommends changes based on its evaluation.
			The risk and controls group's recommendations are reviewed and approved by senior management. An owner is assigned for each remediation plan in risk assessments.
			The entity uses a configuration management database and related process to capture key system components, as well as technical and installation specific implementation details, and to support ongoing asset and service management commitments and requirements.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Changes that are not properly identified create risks due to the failure of those changes to undergo the risk management process.	During the risk assessment and management process, risk management personnel identify environmental, regulatory, and technological changes that have occurred. In response to the identification of such risks, management updates its policies, procedures, processes, and controls, as needed.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, and updates the controls, as necessary.	Controls and mitigation strategies selected, developed, and deployed do not adequately mitigate risk.	Control self-assessments are performed by operating units on a quarterly basis.
			Internal audits are performed based on the annual risk-based internal audit plan.
			Business and system recovery plans are tested annually.
			Internal and external vulnerability scans are performed quarterly and annually and their frequency is adjusted as required to meet ongoing and changing commitments and requirements. Management takes action based on the results of the scans.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Policies and procedures related to risk management are developed, implemented, and communicated to personnel.
		Deployed controls and mitigation strategies create new risks that fail to be assessed.	See CC3.1 illustrative controls.
CC4.0	***Common Criteria Related to Monitoring of Controls***		
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*], and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Controls are not suitably designed, configured in accordance with established policies, or operating in an effective manner, resulting in a system that does not meet commitments and system requirements.	Internal audit performs control assessments on a quarterly basis and communicates results to the audit committee for monitoring of corrective actions.
			Management and internal audit periodically receive reports summarizing incidents, root cause of incidents, and corrective action plans. Internal audit monitors for completion of corrective action plans.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Control self-assessments (including assessment of controls addressing privacy risks) are performed by operating units on a quarterly basis, and the results of these are reported to management for additional control monitoring purposes.
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***		
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	Not all system infrastructure or system components are protected by logical access security measures resulting in unauthorized modification or use.	Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Network scans are performed for infrastructure elements to identify variance from entity standards. Static and dynamic code analysis testing is performed on new application systems and on changes made to existing system source code prior to and after such systems are placed into production. Management takes appropriate action based on the results of the scans.
			Information system assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed and periodically evaluate access for assets under their custody or stewardship.
			Online applications match each user ID to a single customer account number. Requests for access to system records require the matching of the customer account number against a list of privileges each user possesses when granted access to the system initially.
		Logical access security measures do not identify or authenticate internal and external users prior to permitting access to IT components.	Infrastructure components and software are configured to use the shared sign-on functionality when available. Systems not using the shared sign-on functionality are required to be implemented with separate user ID and password submission.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			External access by personnel is permitted only through a two-factor (for example, a swipe card and a password) encrypted virtual private network (VPN) connection.
		Logical access security measures do not provide for the segregation of duties required by the system design.	A role based security process has been defined with an access control system that is required to use roles when possible.
			Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles. Roles are periodically reviewed and updated by asset owners and the risk and controls group on an annual basis. Access change requests resulting from the review are submitted to the security group via a change request record.
			For software or infrastructure that does not support the use of role-based security, a separate database of roles and related access privileges is maintained. The security group uses this database when specifying and entering access rules in these systems.

Criteria		Illustrative Risks	Illustrative Types of Controls
		Logical access security measures do not restrict access to system configurations, privileged functionality, master passwords, powerful utilities, security devices, and other high risk resources.	Privileged access to sensitive resources is restricted to defined user roles, and logical access to these roles must be approved by the chief information security officer. This access is reviewed by the chief information security officer on a periodic basis.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*]. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Valid user identities are granted to unauthorized persons.	On a daily basis, workforce member user IDs are automatically created in or removed from the active directory and VPN systems as of the date of employment using an automated feed of new internal and external users collected from workforce member changes in the human resource management system.
			Workforce access to protected resources is created or modified by the security group based on an authorized change request from the system's asset owner.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Contractor and vendor IDs are created by the security group based on an authorized change request from the contractor office. These IDs are valid for the lesser of the expected period of relationship or XX days.
			Privileged customer accounts are created based on a written authorization request from the designated customer point of contact. These accounts are used by customers to create customer user access accounts and their related privileges.
			System security is configured to require internal and external users to change their passwords upon their initial system sign-on and thereafter every XX days after their initial sign-on.
		A user that is no longer authorized continues to access system resources.	On a daily basis, the human resources system sends an automated feed to the active directory and the VPN for removal of access for personnel for whom it is the last day of employment. The list is used by security personnel to remove access. The removal of the access is verified by the security manager.

Criteria		Illustrative Risks	Illustrative Types of Controls
			On a weekly basis, the human resources system sends to the security group a list of terminated personnel whose access is to be removed. The list is used by security personnel to remove access. The removal of the access is verified by a security manager.
			On a weekly basis, the contractor office sends to the security group a list of terminated vendors and contractors whose access is to be removed. The list is used by security personnel to remove access. The removal of the access is verified by a security manager.
			Entity policies prohibit the reactivation or use of a terminated workforce member's ID without written approval of the chief information security officer. Requests for reactivation are made using the change management record system and must include the purpose and justification of the access (for business need), the systems that are to be reactivated, and the time period for which the account will be active (no more than XX days). The account is reset with a new password and is activated for the time period requested. All use of the account is logged and reviewed by security personnel.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Account sharing is prohibited unless a variance from policy is granted by the chief information security officer as might be provided by the entity using an account and password vaulting software product that provides account sharing under tightly controlled circumstances, the active logging of each use, and the resetting of the account password after each use. Otherwise, shared accounts are permitted for low risk applications (for example, an informational system where access with shared IDs cannot compromise segregation of duties) or when system technical limitations require their use (for example, UNIX root access). The chief information security officer must approve the use of all shared accounts. Mitigating controls are implemented when possible (for example, required use of *su* when accessing the UNIX root account).
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and	Internal and external users are not identified when accessing information system components.	Entity standards are established for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration

Criteria		Illustrative Risks	Illustrative Types of Controls
	system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].		standards, and standardized access control lists.
			Account sharing is prohibited unless a variance from policy is granted by the chief information security officer as might be provided by the entity using an account and password vaulting software product that provides account sharing under tightly controlled circumstances, active logging of each use, and the resetting of the account password after each use. Otherwise, shared accounts are permitted for low risk applications (for example, informational system where access with shared IDs cannot compromise segregation of duties) or when system technical limitations require their use (for example, UNIX root access). The chief information security officer must approve the use of all shared accounts. Mitigating controls are implemented when possible (for example, required use of *su* when accessing the UNIX root account).

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Valid user identities are assumed by an unauthorized person to access the system.	The online application authenticates the legitimacy of each customer user privileges by matching each users' ID upon entry to a single customer account number. Requests for access (for example, user attempts to access) to system records require the matching of the customer account number. Applications provide reporting functionality on user entitlements.
			Two-factor authentication and use of encrypted VPN channels help to ensure that only valid external users gain remote and local access to IT system components.
			Infrastructure components and software are configured to use the active directory shared sign-on functionality when available. Systems not using the shared sign-on functionality are configured to require a separate user ID and password. Applications provide reporting functionality on user entitlements.
		External user access credentials are compromised, allowing an unauthorized person to perform activities reserved for authorized persons.	External users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Password complexity standards are established to enforce control over access control software passwords.
			Administrative accounts are set up, and the user administration function is segregated for managing privileged accounts**.**
CC5.4	Access to data, software, functions, and other IT resources is authorized and modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	Valid internal or external users obtain unauthorized access to the system resulting in a breakdown in segregation of duties or an increase in the risk of intentional malicious acts or error.	When possible, formal role-based access controls to limit access to the system and infrastructure components are created and enforced by the access control system. When it is not possible, authorized user IDs with two-factor authentication are used.
			User access requests for a specific role are approved by the user's manager and submitted to the security group via the change management record system. Separation of duties exists between individuals who request access, authorize access, grant access, and review access.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Access granted through the provisioning process compromises segregation of duties or increases the risk of intentional malicious acts or error.	When possible, formal role-based access controls to limit access to the system and infrastructure components are created and enforced by the access control system. When it is not possible, authorized user IDs with two-factor authentication are used.
			Roles are reviewed and updated by both asset owners and the risk and controls group on an annual basis. Access change requests resulting from the review are submitted to the security group via a change request record.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	Unauthorized persons gain physical access to system components resulting in damage to components (including threats to personnel), fraudulent or erroneous processing, unauthorized logical access, or compromise of information.	An ID card-based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.
			ID cards that include a workforce member picture must be worn at all times when accessing or leaving the facility.

Criteria		Illustrative Risks	Illustrative Types of Controls
			ID cards are created by the human resources department during the workforce member orientation period and distributed after all required background investigations are completed. ID cards initially provide access only to non-sensitive areas.
			Access to sensitive areas is added to ID cards by the physical security director based on a request for access approved by the owner of the sensitive area and after required background investigations have been performed and any issues resolved. Requests for access and changes to access are made, approved, and communicated through the change management record system.
			The contractor office may request ID cards for vendors and contractors. Cards are created by the physical security director upon approval of authorized manager. Requests are made, approved, and communicated through the change management record system.
			Visitors must be signed in by an authorized workforce member before a single-day visitor badge that identifies them as an authorized visitor can be issued.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Visitor badges are for identification purposes only and do not permit access to any secured areas of the facility.
			All visitors must be escorted by a workforce member when visiting facilities where sensitive system and system components are maintained and operated.
		Formerly appropriate physical access becomes inappropriate due to changes in user job responsibilities or system changes, resulting in a breakdown in segregation of duties or an increase in the risk of intentional malicious acts or error.	Owners of sensitive areas of the facilities review the list of names and roles of those granted physical access to their areas on a semiannual basis to check for continued business need. Requests for changes are made through the change management record system.
		A formerly authorized person continues to access system resources after that person is no longer authorized.	Owners of sensitive areas of the facilities review access to their areas on a semiannual basis. Requests for changes are made through the change management record system.
			Vendors are asked to review a list of personnel with ID cards on a semiannual basis, recertify access entitlements, and request any modifications. The contractor office requests changes based on the vendor review.

Criteria		Illustrative Risks	Illustrative Types of Controls
			On a daily basis, as of the last day of employment, the human resources system sends to physical security a list of terminated personnel for whom it is the last day of employment and whose access is to be removed and their pass cards to be disabled.
		A user obtains the identification credentials and authentication credentials of a formerly authorized person and uses them to gain unauthorized access to the system.	On a weekly basis, the contractor office sends to the security group a list of terminated vendors and contractors for whom access is to be removed.
			On a weekly basis, or immediately upon termination of employment, the human resources system sends to the physical security group a list of terminated personnel for whom access is to be removed.
			Personnel are required to return their ID cards during exit interviews, and all ID badges are disabled prior to exit interviews. Therefore, personnel must be physically escorted from the entity's facilities at the completion of the exit interview.
			The sharing of access badges and tailgating are prohibited by policy.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Mantraps or other physical devices are used for controlling access to highly sensitive facilities.
			Doors that bypass mantraps can only be opened by the ID cards of designated members of management.
			A monitoring process exists to monitor entry or exit points. Measures such as, but not limited to, alarm systems, surveillance cameras, trained security guards, and so forth are adopted. The information (for example, logs, tapes, and so forth) is maintained for an agreed to period of time for future reference.
CC5.6	Logical access security measures have been implemented to protect against [*insert the principle(s) addressed by the engagement: security, availability, processing integrity confidentiality, or privacy, or any combination thereof*] threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Threats to the system are obtained through external points of connectivity.	Defined entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists that define which privileges are attributable to each user or system account.

Criteria		Illustrative Risks	Illustrative Types of Controls
			External points of connectivity are protected by a firewall complex, network segmentation, data loss prevention (DLP), and several layers of defense to prevent unauthorized external users from gaining access to the organization's internal systems and devices.
			Firewall hardening standards are based on relevant applicable technical specifications that are compared against product and industry recommended practices and updated periodically. Security Incident and Event Management (SIEM) software continually collects firewall logs and parses the entries using business rules and known threat signatures and creates alerts to the security and network operations teams when anomalous traffic or packets are identified so that firewall rules can be immediately updated to reduce security threat risks in the network, systems, and data stores.
			External access to nonpublic sites is restricted through the use of user authentication and message encryption systems such as VPN and SSL.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Authorized connections to the system are compromised and used to gain unauthorized access to the system.	Firewall rules and the online system limit the times when remote access can be granted and the types of activities and service requests (for example, disable copy/paste or remote print and drive mappings) that can be performed from external connections.
		Data stored temporarily outside its normal location (for example, stored during disaster recovery testing) is accessed by unauthorized persons.	Data written to the data storage systems within the disaster recovery facility is subject to sanitization procedures at the conclusion of disaster recovery testing prior to the return of control of storage to the facility vendor.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	Nonpublic information is disclosed during transmission over public communication paths.	VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity and to protect communications between the processing center and users connecting to the processing center from within or external to customer networks.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, email) unless it is encrypted.
			DLP software is used to scan for sensitive information in outgoing transmissions over public communication paths. Information that is restricted (Social Security numbers [SSNs], dates of birth, and so forth) is blocked, stripped, or both from outgoing transmissions.
		Removable media (for example, USB drives, DVDs, or tapes) are lost, intercepted, or copied during physical movement between locations.	Backup media are encrypted during creation.
			Storage for workstations and laptops is encrypted. Removable media for workstations and laptops are encrypted automatically by the software. Removable media is readable only by other entity-owned devices.
			Other removable media are produced by data center operations and are transported via courier.
			Use of removable media is prohibited by policy except when authorized by management

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Removable media used to make unauthorized copies of software or data are taken beyond the boundaries of the system.	Storage for workstations and laptops is encrypted. Removable media for these devices is encrypted automatically by the software. Removable media is readable only by other entity-owned devices.
			Backup media are encrypted during creation.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	Malicious or otherwise unauthorized code is used to intentionally or unintentionally compromise logical access controls or system functionality through data transmission, removable media, and portable or mobile devices.	The ability to install software on workstations and laptops is restricted to IT support personnel.
			Antivirus software is installed on workstations, laptops, and servers supporting such software. The antivirus program covers any piece of hardware that may be accessing the network, both internally and externally, as well as bring your own device (BYOD).

Criteria		Illustrative Risks	Illustrative Types of Controls
			Antivirus software is configured to receive an updated virus signature at least daily. A network operation receives a report of devices that have not been updated in 30 days and follows up on the devices.
		Business owners obtain and install applications without proper authorization.	The ability to install applications on systems is restricted to change implementation and system administration personnel.
CC6.0	***Common Criteria Related to System Operations***		
CC6.1	Vulnerabilities of system components to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	Vulnerabilities that could lead to a breach or incident are not detected in a timely manner.	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems; to monitor system performance, potential security threats and vulnerabilities, and resource utilization; and to detect unusual system activity or service requests. This software sends a message to the operations center and security organization and automatically opens a priority incident or problem ticket and change management system record item.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Call center personnel receive telephone and email requests for support, which may include requests to reset user passwords or notify entity personnel of potential breaches and incidents. Call center personnel follow defined protocols for recording, resolving, and escalating received requests.
			Vulnerability monitoring scans are performed on a periodic basis. Management takes appropriate action based on the results of the scans.
			Data loss prevention and detection tools are deployed at system boundaries to identify transmission of personal information.
			Data center operation personnel implement documented counter measures strategies when vulnerabilities are detected.
		Security or other system configuration information is corrupted or otherwise destroyed, preventing the system from functioning as designed.	Weekly full-system and daily incremental backups are performed using an automated system.

Criteria		Illustrative Risks	Illustrative Types of Controls
CC6.2	[*Insert the principle(s)addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	Breaches and incidents are not identified, prioritized, or evaluated for effects.	Operations personnel follow defined protocols for evaluating reported system events that may indicate a breach or other related incident. Security related events are assigned to the security group for evaluation. Privacy incidents are assigned to appropriate privacy personnel for evaluation.
		Corrective measures to address breaches and incidents are not implemented in a timely manner.	Operations and security personnel follow defined protocols for resolving and escalating reported events. This includes root cause analysis that is escalated to management as required.
			Resolution of security events (incidents or problems) is reviewed at the daily and weekly operations and security group meetings.
			Internal and external users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.
		Corrective measures are not effective or sufficient.	Resolution of events is reviewed at the weekly operations and security group meetings.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Change management requests are opened for events that require permanent fixes.
		Lack of compliance with policies and procedures is not addressed through sanctions or remedial actions, resulting in increased noncompliance in the future.	The resolution of events is reviewed at the weekly operations and security group meetings. Relevant events with effects on internal and external users or customers are referred to user and customer care management to be addressed.
			Entity policies include probation, suspension, and termination as potential sanctions for workforce member's misconduct.
		Breaches and incidents recur because preventive measures are not implemented after a previous event.	Change management requests are opened for events that require permanent fixes.
CC7.0	***Common Criteria Related to Change Management***		
CC7.1	The entity's commitments and system requirements, as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*], are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	Commitments and system requirements are not addressed at one or more points during the system development lifecycle, resulting in a system that does not meet commitments and system requirements.	System change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, confidentiality commitments, and system requirements throughout the change management process.

Criteria		Illustrative Risks	Illustrative Types of Controls
			System changes, other than those classified as minor, require the approval of the chief information security officer and operations manager prior to implementation.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	System components are not updated for changes in requirements, resulting in a system that does not meet commitments and system requirements.	During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are created based on the identified needs.
			For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*].	Identified breaches, incidents, and other system impairments are not considered during the change management lifecycle.	For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.
			A process exists to manage emergency changes.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's [*insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof*] commitments and system requirements.	System changes are not authorized by those responsible for the design and operation of the system, resulting in changes to the system that impairs its ability to meet commitments and system requirements.	System change requests must be reviewed and approved by the owner of the infrastructure or software and the change advisory board prior to work commencing on the requested change. Separate personnel are responsible to authorize changes and to implement the changes.
		System changes do not function as intended, resulting in a system that does not meet commitments and system requirements.	Functional and detailed designs are prepared for other than minor changes (more than XX hours). Functional designs are reviewed and approved by the application or infrastructure and software owner, and detailed designs are

Criteria		Illustrative Risks	Illustrative Types of Controls
			approved by the director of development for the application and the change advisory board prior to work commencing on the requested change or development project.
			Test plans and test data are created and used in required system and regression testing. Test plans and test data are reviewed and approved by the testing manager prior to and at the completion of testing, and they are reviewed by the change advisory board prior to newly developed or changed software being authorized for migration to production. Security vulnerability testing is included in the types of tests performed on relevant application, database, network, and operating system changes.
			System and regression testing is prepared by the testing department using approved test plans and test data. Deviations from planned results are analyzed and submitted to the developer.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Security vulnerability scans on developed source and object code libraries using Static Code Analysis tools are performed. Management remediates significant security vulnerabilities and coding defects prior to compiling computer programs and integrating them into the production environment.
			Code review or walkthrough is required for high impact changes that meet established criteria (that mandate code reviews and walkthroughs). These are performed by a peer programmer who does not have responsibility for the change.
			Changes are reviewed and approved by the change advisory board prior to implementation.
			Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.
			Changes to hardening standards are reviewed and approved by the director in infrastructure management.

Criteria		Illustrative Risks	Illustrative Types of Controls
		Unauthorized changes are made to the system, resulting in a system that does not meet commitments and system requirements.	Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in testing or production.
			Logical access controls and change management tools restrict the ability to migrate from development, test, and production to change deployment personnel.
			Changes are reviewed and approved by the change advisory board prior to implementation.
		Unforeseen system implementation problems impair system operation, resulting in a system that does not function as designed.	A turnover process that includes verification of operation and back out steps is used for every migration.
			Postimplementation procedures that are designed to verify the operation of system changes are performed for a defined period, as determined during project planning, after the implementation for other than minor changes, and results are shared with internal and external users and customers as required to meet commitments and system requirements.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Incompatible duties exist within the change management process, particularly between approvers, designers, implementers, testers, and owners, resulting in the implemented system not functioning as intended.	The change management process has defined the following roles and assignments: • Authorization of change requests—owner or business unit manager • Development—application design and support department • Testing—quality assurance department • Implementation—software change management group
Additional Criteria for Availability			
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	Current processing capacity is not sufficient to meet availability commitments and system requirements in the event of the loss of individual elements within the system components.	Processing capacity is monitored on an ongoing basis in accordance with SLAs, key performance indicators (KPIs), and other performance related parameters.
			Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.
		Processing capacity is not monitored, planned, and expanded or modified, as necessary, to provide for the continued availability of the system to meet the entity's commitments and system requirements.	Processing capacity is monitored on a daily basis.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Future processing demand is forecasted and compared to scheduled capacity on an ongoing basis. Forecasts are reviewed and approved by senior operations management. Change requests are initiated as needed based on approved forecasts.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Environmental vulnerabilities and changing environmental conditions are not identified or addressed through the use of environmental protections resulting in a loss of system availability.	Environmental protections have been installed including the following: • Cooling systems • Battery and natural gas generator backup in the event of power failure • Redundant communications lines • Smoke detectors • Dry pipe sprinklers • Vermin and pest control
		Environmental vulnerabilities are not monitored or acted upon increasing the severity of an environmental event.	Operations personnel monitor the status of environmental protections during each shift. Alert mechanisms have been installed to communicate any discrepancies in environmental thresholds.
			Environmental protections receive maintenance on at least an annual basis.
		Software or data are lost or not available due to processing error, intentional act, or environmental event.	Weekly full-system and daily incremental backups are performed using an automated system.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Backups are monitored for failure using an automated system, and the incident management process is automatically invoked.
			Backups are transported and stored offsite by a third-party storage provider in an environmentally controlled setting, transported by authorized courier (if stored offsite), and when encryption is not present, accompanied by chaperon.
		Availability commitments and system requirements are not met due to a lack of recovery infrastructure.	Business continuity and disaster recovery plans have been developed, updated, and tested annually.
			The entity has contracted with a third-party recovery facility to permit the resumption of IT operations in the event of a disaster at the IT data center.
			The entity uses a multilocation strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	Recovery plans are not suitably designed and backups are not sufficient to permit recovery of system operation to meet the entity's commitments and system requirements.	Business continuity and disaster recovery plans, including restoration of backups, and emergency notification systems are tested annually.
			Test results are reviewed and the contingency plan is adjusted.

Criteria		Illustrative Risks	Illustrative Types of Controls
Additional Criteria for Processing Integrity			
PI1.1	Procedures exist to prevent, or detect and correct, processing errors to meet the entity's processing integrity commitments and system requirements.	Software or data are lost or not available due to processing error, intentional act, or environmental event.	Weekly full-system and daily incremental backups are performed using an automated system.
			Backups are monitored for failure using an automated system, and the incident management process is automatically invoked.
			Backups are transported and stored offsite by a third-party storage provider.
		Environmental vulnerabilities are not addressed through the use of environmental protections, resulting in a loss of system availability.	Environmental protections have been installed including the following: • Cooling systems • Battery and natural gas generator backup in the event of power failure • Redundant communications lines • Smoke detectors • Dry pipe sprinklers
		Environmental vulnerabilities are not monitored or acted upon, increasing the severity of an environmental event.	Operations personnel monitor the status of environmental protections during each shift.
			Environmental protections receive maintenance on at least an annual basis.
		Current processing capacity is not sufficient to meet processing requirements, resulting in processing errors.	Processing capacity is monitored on a daily basis.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Critical infrastructure components have a defined level of redundancy based on risk assessment.
PI1.2	System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.	Inputs are captured incorrectly.	Application edits limit input to acceptable value ranges.
			The data preparation clerk batches documents by date received and enters the date and number of sheets on the batch ticket. Batched forms are scanned by a purchased imaging system. Upon completion of the scanning process, the scanned sheets are compared to the count per the batch ticket by the scanning operator.
			Scanned images are processed through the optical character recognition (OCR) system. Key fields including customer identifier, customer name, and record type are validated by the system against records in the master data file.
			Text from free-form sections from scan sheets is manually entered. This information is input twice by two separate clerks. The input information is compared, and records with differences are sent to a third clerk for resolution.

Criteria		Illustrative Risks	Illustrative Types of Controls
		Inputs are not captured or captured completely.	System edits require mandatory fields to be complete before record entry is accepted.
			The data preparation clerk batches documents by date received and enters the date and number of sheets on the batch ticket. Batched forms are scanned by a purchased imaging system. Upon completion of the scanning process, the sheets scanned are compared to the count per the batch ticket by the scanning operator.
			Scanned images are processed through the OCR system. Key fields, including customer identifier, customer name, and record type, are validated by the system against records in the master data file.
			Text from free-form sections from scan sheets is manually entered. This information is input twice by two separate clerks. The input information is compared, and records with differences are sent to a third clerk for resolution.
			Electronic files received contain batch control totals. During the load processing data captured is reconciled to batch totals automatically by the application.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Inputs are not captured in a timely manner.	Electronic files are processed when received. The application monitors files that fail to process completely and generates an incident management error record.
			Manual forms for data entry are batched upon receipt. Batches are traced to batches entered for processing daily by the date entry supervisor, and differences are investigated.
		The final disposition of input cannot be traced to its source to validate that it was processed correctly, and the results of processing cannot be traced to initial input to validate completeness and accuracy.	Inputs are coded with identification numbers, registration numbers, registration information, or time stamps to enable them to be traced from initial input to output and final disposition and from output to source inputs.
PI1.3	Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.	Data is lost during processing.	Input record counts are traced from entry to final processing. Any differences are investigated.
		Data is inaccurately modified during processing.	Application regression testing validates key processing for the application during the change management process.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Output values are compared against prior cycle values. Variances greater than X percent are flagged on the variance report, logged to the incident management system, and investigated by the output clerk. Resolutions are documented in the incident management system. Open incidents are reviewed daily by the operations manager.
			Daily, weekly, and monthly trend reports are reviewed by the operations manager for unusual trends.
		Newly created data is inaccurate.	Application regression testing validates key processing for the application during the change management process.
			The system compares generated data to allowable values. Values outside the allowable values are written to the value exception report. Items on the value exception report are reviewed by the output clerk on a daily basis.
		Processing is not completed within required timeframes.	Scheduling software is used to control the submission and monitoring of job execution. An incident management record is generated automatically in the service management system when processing errors are identified.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
PI1.4	Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the entity's processing integrity commitments and system requirements.	Data is not available for use as committed or agreed.	A mirror image of application data files is created nightly and stored on a second system for use in recovery and restoration in the event of a system disruption or outage.
		Stored data is inaccurate.	Logical access to stored data is restricted to the application and database administrators.
		Stored data is incomplete.	Data is reconciled on a monthly basis by rolling forward prior period balances with monthly activity and comparing results to the stored data balances.
PI1.5	System output is complete, accurate, and distributed to meet the entity's processing integrity commitments and system requirements.	System output is not complete.	Application regression testing validates key processing for the application during the change management process.
			Output values are compared against prior cycle values. Variances greater than X percent are flagged on the variance report, logged to the incident management system, and investigated by the output clerk. Resolutions are documented in the incident management system. Open incidents are reviewed daily by the operations manager.

Criteria		Illustrative Risks	Illustrative Types of Controls
			On a monthly basis, total records processed are compared with total records received via electronic submission, manual entry, and sheet scanned by the OCR system.
		System output is not accurate.	Application regression testing validates key processing for the application during the change management process.
			Output values are compared against prior cycle values. Variances greater than X percent are flagged on the variance report, logged to the incident management system, and investigated by the output clerk. Resolutions are documented in the incident management system. Open incidents are reviewed daily by the operations manager.
			Daily, weekly, and monthly trend reports are reviewed by the operations manager for unusual trends.
		System output is provided to unauthorized recipients.	Application security restricts output to approved user IDs.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		System output is not available to authorized recipients.	Output is generated by the system based on a master schedule. Changes to the master schedule are managed through the change management process and are approved by the customer service executive. On a daily basis, an automated routine scans output files to validate that all required output has been generated. The routine generates an incident record for any missing output. Incident tickets are managed through the incident management process.
PI1.6	Modification of data, other than routine transaction processing, is authorized and processed to meet the entity's processing integrity commitments and system requirements.	Data is modified by an unauthorized process or procedure resulting in inaccurate or incomplete data.	Application regression testing validates key processing for the application during the change management process.
			Access to data is restricted to authorized applications through access control software. Access rules are created and maintained by information security personnel during the application development process.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Application level security restricts the ability to access, modify, and delete data to authenticated internal and external users who have been granted access through a record in the access control list. Creation and modification of access control records occurs through the access provisioning process.
		Data is modified without authorization.	Logical access to stored data is restricted to the application and database administrators.
		Data is lost or destroyed.	Logical access to stored data is restricted to the application and database administrators.
			A mirror image of application data files is created nightly and stored on a second secure system for use in recovery and restoration in the event of a system disruption or outage.
Additional Criteria for Confidentiality			
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.	Data used in nonproduction environments is not protected from unauthorized access as committed.	The entity creates test data using data masking software that replaces confidential information with test information prior to the creation of test databases.
			Data owners approve any storage or use of production information in nonproduction environments.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.	Unauthorized access to confidential information is obtained during processing.	Access to data is restricted to authorized applications through access control software. Access rules are created and maintained by information security personnel during the application development process.
			Logical access other than through authorized application is restricted to administrators through database management system native security. Creation and modification of access control records for the database management systems occurs through the access provisioning process.
			Application level security restricts the ability to access, modify, and delete data to authenticated internal and external users who have been granted access through a record in the access control list. Creation and modification of access control records occurs through the access provisioning process.
		Unauthorized access to confidential information in output is obtained after processing.	Application security restricts output to approved roles or user IDs.

Criteria		Illustrative Risks	Illustrative Types of Controls
			Output containing sensitive information is printed at the secure print facility and is marked with the legend "Confidential."
			Paper forms are physically secured after data entry. Physical access is restricted to storage clerks.
			Personal information (both public and sensitive information) involved in business processes, systems, and third-party involvement is clearly identified and classified based on severity and risk within data management policies and procedures. The quantities of personal and sensitive information are identified.
			Awareness training is provided to personnel around the policy and usage of personal information.
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.	Confidential information transmitted beyond the boundaries of the system is provided to unauthorized user entity personnel.	Application security restricts output to approved user IDs.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Transmission of digital output beyond the boundary of the system occurs through the use of authorized software supporting the advanced encryption standard (AES).
			Logical access to stored data is restricted to application and database administrators.
			Data is stored in encrypted format using software supporting the AES.
			Use of removable media is prohibited by policy except when authorized by management.
		Confidential information is transmitted to related parties, vendors, or other approved parties contravening confidentiality commitments.	Application security restricts output to approved user IDs.
			Transmission of digital output beyond the boundary of the system occurs through the use authorized software supporting the AES.
			Confidential paper records are stored in locked containers in accordance with the retention schedule. The entity has the capability to identify, capture, preserve, and transfer client data, in the event of a legal preservation request, without impacting other client data.

Criteria		Illustrative Risks	Illustrative Types of Controls
			A nondisclosure or confidentiality agreement is signed by all personnel with access to confidential information.
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	Related party and vendor personnel are unaware of the entity's confidentiality commitments.	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. Agreement terms include requirements for marking and identifying data as confidential, handling standards for confidential data in the custody of related parties and vendors, and returning and disposing of confidential information when no longer required.
		Requirements for handling of confidential information are not communicated to and agreed to by related parties and vendors.	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity.
C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	Related party and vendor systems are not suitably designed or operating effectively to comply with confidentiality commitments.	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management guidelines.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
C1.6	Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	Confidentiality practices and commitments are changed without the knowledge or consent of internal and external users.	The chief information security officer is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate these changes to internal and external users, related parties, and vendors.
		Confidentiality practices and commitments are changed without the knowledge of related parties or vendors resulting in their systems not complying with the required practices and not meeting the commitments.	The chief information security officer is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate these changes to internal and external users, related parties, and vendors.
			Related party and vendor agreements are modified to reflect changes in confidentiality practices and commitments.
			Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management guidelines.

Criteria		Illustrative Risks	Illustrative Types of Controls
C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.	Confidential information is retained in excess of that associated with the stated purpose, longer than necessary to fulfill the stated purpose or longer than allowed by the entity's confidentiality commitments and system requirements.	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity • has automated system processes in place to delete confidential information in accordance with specific retention requirements. • deletes backup information in accordance with a defined schedule. • requires approval for confidential information to be retained beyond its retention period and specifically marks such information for retention. • reviews annually information marked for retention.
C1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.	Confidential information is not destroyed in accordance with confidentiality commitments and system requirements.	The entity • locates and removes or redacts specified confidential information as required. • regularly and systematically destroys, erases, or makes anonymous confidential information that is no longer required for the purposes identified in its confidentiality commitments or system requirements.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			• erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based). • disposes of original, archived, backup, and ad hoc or personal copies of records in accordance with its destruction policies. • documents the disposal of confidential information.
Additional Criteria for Privacy			
P1.0	***Privacy Criteria Related to Notice and Communication of Commitments and System Requirements***		
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's privacy commitments and system requirements. 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 privacy commitments and system requirements.	Data subjects are not notified of the purpose for the collection, use, and retention of their personal information thereby creating the potential for regulatory compliance violation (for example, with respect to Fair Information Practice Principles FIPPs, the Health Insurance Portability and Accountability Act [HIPAA], or Federal Trade Commission) or diminishment of the entity's reputation.	The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is • readily accessible and made available when personal information is first collected from the data subject. • provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable data subjects to decide whether or not to submit personal information to the entity.

Criteria		Illustrative Risks	Illustrative Types of Controls
			• clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. In addition, the entity • tracks previous iterations of the entity's privacy notices. • informs data subjects of a change to a previously communicated privacy notice (for example, by posting the notification on the entity's website, by sending written notice via postal mail, or by sending an email). • documents the changes to privacy practices that were communicated to data subjects.
			On a quarterly basis, the CPO and privacy staff meet to discuss the new types of personal information that is collected and the effect on privacy practices, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information items. For any new personal information that is collected, systems and processes are updated to provide notice to the data subjects.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Data subjects are not notified of one or more of the following: • The collection of their personal information or the choice and consent mechanisms in place to opt-out of the collection • The retention, sharing, disclosure and disposal of their personal information • Processes in place to obtain access to, make changes to, or make contact or inquiries regarding personal information • Additional sources of the personal information collected other than provided by the data subject	The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The CPO reviews the notice and documents his or her approval that the notice includes the following disclosures: • Notification of a mechanism to opt-out of the collection and use of their personal information upon collection and upon changes to the purpose and use of personal information • Policies regarding retention, sharing, disclosure, and disposal of their personal information • The mechanism(s) to access, make changes to, or make inquiries regarding their personal information • Additional sources of personal information used to enhance, enrich, or infer (through cross-reference) personal information already provided by the data subject upon collection

Criteria		Illustrative Risks	Illustrative Types of Controls
P1.2	The entity's privacy commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Internal and external users are not notified or aware of personal information collected through both active and passive means.	The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices through email and surface mail).
		The privacy commitments and system requirements are not communicated to internal and external users before personal information is collected, or as soon as practical thereafter.	Before personal information is collected, the entity communicates to the internal and external users the purpose and use of the collection of personal information, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information.
		Internal and external users are not notified of changes to the privacy commitments or system requirements for use of information in a timely manner to opt-out of the collection or use of personal information.	Before changes are made, the entity communicates to internal and external users' changes to the purpose and use of personal information, including changes to the detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Internal and external users are not given sufficient information regarding the nature and extent of the entity's use of personal information.	Before personal information is collected, the entity communicates to internal and external users the purpose and use of the collection of personal information, including detailed use, ability to opt-out, enhancement (enrichment) or inference, sharing, disclosure, access, security, retention, and disposal of personal information.
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 the data subject or other authorized person, if required, and such consent is obtained only for the purpose for which the information is intended consistent with the entity's privacy commitments and system requirements. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	Consent policies and procedures do not address the choice and consent options. A data subject does not "signify" their agreement indicating that there is active communication.	Policies and procedures containing information about choice and consent options include the following: • Consent is obtained before the personal information is processed or handled. • To ensure that consent is freely given, requests for consent are designed not to be deceptive intimidating or imply that failure to provide consent will result in significant negative consequences. • When authorization is required (explicit consent), the authorization is obtained in writing. • Implicit consent has clear actions on how a data subject opts out. • Action by a data subject to constitute valid consent. • Requests for consent are designed to be appropriate to the age and capacity of the data subject and to the particular circumstances.

Criteria		Illustrative Risks	Illustrative Types of Controls
		Processes are not in place to determine whether implicit or explicit consent is appropriate for the collection of personal information.	On annual basis, the privacy staff reviews collection processes to determine whether the consents obtained are appropriate (specifically, whether implicit or explicit consent is appropriately collected depending on the collection process).
		Data subjects are not notified of choices available related to collection, use, or disclosure of personal information.	Annually, the privacy staff checks that notice is provided to internal and external users; that the notice is clear, comprehensive, and visible to users; and that it includes the purpose and intended use of the collected personal information, encompassing detailed use, consent, ability to opt-out, authorization, sharing, disclosure, access, security, retention, and disposal of personal information.
		Lack of understanding of when consent is required due to specific law or regulations.	The privacy staff reviews quarterly relevant privacy laws and regulations to determine whether they require the entity to obtain consent and reviews and updates the entity's policies for conformity to the requirements.
		Denial or withdrawal of consent is not recognized or administered.	On an annual basis, the entity sends written notification informing data subjects of their current choice and offers them the option of either confirming or withdrawing their previously given consents. Denial or withdrawal of consents is tracked by privacy staff for further processing.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Implicit consent is relied upon when explicit or opt out consent is required.	The privacy staff obtains and evaluates requirements to determine whether implicit or explicit consent applies and compares such requirement to consents used.
		Opt-out consent is used without communicating the impact of that choice to the user.	Explanatory information is provided when data subjects are given the choice to opt out.
		Sensitive personal information is collected without obtaining without legal grounds and explicit consent.	The privacy staff reviews procedures to assess the nature of the information collected to determine whether personal information received requires an explicit consent.
			The privacy staff reviews quarterly relevant privacy laws and regulations to determine whether they require the entity to obtain consent, or whether the entity possesses other legal ground to process the data. It also reviews and updates the entity's policies for conformity to the requirement
		There is a lack of clear definition at the entity related to what personal information is considered "sensitive" personal information.	On an annual basis, the CPO reviews its policies to ensure the definition of "sensitive" personal information is properly delineated and communicated to personnel.
			The entity provides updated training and awareness to personnel that includes defining what constitutes personal information and what personal information is considered sensitive

Criteria		Illustrative Risks	Illustrative Types of Controls
		Consent is not obtained for new purposes or uses when required.	The privacy office establishes procedures to assess the need for obtaining and recording consents with respect to new products, software, relationships, and transactions.
P3.0	***Privacy Criteria Related to Collection***		
P3.1	Personal information is collected consistent with the entity's privacy commitments and system requirements.	Personal information is collected in a manner that is inconsistent with privacy commitments and system requirements and thereby • causes the entity to be subject to regulatory claims for unfair or deceptive trade practices. • subjects the entity to data subject or class action legal proceedings. • creates damage to the entity's reputation due to negative publicity. • enables competitors to leverage this situation to gain market share.	Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.
			Privacy related complaints are investigated monthly to identify whether there were incidents of unfair or unlawful practices.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		The entity does not have explicit or implicit consent to collect the information necessary for the provision of services.	Members of the privacy staff verify that the entity has legal ground to collect data from the data subjects and that such legal grounds are documented prior to collection. Additionally, members of the privacy staff verify, on a test basis, that the entity has requested and received explicit written consent from the data subjects, when such consent is required.
			Privacy related complaints are investigated upon receipt to identify whether there were incidents of unfair or unlawful practices.
		Personal information is collected in excess of the minimum necessary information needed to provide services in accordance with privacy commitments and system requirements.	Members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfill the business purpose by • reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information. • reviewing the privacy policies and personal information collection methods of third parties prior to contract execution.

Criteria		Illustrative Risks	Illustrative Types of Controls
			• reviewing contracts to determine whether they include provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.
			Privacy related complaints are investigated on a bi-weekly basis to identify whether there were incidents of unfair or unlawful practices.
		System changes result in the collection of personal information in excess of, or inconsistent with, privacy commitments and system requirements.	PIAs are conducted so that system changes are assessed for privacy implications. Personnel who are authorized to make system changes are properly trained so that they execute the PIA appropriately. Legal counsel reviews system changes that have privacy implications.
		Management is unaware that the entity collects personal information from third parties and is unaware of the types of personal information, as well as the means and methods by which the personal information was collected.	For each new third-party contract or agreement, members of the privacy staff determine whether personal information is collected only for the purposes identified in the privacy notice and only the minimum necessary personal information is collected to fulfill the business purpose by • reviewing and approving system change requests, when changes involve use of personal information or collection of new personal information.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			• reviewing the privacy policies and personal information collection methods of third parties before prior to contract execution. • reviewing contract to determine whether it includes provisions requiring that personal information be collected fairly without intimidation or deception and lawfully adhering to all relevant laws and regulations.
		The entity does not inform data subjects that it has acquired or is collecting additional personal information; therefore, data subjects are unaware that the entity has personal information beyond what is stated in the entity's privacy notice.	The entity provides notice of its privacy practices to data subjects of the system (upon data collection, from each mode of collection, and when any changes are made to the entity's privacy practices). The notice is • readily accessible and made available when personal information is first collected from the data subject. • provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable data subjects to decide whether or not to submit personal information to the entity. • clearly dated to allow data subjects to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity.

Criteria		Illustrative Risks	Illustrative Types of Controls
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 the request for personal information, and obtains the consent prior to the collection of the information consistent with the entity's privacy commitments and system requirements.	The entity does not obtain explicit consent directly from the data subject when sensitive personal information is collected, used, or disclosed.	• The entity change management policies require system processes to obtain explicit consent when required. CPO staff review and approve all system changes for compliance with the policy prior to implementation.
		Consent for online data transfers to or from a data subject's computer or other similar electronic device is not obtained.	The entity's application(s) provide for user interface (UI) screens that have a click button that captures and records a data subject's consent before the data subject submits the information.
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 privacy commitments and system requirements.	Personal information is used for purposes not identified in privacy commitments and system requirements for which consents have not been obtained and for purposes not permitted or in accordance with applicable laws and regulations.	The entity maintains policies and procedures that define allowable use and disclosure scenarios. Management personnel responsible for the entity's operations that involve the potential use and disclosure of personal information formally acknowledge their receipt and understanding of these policies.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			On an annual basis the entity reviews privacy policies and procedures to ensure that personal information is used in • conformity with the purposes identified in the entity's privacy notice. • conformity with the consent received from the data subject. • compliance with applicable laws and regulations.
P4.2	The entity retains personal information consistent with the entity's privacy commitments and system requirements.	Personal information is retained in excess of that associated with the stated purpose, longer than necessary to fulfill the stated purpose or longer than allowed by law or regulations, thereby creating potential for compliance violations and increased data breach exposure.	The entity establishes written policies related to retention periods for each type of information it maintains. The entity • has automated system processes in place to delete information in accordance with specific retention requirements. • deletes backup information in accordance with a defined schedule. • requires approval by the CPO for information to be retained beyond its retention period and specifically marks such information for retention. • reviews annually information marked for retention.
		Storage locations of personal information are not identified and tracked, thereby increasing risks of data breaches.	An annual review of the organization's data inventory is performed to verify that the documentation is kept current and includes the location of the data, a description of the data, and identified data owners.

Criteria		Illustrative Risks	Illustrative Types of Controls
		Personal information is retained in a manner that violates applicable laws and regulations.	The entity has documented its personal information retention policies and procedures, which are reviewed on at least an annual basis by legal counsel for consistency with applicable laws and regulations. Personal information retention laws and regulations are reviewed on at least an annual basis by members of the privacy staff and legal counsel for any new or revised applicable laws or regulations. Entity retention policies and procedures are reviewed for consistency with applicable laws and regulations. Any personal information retention policies and procedures that are not aligned with the current applicable laws and regulations are escalated to management for corrective action (for example, updating of the entity's policies and procedures as necessary.).
P4.3	The entity securely disposes of personal information consistent with the entity's privacy commitments and system requirements.	Personal information is not destroyed to meet the entity's privacy commitments and system requirements and applicable laws and regulations, thereby creating the potential for compliance violations and increased data breach exposure.	On a weekly basis data center personnel complete a checklist that documents the entity • erased or destroyed records in accordance with its retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based).

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			• disposed of original, archived, backup, and ad hoc or personal copies of records in accordance with its destruction policies. • documented the disposal of personal information. • located and removed or redacted specified personal information about a data subject as required within the limits of technology (for example, removing credit card numbers after the transaction is complete). • destroyed, erased, or made anonymous personal information that is no longer required for the purposes identified in its privacy commitments or as required by law or regulation. Data center personnel complete the preceding items in accordance with destruction procedures and attach documentation of the performance of those procedures to the checklist. CPO staff perform quarterly compliance assessment for a sample of business units to verify compliance with privacy and security policies by reviewing the checklists and associated documentations.

Criteria		Illustrative Risks	Illustrative Types of Controls
5.0	***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 the data subject consistent with the entity's privacy commitments and system requirements. If access is denied, the data subject is informed of the denial and reason for such denial, as required, consistent with the entity's privacy commitments and system requirements.	Data subjects are not aware of the process for requesting access to or a copy of their personal information creating the potential for compliance violations or data integrity issues.	Privacy staff annually review processes that involve direct communication with data subjects, online notices, privacy statements, mailings, and training and awareness programs for staff to determine whether they address the process for providing data subjects with access to their personal information and updating their information. The CPO establishes written procedures to update communications to data subjects when changes occur to access policies, procedures, and practices.
			The entity's privacy notice is made available to data subjects at the time an agreement for services is entered into as well as on the entity's website, which explains the process for providing data subjects with access to their personal information and updating their information.
			The CPO establishes written privacy policies and procedures that define how entity personnel are to respond to requests by data subjects to access their information.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Access is provided to unauthorized individuals who are not authenticated prior to providing them with access.	The CPO establishes written procedures to track and monitor the authentication of data subjects before they are granted access to personal information.
		Information provided to the data subject is incomplete, inaccurate, or not received in a timely manner.	Annually, the CPO reviews reports that summarize the response times in providing personal information, the associated costs incurred by the entity, and any charges to the data subjects. Annual assessments of the understandability of the format for information provided to data subjects are conducted by privacy staff.
		When data subjects are denied access, the data subjects are not informed of the reason for the denial in accordance with the entity's privacy commitments and system requirements.	Annually, the CPO reviews reports that summarize the response time to data subjects whose access request has been denied and reasons for such denials, as well as any communications regarding challenges.
P5.2	The entity corrects, amends, or appends personal information based on information provided by the data subjects and communicates such information to third parties, as committed or required, consistent with the entity's privacy commitments and system requirements. If a request for correction is denied, the data subject is informed of the denial and reason for such denial consistent with the entity's privacy commitments and system requirements.	Requests received for corrections, amendments, or additions are not processed correctly, timely, or by an authorized data subject in accordance with the entity's privacy commitments and system requirements.	The CPO establishes written policies and procedures to consistently and uniformly inform data subjects of how to update or correct personal information held by the entity.

Criteria		Illustrative Risks	Illustrative Types of Controls
			The CPO establishes written procedures to track data update and correction requests and to validate the accuracy and completeness of such data. Annually, the CPO reviews reports of updates and correction requests and response time to update records. Authorized data subjects are designated with the responsibility of making updates or amendments to personal information when self-service functionality is available to the data subject.
		Corrected, amended, or appended personal information is not communicated to vendors or other third parties that previously received that personal information in accordance with the entity's privacy commitments and system requirements.	The CPO establishes written procedures to consistently and uniformly provide updated information to vendors or other third parties that previously received the data subject's personal information. Documentation or justification is kept for not providing information updates to relevant vendors and other third parties.
		Data subjects are not informed that their request to correct, amend, or add to personal information has been denied or the reason for the denial in accordance with the entity's privacy commitments and system requirements.	The CPO establishes written policies and procedures that cover relevant aspects related to informing data subjects in writing about the reason a request for correction of personal information was denied and how they may appeal.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			The CPO annually reviews denials to verify that the justifications for denying requests for correction of personal information were appropriately documented and supported.
			The CPO annually reviews cases that involve disagreements over the accuracy and completeness of personal information to validate that the appropriate justifications and supporting documentation is retained.
P6.0	***Privacy Criteria Related to Disclosure and Notification***		
P6.1	The entity discloses personal Information to third parties with the explicit consent of the data subject to meet the entity's privacy commitments and system requirements, and such consent is obtained prior to disclosure.	Authorized use and disclosure scenarios are not defined and documented.	Business unit leaders identify and document authorized uses and disclosures of personal information relevant to their area. On an annual basis, the uses and disclosures are reviewed and approved by the privacy staff.
			A PIA is completed for new types of disclosures of personal information and disclosures to new third-party recipients. As part of the assessment, the privacy staff determines whether the disclosure is consistent with notice, consent, and privacy commitments and system requirements.

Criteria		Illustrative Risks	Illustrative Types of Controls
			As part of the change management process, the CPO reviews and approves new automated disclosures and transmissions to third parties and changes to existing automated disclosures and transmissions.
		Personal information is disclosed to vendors and other third parties without obtaining explicit consent of the data subject and does not meet the entity's privacy commitments and system requirements.	When explicit consent is required, business unit personnel implement a process for obtaining explicit consent. Updates to the consent process are reviewed and approved by the CPO.
			Requests for disclosure are recorded by business unit personnel and compared to preapproved types of disclosures before processing. When required, consent of the data subject is obtained prior to processing.
			Approved data subject and ad hoc requests requiring explicit consent are rejected if consent is not received. Rejections are recorded in a repository.
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information consistent with the entity's privacy commitments and system requirements.	Unauthorized disclosures are made, thereby creating potential for data breach.	When the disclosure of personal information requires explicit consent, the information to be disclosed through automated processes is compared to the consent records to confirm consent prior to disclosure.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		The entity does not maintain records for tracking purposes of disclosures made.	Automated disclosures are recorded in a database of disclosures that is retained in accordance with the entity's privacy commitments and requirements. Authorized disclosures are recorded and retained in accordance with the entity's privacy commitments and system requirements.
			Requests for disclosure are recorded by business unit personnel and compared to preapproved types of disclosures before processing. Requests not in accordance with preapproved disclosures types are evaluated for appropriateness in consultation with the privacy officer. When required, explicit consent of the data subject is obtained prior to processing.
		Disclosure requests made by data subjects are not recorded.	Requests for disclosure are recorded by business unit personnel, including the date received and specific details regarding the request (for example, information requested, requestor name, or period of time requested). The privacy staff reviews a report of data subjects and ad hoc disclosure requests on a weekly basis for unprocessed requests and unusual activity. Unprocessed requests are investigated, and unusual requests are recorded in the incident management system for formal investigation and resolution.

Criteria		Illustrative Risks	Illustrative Types of Controls
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures of personal information, including breaches, consistent with the entity's privacy commitments and system requirements.	Disclosures identified as part of incident management or reported by data subjects and other external parties are not identified as privacy incidents.	An automated message is sent to the privacy office informing them of unauthorized disclosures and potential disclosures detected as part of the incident management process. Resolution of all incidents flagged as privacy issues must be approved by privacy staff before the record is closed.
			Incident management procedures include detailed instructions on how to escalate a suspected incident to the Information Security Team and, when necessary, to the Privacy or Legal department. The entity has a standard incident report template that must be completed for each incident. The incident management procedures and templates are communicated to personnel who handle personal information.
P6.4	The entity obtains privacy commitments from vendors and other third parties whose products and services are part of the system and who have access to personal information processed by the system that are consistent with the entity's privacy commitments and system requirements.	Contractual agreements are not in place between the entity and vendors or other third parties involved in the processing of personal information.	Contracts with vendors or other third parties are required in order to set up a vendor or other third party in the accounts payable system. On an annual basis, the privacy staff obtains a list of paid vendors or other third parties and identifies those that process personal information. The privacy staff also reviews the contracts with those vendors or other third parties to determine whether the contracts contain

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			privacy and security commitments and system requirements that are consistent with those of the entity commitments for privacy and security.
		The vendor or other third party does not implement its practices in accordance with the entity's privacy commitments and system requirements.	Vendors or other third parties are required to undergo a privacy and security assessment supplied by the entity before the entity enters into a contract with those parties, and [annually or biannually] thereafter, to confirm that administrative, technical, and physical safeguards are consistent with the entity's commitments and system requirements and are in place. Alternatively, vendors or other third parties can provide a privacy SOC 2 report. If a SOC 2 report is provided, the privacy staff reviews the report to verify that the appropriate regulatory requirements are included and met. The privacy staff reviews the results of the submitted assessment or SOC 2 report to determine whether there are privacy or security risks that require remediation. The privacy office monitors whether any needed remediation is completed timely.

Criteria		Illustrative Risks	Illustrative Types of Controls
			The entity periodically reviews contracts to confirm ongoing alignment with the entity's revised privacy and security policies and procedures.
		Contracts between the entity and vendor or other third party do not provide instructions, requirements, or commitments for handling personal information.	Standard contractual templates are used for contracts involving personal information. The contracts contain instructions for approved handling of personal information. Deviations from standard templates require approval from the CPO. Contract templates are reviewed on a periodic basis to determine whether changes are required as a result of changes to system requirements (for example, regulatory requirements or commitments for handling personal information).
P6.5	Compliance with the entity's privacy commitments and system requirements by vendors and others third parties whose products and services are part of the system and who have access to personal information processed by the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	The vendor or other third party does not have the appropriate privacy and security capabilities to comply with contractual commitments.	Standard contractual templates are used for contracts involving personal information containing the requirement for an independent third party assessment or the right to audit the vendor or third party. Deviations from standard templates require approval from the CPO.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
			Vendors and other third parties are required to undergo a privacy and security assessment prior to entering into a contract with the entity, and annually thereafter, to confirm that administrative, technical, and physical safeguards that are consistent with those of the entity are in place. Alternatively, vendors and other third parties can provide a privacy SOC 2 Report. The privacy staff reviews the results of the assessment or SOC 2 report to determine whether there are privacy or security risks that require remediation.
		Changes in the vendor's or other third party's privacy procedures or controls have a detrimental impact on the processing by the vendor or other third party of personal information.	Standard contractual templates are used for contracts involving personal information that contain the requirement for vendors or other third parties to inform the entity of changes to vendor's or other third party's privacy procedures or controls that impact the processing of personal information. Deviations from standard templates require approval from the CPO. The entity meets with the third party on a quarterly basis to discuss any changes in the vendor's or other third party's privacy procedures or controls that impact the processing of personal information.

Criteria		Illustrative Risks	Illustrative Types of Controls
		Upon termination of a contract, assurances are not obtained from the vendor or other third party to confirm the return or destruction of personal information.	Standard contractual templates are used for contracts involving personal information that contain requirements for vendors or other third parties to provide documentation that confirms that personal information has been appropriately returned or destroyed in accordance with the contractual requirements. Deviations from standard templates require approval from the CPO. Vendor or other third party relationship managers are required by policy to obtain such assurances and provide the supporting documentation to the privacy staff. Upon determination that a contract is to be terminated, the entity provides the vendor or third party with a checklist of procedures to be performed regarding the return or destruction of the information and a template for written certification of the completion of procedures.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
P6.6	The entity obtains commitments from vendors and other third parties that may have access to personal information processed by the system 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 to meet the entity's established incident response procedures, privacy commitments, and system requirements.	Vendors and other third parties are not obligated by commitment or requirement to notify the entity of a breach or unauthorized disclosure of personal information in a timely manner.	Standard contractual templates are used for contracts involving personal information containing requirements to notify the entity of a breach or unauthorized disclosure of personal information. Deviations from standard templates require approval from the CPO.
		The vendor's or other third party's incident response procedures do not exist.	Prior to contracting with vendors and other third parties, vendors and other third parties are required to provide a copy of their incident response procedures. Vendors and other third parties are provided with specific instructions on who should be contacted in the event of a privacy or security incident as well as the timeframe in which the notification must occur.
P6.7	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others consistent with the entity's privacy commitments and system requirements.	Unauthorized uses and disclosures are not assessed to determine whether they constitute breaches.	Privacy related disclosures and potential disclosures identified during the incident management process are assessed by privacy staff using predetermined assessment guidelines. Assessments are documented in the incident management system. Unauthorized uses and disclosures that constitute a breach

Criteria		Illustrative Risks	Illustrative Types of Controls
			based on the type, sensitivity, value, and amount of personal information that is used or disclosed inappropriately are recorded in a separate repository.
		Unauthorized uses and disclosures are not properly identified as breaches.	A comprehensive incident identification and breach response procedure is documented that provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The procedure is communicated to personnel who handle personal information.
		Identified breaches and incidents are not recorded in accordance with the entity's privacy commitments and system requirements.	Unauthorized uses and disclosures that constitute a breach based on the type, sensitivity, value, and amount of personal information that is used or disclosed inappropriately are recorded in a separate repository. Breaches and incidents are reviewed by the CPO.
		Notification of breaches and incidents is not completed in accordance with commitments and system requirements.	Breach notification procedures are reviewed on a regular basis to determine whether the procedures are aligned with commitments and system requirements. Breach notification activities are reviewed against breach notification procedures and notifications are approved by the CPO.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
P6.8	The entity provides, to the data subjects, an accounting of the personal information held and disclosure of a data subject's personal information, upon the data subject's request, consistent with the entity's privacy commitments and system requirements.	Requests for an accounting of disclosures are not processed.	Requests for an accounting of disclosures are recorded in a repository. The date of completion of the processing of the requests and the person generating the accounting is documented in the repository.
		The accounting of disclosures is provided to an unauthorized person.	Requestor identification procedures are defined in the procedures for processing requests. The type of identification obtained is documented in the repository.
		The accounting of disclosures is incomplete or inaccurate.	Predefined queries have been developed for each record of disclosures. The request repository contains a checklist of each system application to be queried. Queries are automatically returned to the processor's workstation in a predefined report format. The processor stores the results of each query to the repository. Upon completion, the processor requests generation of the disclosure report from the repository.
		The accounting of disclosures contains personal information for other data subjects.	All queries are based on the specific requesting data subject's unique identification number. Only one identification number can be processed at a time.

Criteria		Illustrative Risks	Illustrative Types of Controls
P7.0	***Privacy Criteria Related to Quality***		
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information consistent with the entity's privacy commitments and system requirements.	Personal information that is collected is inaccurate or incomplete.	As personal information is collected, automated edit checks and balances help ensure that data entry fields are completed properly (for example, only 9 digits are allowed when SSNs are entered).
			As personal information is collected, users are asked to confirm that their information is correct prior to submitting the information to the entity.
		The personal information that is collected is modified inaccurately.	Automated controls exist to identify and provide notification within the entity when personal information within the IT systems is altered. Such alterations must be reviewed and approved by operations personnel prior to finalization of the records.
			When personal information within the IT systems is altered, notification is sent to the data subject. The entity requests the data subject communicate any inaccuracies within 30 days.
		The personal information is altered within the entity, whether intentionally or unintentionally, such that it is no longer accurate and complete.	Automated controls exist to provide notification within the entity when personal information within the IT application systems is altered. Such alterations must be reviewed and approved by operations personnel prior to finalization of the records.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Information that is not relevant to the purpose is collected. Information is collected and used for a purpose that is not disclosed to the data subject.	Personal information collected and the intended purpose of collection is compared to the privacy notice for completeness and accuracy.
			The entity maintains an up-to-date inventory of data for which business units are required to supply regular updates. The CPO reviews the inventory on a regular basis.
			Changes to the way that personal information is collected and the purposes for which the information is used are communicated to the appropriate individuals responsible for governance within the entity. These individuals assess the changes, determine their appropriateness, and alter the privacy notice as needed.
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 with the entity's privacy commitments and system requirements; corrections and other necessary actions related to identify deficiencies are taken in a timely manner.	Data subjects are not informed about how to contact the entity with inquiries, complaints, and disputes.	The entity monitors the status of privacy controls and the entity's adherence to the entity's commitments to customers and data subjects related to the protection of the privacy of customer personal information and provides customers and data subjects with information on how to contact the entity with inquiries, complaints, and disputes.

Criteria		Illustrative Risks	Illustrative Types of Controls
		Inability for a complaint to be submitted, which creates necessity for data subjects to report complaints to regulatory agencies.	The entity provides an automated, confidential, customer privacy complaint system for capturing and tracking customer privacy concerns and issues.
			Customer privacy concerns captured by the complaint tracking system are shared with the entity's board of directors and relevant oversight bodies or regulatory authorities as may be required by law or regulation.
		Failure to assess complaints to determine whether a breach or inappropriate access requires action, such as a formal reporting or corrective action plan.	The entity implements a Data Privacy Task Force comprising senior service entity team leads who are responsible for monitoring adherence to the entity's privacy policies and procedures. The Data Privacy Task Force is responsible for evaluating customer privacy concerns and complaints, determining whether urgent reporting or remediation actions are required, and directly responding to customers on actions taken to address such concerns and complaints.
		Corrective action plans are not developed or monitored to ensure that an issue does not reoccur.	The privacy staff monitors the development and execution of corrective action plans that were developed to address identified or suspected privacy incidents and related data processing issues that could affect privacy controls.

(continued)

Criteria		Illustrative Risks	Illustrative Types of Controls
		Policies and procedures are out of date and do not support current regulations, agreements, or contracts.	The privacy staff monitors the continued relevance and applicability of the entity's policies and procedures related to privacy regulations, agreements, and contracts.
		Lack of documented activity related to monitoring or auditing may deem the program ineffective.	The CPO establishes written policies and procedures to monitor its privacy controls and compliance with the entity's privacy policies and procedures, laws, regulations, and other requirements. Selection of controls to be monitored and frequency with which they are monitored are based on a risk assessment. Annually, compliance monitoring results and remediation activities are analyzed by the privacy office and provided to management.
		Lack of written action plans may deem the program ineffective.	Written action plans are used by management to help ensure that the entity's privacy program is operating effectively in identifying, monitoring, and addressing privacy related concerns.

.19

Appendix C—Mapping of the Trust Services Principles and Criteria to Extant Generally Accepted Privacy Principles

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
CC1.1	1	**Management Principle and Criteria**	**Management Principle: The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.**
CC1.1	1.1.0	Privacy Policies	The entity defines and documents its privacy policies with respect to the following: *a.* Notice (See 2.1.0) *b.* Choice and consent (See 3.1.0) *c.* Collection (See 4.1.0) *d.* Use, retention, and disposal (See 5.1.0) *e.* Access (See 6.1.0) *f.* Disclosure to third parties (See 7.1.0) *g.* Security for privacy (See 8.1.0) *h.* Quality (See 9.1.0) *i.* Monitoring and enforcement (See 10.1.0)
CC2.2, CC1.4, CC2.6	1.1.1	Communication to Internal Personnel	Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.
CC1.1, CC1.2, CC3.2, CC4.1	1.1.2	Responsibility and Accountability for Policies	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.
CC1.2	1.2.1	Review and Approval	Privacy policies and procedures, and changes thereto, are reviewed and approved by management.

(continued)

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
CC1.1, CC1.2	1.2.2	Consistency of Privacy Policies and Procedures With Laws and Regulations	Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.
CC3.1	1.2.3	Personal Information Identification and Classification	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. Such information is covered by the entity's privacy and related security policies and procedures.
CC3.1	1.2.4	Risk Assessment	A risk assessment process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and to develop and update responses to such risks.
CC1.1, CC1.2, CC3.1	1.2.5	Consistency of Commitments With Privacy Policies and Procedures	Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.
CC7.1, CC7.4, C1.1	1.2.6	Infrastructure and Systems Management	The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification, and management of the following: • Infrastructure • Systems • Applications • Websites • Procedures • Products and services • Databases and information repositories • Mobile computing and other similar electronic devices

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
CC2.5, CC6.2, P6.6	1.2.7	Privacy Incident and Breach Management	A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following: • Procedures for the identification, management, and resolution of privacy incidents and breaches • Defined responsibilities • A process to identify incident severity and determine required actions and escalation procedures • A process for complying with breach laws and regulations, including stakeholders breach notification, if required • An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate • A process for periodic review (at least on an annual basis) of actual incidents to identify necessary program updates based on the following: — Incident patterns and root cause — Changes in the internal control environment or external requirements (regulation or legislation) — Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed
CC1.3	1.2.8	Supporting Resources	Resources are provided by the entity to implement and support its privacy policies.
CC1.3, CC1.4	1.2.9	Qualifications of Internal Personnel	The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.

(continued)

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
CC2.3	1.2.10	Privacy Awareness and Training	A privacy awareness program about the entity's privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.
CC1.1, CC1.2, CC3.1	1.2.11	Changes in Regulatory and Business Requirements	For each jurisdiction in which the entity operates, the effect on privacy requirements from changes in the following factors is identified and addressed: • Legal and regulatory • Contracts, including service-level agreements • Industry requirements • Business operations and processes • People, roles, and responsibilities • Technology Privacy policies and procedures are updated to reflect changes in requirements.
	2	**Notice Principle and Criteria**	**Notice Principle: The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.**
CC1.1, CC1.2, P1.2	2.1.0	Privacy Policies	The entity's privacy policies address providing notice to individuals.
P1.1, P1.2	2.1.1	Communication to Individuals	Notice is provided to individuals regarding the following privacy policies: *a.* Purpose for collecting personal information *b.* Choice and consent (See 3.1.1) *c.* Collection (See 4.1.1) *d.* Use, retention, and disposal (See 5.1.1) *e.* Access (See 6.1.1) *f.* Disclosure to third parties (See 7.1.1) *g.* Security for privacy (See 8.1.1) *h.* Quality (See 9.1.1) *i.* Monitoring and enforcement (See 10.1.1) If personal information is collected from sources other than the individual, such sources are described in the notice.

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
P1.1	2.2.1	Provision of Notice	Notice is provided to the individual about the entity's privacy policies and procedures (*a*) at or before the time personal information is collected, or as soon as practical thereafter, (*b*) at or before the entity changes its privacy policies and procedures, or as soon as practical thereafter, or (*c*) before personal information is used for new purposes not previously identified.
P1.1, P1.2	2.2.2	Entities and Activities Covered	An objective description of the entities and activities covered by the privacy policies and procedures is included in the entity's privacy notice.
P1.1, P1.2, P2.2	2.2.3	Clear and Conspicuous	The entity's privacy notice is conspicuous and uses clear language.
P2.1	3	**Choice and Consent Principle and Criteria**	**Choice and Consent Principle: The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.**
CC1.1, CC1.2, P1.1, P1.2	3.1.0	Privacy Policies	The entity's privacy policies address the choices available to individuals and the consent to be obtained.
P1.1	3.1.1	Communication to Individuals	Individuals are informed about (*a*) 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.
P2.1	3.1.2	Consequences of Denying or Withdrawing Consent	When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.
P2.1	3.2.1	Implicit or Explicit Consent	Implicit or explicit consent is obtained from the individual 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.

(continued)

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
P2.1	3.2.2	Consent for New Purposes and Uses	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 individual is notified, and implicit or explicit consent is obtained prior to such new use or purpose.
P2.1	3.2.3	Explicit Consent for Sensitive Information	Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.
P2.1	3.2.4	Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices	Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.
	4	**Collection Principle and Criteria**	**Collection Principle: The entity collects personal information only for the purposes identified in the notice.**
CC1.1, CC1.2, P1.2	4.1.0	Privacy Policies	The entity's privacy policies address the collection of personal information.
P1.1, P2.1	4.1.1	Communication to Individuals	Individuals are informed that personal information is collected only for the purposes identified in the notice.
P1.1, P1.2, P2.1	4.1.2	Types of Personal Information Collected and Methods of Collection	The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.
P3.1	4.2.1	Collection Limited to Identified Purpose	The collection of personal information is limited to that necessary for the purposes identified in the notice.
CC3.1, CC3.2, CC4.1, P8.1, P3.1	4.2.2	Collection by Fair and Lawful Means	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.

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
CC1.0, P1.1, P3.1	4.2.3	Collection From Third Parties	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.
P1.1, P2.1	4.2.4	Information Developed About Individuals	Individuals are informed if the entity develops or acquires additional information about them for its use.
	5	**Use, Retention, and Disposal Principle and Criteria**	**Use, Retention, and Disposal Principle: The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.**
CC1.1, CC1.2, CC2.1, CC2.2, CC2.4, P1.2	5.1.0	Privacy Policies	The entity's privacy policies address the use, retention, and disposal of personal information.
P1.1	5.1.1	Communication to Individuals	Individuals are informed that personal information is (*a*) used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise, (*b*) retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation, and (*c*) disposed of in a manner that prevents loss, theft, misuse, or unauthorized access.
P4.1	5.2.1	Use of Personal Information	Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.
P4.2	5.2.2	Retention of Personal Information	Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.

(continued)

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
P4.2, P4.3	5.2.3	Disposal, Destruction, and Redaction of Personal Information	Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.
	6	**Access Principle and Criteria**	**Access Principle: The entity provides individuals with access to their personal information for review and update.**
	6.1.0	Privacy Policies	The entity's privacy policies address providing individuals with access to their personal information.
CC1.1, CC1.2, P1.2, P5.1	6.1.1	Communication to Individuals	Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information.
P2.1, P5.1	6.2.1	Access by Individuals to Their Personal Information	Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.
P5.1, P6.2	6.2.2	Confirmation of an Individual's Identity	The identity of individuals who request access to their personal information is authenticated before they are given access to that information.
P5.1	6.2.3	Understandable Personal Information, Time Frame, and Cost	Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.
P5.1, P5.2	6.2.4	Denial of Access	Individuals 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.
P5.2	6.2.5	Updating or Correcting Personal Information	Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information.
P5.2	6.2.6	Statement of Disagreement	Individuals are informed, in writing, about the reason a request for correction of personal information was denied and how they may appeal.

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
	7	**Disclosure to Third Parties Principle and Criteria**	**Disclosure to Third Parties Principle: The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.**
CC1.1, CC1.2, P1.2	7.1.0	Privacy Policies	The entity's privacy policies address the disclosure of personal information to third parties.
P1.1, P6.1, P6.2	7.1.1	Communication to Individuals	Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise.
P1.2	7.1.2	Communication to Third Parties	Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.
P1.1, P6.1	7.2.1	Disclosure of Personal Information	Personal information is disclosed to third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically requires or allows otherwise.
P6.4, P6.5	7.2.2	Protection of Personal Information	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 policies or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.
P3.1, P6.1, P6.4	7.2.3	New Purposes and Uses	Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.
P6.7, P6.8	7.2.4	Misuse of Personal Information by a Third Party	The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.

(continued)

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
	8	**Security for Privacy Principle and Criteria**	**Security for Privacy Principle: The entity protects personal information against unauthorized access (both physical and logical).**
CC1.1, CC1.2, P1.2, CC5.1–CC5.8	8.1.0	Privacy Policies	The entity's privacy policies (including any relevant security policies) address the security of personal information.
P1.1	8.1.1	Communication to Individuals	Individuals are informed that precautions are taken to protect personal information.
CC3.1, CC3.2, CC5.1–CC5.8, P6.5, P8.1	8.2.1	Information Security Program	A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas, insofar as they relate to the security of personal information: *a.* Risk assessment and treatment (See 1.2.4) *b.* Security policy (See 8.1.0) *c.* Organization of information security (See 1, 7, and 10) *d.* Asset management (See 1) *e.* Human resources security (See 1) *f.* Physical and environmental security (See 8.2.3 and 8.2.4) *g.* Communications and operations management (See 1, 7, and 10) *h.* Access control (See 1, 8.2, and 10) *i.* Information systems acquisition, development, and maintenance (See 1.2.6) *j.* Information security incident management (See 1.2.7) *k.* Business continuity management (See 8.2) *l.* Compliance (See 1 and 10)

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
CC5.0, CC5.2–CC5.4, CC5.6–CC5.8	8.2.2	Logical Access Controls	Logical access to personal information is restricted by procedures that address the following matters: *a.* Authorizing and registering internal personnel and individuals *b.* Identifying and authenticating internal personnel and individuals *c.* Making changes and updating access profiles *d.* Granting privileges and permissions for access to IT infrastructure components and personal information *e.* Preventing individuals from accessing anything other than their own personal or sensitive information *f.* Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities *g.* Distributing output only to authorized internal personnel *h.* Restricting logical access to offline storage, backup data, systems, and media *i.* Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls) *j.* Preventing the introduction of viruses, malicious code, and unauthorized software
CC5.5	8.2.3	Physical Access Controls	Physical access is restricted to personal information in any form (including the components of the entity's system[(s) that contain or protect personal information).
CC6.1	8.2.4	Environmental Safeguards	Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.

(continued)

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
CC5.7	8.2.5	Transmitted Personal Information	Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other nonsecure networks, and wireless networks is protected by deploying industry standard encryption technology for transferring and receiving personal information.
CC5.1, CC5.4	8.2.6	Personal Information on Portable Media	Personal information stored on portable media or devices is protected from unauthorized access.
CC4.1, P8.1	8.2.7	Testing Security Safeguards	Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.
	9	**Quality Principle and Criteria**	**Quality Principle: The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.**
CC1.1, CC1.2, P1.2	9.1.0	Privacy Policies	The entity's privacy policies address the quality of personal information.
P1.1	9.1.1	Communication to Individuals	Individuals are informed that they are responsible for providing the entity with accurate and complete personal information and for contacting the entity if correction of such information is required.
P5.2, P7.1, P8.1	9.2.1	Accuracy and Completeness of Personal Information	Personal information is accurate and complete for the purposes for which it is to be used.
P4.1	9.2.2	Relevance of Personal Information	Personal information is relevant to the purposes for which it is to be used.
	10	**Monitoring and Enforcement Principle and Criteria**	**Monitoring and Enforcement Principle: The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints, and disputes.**
CC1.1, CC1.2, P1.2	10.1.0	Privacy Policies	The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.
P1.1, P5.1, P5.2	10.1.1	Communication to Individuals	Individuals are informed about how to contact the entity with inquiries, complaints, and disputes.

Mapping of the Trust Services Principles and Criteria (TSPC) to Extant Generally Accepted Privacy Principles (GAPP)			
TSPC	***Ref***	***Title***	***Extant GAPP Criterion***
CC6.1, CC6.2, CC5.1, CC5.2, P8.1	10.2.1	Inquiry, Complaint, and Dispute Process	A process is in place to address inquiries, complaints, and disputes.
CC6.1, CC6.2, CC5.1, CC5.2, P8.1	10.2.2	Dispute Resolution and Recourse	Each complaint is addressed, and the resolution is documented and communicated to the individual.
C3.2, CC4.1, P8.1	10.2.3	Compliance Review	Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts is reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.
CC6.2, P8.1	10.2.4	Instances of Noncompliance	Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.
CC4.1, P8.1	10.2.5	Ongoing Monitoring	Ongoing procedures are performed for monitoring the effectiveness of controls over personal information, based on a risk assessment [1.2.4], and for taking timely corrective actions where necessary.

TSP Section 100A-1

Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2014)

(To supersede the 2009 version of *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy.* The privacy criteria are presented in appendix C.)

Introduction

.01 The AICPA Assurance Services Executive Committee (ASEC) has developed a set of principles and criteria (trust services principles and criteria) to be used in evaluating controls relevant to the security, availability, and processing integrity of a system, and the confidentiality and privacy of the information processed by the system. In this document, a *system* is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management-specified requirements. System components can be classified into the following five categories:

- *Infrastructure.* The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
- *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- *Processes.* The automated and manual procedures.
- *Data.* Transaction streams, files, databases, tables, and output used or processed by a system.

.02 This document presents the trust services principles and criteria for assessing the effectiveness of an entity's controls over a system relevant to the security, availability, or processing integrity of the system, or the confidentiality or privacy of the information processed by the system. Management of an entity may use the principles and criteria to evaluate its controls over a system or may engage a CPA to report on or provide consulting services related to those controls.

.03 Attestation services, performed under the AICPA's Statements on Standards for Attestation Engagements (commonly known as the *attestation standards*), include examination, review,[1] and agreed-upon procedures

[1] Review engagements generally consist of the performance of inquiries and analytical procedures designed to provide a moderate level of assurance (that is, negative assurance). However, the Assurance Services Executive Committee believes that a practitioner ordinarily could not perform meaningful analytical procedures on an entity's controls or compliance with requirements of specified laws, regulations, rules, contracts, or grants to achieve this level of assurance, and it is uncertain what other procedures could be identified that, when combined with inquiry procedures, could form the basis for a review engagement. Also due to this uncertainty, users of a review report are at greater risk of misunderstanding the nature and extent of the practitioner's procedures. Accordingly, the feasibility of a review engagement related to trust services is uncertain.

engagements. In the attestation standards, the CPA performing an attest engagement is known as a practitioner. In an examination engagement, the practitioner provides a report that expresses an opinion about subject matter or an assertion about subject matter in relation to an identified set of criteria. For example, a practitioner may report on whether controls over a system were operating effectively to meet the trust services criteria for processing integrity and confidentiality. In an agreed-upon procedures engagement, the practitioner does not express an opinion but rather performs procedures agreed upon by specified parties and reports the results of those procedures. Examination engagements are performed in accordance with AT section 101, *Attest Engagements*, of the attestation standards and agreed-upon procedures engagements are performed in accordance with AT section 201, *Agreed-Upon Procedures Engagements* (AICPA, *Professional Standards*).

.04 The following are the types of subject matter a practitioner may examine and report on using the trust services principles and criteria:

- The design and operating effectiveness of a service organization's controls over a system relevant to one or more of the trust services principles of security, availability, processing integrity, confidentiality, and privacy (SOC 3^{SM} engagement).
- The fairness of the presentation of a description of a service organization's system relevant to one or more of the trust services principles of security, availability, processing integrity, confidentiality, and privacy using the description criteria in paragraph 1.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2^{SM})*, and additionally in paragraph 1.35 for the privacy principle; for a type 1 report, the suitability of the design of controls to meet the related trust services criteria; and, for a type 2 report, the operating effectiveness of those controls throughout a specified period to meet those trust services criteria (SOC 2 engagement).
- The suitability of the design of an entity's controls over a system relevant to one or more of the trust services principles of security, availability, processing integrity, confidentiality, and privacy to meet the related trust services criteria. (This engagement would typically be performed prior to the system's implementation.)

.05 The nature and extent of the services that an organization provides to each user entity may vary significantly depending on the user entity's needs. For example, a social organization that uses a website for a monthly newsletter would have a much more limited need for data center hosting service availability than would a securities trading firm. The social organization is likely to be only slightly inconvenienced if its newsletter is unavailable for one day; whereas, the securities trading firm could experience a significant financial loss if the system is unavailable for 15 minutes. Such user needs generally are addressed by management declarations in written contracts, service level agreements, or public statements (for example, a privacy notice). These management declarations are referred to in the trust services principles and criteria as *commitments*. Specifications regarding how the system should function to enable management to meet its business objectives, commitments, and obligations (for example, legal and regulatory) are referred to as *requirements* in the trust

services principles and criteria. For example, security requirements may result from management's commitments relating to security, availability, processing integrity, confidentiality, or privacy.

Commitments and requirements are the objectives for which the entity implements controls, and, consequently, the objectives of the trust services criteria. Accordingly, many of the trust services criteria refer to commitments and requirements. For example, "The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to [*insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality*]." In an engagement in which the practitioner expresses an opinion on compliance with or achievement of the commitments and requirements, they serve as the engagement criteria.

.06 Management is responsible for maintaining a record of and complying with its commitments and requirements. In identifying its commitments and requirements, management should specify in its assertion what its commitments and requirements consist of for the particular engagement, for example:

- Obligations included in written customer contracts
- Baseline obligations that are applicable to all customers but which exclude special commitments made to particular customers when those commitments result in the implementation of additional processes or controls outside the services provided to a broad range of users

In addition, trust services engagements do not require the practitioner to report on the entity's compliance, or internal control over compliance, with laws, regulations, rules, contracts, or grant agreements, related to the principles being reported upon. If the practitioner is engaged to report on compliance with laws, regulations, rules, contracts, or grant agreements in conjunction with an engagement to report on the operating effectiveness of an entity's controls (for example, a SOC 3 privacy engagement), such an engagement would be performed in accordance with AT section 601, *Compliance Attestation* (AICPA, *Professional Standards*).

.07 Consulting services include developing findings and recommendations for the consideration and use of management of an entity when making decisions. The practitioner does not express an opinion or form a conclusion about the subject matter in these engagements. Generally, the work is performed only for the use and benefit of the client. Practitioners providing such services follow CS section 100, *Consulting Services: Definitions and Standards* (AICPA, *Professional Standards*).

Principles, Criteria, Controls, and Risks

.08 Trust services principles represent attributes of a system that support the achievement of management's objectives.

.09 For each of the principles there are detailed criteria that serve as benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. The attributes of suitable criteria are as follows:

- *Objectivity*. Criteria should be free from bias.
- *Measurability*. Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- *Completeness*. Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted.
- *Relevance*. Criteria should be relevant to the subject matter.

.10 ASEC has concluded that the trust services criteria for each individual principle that include the common criteria have all of the attributes of suitable criteria. In addition to being suitable, AT section 101 indicates that the criteria must be available to users of the practitioner's report. The publication of the principles and criteria makes the criteria available to users.

.11 The trust services principles and criteria are designed to be flexible and enable the achievement of the objectives of users and management. Accordingly, a practitioner may be engaged to perform an engagement related to a single principle, multiple principles, or all of the principles.

.12 The environment in which the system operates; the commitments, agreements, and responsibilities of the entity operating the system; as well as the nature of the components of the system result in risks that the criteria will not be met. These risks are addressed through the implementation of suitably designed controls that, if operating effectively, provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, management of an entity needs to identify the specific risks that the criteria will not be met and the controls necessary to address those risks. Appendix B provides examples of risks that may prevent the criteria from being met as well as examples of controls that would address those risks. These illustrations are not intended to be applicable to any particular entity or all-inclusive of the risks to meeting the criteria or the controls necessary to address those risks.

Trust Services Principles

.13 The following are the trust services principles:[2]

a. *Security.* The system is protected against unauthorized access, use, or modification.

The *security principle* refers to the protection of the system resources through logical and physical access control measures in order to support the achievement of management's commitments and requirements related to security, availability, processing integrity, and confidentiality. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and

[2] SysTrust℠, SysTrust for Service Organizations℠, and WebTrust℠ are specific branded assurance services offerings developed by the AICPA and Canadian Institute of Chartered Accountants (CICA) that are based on the trust services principles and criteria. Practitioners must be licensed by CICA to use these registered service marks. Service marks can only be issued for engagements that result in an unqualified examination opinion. For more information on licensure, see www.webtrust.org.

improper access to, or use of, alteration, destruction, or disclosure of information.

b. Availability. The system is available for operation and use as committed or agreed.

The *availability principle* refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The *availability principle* does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.

c. Processing integrity. System processing is complete, valid, accurate, timely, and authorized.

The *processing integrity principle* refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the system achieves its aim or the purpose for which it exists, and whether it performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Processing integrity does not automatically imply that the information received and stored by the system is complete, valid, accurate, current, and authorized. The risk that data contains errors introduced prior to its input in the system often cannot be addressed by system controls and detecting such errors is not usually the responsibility of the entity. Similarly, users outside the boundary of the system may be responsible for initiating processing. In these instances, the data may become invalid, inaccurate, or otherwise inappropriate even though the system is processing with integrity.

d. Confidentiality. Information designated as confidential is protected as committed or agreed.

The *confidentiality principle* addresses the system's ability to protect information designated as confidential in accordance with the organization's commitments and requirements through its final disposition and removal from the system. Information is confidential if the custodian of the information, either by law or regulation, the custodian's own assertion, commitment, or other agreement, is obligated to limit its access, use, and retention, and restrict its disclosure to a specified set of persons or organizations (including those that may otherwise have authorized access within the boundaries of the system). The need for information to be confidential may arise for many different reasons. For example, the information is proprietary information, information intended only for company personnel, personal information, or merely embarrassing information. Confidentiality is distinguished from privacy in that (i) privacy deals with personal information whereas, confidentiality refers to a broader range of information that is not restricted to personal information; and (ii) privacy addresses requirement for the treatment, processing, and handling of personal information.

e. Privacy.

The *privacy principle* addresses the system's collection, use, retention, disclosure, and disposal of personal information[3] in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants (see appendix C, "Generally Accepted Privacy Principles"). GAPP is a management framework that includes the measurement criteria for the trust services privacy principle. GAPP consists of 10 sub-principles:

i. *Management.* The entity defines documents, communicates, and assigns accountability for its privacy policies and procedures.

ii. *Notice.* The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

iii. *Choice and consent.* The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

iv. *Collection.* The entity collects personal information only for the purposes identified in the notice.

v. *Use and retention.* The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

vi. *Access.* The entity provides individuals with access to their personal information for review and update.

vii. *Disclosure to third parties.* The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

viii. *Security for privacy.* The entity protects personal information against unauthorized access (both physical and logical).

ix. *Quality.* The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

x. *Monitoring and enforcement.* The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

---

[3] Personal information is information that is about or can be related to an identifiable individual. It may include information about customers, employees, and other individuals.

Trust Services Criteria

.14 Many of the criteria used to evaluate a system are shared amongst all of the principles; for example, the criteria related to risk management apply to the security, availability, processing integrity, and confidentiality principles. As a result, the criteria for the security, availability, processing integrity, and confidentiality principles are organized into (*a*) the criteria that are applicable to all four principles (common criteria) and (*b*) criteria applicable only to a single principle. The common criteria constitute the complete set of criteria for the security principle. For the principles of availability, processing integrity, and confidentiality, a complete set of criteria is comprised of all of the common criteria and all of the criteria applicable to the principle(s) being reported on.

The common criteria are organized into seven categories:

a. *Organization and management*. The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

b. *Communications*. The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

c. *Risk management and design and implementation of controls.* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

d. *Monitoring of controls.* The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

e. *Logical and physical access controls.* The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

f. *System operations.* The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

g. *Change management*. The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

The GAPP management framework does not use the common criteria structure for organizing the criteria. See appendix C for GAPP criteria.

Trust Services Principles and Criteria

.15

Criteria Common to All [Security, Availability, Processing Integrity, and Confidentiality] Principles	
CC1.0	***Common Criteria Related to Organization and Management***
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*].
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and placed in operation.
CC1.3	Personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] have the qualifications and resources to fulfill their responsibilities.
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*].
CC2.0	***Common Criteria Related to Communications***
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.
CC2.2	The entity's [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.
CC2.3	The entity communicates the responsibilities of internal and external users and others whose roles affect system operation.

Criteria Common to All [Security, Availability, Processing Integrity, and Confidentiality] Principles	
CC2.4	Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] of the system, have the information necessary to carry out those responsibilities.
CC2.5	Internal and external system users have been provided with information on how to report [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] failures, incidents, concerns, and other complaints to appropriate personnel.
CC2.6	System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] are communicated to those users in a timely manner.
CC3.0	***Common Criteria Related to Risk Management and Design and Implementation of Controls***
CC3.1	The entity (1) identifies potential threats that would impair system [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).
CC3.2	The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.
CC3.3	The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.
CC4.0	***Common Criteria Related to Monitoring of Controls***
CC4.1	The design and operating effectiveness of controls are periodically evaluated against [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] commitments and requirements, corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.

(continued)

Criteria Common to All [Security, Availability, Processing Integrity, and Confidentiality] Principles	
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.
CC5.2	New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.
CC5.3	Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.
CC5.6	Logical access security measures have been implemented to protect against [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] threats from sources outside the boundaries of the system.
CC5.7	The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*].
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.
CC6.0	***Common Criteria Related to System Operations***
CC6.1	Vulnerabilities of system components to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.

Criteria Common to All [Security, Availability, Processing Integrity, and Confidentiality] Principles	
CC6.2	[*Insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.
CC7.0	***Common Criteria Related to Change Management***
CC7.1	[*Insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] commitments and requirements, are addressed, during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.
CC7.2	Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*].
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] commitments and requirements.
Additional Criteria for Availability	
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.
A1.3	Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.
Additional Criteria for Processing Integrity	
PI1.1	Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements.

(continued)

Criteria Common to All [Security, Availability, Processing Integrity, and Confidentiality] Principles	
PI1.2	System inputs are measured and recorded completely, accurately, and timely in accordance with processing integrity commitments and requirements.
PI1.3	Data is processed completely, accurately, and timely as authorized in accordance with processing integrity commitments and requirements.
PI1.4	Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.
PI1.5	System output is complete, accurate, distributed, and retained in accordance with processing integrity commitments and requirements.
PI1.6	Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.
Additional Criteria for Confidentiality	
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes in accordance with confidentiality commitments and requirements.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality commitments and requirements.
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties in accordance with confidentiality commitments and requirements.
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality requirements from vendors and other third parties whose products and services comprise part of the system and have access to confidential information.
C1.5	Compliance with confidentiality commitments and requirements by vendors and others third parties whose products and services comprise part of the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.
C1.6	Changes to confidentiality commitments and requirements are communicated to internal and external users, vendors, and other third parties whose products and services are included in the system.

Privacy Principles and Criteria

.16 These criteria are set forth in appendix C.

Effective Date

.17 The trust services principles and criteria are effective for periods ending on or after December 15, 2014. Early implementation is permitted.

.18

Appendix A—Definitions

accuracy. The key information associated with the submitted transaction remains accurate throughout the processing of the transaction and that the transaction or service is processed or performed as intended.

authorization. The processing is performed in accordance with and subject to the required approvals and privileges defined by policies governing system processing.

authorized access. Access is authorized only if (*a*) the access has been approved by a person designated to do so by management, and (*b*) the access does not compromise segregation of duties, confidentiality commitments, or otherwise increase risk to the system beyond the levels approved by management (that is, access is appropriate).

boundary of the system. The physical and logical perimeter of that portion of an entity's operations that is used to achieve management's specific business objectives of a system. The boundary includes all components of the system for which the entity is responsible, including those provided by vendors and other third parties.

For a privacy or confidentiality engagement, the boundary of the system includes the components starting with the capture of the information through its disclosure and final disposition (often referred to as the information life cycle). The boundary of the system includes (*a*) the collection, use, retention, disclosure and de-identification, or anonymization of the information until its destruction and (*b*) all business segments and locations for the entire entity or only certain identified segments of the business (for example, retail operations but not manufacturing operations or only operations originating on the entity's website or specified Web domains) or geographic locations (for example, only Canadian operations).

commitments. Declarations made by management to customers regarding the performance of a system. Commitments can be communicated through individual agreements, standardized contracts, service level agreements, or published statements (for example, security practices statement). An individual commitment may relate to one or more principles. The practitioner need only consider commitments related to the principles on which he or she is engaged to report. Commitments may take many forms including the following:

- Specification of the algorithm used in a calculation
- Contractual agreement that states the hours a system will be available
- Published password standards
- Encryption standards used to encrypt stored customer data

completeness. Transactions are processed or all services are performed without omission.

environmental protections. Measures implemented by the entity to detect, prevent, and manage the risk of casualty damage to the physical parts of the system (for example, protections from fire, flood, wind, earthquake, power surge, or power outage).

external users. Individuals outside the boundary of the system who are authorized by customers, entity management, or other authorized persons to interact with the system.

internal users. Entity and entity vendor personnel whose job function causes them to be members of the people component of the system.

report users. Intended users of the practitioner's report in accordance with AT section 101, *Attest Engagements* (AICPA, *Professional Standards*). Report users may be the general public or may be restricted to specified parties in accordance with AT section 101 paragraph .78.

requirements. Specifications regarding how the system should function to meet management's business objectives, commitments to customers, and obligations (for example, legal and regulatory). Requirements are often specified in the system policies, system design documentation, contracts with customers, and government regulations. Examples of requirements are

- employee fingerprinting and background checks established in government banking regulations.
- input edits defined in application design documents.
- maximum acceptable intervals between periodic review of employee logical access as documented in the security policy manual.
- data definition and tagging standards, including any associated metadata requirements, established by industry groups of other bodies, such as the Simple Object Access Protocol.
- business processing rules and standards established by regulators; for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA).

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

SOC 2 engagement. An examination engagement to report on the suitability of design (type 1) or suitability of design and operating effectiveness (type 2) of controls at a service organization using the Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2).*

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 trust services principles.

timeliness. The provision of services or the delivery of goods addressed in the context of commitments made for such delivery.

trust services. A set of professional attestation and advisory services based on a core set of principles and criteria that address the operation and protection of a system and related data.

workforce. Employees, contractors and others engaged by company to perform activities as part of the system.

.19

Appendix B—Illustrative Risks and Controls

The illustrative risks and controls presented in this appendix are for illustrative purposes only. They are based on a hypothetical entity in a hypothetical industry. They are not intended to be a comprehensive set of risks and controls or applicable to any particular entity. Accordingly, they should not be used as a checklist of risks and controls for the criteria. Practitioners should consider using other frameworks such as, NIST 800-53, Cloud Controls Matrix (CCM) for such guidance.

Criteria		Risks	Illustrative Controls
Criteria Common to All [Security, Availability, Processing Integrity, and Confidentiality] Principles			
CC1.0	***Common Criteria Related to Organization and Management***		
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*].	The entity's organizational structure does not provide the necessary information flow to manage [*security, availability, processing integrity, or confidentiality*] activities.	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.
		The roles and responsibilities of key managers are not sufficiently defined to permit proper oversight, management, and monitoring of [*security, availability, processing integrity, or confidentiality*] activities.	Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.

(continued)

Criteria		Risks	Illustrative Controls
			Job descriptions are reviewed by entity management on an annual basis for needed changes and where job duty changes are required necessary changes to these job descriptions are also made.
		Reporting relationships and organizational structure do not permit effective senior management oversight of *[security, availability, processing integrity, or confidentiality*] activities.	Reporting relationships and organizational structures are reviewed periodically by senior management as part of organizational planning and adjusted as needed based on changing entity commitments and requirements.
		Personnel have not been assigned responsibility or delegated insufficient authority to meet [*security, availability, processing integrity, or confidentiality*] commitments and requirements.	Roles and responsibilities are defined in written job descriptions.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies, and other system requirements are effectively promulgated and placed in operation.	Personnel have not been assigned responsibility or delegated insufficient authority to meet [*security, availability, processing integrity, or confidentiality*] commitments and requirements.	Roles and responsibilities are defined in written job descriptions.

Criteria		Risks	Illustrative Controls
			Job descriptions are reviewed on a periodic basis for needed changes and updated if such changes are identified.
CC1.3	Personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] have the qualifications and resources to fulfill their responsibilities.	Newly hired or transferred personnel do not have sufficient knowledge and experience to perform their responsibilities.	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.
			The experience and training of candidates for employment of transfer are evaluated before they assume the responsibilities of their position.
		Personnel do not have sufficient continuous training to perform their responsibilities.	Management establishes skills and continued training with its commitments and requirements for employees.
			Management monitors compliance with training requirements.
		Tools and knowledge resources are insufficient to perform assigned tasks.	Management evaluates the need for additional tools and resources in order to achieve business objectives, during its ongoing and periodic business planning and budgeting process and as part of its ongoing risk assessment and management process.

(continued)

Criteria		Risks	Illustrative Controls
CC1.4	The entity has established workplace conduct standards, implemented workplace candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*].	Personnel do not adhere to the code of conduct.	Management monitors employees' compliance with the code of conduct through monitoring of customer and employee complaints and the use of an anonymous third-party administered ethics hotline.
			Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and to formally re-affirm them annually thereafter.
		Candidate has a background considered to be unacceptable by management of the entity.	Senior management develops a list of characteristics that would preclude employee candidate from being hired based on sensitivity or skill requirements for the given position.
			Personnel must pass a criminal and financial trust background check before they may be hired by the entity or third party vendors hired by the entity.

Criteria		Risks	Illustrative Controls
CC2.0	***Common Criteria Related to Communications***		
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	Users misuse the system due to their failure to understand its scope, purpose, and design.	System descriptions are available to authorized external users that delineate the boundaries of the system and describe relevant system components as well as the purpose and design of the system. Documentation of the system description is available to authorized users via the entity's customer-facing website.
			A description of the system is posted on the entity's intranet and is available to the entity's internal users. This description delineates the boundaries of the system and key aspects of processing.
		Users are unaware of key organization and system support functions, processes, and roles and responsibilities.	A description of the entity organization structure, system support functions, processes, and organizational roles and responsibilities is posted on the entity's intranet and available to entity internal users. The description delineates the parties responsible, accountable, consented, and informed of changes in design and operation of key system components.

(continued)

Criteria		Risks	Illustrative Controls
		External users fail to address risks for which they are responsible that arise outside the boundaries of the system.	System descriptions are available to authorized external users that delineate the boundaries of the system and describe significant system components as well as the purpose and design of the system. The system description is available to users via ongoing communications with customers or via the customer website.
CC2.2	The entity's [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.	Users misunderstand the capabilities of the system in providing for [*security, availability, processing integrity, or confidentiality*] and take actions based on the misunderstanding.	The entity's [*security, availability, processing integrity, or confidentiality*] commitments regarding the system are included in the master services agreement and customer-specific service level agreements. In addition, a summary of these commitments is available on the entity's customer facing website.
		The entity fails to meet its commitments due to lack of understanding on the part of personnel responsible for providing the service.	Policy and procedures documents for significant processes are available on the entity's intranet.
			Personnel are required to attend annual security, confidentiality, and privacy training.

Criteria		Risks	Illustrative Controls
			Personnel are required to read and accept the entity's code of conduct and the statement of security, confidentiality, and privacy practices upon hire and annually thereafter.
			Processes are monitored through service level management procedures that monitor compliance with service level commitments and agreements. Results are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties, including customers, when such commitments and agreements are not met.
CC2.3	The entity communicates the responsibilities of internal and external users and others whose roles affect system operation.	The system fails to function as designed due to internal user failure to comply with their responsibilities.	Policy and procedures documents for significant processes that address system requirements are available on the intranet.
			Personnel are required to attend annual security, confidentiality, and privacy training.
			Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon hire and annually thereafter.

(continued)

Criteria		Risks	Illustrative Controls
			Processes are monitored through service level management procedures that monitor compliance with commitments and requirements. Results are shared with applicable personnel and customers.
		The system fails to function as designed due to external users' failure to meet their responsibilities.	Customer responsibilities are described on the customer website and in system documentation.
CC2.4	Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] of the system, have the information necessary to carry out those responsibilities.	Controls fail to function as designed or operate effectively due to misunderstanding on the part of personnel responsible for implementing and performing those controls resulting in failure to achieve [*security, availability, processing integrity, or confidentiality*] commitments and requirements.	Policy and procedures documents for significant processes are available on the intranet.
			Processes are monitored following service level management procedures that monitor compliance with commitments and requirements. Results are shared according to policies.
			Customer responsibilities are described on the customer website and in system documentation.

Criteria		Risks	Illustrative Controls
CC2.5	Internal and external system users have been provided with information on how to report [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] failures, incidents, concerns, and other complaints to appropriate personnel.	System anomalies are detected by internal or external users but the failures are not reported to appropriate personnel resulting in the system failing to achieve its [*security, availability, processing integrity, or confidentiality*] commitments and requirements.	Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and available on the intranet.
			Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on the customer website and in system documentation.
CC2.6	System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] are communicated to those users in a timely manner.	Users misunderstand changes in system capabilities or their responsibilities in providing for [*security, availability, processing integrity, or confidentiality*] due to system changes and take actions based on the misunderstanding.	Proposed system changes affecting customers are published on the customer website XX days before their implementation. Users are given the chance to participate in user acceptance testing for major changes XX days prior to implementation. Changes made to systems are communicated and confirmed with customers through ongoing communications mechanisms such as customer care meetings and via the customer website.

(continued)

Criteria		Risks	Illustrative Controls
			Management of the business unit must confirm understanding of changes by authorizing them.
			The system change calendar that describes changes to be implemented is posted on the entity intranet.
			Updated system documentation is published on the customer website and intranet 30 days prior to implementation.
			System changes that result from incidents are communicated to internal and external users through e-mail as part of the implementation process.
		Changes in roles and responsibilities and changes to key personnel are not communicated to internal and external users in a timely manner.	Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal and external users via e-mail as part of the change management process.
CC3.0	***Common Criteria Related to Risk Management and Design and Implementation of Controls***		
CC3.1	The entity (1) identifies potential threats that would impair system [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] commitments and requirements, (2) analyzes the significance of risks associated with the	Not all system components are included in the risk management process resulting in a failure to identify and mitigate or accept risks.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.

Criteria		Risks	Illustrative Controls
	identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).		
		Personnel involved in the risk management process do not have sufficient information to evaluate risks and the tolerance of the entity for those risks.	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
		One or more internal or external risks, that are significant, threaten the achievement of [*security, availability, processing integrity, or confidentiality*] commitments and requirements that can be addressed by security controls, are not identified.	During the risk assessment and management process, risk management office personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.
			Identified risks are rated using a risk evaluation process and ratings are reviewed by management.
			The risk and controls group evaluates the effectiveness of controls and mitigation strategies in meeting identified risks and recommends changes based on its evaluation.

(continued)

Criteria		Risks	Illustrative Controls
			The risk and controls group's recommendations are reviewed and approved by senior management.
			The entity uses a configuration management database and related process to capture key system components, technical and installation specific implementation details, and to support ongoing asset and service management commitments and requirements.
CC3.2	The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.	Controls and mitigation strategies selected, developed, and deployed do not adequately mitigate risk.	Control self-assessments are performed by operating units on a quarterly basis.
			Internal audits are performed based on the annual risk-based internal audit plan.
			Business recovery plans are tested annually.
			Internal and external vulnerability scans are performed quarterly and annually and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.
		Deployed controls and mitigation strategies create new risks that fail to be assessed.	See CC3.1 illustrative controls.

Criteria		Risks	Illustrative Controls
CC3.3	The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological) that could significantly affect the system of internal control for [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.	Not all changes that significantly affect the system are identified resulting in a failure to reassess related risks.	During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.
		Changes that are not properly identified create risks due to the failure of those changes to undergo the risk management process.	During the risk assessment and management process, risk management office personnel identify environmental, regulatory, and technological changes that have occurred.
CC4.0	***Common Criteria Related to Monitoring of Controls***		
CC4.1	The design and operating effectiveness of controls are periodically evaluated against [*insert the principle(s) being reported on: security, availability,*]	Controls are not suitably designed, configured in accordance with established policies, or operating in an effective manner resulting in a system that does not meet	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software

(continued)

Criteria		Risks	Illustrative Controls
	processing integrity, or confidentiality or any combination thereof] commitments and requirements, corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	system commitments and requirements.	sends a message to the operations center and automatically opens an incident, problem, or change management "ticket" record when specific predefined thresholds are met.
			Operations and security personnel follow defined protocols for resolving and escalating reported events.
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***		
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	Not all system infrastructure or system components are protected by logical access security measures resulting in unauthorized modification or use.	Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.
			Network scans are performed for infrastructure elements to identify variance from entity standards.

Criteria		Risks	Illustrative Controls
			Assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed and periodically evaluate access for assets under their custody or stewardship.
			Online applications match each user ID to a single customer account number. Requests for access to system records require the matching of the customer account number against a list of privileges each user possesses when granted access to the system initially.
		Logical access security measures do not identify or authenticate users prior to permitting access to IT components.	Infrastructure components and software are configured to use the shared sign-on functionality when available. Systems not using the shared sign-on functionality are required to be implemented with separate user ID and password submission.
			External access by employees is permitted only through a two factor (for example, a swipe card and a password) encrypted virtual private network (VPN) connection.

(continued)

Criteria		Risks	Illustrative Controls
		Logical access security measures do not provide for the segregation of duties required by the system design.	A role based security process has been defined with an access control system that is required to use roles when possible.
			Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles. Roles are periodically reviewed and updated by asset owners and the risk and controls group on an annual basis. Access change requests resulting from the review are submitted to the security group via a change request record.
			For software or infrastructure that does not support the use of role-based security, a separate database of roles and related access is maintained. The security group uses this database when entering access rules in these systems.
		Logical access security measures do not restrict access to system configurations, privileged functionality, master passwords, powerful utilities, security devices, and other high risk resources.	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by the chief information security officer. This access is reviewed by the chief information security officer on a periodic basis as established by the chief information security officer.

Criteria		Risks	Illustrative Controls
CC5.2	New internal and external system users are registered and authorized prior to being issued system credentials and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.	Valid user identities are granted to unauthorized persons.	On a daily basis, employee user IDs are automatically created in or removed from the active directory and the VPN systems as of the date of employment using an automated feed of new users collected from employee changes in the human resource management system.
			Employee access to protected resources is created or modified by the security group based on an authorized change request from the system's asset owner.
			Contractor and vendor IDs are created by the security group based on an authorized change request from the contractor office. These IDs are valid for the lesser of the expected period of relationship or XX days.
			Privileged customer accounts are created based on a written authorization request from the designated customer point of contact. These accounts are used by customers to create customer user access.
			System security is configured to require users to change their password upon initial sign-on and every XX days thereafter.

(continued)

Criteria		Risks	Illustrative Controls
		A user that is no longer authorized continues to access system resources.	On a daily basis, the human resources system sends an automated feed to the active directory and the VPN for removal of access for employees for whom it is the last day of employment. The list is used by security personnel to remove access. The removal of the access is verified by the security manager.
			On a weekly basis, the human resources system sends to the security group a list of terminated employees for whose access is to be removed. The list is used by security personnel to remove access. The removal of the access is verified by a security manager.
			On a weekly basis, the contractor office sends to the security group a list of terminated vendors and contractors whose access is to be removed. The list is used by security personnel to remove access. The removal of the access is verified by a security manager.
			Entity policies prohibit the reactivation or use of a terminated employee's ID without written approval of the chief information security officer. Requests for reactivation are made using the change management record system and must include the purpose and justification of the

Criteria		Risks	Illustrative Controls
			access (for business need), the systems that are to be reactivated, and the time period for which the account will be active (no more than XX days). The account is reset with a new password and is activated for the time period requested. All use of the account is logged and reviewed by security personnel.
			Account sharing is prohibited unless a variance from policy is granted by the chief information security officer as might be provided by the entity using an account and password vaulting software product that provides account sharing controlled circumstances and active logging of each use. Otherwise, shared accounts are permitted for low risk applications (for example, informational system where access with shared IDs cannot compromise segregation of duties) or when system technical limitations require their use (for example, UNIX root access). The chief information security officer must approve the use of all shared accounts. Mitigating controls are implemented when possible (for example, required use of *su* when accessing the UNIX root account).

(continued)

Criteria		Risks	Illustrative Controls
CC5.3	Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).	Users are not identified when accessing information system components.	Entity standards are established for infrastructure and software hardening and configuration that includes requirements for implementation of access control software, entity configuration standards, and standardized access control lists.
			Account sharing is prohibited unless a variance from policy is granted by the chief information security officer as might be provided by the entity using an account and password vaulting software product that provides account sharing controlled circumstances and active logging of each use. Otherwise, shared accounts are permitted for low risk applications (for example, informational system where access with shared IDs cannot compromise segregation of duties) or when system technical limitations require their use (for example, UNIX root access). The chief information security officer must approve the use of all shared accounts. Mitigating controls are implemented when possible (for example, required use of *su* when accessing the UNIX root account).

Criteria		Risks	Illustrative Controls
		Valid user identities are assumed by an unauthorized person to access the system.	The online application matches each user ID to a single customer account number. Requests for access to system records require the matching of the customer account number.
			Two factor authentication and use of encrypted VPN channels help to ensure that only valid users gain access to IT components.
			Infrastructure components and software are configured to use the active directory shared sign-on functionality when available. Systems not using the shared sign-on functionality are configured to require a separate user ID and password.
		User access credentials are compromised allowing an unauthorized person to perform activities reserved for authorized persons.	Users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system.
			Password complexity standards are established to enforce control over access control software passwords.

(continued)

Criteria		Risks	Illustrative Controls
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.	Valid users obtain unauthorized access to the system resulting in a breakdown in segregation of duties or an increase in the risk of intentional malicious acts or error.	When possible, formal role-based access controls limit access to system and infrastructure components are created and these are enforced by the access control system. When it is not possible, authorized user IDs with two factor authentication are used.
			User access requests for a specific role are approved by the user manager and are submitted to the security group via the change management record system.
		Access granted through the provisioning process compromises segregation of duties or increases the risk of intentional malicious acts or error.	When possible, formal role-based access controls limit access to system and infrastructure components and these are enforced by the access control system. When it is not possible, authorized user IDs with two factor authentication are used.
			Roles are reviewed and updated by asset owners and the risk and controls group on an annual basis. Access change requests resulting from the review are submitted to the security group via a change request record.

Criteria		Risks	Illustrative Controls
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.	Unauthorized persons gain physical access to system components resulting in damage to components (including threats to personnel), fraudulent or erroneous processing, unauthorized logical access, or compromise of information.	An ID card-based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.
			ID cards that include an employee picture must be worn at all times when accessing or leaving the facility.
			ID cards are created by the human resources department during the employee orientation period and distributed after all required background investigations are completed. ID cards initially provide access only to nonsensitive areas.
			Access to sensitive areas is added to ID cards by the physical security director based on a request for access approved by the owner of the sensitive area and after required background investigations have been performed and any issues resolved. Requests for access and changes to access are made, approved, and communicated through the change management record system.

(continued)

Criteria		Risks	Illustrative Controls
			The contractor office may request ID cards for vendors and contractors. Cards are created by the physical security director. Requests are made, approved, and communicated through the change management record system.
			Visitors must be signed in by an employee before a single-day visitor badge that identifies them as an authorized visitor can be issued.
			Visitor badges are for identification purposes only and do not permit access to any secured areas of the facility.
			All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.
		Formerly appropriate physical access becomes inappropriate due to changes in user job responsibilities or system changes resulting in a breakdown in segregation of duties or an increase in the risk of intentional malicious acts or error.	Owners of sensitive areas of the facilities review the list of names and roles of those granted physical access to their areas on a semi-annual basis to check for continued business need. Requests for changes are made through the change management record system.

Criteria		Risks	Illustrative Controls
		A formerly authorized person continues to access system resources after that person is no longer authorized.	Owners of sensitive areas of the facilities review access to their areas on a semi-annual basis. Requests for changes are made through the change management record system.
			Vendors are asked to review a list of employees with ID cards on a semi-annual basis and request any modifications. The contractor office requests changes based on the vendor review.
			On a daily basis, as of the last day of employment, the human resources system sends to physical security a list of terminated employees for whom it is the last day of employment and whose access is to be removed and their pass cards to be disabled.
		A user obtains the identification credentials and authentication credentials of a formerly authorized person and uses them to gain unauthorized access to the system.	On a weekly basis, the contractor office sends to the security group a list of terminated vendors and contractors for whom access is to be removed.
			On a weekly basis, the human resources system sends to the physical security group a list of terminated employees for whom access is to be removed.

(continued)

Criteria		Risks	Illustrative Controls
			Employees and contractors are required to return their ID cards during exit interviews, and all ID badges are disabled prior to exit interviews therefore employees and contractors must be physically escorted from the entity's facilities at the completion of the exit interview.
			The sharing of access badges and tailgating are prohibited by policy.
			Mantraps or other physical devices are used for controlling accessing highly sensitive facilities.
			Doors that bypass mantraps can only be opened by the ID cards of designated members of management.
CC5.6	Logical access security measures have been implemented to protect against [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] threats from sources outside the boundaries of the system.	Threats to the system are obtained through external points of connectivity.	Defined entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists that define which privileges are attributable to each user or system account.
			External points of connectivity are protected by a firewall complex.

Criteria		Risks	Illustrative Controls
			Firewall hardening standards are based on relevant applicable technical specifications and these are compared against product and industry recommended practices and updated periodically.
			External access to nonpublic sites is restricted through the use of user authentication and message encryption systems such as VPN and SSL.
		Authorized connections to the system are compromised and used to gain unauthorized access to the system.	Firewall rules and the online system limit the times when remote access can be granted and the types of activities and service requests that can be performed from external connections.
CC5.7	The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*].	Nonpublic information is disclosed during transmission over public communication paths.	VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity and to protect communications between the processing center and users connecting to the processing center from within or external to customer networks.

(continued)

Criteria		Risks	Illustrative Controls
			Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted.
			Data loss prevention software is used to scan for sensitive information in outgoing transmissions over public communication paths.
		Removable media (for example, USB drives, DVDs, or tapes) are lost, intercepted, or copied during physical movement between locations.	Backup media are encrypted during creation.
			Storage for workstations and laptops is encrypted. Removable media for workstations and laptops are encrypted automatically by the software. Removable media is readable only by other entity owned devices.
			Other removable media are produced by data center operations and are transported via courier.
		Removable media used to make unauthorized copies of software or data are taken beyond the boundaries of the system.	Storage for workstations and laptops is encrypted. Removable media for these devices is encrypted automatically by the software. Removable media is readable only by other entity owned devices.
			Backup media are encrypted during creation.

Criteria		Risks	Illustrative Controls
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.	Malicious or otherwise unauthorized code is used to intentionally or unintentionally compromise logical access controls or system functionality through data transmission, removable media, and portable or mobile devices.	The ability to install software on workstations and laptops is restricted to IT support personnel.
			Antivirus software is installed on workstations, laptops, and servers supporting such software.
			Antivirus software is configured to receive an updated virus signature at least daily. A network operation receives a report of devices that have not been updated in 30 days and follows up on the devices.
			The ability to install applications on systems is restricted to change implementation and system administration personnel.
CC6.0	***Common Criteria Related to System Operations***		
CC6.1	Vulnerabilities of system components to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and	Vulnerabilities that could lead to a breach or incident are not detected in a timely manner.	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual

(continued)

Criteria		Risks	Illustrative Controls
	countermeasures are implemented to compensate for known and new vulnerabilities.	Vulnerabilities that could lead to a breach or incident are not detected in a timely manner.	system activity or service requests. This software sends a message to the operations center and security organization and automatically opens a priority incident or problem ticket and change management system record item.
			Call center personnel receive telephone and e-mail requests for support, which may include requests to reset user passwords or notify entity personnel of potential breaches and incidents. Call center personnel follow defined protocols for recording, resolving, and escalating received requests.
		Security or other system configuration information is corrupted or otherwise destroyed, preventing the system from functioning as designed.	Weekly full-system and daily incremental backups are performed using an automated system.
CC6.2	[*Insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] incidents, including logical and physical security breaches, failures, concerns, and other complaints are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.	Breaches and incidents are not identified, prioritized, or evaluated for effects.	Operations personnel follow defined protocols for evaluating reported events. Security related events are assigned to the security group for evaluation

Criteria		Risks	Illustrative Controls
		Corrective measures to address breaches and incidents are not implemented in a timely manner.	Operations and security personnel follow defined protocols for resolving and escalating reported events.
			Resolution of security events (incidents or problems) is reviewed at the daily and weekly operations and security group meetings.
			Internal and external users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.
		Corrective measures are not effective or sufficient.	Resolution of events is reviewed at the weekly operations and security group meetings.
			Change management requests are opened for events that require permanent fixes.
		Lack of compliance with policies and procedures is not addressed through sanctions or remedial actions resulting in increased noncompliance in the future.	The resolution of events is reviewed at the weekly operations and security group meetings. Relevant events with effects on user or customer are referred to user and customer care management to be addressed.
			Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.
		Breaches and incidents recur because preventive measures are not implemented after a previous event.	Change management requests are opened for events that require permanent fixes.

(continued)

Criteria		Risks	Illustrative Controls
CC7.0	***Common Criteria Related to Change Management***		
CC7.1	[*Insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] commitments and requirements are addressed during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.	Commitments and requirements are not addressed at one or more points during the system development lifecycle resulting in a system that does not meet system commitments and requirements.	System change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, and confidentiality commitments and requirements throughout the change management process.
			System changes other than those classified as minor require the approval of the chief information security officer and operations manager prior to implementation.
CC7.2	Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*].	System components are not updated for changes in requirements resulting in a system that does not meet system commitments and requirements.	During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are created based on the identified needs.

Criteria		Risks	Illustrative Controls
			For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Identified breaches, incidents, and other system impairments are not considered during the change management lifecycle.	For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with [*insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof*] commitments and requirements.	System changes are not authorized by those responsible for the design and operation of the system resulting in changes to the system that impairs its ability to meet system commitments and requirements.	System change requests must be reviewed and approved by the owner of the infrastructure or software and the change advisory board prior to work commencing on the requested change.

(continued)

Criteria		Risks	Illustrative Controls
		System changes do not function as intended resulting in a system that does not meet system commitments and requirements.	Functional and detailed designs are prepared for other than minor changes (more than XX hours). Functional designs are reviewed and approved by the application or infrastructure and software owner and detailed designs are approved by the director of development for the application and the change advisory board prior to work commencing on the requested change or development project.
			Test plans and test data are created and used in required system and regression testing. Test plans and test data are reviewed and approved by the testing manager prior to and at the completion of testing, and reviewed by the change advisory board prior to newly developed or changed software being authorized for migration to production. Security vulnerability testing is included in the types of tests performed on relevant application, database, network, and operating system changes.

Criteria		Risks	Illustrative Controls
			System and regression testing is prepared by the testing department using approved test plans and test data. Deviations from planned results are analyzed and submitted to the developer.
			Code review or walkthrough is required for high impact changes that meet established criteria (that mandate code reviews and walkthroughs) and these are performed by a peer programmer that does not have responsibility for the change.
			Changes are reviewed and approved by the change advisory board prior to implementation.
			Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.
			Changes to hardening standards are reviewed and approved by the director in infrastructure management.

(continued)

Criteria		Risks	Illustrative Controls
		Unauthorized changes are made to the system resulting in a system that does not meet system commitments and requirements.	Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in testing or production.
			Logical access controls and change management tools restrict the ability to migrate between development, test, and production to change deployment personnel.
			Changes are reviewed and approved by the change advisory board prior to implementation.
		Unforeseen system implementation problems impair system operation resulting in a system that does not function as designed.	A turnover process that includes verification of operation and back out steps is used for every migration.
			Post implementation procedures that are designed to verify the operation of system changes are performed for one week after the implementation for other than minor changes, and results are shared with users and customers as required to meet commitments and requirements.

Criteria		Risks	Illustrative Controls
		Incompatibility duties exist within the change management process, particularly between approvers, designers, implementers, testers, and owners, resulting in the implemented system not functioning as intended.	The change management process has defined the following roles and assignments: • Authorization of change requests—owner or business unit manager • Development—application design and support department • Testing—quality assurance department • Implementation—software change management group
Additional Criteria for Availability			
A1.1	Current processing capacity and usage are maintained, monitored and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.	Current processing capacity is not sufficient to meet availability commitments and requirements in the event of the loss of individual elements within the system components.	Processing capacity is monitored on an ongoing basis.
			Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.
		Processing capacity is not monitored, planned, and expanded or modified, as necessary, to provide for the continued availability of the system in accordance with system commitments and requirements.	Processing capacity is monitored on a daily basis.

(continued)

Criteria		Risks	Illustrative Controls
			Future processing demand is forecasted and compared to scheduled capacity on an ongoing basis. Forecasts are reviewed and approved by senior operations management. Change requests are initiated as needed based on approved forecasts.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	Environmental vulnerabilities and changing environmental conditions are not identified or addressed through the use of environmental protections resulting in a loss of system availability.	Environmental protections have been installed including the following: • Cooling systems • Battery and natural gas generator backup in the event of power failure • Redundant communications lines • Smoke detectors • Dry pipe sprinklers
		Environmental vulnerabilities are not monitored or acted upon increasing the severity of an environmental event.	Operations personnel monitor the status of environmental protections during each shift.
			Environmental protections receive maintenance on at least an annual basis.
		Software or data are lost or not available due to processing error, intentional act, or environmental event.	Weekly full-system and daily incremental backups are performed using an automated system.
			Backups are monitored for failure using an automated system and the incident management process is automatically invoked.

Criteria		Risks	Illustrative Controls
			Backups are transported and stored offsite by a third-party storage provider.
		System availability commitments and requirements are not met due to a lack of recovery infrastructure.	Business continuity and disaster recovery plans have been developed and updated annually.
			The entity has contracted with a third-party recovery facility to permit the resumption of IT operations in the event of a disaster at it data center.
			The entity uses a multi-location strategy for its facilities to permit the resumption of operations at other entity facilities in the event of loss of a facility.
A1.3	Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.	Recovery plans are not suitably designed and backups are not sufficient to permit recovery of system operation in accordance with commitments and requirements.	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.
			Test results are reviewed and the contingency plan is adjusted.
Additional Criteria for Processing Integrity			
PI1.1	Procedures exist to prevent and detect and correct processing errors to meet processing integrity commitments and requirements.	Software or data are lost or not available due to processing error, intentional act, or environmental event.	Weekly full-system and daily incremental backups are performed using an automated system.

(continued)

Criteria		Risks	Illustrative Controls
			Backups are monitored for failure using an automated system and the incident management process is automatically invoked.
			Backups are transported and stored offsite by a third-party storage provider.
		Environmental vulnerabilities are not addressed through the use of environmental protections resulting in a loss of system availability.	Environmental protections have been installed including the following: • Cooling systems • Battery and natural gas generator backup in the event of power failure • Redundant communications lines • Smoke detectors • Dry pipe sprinklers
		Environmental vulnerabilities are not monitored or acted upon increasing the severity of an environmental event.	Operations personnel monitor the status of environmental protections during each shift.
			Environmental protections receive maintenance on at least an annual basis.
		Current processing capacity is not sufficient to meet processing requirements resulting in processing errors.	Processing capacity is monitored on a daily basis.
			Critical infrastructure components have at a minimum level of redundancy.

Criteria		Risks	Illustrative Controls
PI1.2	System inputs are measured and recorded completely, accurately, and timely in accordance with processing integrity commitments and requirements.	Inputs are captured incorrectly.	Application edits limit input to acceptable value ranges.
			The data preparation clerk batches documents by date received and enters the date and number of sheets on the batch ticket. Batched forms are scanned by a purchased imaging system. Upon completion of the scanning process, the scanned sheets are compared to the count per the batch ticket by the scanning operator.
			Scanned images are processed through the optical character recognition (OCR) system. Key fields including customer identifier, customer name, and record type are validated by the system against records in the master data file.
			Text from free form sections from scan sheets is manually entered. This information is input twice by two separate clerks. The input information is compared and records with differences are sent to a third clerk for resolution.
		Inputs are not captured or captured completely.	System edits require mandatory fields to be complete before record entry is accepted.

(continued)

Criteria		Risks	Illustrative Controls
			The data preparation clerk batches documents by date received and enters the date and number of sheets on the batch ticket. Batched forms are scanned by a purchased imaging system. Upon completion of the scanning process, the sheets scanned are compared to the count per the batch ticket by the scanning operator.
			Scanned images are processed through the OCR system. Key fields including customer identifier, customer name, and record type are validated by the system against records in the master data file.
			Text from free form sections from scan sheets is manually entered. This information is input twice by two separate clerks. The input information is compared and records with differences are sent to a third clerk for resolution.
			Electronic files received contain batch control totals. During the load processing data captured is reconciled to batch totals automatically by the application.

Criteria		Risks	Illustrative Controls
		Inputs are not captured in a timely manner.	Electronic files received are processed as received. The application monitors files that fail to process completely and generate an incident management error record.
			Manual forms for data entry are batched upon receipt. Batches are traced to batches entered for processing daily by the date entry supervisor and differences are investigated.
		The final disposition of input cannot be traced to its source to validate that it was processed correctly and the results of processing cannot be traced to initial input to validate completeness and accuracy.	Inputs are coded with identification numbers, registration numbers, registration information, or time stamps to enable them to be traced from initial input to output and final disposition and from output to source inputs.
PI1.3	Data is processed completely, accurately, and timely as authorized in accordance with processing integrity commitments and requirements.	Data is lost during processing.	Input record counts are traced from entry to final processing. Any differences are investigated.
		Data is inaccurately modified during processing.	Application regression testing validates key processing for the application during the change management process.

(continued)

Criteria		Risks	Illustrative Controls
			Output values are compared against prior cycle values. Variances greater than X percent are flagged on the variance report, logged to the incident management system, and investigated by the output clerk. Resolutions are documented in the incident management system. Open incidents are reviewed daily by the operations manager.
			Daily, weekly, and monthly trend reports are reviewed by the operations manager for unusual trends.
		Newly created data is inaccurate.	Application regression testing validates key processing for the application during the change management process.
			The system compares generated data to allowable values. Values outside the allowable values are written to the value exception report. Items on the value exception report are reviewed by the output clerk on a daily basis.
		Processing is not completed within required timeframes.	Scheduling software is used to control the submission and monitoring of job execution. An incident management record is generated automatically when processing errors are identified.

Criteria		Risks	Illustrative Controls
PI1.4	Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.	Data is not available for use as committed or agreed.	A mirror image of application data files is created nightly and stored on a second system for use in recovery and restoration in the event of a system disruption or outage.
		Stored data is inaccurate.	Logical access to stored data is restricted to the application and database administrators.
		Stored data is incomplete.	Data is reconciled on a monthly basis to help meet customer commitments and requirements.
PI1.5	System output is complete, accurate, distributed, and retained in accordance with processing integrity commitments and requirements.	System output is not complete.	Application regression testing validates key processing for the application during the change management process.
			Output values are compared against prior cycle values. Variances greater than five percent are flagged on the variance report, logged to the incident management system, and investigated by the output clerk. Resolutions are documented in the incident management system. Open incidents are reviewed daily by the operations manager.

(continued)

Criteria		Risks	Illustrative Controls
			On a monthly basis, total records processed are compared versus total records received via electronic submission, manual entry, and sheet scanned by the OCR system.
		System output is not accurate.	Application regression testing validates key processing for the application during the change management process.
			Output values are compared against prior cycle values. Variances greater than x percent are flagged on the variance report, logged to the incident management system, and investigated by the output clerk. Resolutions are documented in the incident management system. Open incidents are reviewed daily by the operations manager.
			Daily, weekly, and monthly trend reports are reviewed by the operations manager for unusual trends.
		System output is provided to unauthorized recipients.	Application security restricts output to approved user IDs.
		System output is not available to authorized recipients.	Application regression testing validates key processing for the application during the change management process.

Criteria		Risks	Illustrative Controls
			Output is generated by the system based on a master schedule. Changes to the master schedule are managed through the change management process and are approved by the customer service executive. On a daily basis, an automated routine scans output files to validate that all required output has been generated. The routine generates an incident record for any missing output. Incident tickets are managed through the incident management process.
PI1.6	Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	Data is modified by an unauthorized process or procedure resulting in inaccurate or incomplete data.	Application regression testing validates key processing for the application during the change management process.
			Access to data is restricted to authorized applications through access control software. Access rules are created and maintained by information security personnel during the application development process.
			Application level security restricts the ability to access, modify, and delete data to authenticated users who have been granted access through a record in the access control list. Creation and modification of access control records occurs through the access provisioning process.

(continued)

Criteria		Risks	Illustrative Controls
		Data is modified without authorization.	Logical access to stored data is restricted to the application and database administrators.
		Data is lost or destroyed.	Logical access to stored data is restricted to the application and database administrators.
			A mirror image of application data files is created nightly and stored on a second secure system for use in recovery and restoration in the event of a system disruption or outage.
Additional Criteria for Confidentiality			
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes in accordance with confidentiality commitments and requirements.	Data used in nonproduction environments is not protected from unauthorized access as committed.	The entity creates test data using data masking software that replaces confidential information with test information prior to the creation of test databases.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality commitments and requirements.	Unauthorized access to confidential information is obtained during processing.	Access to data is restricted to authorized applications through access control software. Access rules are created and maintained by information security personnel during the application development process.

Criteria		Risks	Illustrative Controls
			Logical access other than through authorized application is restricted to administrators through database management system native security. Creation and modification of access control records for the database management systems occurs through the access provisioning process.
			Application level security restricts the ability to access, modify, and delete data to authenticated users who have been granted access through a record in the access control list. Creation and modification of access control records occurs through the access provisioning process.
		Unauthorized access to confidential information in output is obtained after processing.	Application security restricts output to approved roles or user IDs.
			Output containing sensitive information is printed at the secure print facility and is marked with the legend "Confidential."
			Paper forms are physically secured after data entry. Physical access is restricted to storage clerks.

(continued)

Criteria		Risks	Illustrative Controls
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties in accordance with confidentiality commitments and requirements.	Confidential information transmitted beyond the boundaries of the system is provided to unauthorized user entity personnel.	Application security restricts output to approved user IDs.
			Transmission of digital output beyond the boundary of the system occurs through the use of authorized software supporting the advanced encryption standard (AES).
			Logical access to stored data is restricted to application and database administrators.
			Data is stored in encrypted format using software supporting the AES.
		Confidential information is transmitted to related parties, vendors, or other approved parties contravening confidentiality commitments.	Application security restricts output to approved user IDs.
			Transmission of digital output beyond the boundary of the system occurs through the use authorized software supporting the advanced encryption standard.

Criteria		Risks	Illustrative Controls
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality requirements, from vendors and other third parties whose products and services comprise part of the system and have access to confidential information.	Related party and vendor personnel are unaware of the entity's confidentiality commitments.	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. Agreement terms include requirements for marking and identifying data as confidential, handling standards for confidential data in the custody of related parties and vendors, and return and disposal of confidential information when no longer required.
		Requirements for handling of confidential information are not communicated to and agreed to by related parties and vendors.	Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity.
C1.5	Compliance with confidentiality commitments and requirements by vendors and others third parties whose products and services comprise part of the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.	Related party and vendor systems are not suitably designed or operating effectively to comply with confidentiality commitments.	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria.

(continued)

Criteria		Risks	Illustrative Controls
C1.6	Changes to confidentiality commitments and requirements are communicated to internal and external users, vendors, and other third parties whose products and services are included in the system.	Confidentiality practices and commitments are changed without the knowledge or ascent of user entities.	The chief information security officer is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate these changes to users, related parties, and vendors.
		Confidentiality practices and commitments are changed without the knowledge of related parties or vendors resulting in their systems not complying with the required practices and not meeting the commitments.	The chief information security officer is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate these changes to users, related parties, and vendors.
			Related party and vendor agreements are modified to reflect changes in confidentiality practices and commitments.
			Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria.

.20

Appendix C—Generally Accepted Privacy Principles

[Notice to Readers: The criteria for the trust services privacy principle are currently under revision. These criteria are being revised separately from the trust services principles and criteria for security, availability, processing integrity, and confidentiality. Accordingly, until the criteria for the trust service privacy principle are finalized, the 2009 version of the generally accepted privacy principles contained in this appendix should be used.**]**

Generally Accepted Privacy Principles

August 2009

Foreword

The AICPA and the Canadian Institute of Chartered Accountants (CICA) strongly believe that privacy is a business issue. Considering what organizations face when trying to address privacy issues, we quickly concluded that businesses did not have a comprehensive framework to manage their privacy risks effectively. The institutes decided that they could provide a significant contribution by developing a privacy framework that would address the needs of all of the parties affected by privacy requirements or expectations. Therefore, the institutes developed a privacy framework called AICPA and CICA *Generally Accepted Privacy Principles*. The institutes are making these principles and criteria widely available to all parties interested in addressing privacy issues.

These principles and criteria were developed and updated by volunteers who considered both current international privacy regulatory requirements and best practices. These principles and criteria were issued following the due process procedures of both institutes, which included exposure for public comment. The adoption of these principles and criteria is voluntary.

An underlying premise to these principles is that good privacy is good business. Good privacy practices are a key component of corporate governance and accountability. One of today's key business imperatives is maintaining the privacy of personal information collected and held by an organization. As business systems and processes become increasingly complex and sophisticated, growing amounts of personal information are being collected. Because more data is being collected and held, most often in electronic format, personal information may be at risk to a variety of vulnerabilities, including loss, misuse, unauthorized access, and unauthorized disclosure. Those vulnerabilities raise concerns for organizations, governments, individuals, and the public in general.

For organizations operating in a multijurisdictional environment, managing privacy risk can be an even more significant challenge. Adherence to generally accepted privacy principles does not guarantee compliance with all laws and regulations to which an organization is subject. Organizations need to be aware of the significant privacy requirements in all of the jurisdictions in which they do business. Although this framework provides guidance on privacy in general, organizations should consult their own legal counsel to obtain advice and guidance on particular laws and regulations governing an organization's specific situation.

With these issues in mind, the AICPA and CICA developed *Generally Accepted Privacy Principles* to be used as an operational framework to help management address privacy in a manner that takes into consideration many local, national, or international requirements. The primary objective is to facilitate

privacy compliance and effective privacy management. The secondary objective is to provide suitable criteria against which a privacy attestation engagement (usually referred to as a privacy audit) can be performed.

Generally Accepted Privacy Principles represents the AICPA and CICA contribution to aid organizations in maintaining the effective management of privacy risk, recognizing the needs of organizations, and reflecting the public interest. Additional history about the development and additional privacy resources can be found online at www.aicpa.org/INTERESTAREAS/INFORMATION TECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx and www.cica.ca/privacy. *Generally Accepted Privacy Principles* can be downloaded from the AICPA and the CICA websites, at www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx and www.cica.ca/privacy, respectively.

Because the privacy environment is constantly changing, *Generally Accepted Privacy Principles* will need to be revised from time to time; accordingly, please forward any comments about this document by e-mail to the AICPA (GAPP@aicpa.org) or the CICA (privacy@cica.ca).

AICPA

CICA

Privacy—An Introduction to Generally Accepted Privacy Principles

Introduction

Many organizations find challenges in managing privacy[1] on local, national, or international bases. Most are faced with a number of differing privacy laws and regulations whose requirements need to be operationalized.

Generally Accepted Privacy Principles (GAPP) has been developed from a business perspective, referencing some, but by no means all, significant local, national, and international privacy regulations. GAPP operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by objective, measurable criteria that form the basis for effective management of privacy risk and compliance in an organization. Illustrative policy requirements, communications, and controls, including monitoring controls, are provided as support for the criteria.

GAPP can be used by any organization as part of its privacy program. GAPP has been developed to help management create an effective privacy program that addresses privacy risks and obligations, and business opportunities. It can also be a useful tool to boards and others charged with governance and providing oversight. This introduction includes a definition of privacy and an explanation of why privacy is a business issue and not solely a compliance issue. Also illustrated is how these principles can be applied to outsourcing scenarios and the potential types of privacy initiatives that can be undertaken for the benefit of organizations and their customers.

This introduction and the set of privacy principles and related criteria that follow will be useful to those who

- oversee and monitor privacy and security programs.
- implement and manage privacy in an organization.
- implement and manage security in an organization.

---

[1] The first occurrence of each word contained in the glossary is linked to the top of glossary.

- oversee and manage risks and compliance in an organization.
- assess compliance and audit privacy and security programs.
- regulate privacy.

Why Privacy Is a Business Issue

Good privacy is good business. Good privacy practices are a key part of corporate governance and accountability. One of today's key business imperatives is maintaining the privacy of personal information. As business systems and processes become increasingly complex and sophisticated, organizations are collecting growing amounts of personal information. As a result, personal information is vulnerable to a variety of risks, including loss, misuse, unauthorized access, and unauthorized disclosure. Those vulnerabilities raise concerns for organizations, governments, and the public in general.

Organizations are trying to strike a balance between the proper collection and use of their customers' personal information. Governments are trying to protect the public interest and, at the same time, manage their cache of personal information gathered from citizens. Consumers are very concerned about their personal information, and many believe they have lost control of it. Furthermore, the public has a significant concern about identity theft and inappropriate access to personal information, especially financial and medical records, and information about children.

Individuals expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. They are no longer willing to overlook an organization's failure to protect their privacy. Therefore, all businesses need to effectively address privacy as a risk management issue. The following are specific risks of having inadequate privacy policies and procedures:

- Damage to the organization's reputation, brand, or business relationships
- Legal liability and industry or regulatory sanctions
- Charges of deceptive business practices
- Customer or employee distrust
- Denial of consent by individuals to have their personal information used for business purposes
- Lost business and consequential reduction in revenue and market share
- Disruption of international business operations
- Liability resulting from identity theft

International Privacy Considerations

For organizations operating in more than one country, the management of their privacy risk can be a significant challenge.

For example, the global nature of the Internet and business means regulatory actions in one country may affect the rights and obligations of individual users and customers around the world. Many countries have laws regulating transborder data flow, including the European Union's (EU) directives on data protection and privacy, with which an organization must comply if it wants to do business in those countries. Therefore, organizations need to comply with changing privacy requirements around the world. Further, different jurisdictions have different privacy philosophies, making international compliance a

complex task. To illustrate this, some countries view personal information as belonging to the individual and take the position that the enterprise has a fiduciary-like relationship when collecting and maintaining such information. Alternatively, other countries view personal information as belonging to the enterprise that collects it.

In addition, organizations are challenged to try and stay up to date with the requirements for each country in which they do business. By adhering to a high global standard, such as those set out in this document, compliance with many regulations will be facilitated.

Even organizations with limited international exposure often face issues of compliance with privacy requirements in other countries. Many of these organizations are unsure how to address often stricter overseas regulations. This increases the risk that an organization inadvertently could commit a breach that becomes an example to be publicized by the offended host country.

Furthermore, many local jurisdictions (such as states or provinces) and certain industries, such as healthcare or banking, have specific requirements related to privacy.

Outsourcing and Privacy

Outsourcing increases the complexity for dealing with privacy. An organization may outsource a part of its business process and, with it, some responsibility for privacy; however, the organization cannot outsource its ultimate responsibility for privacy for its business processes. Complexity increases when the entity that performs the outsourced service is in a different country and may be subject to different privacy laws or perhaps no privacy requirements at all. In such circumstances, the organization that outsources a business process will need to ensure it manages its privacy responsibilities appropriately.

GAPP and its supporting criteria can assist an organization in completing assessments (including independent examinations) about the privacy policies, procedures, and practices of the third party providing the outsourced services.

The fact that these principles and criteria have global application can provide comfort to an outsourcer that privacy assessments can be undertaken using a consistent measurement based on internationally known fair information practices.

What Is Privacy?

Privacy Definition

Privacy is defined in *Generally Accepted Privacy Principles* as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information."

Personal Information

Personal information (sometimes referred to as personally identifiable information) is information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Individuals, for this purpose, include prospective, current, and former customers, employees, and others with whom the entity has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be

attributed to an identified individual. Some examples of personal information are as follows:

- Name
- Home or e-mail address
- Identification number (for example, a Social Security or Social Insurance Number)
- Physical characteristics
- Consumer purchase history

Some personal information is considered sensitive. Some laws and regulations define the following to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, some jurisdictions may require explicit consent rather than implicit consent for the collection and use of sensitive information.

Some information about or related to people cannot be associated with specific individuals. Such information is referred to as *nonpersonal information*. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains because the information is deidentified or anonymized. Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual. However, some organizations may still have obligations over nonpersonal information due to other regulations and agreements (for example, clinical research and market research).

Privacy or Confidentiality?

Unlike personal information, which is often defined by law or regulation, no single definition of confidential information exists that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires be maintained on a "need to know" basis. Examples of the kinds of information that may be subject to a confidentiality requirement include the following:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists

- Legal documents
- Revenue by client and industry

Also, unlike personal information, rights of access to confidential information to ensure its accuracy and completeness are not clearly defined. As a result, interpretations of what is considered to be confidential information can vary significantly from organization to organization and, in most cases, are driven by contractual arrangements. For additional information on criteria for confidentiality, refer to the AICPA and CICA *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (see www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/TRUSTSERVICES/Pages/default.aspx or www.webtrust.org).

Introducing Generally Accepted Privacy Principles

GAPP is designed to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities.

The privacy principles and criteria are founded on key concepts from significant local, national, and international privacy laws, regulations, guidelines,[2] and good business practices. By using GAPP, organizations can proactively address the significant challenges that they face in establishing and managing their privacy programs and risks from a business perspective. GAPP also facilitates the management of privacy risk on a multijurisdictional basis.

Overall Privacy Objective

The privacy principles and criteria are founded on the following privacy objective.

Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in *Generally Accepted Privacy Principles* issued by the AICPA and CICA.

Generally Accepted Privacy Principles

The privacy principles are essential to the proper protection and management of personal information. They are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices.

The following are the 10 *generally accepted privacy principles*:

1. *Management.* The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

[2] For example, the Organisation for Economic Co-operation and Development has issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the European Union has issued Directive on Data Privacy (Directive 95/46/EC). In addition, the United States has enacted the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Children's Online Privacy Protection Act. Canada has enacted the Personal Information Protection and Electronic Documents Act and Australia has enacted the Australian Privacy Act of 1988, as amended in 2001. A chart comparing these international privacy concepts with generally accepted privacy principles can be found online at www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx. Compliance with this set of generally accepted privacy principles and criteria may not necessarily result in compliance with applicable privacy laws and regulations, and entities should seek appropriate legal advice regarding compliance with any laws and regulations.

2. *Notice.* The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. *Choice and consent.* The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. *Collection.* The entity collects personal information only for the purposes identified in the notice.
5. *Use, retention, and disposal.* The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. *Access.* The entity provides individuals with access to their personal information for review and update.
7. *Disclosure to third parties.* The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. *Security for privacy.* The entity protects personal information against unauthorized access (both physical and logical).
9. *Quality.* The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. *Monitoring and enforcement.* The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

For each of the 10 privacy principles, relevant, objective, complete, and measurable criteria have been specified to guide the development and evaluation of an entity's privacy policies, communications, and procedures and controls. *Privacy policies* are written statements that convey management's intent, objectives, requirements, responsibilities, and standards. *Communications* refers to the organization's communication to individuals, internal personnel, and third parties about its privacy notice and its commitments therein and other relevant information. *Procedures and controls* are the other actions the organization takes to achieve the criteria.

Using GAPP

GAPP can be used by organizations for the following:

- Designing, implementing, and communicating privacy policy
- Establishing and managing privacy programs
- Monitoring and auditing privacy programs
- Measuring performance and benchmarking

Establishing and managing a privacy program involves the following activities:

- **Strategizing.** Performing privacy strategic and business planning.
- **Diagnosing.** Performing privacy gap and risk analyses.
- **Implementing.** Developing, documenting, introducing, and institutionalizing the program's action plan, including establishing controls over personal information.

- **Sustaining and managing.** Monitoring activities of a privacy program.
- **Auditing.** Internal or external auditors evaluating the organization's privacy program.

The following table summarizes and illustrates how GAPP can be used by an organization to address these business activities.

Activity	*General Discussion*	*Potential Use of Generally Accepted Privacy Principles*
Strategizing	**Vision.** An entity's strategy is concerned with its long-term direction and prosperity. The vision identifies the entity's culture and helps shape and determine how the entity will interact with its external environment, including customers, competitors, and legal, social, and ethical issues. **Strategic Planning.** This is an entity's overall master plan, encompassing its strategic direction. Its objective is to ensure that the entity's efforts are all headed in a common direction. The strategic plan identifies the entity's long-term goals and major issues for becoming privacy compliant. **Resource Allocation.** This step identifies the human, financial, and other resources allocated to achieve the goals and objectives set forth in the strategic plan or business plan.	**Vision.** Within an entity's privacy effort, establishing the vision helps the entity integrate preferences and prioritize goals. **Strategic Planning.** Within an entity's privacy effort, *Generally Accepted Privacy Principles* (GAPP) can be used to assist the organization in identifying significant components that need to be addressed. **Resource Allocation.** Using GAPP, the entity would identify the people working with and responsible for areas that might include systems management, privacy and security concerns, and stipulate the resourcing for their activities. **Overall Strategy.** A strategic document describes expected or intended future development. GAPP can assist an entity in clarifying plans for the systems under consideration or for the business's privacy objectives. The plan identifies the process to achieve goals and milestones. It also provides a mechanism to communicate critical implementation elements, including details on services, budgets, development costs, promotion, and privacy advertising.

Activity	*General Discussion*	*Potential Use of Generally Accepted Privacy Principles*
Diagnosing	This stage, often referred to as the assessment phase, encompasses a thorough analysis of the entity's environment, identifying opportunities where weaknesses, vulnerability, and threats exist. The most common initial project for an organization is a diagnostic assessment. The purpose of such an assessment is to evaluate the entity against its privacy goals and objectives and determine to what extent the organization is achieving those goals and objectives.	GAPP can assist the entity in understanding its high-level risks, opportunities, needs, privacy policy and practices, competitive pressures, and the requirements of the relevant laws and regulations to which the entity is subject. GAPP provides a legislative neutral benchmark to allow the entity to assess the current state of privacy against the desired state.
Implementing	At this point, an action plan is mobilized or a diagnostic recommendation is put into effect, or both. Implementing involves developing and documenting a privacy program and action plan and the execution of all planned and other tasks necessary to make the action plan operational. It includes defining who will perform what tasks, assigning responsibilities, and establishing schedules and milestones. This involves the planning and implementation of a series of planned projects to provide guidance, direction, methodology, and tools to the organization in developing its initiatives.	GAPP can assist the entity in meeting its implementation goals. At the completion of the implementation phase, the entity should have developed the following deliverables: • Systems, procedures, and processes to address the privacy requirements • Updated privacy compliant forms, brochures, and contracts • Internal and external privacy awareness programs

(continued)

Activity	*General Discussion*	*Potential Use of Generally Accepted Privacy Principles*
Sustaining and managing	Sustaining and managing involves monitoring the work to identify how progress differs from the action plan in time to initiate corrective action. Monitoring refers to the management policies, processes, and supporting technology to ensure compliance with organizational privacy policies and procedures and the ability to exhibit due diligence.	The entity can use GAPP to develop appropriate reporting criteria for monitoring requests for information, the sources used to compile the information and the information actually disclosed. It can also be used for determining validation procedures to ensure that the parties to whom the information was disclosed are entitled to receive that information.
Internal privacy audit	Internal auditors provide objective assurance and consulting services designed to add value and improve an entity's operations. They help an entity accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.	Internal auditors can evaluate an entity's privacy program and controls using GAPP as a benchmark and provide useful information and reporting to management.
External privacy audit	External auditors, notably certified public accountants (CPAs) and chartered accountants (CAs), can perform attestation and assurance services. Generally, these services, whether performed on financial and nonfinancial information, build trust and confidence for individuals, management, customers, business partners, and other users.	An external auditor can evaluate an entity's privacy program and controls in accordance with GAPP and provide reports useful to individuals, management, customers, business partners, and other users.

Presentation of Generally Accepted Privacy Principles and Criteria

Under each principle, the criteria are presented in a three column format. The first column contains the measurement criteria. The second column contains illustrative controls and procedures, which are designed to provide examples and enhance the understanding of how the criteria might be applied. The illustrations are not intended to be comprehensive, nor are any of the illustrations required for an entity to have met the criteria. The third column contains additional considerations, including supplemental information such as good privacy practices and selected requirements of specific laws and regulations that may pertain to a certain industry or country.

Some of the criteria may not be directly applicable to some organizations or some processes. When a criterion is considered not applicable, the entity should consider justifying that decision to support future evaluation.

These principles and criteria provide a basis for designing, implementing, maintaining, evaluating, and auditing a privacy program to meet an entity's needs.

Generally Accepted Privacy Principles and Criteria

Management

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
1.0	**The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.**		
1.1	**Policies and Communications**		
1.1.0	**Privacy Policies** The entity defines and documents its privacy policies with respect to the following: *a.* Notice (See 2.1.0) *b.* Choice and consent (See 3.1.0) *c.* Collection (See 4.1.0) *d.* Use, retention, and disposal (See 5.1.0) *e.* Access (See 6.1.0) *f.* Disclosure to third parties (See 7.1.0) *g.* Security for privacy (See 8.1.0) *h.* Quality (See 9.1.0) *i.* Monitoring and enforcement (See 10.1.0)	Privacy policies are documented in writing and made readily available to internal personnel and third parties who need them.	

(continued)

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
1.1.1	**Communication to Internal Personnel** Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	The entity • periodically communicates to internal personnel (for example, on a network or a website) relevant information about the entity's privacy policies. Changes to its privacy policies are communicated shortly after approval. • requires internal personnel to confirm (initially and periodically) their understanding of the entity's privacy policies and their agreement to comply with them.	Privacy policies (as used herein) include security policies relevant to the protection of personal information.
1.1.2	**Responsibility and Accountability for Policies** Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	The entity assigns responsibility for privacy policies to a designated person, such as a corporate privacy officer. (Those assigned responsibility for privacy policies may be different from those assigned for other policies, such as security). The responsibility, authority, and accountability of the designated person or group are clearly documented. Responsibilities include the following: • Establishing with management the standards used to classify the sensitivity of personal information and to determine the level of protection required	The individual identified as being accountable for privacy should be from within the entity.

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• Formulating and maintaining the entity's privacy policies • Monitoring and updating the entity's privacy policies • Delegating authority for enforcing the entity's privacy policies • Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices A committee of the board of directors includes privacy periodically in its regular review of overall corporate governance.	
1.2	**Procedures and Controls**		
1.2.1	**Review and Approval** Privacy policies and procedures, and changes thereto, are reviewed and approved by management.	Privacy policies and procedures are • reviewed and approved by senior management or a management committee. • reviewed at least annually and updated as needed.	
1.2.2	**Consistency of Privacy Policies and Procedures With Laws and Regulations** Policies and procedures are reviewed and	Corporate counsel or the legal department • determines which privacy laws and regulations are applicable in the jurisdictions in which the entity operates.	In addition to legal and regulatory requirements, some entities may elect to comply with certain standards, such as those published by International

(continued)

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
	compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.	• identifies other standards applicable to the entity. • reviews the entity's privacy policies and procedures to ensure they are consistent with the applicable laws, regulations, and appropriate standards.	Organization for Standardization (ISO), or may be required to comply with certain standards, such as those published by the payment card industry, as a condition of doing business. Entities may include such standards as part of this process.
1.2.3	**Personal Information Identification and Classification** 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. Such information is covered by the entity's privacy and related security policies and procedures.	The entity has both an information classification policy and process, which include the following: • A classification process, which identifies and classifies information into one or more of the following categories: — Business confidential — Personal information (sensitive and other personal information) — Business general — Public • Identifying processes, systems, and third parties that handle personal information • Specific security and privacy policies and procedures that apply to each category of information	

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
1.2.4	**Risk Assessment** A risk assessment process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and to develop and update responses to such risks.	A process is in place to periodically identify the risks to the entity's personal information. Such risks may be external (such as loss of information by vendors or failure to comply with regulatory requirements) or internal (such as e-mailing unprotected sensitive information). When new or changed risks are identified, the privacy risk assessment and the response strategies are updated. The process considers factors such as experience with privacy incident management, the complaint and dispute resolution process, and monitoring activities.	Ideally, the privacy risk assessment should be integrated with the security risk assessment and be a part of the entity's overall enterprise risk management program. The board or a committee of the board should provide oversight and review of the privacy risk assessment.
1.2.5	**Consistency of Commitments With Privacy Policies and Procedures** Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.	Both management and the legal department review all contracts and service-level agreements for consistency with the entity's privacy policies and procedures.	
1.2.6	**Infrastructure and Systems Management** The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such	The following are used for addressing privacy impact: • Management assesses the privacy impact of new and significantly changed products, services, business processes, and infrastructure.	Some jurisdictions prohibit the use of personal information for test and development purposes unless it has been anonymized or otherwise protected to the same level required in its policies for production information.

(continued)

Ref.	Management Criteria	Illustrative Controls and Procedures	Additional Considerations
	activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following: • Infrastructure • Systems • Applications • Websites • Procedures • Products and services • Data bases and information repositories • Mobile computing and other similar electronic devices The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected in accordance with the entity's privacy policies and procedures.	• The entity uses a documented systems development and change management process for all information systems and related technology (including manual procedures, application programs, technology infrastructure, organizational structure, and the responsibilities of users and systems personnel), used to collect, use, retain, disclose, and destroy personal information. • The entity assesses planned new systems and changes for their potential effect on privacy. • Changes to system components are tested to minimize the risk of any adverse effect on the protection of personal information. All test data are anonymized. A controlled test database is maintained for full regression testing to ensure that changes to one program do not adversely affect other programs that process personal information. • Procedures ensure the maintenance of integrity and protection of personal information during migration from old to new or changed systems. • Documentation and approval by the privacy officer, security officer,	

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		business unit manager, and IT management are required before implementing the changes to systems and procedures that handle personal information, including those that may affect security. Emergency changes are required to maintain the same level of protection of personal information; however, they may be documented and approved on an after-the-fact basis.	
		The IT function maintains a listing of all software that processes personal information and the respective level, version, and patches that have been applied.	
		Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	
		Where computerized systems are involved, appropriate procedures are followed, such as the use of separate development, test, and production libraries to ensure that access to personal information is appropriately restricted.	
		Personnel responsible for initiating or implementing new systems and changes, and users of new or revised processes and applications, are provided training and awareness sessions related to privacy. Specific roles and responsibilities are assigned related to privacy.	

(continued)

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
1.2.7	**Privacy Incident and Breach Management** A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following: • Procedures for the identification, management, and resolution of privacy incidents and breaches • Defined responsibilities • A process to identify incident severity and determine required actions and escalation procedures • A process for complying with breach laws and regulations, including stakeholders breach notification, if required • An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate • A process for periodic review (at least on an annual basis) of actual incidents to identify necessary program updates based on the following:	A formal, comprehensive privacy incident and breach management program has been implemented, which specifies the following: • Incidents and breaches are reported to a member of the breach team, who assesses if it is privacy or security related, or both, classifies the severity of the incident, initiates required actions, and determines the required involvement by individuals who are responsible for privacy and security. • The chief privacy officer (CPO) has the overall accountability for the program and is supported by the privacy and security steering committees and assisted by the breach team. Incidents and breaches that do not involve personal information are the responsibility of the chief security officer. • The entity has a privacy breach notification policy, supported by (*a*) a process for identifying the notification and related requirements of other applicable jurisdictions relating to the data subjects affected by the breach, (*b*) a process for assessing the need for stakeholders breach notification, if required by law, regulation, or policy, and (*c*) a process	Some entities may adopt a breach notification policy for consistent use across all jurisdictions in which they operate. By necessity, such a policy would, at a minimum, be based on the most comprehensive legal requirements in any such jurisdiction.

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
	— Incident patterns and root cause — Changes in the internal control environment or external requirements (regulation or legislation) • Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed	for delivering the notice in a timely manner. The entity has agreements in place with a third party to manage the notification process and provide credit monitoring services for individuals, if needed. • The program includes a clear escalation path, based on the type or severity, or both, of the incident, up to executive management, legal counsel, and the board. • The program sets forth a process for contacting law enforcement, regulatory, or other authorities when necessary. • Program training for new hires and team members, and awareness training for general staff, is conducted annually, when a significant change in the program is implemented, and after any major incident. The privacy incident and breach management program also specifies the following: • After any major privacy incident, a formal incident evaluation is conducted by internal audit or outside consultants. • A quarterly review of actual incidents is conducted and required program updates are identified based on the following:	

(continued)

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		— Incident root cause — Incident patterns — Changes in the internal control environment and legislation • Results of the quarterly review are reported to the privacy steering committee and annually to the audit committee. • Key metrics are defined, tracked and reported to senior management on a quarterly basis. • The program is tested at least every six months and shortly after the implementation of significant system or procedural changes.	
1.2.8	**Supporting Resources** Resources are provided by the entity to implement and support its privacy policies.	Management annually reviews the assignment of personnel, budgets, and allocation of other resources to its privacy program.	
1.2.9	**Qualifications of Internal Personnel** The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.	The qualifications of internal personnel responsible for protecting the privacy and security of personal information are ensured by procedures such as the following: • Formal job descriptions (including responsibilities, educational and professional requirements, and organizational reporting for key privacy management positions)	

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• Hiring procedures (including the comprehensive screening of credentials, background checks, and reference checking) and formal employment and confidentiality agreements • Performance appraisals (performed by supervisors, including assessments of professional development activities)	
1.2.10	**Privacy Awareness and Training** A privacy awareness program about the entity's privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.	An interactive online privacy and security awareness course is required annually for all employees. New employees, contractors, and others are required to complete this course within the first month following employment in order to retain their access privileges. In-depth training is provided which covers privacy and relevant security policies and procedures, legal and regulatory considerations, incident response, and related topics. Such training is • required annually for all employees who have access to personal information or are responsible for protection of personal information. • tailored to the employee's job responsibilities.	

(continued)

Ref.	*Management Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• supplemented by external training and conferences. Attendance at the entity's privacy training and awareness courses is monitored. Training and awareness courses are reviewed and updated to reflect current legislative, regulatory, industry, and entity policy and procedure requirements.	
1.2.11	**Changes in Regulatory and Business Requirements** For each jurisdiction in which the entity operates, the effect on privacy requirements from changes in the following factors is identified and addressed: • Legal and regulatory • Contracts, including service-level agreements • Industry requirements • Business operations and processes • People, roles, and responsibilities • Technology Privacy policies and procedures are updated to reflect changes in requirements.	The entity has an ongoing process in place to monitor, assess, and address the effect on privacy requirements from changes in the following: • Legal and regulatory environments • Industry requirements (such as those for the Direct Marketing Association) • Contracts, including service-level agreements with third parties (changes that alter the privacy and security related clauses in contracts are reviewed and approved by the privacy officer or legal counsel before they are executed) • Business operations and processes • People assigned responsibility for privacy and security matters • Technology (prior to implementation)	Ideally, these procedures would be coordinated with the risk assessment process. The entity also should consider emerging and good practices, such as breach notification in jurisdictions where none is required.

Notice

Ref.	*Notice Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
2.0	**The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.**		
2.1	**Policies and Communications**		
2.1.0	**Privacy Policies** The entity's privacy policies address providing notice to individuals.		
2.1.1	**Communication to Individuals** Notice is provided to individuals regarding the following privacy policies: *a.* Purpose for collecting personal information *b.* Choice and consent (See 3.1.1) *c.* Collection (See 4.1.1) *d.* Use, retention, and disposal (See 5.1.1) *e.* Access (See 6.1.1) *f.* Disclosure to third parties (See 7.1.1) *g.* Security for privacy (See 8.1.1) *h.* Quality (See 9.1.1) *i.* Monitoring and enforcement (See 10.1.1) If personal information is collected from sources other than the individual, such sources are described in the notice.	The entity's privacy notice • describes the personal information collected, the sources of such information, and purposes for which it is collected. • indicates the purpose for collecting sensitive personal information and whether such purpose is part of a legal requirement. • describes the consequences, if any, of not providing the requested information. • indicates that certain information may be developed about individuals, such as buying patterns. • may be provided in various ways (for example, in a face-to-face conversation, on a telephone interview, on an application form or questionnaire, or electronically). However, written notice is the preferred method.	Notice also may describe situations in which personal information will be disclosed, such as the following: • Certain processing for purposes of public security or defense • Certain processing for purposes of public health or safety • When allowed or required by law The purpose described in the notice should be stated in such a manner that the individual can reasonably understand the purpose and how the personal information is to be used. Such purpose should be consistent with the business purpose of the entity and not overly broad. Consideration should be given to providing a summary level notice with links to more detailed sections of the policy.

(continued)

Ref.	*Notice Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
2.2	**Procedures and Controls**		
2.2.1	**Provision of Notice** Notice is provided to the individual about the entity's privacy policies and procedures (*a*) at or before the time personal information is collected, or as soon as practical thereafter, (*b*) at or before the entity changes its privacy policies and procedures, or as soon as practical thereafter, or (*c*) before personal information is used for new purposes not previously identified.	The privacy notice is • readily accessible and available when personal information is first collected from the individual. • provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal information to the entity. • clearly dated to allow individuals to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. In addition, the entity • tracks previous iterations of the entity's privacy policies and procedures. • informs individuals of a change to a previously communicated privacy notice, for example, by posting the notification on the entity's website, by sending written notice via postal mail, or by sending an e-mail. • documents that changes to privacy policies and procedures were communicated to individuals.	See 3.2.2, "Consent for New Purposes and Uses." Some regulatory requirements indicate that a privacy notice is to be provided on a periodic basis, for example, annually in the Gramm-Leach-Bliley Act (GLBA).

Ref.	*Notice Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
2.2.2	**Entities and Activities Covered** An objective description of the entities and activities covered by the privacy policies and procedures is included in the entity's privacy notice.	The privacy notice describes the particular entities, business segments, locations, and types of information covered, such as: • Operating jurisdictions (legal and political) • Business segments and affiliates • Lines of business • Types of third parties (for example, delivery companies and other types of service providers) • Types of information (for example, information about customers and potential customers) • Sources of information (for example, mail order or online) The entity informs individuals when they might assume they are covered by the entity's privacy policies but, in fact, are no longer covered (for example, linking to another website that is similar to the entity's, or using services on the entity's premises provided by third parties).	
2.2.3	**Clear and Conspicuous** The entity's privacy notice is conspicuous and uses clear language.	The privacy notice is • in plain and simple language. • appropriately labeled, easy to see, and not in unusually small print. • linked to or displayed on the website at points of data collection. • available in the national languages used on the site or in languages required by law.	If multiple notices are used for different subsidiaries or segments of an entity, similar formats are encouraged to avoid consumer confusion and allow consumers to identify any differences. Some regulations may contain specific information that a notice must contain. Illustrative notices are often available for certain industries and types of collection, use, retention, and disclosure.

Choice and Consent

Ref.	*Choice and Consent Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
3.0	**The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.**		
3.1	**Policies and Communications**		
3.1.0	**Privacy Policies** The entity's privacy policies address the choices available to individuals and the consent to be obtained.		
3.1.1	**Communication to Individuals** Individuals are informed about (*a*) 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.	The entity's privacy notice describes, in a clear and concise manner, the following: • The choices available to the individual regarding the collection, use, and disclosure of personal information • The process an individual should follow to exercise these choices (for example, checking an opt out box to decline receiving marketing materials) • The ability of, and process for, an individual to change contact preferences • The consequences of failing to provide personal information required for a transaction or service Individuals are advised of the following: • Personal information not essential to the purposes identified in the privacy notice need not be provided.	Some laws and regulations (such as Principle 11, "Limits on disclosure of personal information," section 1 of the Australian Privacy Act of 1988) provide specific exemptions for the entity not to obtain the individual's consent. Examples of such situations include the following: • The record keeper believes, on reasonable grounds, that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person. • Use of the information for that other purpose is required or authorized by or under law.

Ref.	*Choice and Consent Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• Preferences may be changed, and consent may be withdrawn at a later time, subject to legal or contractual restrictions and reasonable notice. The type of consent required depends on the nature of the personal information and the method of collection (for example, an individual subscribing to a newsletter gives implied consent to receive communications from the entity).	
3.1.2	**Consequences of Denying or Withdrawing Consent** When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.	At the time of collection, the entity informs individuals of the following: • About the consequences of refusing to provide personal information (for example, transactions may not be processed) • About the consequences of denying or withdrawing consent (for example, opting out of receiving information about products and services may result in not being made aware of sales promotions) • About how they will or will not be affected by failing to provide more than the minimum required personal information (for example, services or products will still be provided)	

(continued)

Ref.	*Choice and Consent Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
3.2	**Procedures and Controls**		
3.2.1	**Implicit or Explicit Consent** Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or soon after. The individual's preferences expressed in his or her consent are confirmed and implemented.	The entity • obtains and documents an individual's consent in a timely manner (that is, at or before the time personal information is collected or soon after). • confirms an individual's preferences (in writing or electronically). • documents and manages changes to an individual's preferences. • ensures that an individual's preferences are implemented in a timely fashion. • addresses conflicts in the records about an individual's preferences by providing a process for users to notify and challenge a vendor's interpretation of their contact preferences. • ensures that the use of personal information, throughout the entity and by third parties, is in accordance with an individual's preferences.	

Ref.	*Choice and Consent Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
3.2.2	**Consent for New Purposes and Uses** 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 individual is notified, and implicit or explicit consent is obtained prior to such new use or purpose.	When personal information is to be used for a purpose not previously specified, the entity • notifies the individual and documents the new purpose. • obtains and documents consent or withdrawal of consent to use the personal information for the new purpose. • ensures that personal information is being used in accordance with the new purpose or, if consent was withdrawn, not so used.	
3.2.3	**Explicit Consent for Sensitive Information** Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.	The entity collects sensitive information only if the individual provides explicit consent. *Explicit consent* requires that the individual affirmatively agree, through some action, to the use or disclosure of the sensitive information. Explicit consent is obtained directly from the individual and documented, for example, by requiring the individual to check a box or sign a form. This is sometimes referred to as opt in.	Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Schedule 1, clause 4.3.6, states that an organization should generally seek explicit consent when the information is likely to be considered sensitive. Many jurisdictions prohibit the collection of sensitive data, unless specifically allowed. For example, in the EU member state of Greece, Article 7 of Greece's "Law on the protection of individuals with regard to the processing of personal data" states, "The collection and processing of sensitive data is forbidden." However, a permit to collect and process sensitive data may be obtained.

(continued)

Ref.	Choice and Consent Criteria	Illustrative Controls and Procedures	Additional Considerations
			Some jurisdictions consider government-issued personal identifiers, for example, Social Security numbers or Social Insurance numbers, to be sensitive information.
3.2.4	**Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices** Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.	The entity requests customer permission to store, alter, or copy personal information (other than cookies) in the customer's computer or other similar electronic device. If the customer has indicated to the entity that it does not want cookies, the entity has controls to ensure that cookies are not stored on the customer's computer or other similar electronic device. Entities will not download software that will transfer personal information without obtaining permission.	Consideration should be given to prevent or detect the introduction of software that is designed to mine or extract information from a computer or other similar electronic device and therefore may be used to extract personal information, for example, spyware.

Collection

Ref.	Collection Criteria	Illustrative Controls and Procedures	Additional Considerations
4.0	**The entity collects personal information only for the purposes identified in the notice.**		
4.1	**Policies and Communications**		
4.1.0	**Privacy Policies** The entity's privacy policies address the collection of personal information.		Some jurisdictions, such as some countries in Europe, require entities that collect personal information to register with their regulatory body.

Ref.	*Collection Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
4.1.1	**Communication to Individuals** Individuals are informed that personal information is collected only for the purposes identified in the notice.	The entity's privacy notice discloses the types of personal information collected, the sources and methods used to collect personal information, and whether information is developed or acquired about individuals, such as buying patterns.	
4.1.2	**Types of Personal Information Collected and Methods of Collection** The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.	Types of personal information collected include the following: • Financial (for example, financial account information) • Health (for example, information about physical or mental status or history) • Demographic (for example, age, income range, social geocodes) Methods of collecting and third-party sources of personal information include the following: • Credit reporting agencies • Over the telephone • Via the Internet using forms, cookies, or Web beacons The entity's privacy notice discloses whether it uses cookies and Web beacons and how they are used. The notice also describes the consequences if the cookie is refused.	Some jurisdictions, such as those in the EU, require that individuals have the opportunity to decline the use of cookies.

(continued)

Ref.	*Collection Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
4.2	**Procedures and Controls**		
4.2.1	**Collection Limited to Identified Purpose** The collection of personal information is limited to that necessary for the purposes identified in the notice.	Systems and procedures are in place to • specify the personal information essential for the purposes identified in the notice and differentiate it from optional personal information. • periodically review the entity's program or service needs for personal information (for example, once every five years or when changes to the program or service are made). • obtain explicit consent when sensitive personal information is collected (see 3.2.3, "Explicit Consent for Sensitive Information"). • monitor that the collection of personal information is limited to that necessary for the purposes identified in the privacy notice and that all optional data is identified as such.	
4.2.2	**Collection by Fair and Lawful Means** 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.	The entity's management, privacy officer, and legal counsel, review the methods of collection and any changes thereto.	The following may be considered deceptive practices: • To use tools, such as cookies and Web beacons, on the entity's website to collect personal information without providing notice to the individual • To link information collected during an individual's visit to a website with personal information from other sources without providing notice to the individual

Ref.	*Collection Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
			• To use a third party to collect information in order to avoid providing notice to individuals Entities should consider legal and regulatory requirements in jurisdictions other than the one in which they operate (for example, an entity in Canada collecting personal information about Europeans may be subject to certain European legal requirements). A review of complaints may help to identify whether unfair or unlawful practices exist.
4.2.3	**Collection From Third Parties** 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.	The entity • performs due diligence before establishing a relationship with a third-party data provider. • reviews the privacy policies, collection methods, and types of consents of third parties before accepting personal information from third-party data sources.	Contracts include provisions requiring personal information to be collected fairly and lawfully and from reliable sources.
4.2.4	**Information Developed about Individuals** Individuals are informed if the entity develops or acquires additional information about them for its use.	The entity's privacy notice indicates that, if applicable, it may develop and acquire information about the individual using third-party sources, browsing, credit and purchasing history, and so on.	

(continued)

Use, Retention, and Disposal

Ref.	*Use, Retention, and Disposal Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
5.0	**The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.**		
5.1	**Policies and Communications**		
5.1.0	**Privacy Policies** The entity's privacy policies address the use, retention, and disposal of personal information.		
5.1.1	**Communication to Individuals** Individuals are informed that personal information is (*a*) used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise, (*b*) retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation, and (*c*) disposed of in a manner that prevents loss, theft, misuse, or unauthorized access.	The entity's privacy notice describes the following uses of personal information, for example: • Processing business transactions such as claims and warranties, payroll, taxes, benefits, stock options, bonuses, or other compensation schemes • Addressing inquiries or complaints about products or services, or interacting during the promotion of products or services • Product design and development, or purchasing of products or services • Participation in scientific or medical research activities, marketing, surveys, or market analysis • Personalization of websites or downloading software • Legal requirements • Direct marketing	

Ref.	Use, Retention, and Disposal Criteria	Illustrative Controls and Procedures	Additional Considerations
		The entity's privacy notice explains that personal information will be retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation and thereafter will be disposed of securely or made anonymous so that it cannot be identified to any individual.	
5.2	**Procedures and Controls**		
5.2.1	**Use of Personal Information** Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.	Systems and procedures are in place to ensure that personal information is used • in conformity with the purposes identified in the entity's privacy notice. • in agreement with the consent received from the individual. • in compliance with applicable laws and regulations.	Some regulations have specific provisions concerning the use of personal information. Examples are the GLBA, the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA).
5.2.2	**Retention of Personal Information** Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.	The entity • documents its retention policies and disposal procedures. • retains, stores, and disposes of archived and backup copies of records in accordance with its retention policies. • ensures personal information is not kept beyond the standard retention time unless a justified business or legal reason for doing so exists. Contractual requirements are considered when establishing retention practices when they may be exceptions to normal policies.	Some laws specify the retention period for personal information. For example, HIPAA has retention requirements on accounting for disclosures of personal health information—three years for electronic health records, and six years for nonelectronic health records. Other statutory record retention requirements may exist; for example, certain data may need to be retained for tax purposes or in accordance with employment laws.

(continued)

Ref.	*Use, Retention, and Disposal Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
5.2.3	**Disposal, Destruction and Redaction of Personal Information** Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.	The entity • erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based). • disposes of original, archived, backup and ad hoc or personal copies of records in accordance with its destruction policies. • documents the disposal of personal information. • within the limits of technology, locates and removes or redacts specified personal information about an individual as required, for example, removing credit card numbers after the transaction is complete. • regularly and systematically destroys, erases, or makes anonymous personal information no longer required to fulfill the identified purposes or as required by laws and regulations. Contractual requirements are considered when establishing disposal, destruction, and redaction practices if they may result in exception to the entity's normal policies.	Consideration should be given to using the services of companies that provide secure destruction services for personal information. Certain of these companies will provide a certificate of destruction where needed. Certain archiving techniques, such as DVDs, CDs, microfilm, or microfiche may not permit the removal of individual records without destruction of the entire database contained on such media.

Access

Ref.	*Access Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
6.0	**The entity provides individuals with access to their personal information for review and update.**		
6.1	**Policies and Communications**		
6.1.0	**Privacy Policies** The entity's privacy policies address providing individuals with access to their personal information.		
6.1.1	**Communication to Individuals** Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information.	The entity's privacy notice • explains how individuals may gain access to their personal information and any costs associated with obtaining such access. • outlines the means by which individuals may update and correct their personal information (for example, in writing, by phone, by e-mail, or by using the entity's website). • explains how disagreements related to personal information may be resolved.	
6.2	**Procedures and Controls**		
6.2.1	**Access by Individuals to Their Personal Information** Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.	Procedures are in place to • determine whether the entity holds or controls personal information about an individual. • communicate the steps to be taken to gain access to the personal information. • respond to an individual's request on a timely basis.	Some laws and regulations specify the following: • Provisions and requirements for providing access to personal information (for example, HIPAA) • Requirements that requests for access to personal information be submitted in writing

(continued)

Ref.	*Access Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• provide a copy of personal information, upon request, in printed or electronic form that is convenient to both the individual and the entity. • record requests for access and actions taken, including denial of access and unresolved complaints and disputes.	
6.2.2	**Confirmation of an Individual's Identity** The identity of individuals who request access to their personal information is authenticated before they are given access to that information.	Employees are adequately trained to authenticate the identity of individuals before granting the following: • Access to their personal information • Requests to change sensitive or other personal information (for example, to update information such as address or bank details) The entity • does not use government-issued identifiers (for example, Social Security numbers or Social Insurance numbers) for authentication. • mails information about a change request only to the address of record or, in the case of a change of address, to both the old and new addresses. • requires that a unique user identification and password (or equivalent) be used to access user account information online.	The extent of authentication depends on the type and sensitivity of personal information that is made available. Different techniques may be considered for the different channels, such as the following: • Web • Interactive voice response system • Call center • In person

Ref.	*Access Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
6.2.3	**Understandable Personal Information, Time Frame, and Cost** Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.	The entity • provides personal information to the individual in a format that is understandable (for example, not in code, not in a series of numbers, not in overly technical language or other jargon), and in a form convenient to both the individual and the entity. • makes a reasonable effort to locate the personal information requested and, if personal information cannot be found, keeps sufficient records to demonstrate that a reasonable search was made. • takes reasonable precautions to ensure that personal information released does not identify another person, directly or indirectly. • provides access to personal information in a timeframe that is similar to the entity's normal response times for other business transactions, or as permitted or required by law. • provides access to personal information in archived or backup systems and media. • informs individuals of the cost of access at the time the access request is made or as soon as practicable thereafter. • charges the individual for access to personal information at an amount, if any, which is not excessive in relation to the entity's cost of providing access. • provides an appropriate physical space to inspect personal information.	Entities may provide individuals with access to their personal information at no cost or at a minimal cost because of the potential business and customer-relationship benefits, as well as the opportunity to enhance the quality of the information.

(continued)

Ref.	*Access Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
6.2.4	**Denial of Access** Individuals 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.	The entity • outlines the reasons why access to personal information may be denied. • records all denials of access and unresolved complaints and disputes. • provides the individual with partial access in situations in which access to some of his or her personal information is justifiably denied. • provides the individual with a written explanation about why access to personal information is denied. • provides a formal escalation (appeal) process if access to personal information is denied. • conveys the entity's legal rights and the individual's right to challenge, if applicable.	Some laws and regulations (for example, Principle 5, "Information relating to records kept by record-keeper," point 2 of the Australian Privacy Act of 1988, and PIPEDA, Sections 8.(4), 8.(5), 8.(7), 9, 10, and 28) specify the situations in which access can be denied, the process to be followed (such as notifying the customer of the denial in writing within 30 days), and potential penalties or sanctions for lack of compliance.
6.2.5	**Updating or Correcting Personal Information** Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information.	The entity • describes the process an individual must follow to update or correct personal information records (for example, in writing, by phone, by e-mail, or by using the entity's website). • verifies the accuracy and completeness of personal information that an individual updates or changes (for example, by edit and validation controls, and forced completion of mandatory fields). • records the date, time, and identification of the person making the change if the entity's employee is making a change on behalf of an individual.	In some jurisdictions (for example, PIPEDA, Schedule 1, clauses 4.5.2 and 4.5.3), personal information cannot be erased, but an entity is bound to cease further processing.

Ref.	*Access Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• notifies third parties to whom personal information has been disclosed of amendments, erasures, or blocking of personal information, if it is possible and reasonable to do so.	
6.2.6	**Statement of Disagreement** Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.	If an individual and an entity disagree about whether personal information is complete and accurate, the individual may ask the entity to accept a statement claiming that the personal information is not complete and accurate. The entity • documents instances where an individual and the entity disagree about whether personal information is complete and accurate. • informs the individual, in writing, of the reason a request for correction of personal information is denied, citing the individual's right to appeal. • informs the individual, when access to personal information is requested or when access is actually provided, that the statement of disagreement may include information about the nature of the change sought by the individual and the reason for its refusal by the entity. • if appropriate, notifies third parties who have previously been provided with personal information that there is a disagreement and the nature of the disagreement.	See 10.1.1, "Communications to Individuals," 10.2.1, "Inquiry, Complaint, and Dispute Process," and 10.2.2, "Dispute Resolution and Recourse." Some regulations (for example, HIPAA) have specific requirements for denial of requests and handling of disagreements from individuals. If a challenge is not resolved to the satisfaction of the individual, when appropriate, the existence of such challenge is communicated to third parties having access to the information in question.

Disclosure to Third Parties

Ref.	*Disclosure to Third Parties Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
7.0	**The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.**		
7.1	**Policies and Communications**		
7.1.0	**Privacy Policies** The entity's privacy policies address the disclosure of personal information to third parties.		
7.1.1	**Communication to Individuals** Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise.	The entity's privacy notice • describes the practices related to the sharing of personal information (if any) with third parties and the reasons for information sharing. • identifies third parties or classes of third parties to whom personal information is disclosed. • informs individuals that personal information is disclosed to third parties only for the purposes (*a*) identified in the notice, and (*b*) for which the individual has provided implicit or explicit consent, or as specifically allowed or required by law or regulation.	The entity's privacy notice may disclose the following: • The process used to assure the privacy and security of personal information that has been disclosed to a third party • How personal information shared with a third party will be kept up to date, so that outdated or incorrect information shared with a third party will be changed if the individual has changed his or her information
7.1.2	**Communication to Third Parties** Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.	Prior to sharing personal information with a third party, the entity communicates its privacy policies or other specific instructions or requirements for handling personal information to, and obtains a written agreement from the third party that its privacy practices over the disclosed personal information adhere to those policies or requirements.	

Ref.	Disclosure to Third Parties Criteria	Illustrative Controls and Procedures	Additional Considerations
7.2	**Procedures and Controls**		
7.2.1	**Disclosure of Personal Information** Personal information is disclosed to third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically requires or allows otherwise.	Systems and procedures are in place to • prevent the disclosure of personal information to third parties unless an individual has given implicit or explicit consent for the disclosure. • document the nature and extent of personal information disclosed to third parties. • test whether disclosure to third parties is in compliance with the entity's privacy policies and procedures, or as specifically allowed or required by law or regulation. • document any third-party disclosures for legal reasons.	Personal information may be disclosed through various legal processes to law enforcement or regulatory agencies. Some laws and regulations have specific provisions for the disclosure of personal information. Some permit disclosure of personal information without consent whereas others require verifiable consent.
7.2.2	**Protection of Personal Information** 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 policies or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.	When providing personal information to third parties, the entity enters into contracts that require a level of protection of personal information equivalent to that of the entity's. In doing so, the entity • limits the third party's use of personal information to purposes necessary to fulfill the contract. • communicates the individual's preferences to the third party. • refers any requests for access or complaints about the personal information transferred by the entity to a designated privacy executive, such as a corporate privacy officer.	The entity is responsible for personal information in its possession or custody, including information that has been transferred to a third party. Some regulations (for example, from the U.S. federal financial regulatory agencies) require that an entity take reasonable steps to oversee appropriate service providers by exercising appropriate due diligence in the selection of service providers. Some jurisdictions, including some countries in Europe, require entities that transfer personal information to register with their regulatory body prior to transfer.

(continued)

Ref.	*Disclosure to Third Parties Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• specifies how and when third parties are to dispose of or return any personal information provided by the entity. The entity evaluates compliance with such contract using one or more of the following approaches to obtain an increasing level of assurance depending on its risk assessment: • The third party responds to a questionnaire about their practices. • The third party self-certifies that its practices meet the entity's requirements based on internal audit reports or other procedures. • The entity performs an onsite evaluation of the third party. • The entity receives an audit or similar report provided by an independent auditor.	PIPEDA requires a comparable level of protection while the personal information is being processed by a third party. Article 25 of the EU's Directive requires that such transfers take place only where the third party ensures an adequate level of protection.
7.2.3	**New Purposes and Uses** Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.	Systems and procedures are in place to • notify individuals and obtain their consent prior to disclosing personal information to a third party for purposes not identified in the privacy notice. • document whether the entity has notified the individual and received the individual's consent. • monitor that personal information is being provided to third parties only for uses specified in the privacy notice.	Other types of onward transfers include transfers to third parties who are • subsidiaries or affiliates. • providing a service requested by the individual. • law enforcement or regulatory agencies. • in another country and may be subject to other requirements.

Ref.	*Disclosure to Third Parties Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
7.2.4	**Misuse of Personal Information by a Third Party** The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.	The entity • reviews complaints to identify indications of any misuse of personal information by third parties. • responds to any knowledge of a third party using or disclosing personal information in variance with the entity's privacy policies and procedures or contractual arrangements. • mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures (for example, notify individuals affected, attempt to recover information disclosed to others, void affected numbers and reissue new numbers). • takes remedial action in the event that a third party misuses personal information (for example, contractual clauses address the ramification of misuse of personal information).	

Security for Privacy

Ref.	*Security for Privacy Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
8.0	**The entity protects personal information against unauthorized access (both physical and logical).**		
8.1	**Policies and Communications**		
8.1.0	**Privacy Policies** The entity's privacy policies (including any relevant security policies), address the security of personal information.	Privacy policies adequately address security measures to safeguard the privacy of personal information whether in electronic, paper, or other forms. Security measures are consistent with the sensitivity of the personal information.	Personal information in any location under control of the entity or deemed to be under control of the entity must be protected.
8.1.1	**Communication to Individuals** Individuals are informed that precautions are taken to protect personal information.	The entity's privacy notice describes the general types of security measures used to protect the individual's personal information, for example: • Employees are authorized to access personal information based on job responsibilities. • Authentication is used to prevent unauthorized access to personal information stored electronically. • Physical security is maintained over personal information stored in hard copy form, and encryption is used to prevent unauthorized access to personal information sent over the Internet. • Additional security safeguards are applied to sensitive information.	Users, management, providers, and other parties should strive to develop and adopt good privacy practices and to promote conduct that recognizes security needs and respects the legitimate interests of others. Consideration should be given to disclosing in the privacy notice the security obligations of individuals, such as keeping user IDs and passwords confidential and reporting security compromises. Consideration should be given to limiting the disclosure of detailed security procedures so as not to compromise internal security.

Ref.	*Security for Privacy Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
8.2	**Procedures and Controls**		
8.2.1	**Information Security Program** A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas[3] insofar as they relate to the security of personal information: *a.* Risk assessment and treatment [1.2.4] *b.* Security policy [8.1.0] *c.* Organization of information security [sections 1, 7, and 10] *d.* Asset management [section 1] *e.* Human resources security [section 1] *f.* Physical and environmental security [8.2.3 and 8.2.4]	The entity's security program addresses the following matters related to protection of personal information: • Periodic risk assessments • Identification of all types of personal information and the related processes, systems, and third parties that are involved in the handling of such information • Identification and documentation of the security requirements of authorized users • Allowing access, the nature of that access, and who authorizes such access • Preventing unauthorized access by using effective physical and logical access controls • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access	Safeguards employed may consider the nature and sensitivity of the data, as well as the size and complexity of the entity's operations. For example, the entity may protect personal information and other sensitive information to a level greater than it applies for other information. Some regulations (for example, HIPAA) provide a greater level of detail and guidance on specific security measures to be considered and implemented. Some security rules (for example, GLBA-related rules for safeguarding information) require the following: • Board (or committee or individual appointed by the board) approval and oversight of the entity's information security program. • That an entity take reasonable steps to oversee appropriate service providers by

(continued)

[3] These areas are drawn from ISO/IEC 27002:2005, Information technology—Security techniques—Code of practice for information security management. Permission is granted by the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). Copies of ISO/IEC 27002 can be purchased from ANSI in the United States at http://webstore.ansi.org/ and in Canada from the Standards Council of Canada at www.standardsstore.ca/eSpecs/index.jsp. It is not necessary to meet all of the criteria of ISO/IEC 27002:2005 to satisfy *Generally Accepted Privacy Principles*' criterion 8.2.1. The references associated with each area indicate the most relevant *Generally Accepted Privacy Principles*' criteria for this purpose.

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
	g. Communications and operations management [sections 1, 7, and 10] *h.* Access control [sections 1, 8.2, and 10] *i.* Information systems acquisition, development, and maintenance [1.2.6] *j.* Information security incident management [1.2.7] *k.* Business continuity management [section 8.2] *l.* Compliance [sections 1 and 10]	• Assignment of responsibility and accountability for security • Assignment of responsibility and accountability for system changes and maintenance • Protecting operating system and network software and system files • Protecting cryptographic tools and information • Implementing system software upgrades and patches • Testing, evaluating, and authorizing system components before implementation • Addressing how complaints and requests relating to security issues are resolved • Handling errors and omissions, security breaches, and other incidents • Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing) • Allocating training and other resources to support its security policies • Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies	— exercising appropriate due diligence in the selection of service providers. — requiring service providers by contract to implement and maintain appropriate safeguards for the personal information at issue. The payment card industry has established specific security and privacy requirements for cardholder information from certain brands.

Ref.	*Security for Privacy Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• Business continuity management and disaster recovery plans and related testing • Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts • A requirement that users, management, and third parties confirm (initially and annually) their understanding of an agreement to comply with the entity's privacy policies and procedures related to the security of personal information • Procedures to cancel access privileges and ensure return of computers and other devices used to access or store personal information when personnel are terminated The entity's security program prevents access to personal information in computers, media, and paper based information that are no longer in active use by the organization (for example, computers, media, and paper-based information in storage, sold, or otherwise disposed of).	

(continued)

Ref.	*Security for Privacy Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
8.2.2	**Logical Access Controls** Logical access to personal information is restricted by procedures that address the following matters: *a.* Authorizing and registering internal personnel and individuals *b.* Identifying and authenticating internal personnel and individuals *c.* Making changes and updating access profiles *d.* Granting privileges and permissions for access to IT infrastructure components and personal information *e.* Preventing individuals from accessing anything other than their own personal or sensitive information *f.* Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities *g.* Distributing output only to authorized internal personnel *h.* Restricting logical access to offline storage, backup data, systems, and media	Systems and procedures are in place to • establish the level and nature of access that will be provided to users based on the sensitivity of the data and the user's legitimate business need to access the personal information. • authenticate users, for example, by user name and password, certificate, external token, or biometrics before access is granted to systems handling personal information. • require enhanced security measures for remote access, such as additional or dynamic passwords, callback procedures, digital certificates, secure ID cards, virtual private network (VPN), or properly configured firewalls. • implement intrusion detection and monitoring systems.	User authorization processes consider the following: • How the data is accessed (internal or external network), as well as the media and technology platform of storage • Access to paper and backup media containing personal information • Denial of access to joint accounts without other methods to authenticate the actual individuals Some jurisdictions require stored data (at rest) to be encrypted or otherwise obfuscated.

Ref.	*Security for Privacy Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
	i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls) *j.* Preventing the introduction of viruses, malicious code, and unauthorized software		
8.2.3	**Physical Access Controls** Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).	Systems and procedures are in place to • manage logical and physical access to personal information, including hard copy, archival, and backup copies. • log and monitor access to personal information. • prevent the unauthorized or accidental destruction or loss of personal information. • investigate breaches and attempts to gain unauthorized access. • communicate investigation results to the appropriate designated privacy executive. • maintain physical control over the distribution of reports containing personal information. • securely dispose of waste containing confidential information (for example, shredding).	Physical safeguards may include the use of locked file cabinets, card access systems, physical keys, sign in logs, and other techniques to control access to offices, data centers, and other locations in which personal information is processed or stored.

(continued)

Ref.	Security for Privacy Criteria	Illustrative Controls and Procedures	Additional Considerations
8.2.4	**Environmental Safeguards** Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.	Management maintains measures to protect against environmental factors (for example, fire, flood, dust, power failure, and excessive heat and humidity) based on its risk assessment. The entity's controlled areas are protected against fire using both smoke detectors and a fire suppression system. In addition, the entity maintains physical and other safeguards to prevent accidental disclosure of personal information in the event of an environmental incident.	Some regulations, such as those in the EU Directive, also require that personal information is protected against unlawful destruction, accidental loss, natural disasters, and environmental hazards, in addition to accidental disclosure.
8.2.5	**Transmitted Personal Information** Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other nonsecure networks, and wireless networks is protected by deploying industry standard encryption technology for transferring and receiving personal information.	Systems and procedures are in place to • define minimum levels of encryption and controls. • employ industry standard encryption technology, for example, 128-bit Transport Layer Security (TLS), over VPNs, for transferring and receiving personal information. • approve external network connections. • protect personal information in both hardcopy and electronic forms sent by mail, courier, or other physical means. • encrypt personal information collected and transmitted wirelessly and protect wireless networks from unauthorized access.	Some regulations (for example, HIPAA) have specific provisions for the electronic transmission and authentication of signatures with respect to health information records (that is, associated with the standard transactions). Some credit card vendors have issued minimum requirements for protecting cardholder data, including the requirement to use encryption techniques for credit card and transaction related data in transmission and in storage. As technology, market, and regulatory conditions evolve, new measures may become necessary to meet acceptable levels of protection (for example, 128-bit secure TLS, including user IDs and passwords). Voice transmission from wireless devices (for example, cell phones) of personal information may not be encrypted.

Ref.	*Security for Privacy Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
8.2.6	**Personal Information on Portable Media** Personal information stored on portable media or devices is protected from unauthorized access.	Policies and procedures prohibit the storage of personal information on portable media or devices unless a business need exists and such storage is approved by management. Policies, systems, and procedures are in place to protect personal information accessed or stored in manners such as using the following: • Laptop computers, PDAs, smart-phones and similar devices • Computers and other devices used by employees while, for example, traveling and working at home • USB drives, CDs and DVDs, magnetic tape, or other portable media Such information is encrypted, password protected, physically protected, and subject to the entity's access, retention, and destruction policies. Controls exist over creation, transfer, storage, and disposal of media containing personal information used for backup and recovery. Procedures exist to report loss or potential misuse of media containing personal information. Upon termination of employees or contractors, procedures provide for the return or destruction of portable media and devices used to access and store personal information, and of printed and other copies of such information.	Consideration should be given to the protection needed for any personal information provided to, for example, regulators and auditors.

(continued)

Ref.	*Security for Privacy Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
8.2.7	**Testing Security Safeguards** Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.	Systems and procedures are in place to • regularly test the effectiveness of the key administrative, technical, and physical safeguards protecting personal information. • periodically undertake independent audits of security controls using either internal or external auditors. • test card access systems and other physical security devices at least annually. • document and test disaster recovery and contingency plans at least annually to ensure their viability. • periodically undertake threat and vulnerability testing, including security penetration and Web vulnerability and resilience. • make appropriate modifications to security policies and procedures on a periodic basis, taking into consideration the results of tests performed and new and changing threats and vulnerabilities. • periodically report the results of security testing to management.	The frequency and nature of the testing of security safeguards will vary with the entity's size and complexity, the nature and scope of its activities, and the sensitivity of personal information. Some security regulations (for example, GLBA-related rules for safeguarding information) require an entity to • conduct regular tests of key controls, systems, and procedures by independent third parties or by staff independent of those that develop or maintain security (or at least have these independent parties review results of testing). • assess and possibly adjust its information security at least annually.

Quality

Ref.	*Quality Criteria*	*Illustrative Controls and Procedures*	*Additional Consideration*
9.0	**The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.**		
9.1	**Policies and Communications**		
9.1.0	**Privacy Policies** The entity's privacy policies address the quality of personal information.		
9.1.1	**Communication to Individuals** Individuals are informed that they are responsible for providing the entity with accurate and complete personal information, and for contacting the entity if correction of such information is required.	The entity's privacy notice explains that personal information needs to be kept accurate and complete only when the individual has an ongoing relationship with the entity.	
9.2	**Procedures and Controls**		
9.2.1	**Accuracy and Completeness of Personal Information** Personal information is accurate and complete for the purposes for which it is to be used.	Systems and procedures are in place to • edit and validate personal information as it is collected, created, maintained, and updated. • record the date when the personal information is obtained or updated. • specify when the personal information is no longer valid. • specify when and how the personal information is to be updated and the source for the update (for example, annual reconfirmation of information held and methods for individuals to proactively update personal information).	

(continued)

Ref.	*Quality Criteria*	*Illustrative Controls and Procedures*	*Additional Consideration*
		• indicate how to verify the accuracy and completeness of personal information obtained directly from an individual, received from a third party (see 4.2.3, "Collection From Third Parties"), or disclosed to a third party (see 7.2.2, "Protection of Personal Information"). • ensure personal information used on an ongoing basis is sufficiently accurate and complete to make decisions, unless clear limits exist for the need for accuracy. • ensure personal information is not routinely updated unless such a process is necessary to fulfill the purposes for which it is to be used. The entity undertakes periodic assessments to check the accuracy of personal information records and to correct them, as necessary, to fulfill the stated purpose.	
9.2.2	**Relevance of Personal Information** Personal information is relevant to the purposes for which it is to be used.	Systems and procedures are in place to • ensure personal information is sufficiently relevant for the purposes for which it is to be used and to minimize the possibility that inappropriate information is used to make business decisions about the individual. • periodically assess the relevance of personal information records and to correct them, as necessary, to minimize the use of inappropriate data for decision making.	

Monitoring and Enforcement

Ref.	*Monitoring and Enforcement Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
10.0	**The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes.**		
10.1	**Policies and Communications**		
10.1.0	**Privacy Policies** The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.		
10.1.1	**Communication to Individuals** Individuals are informed about how to contact the entity with inquiries, complaints and disputes.	The entity's privacy notice • describes how individuals can contact the entity with complaints (for example, via an e-mail link to the entity's website or a telephone number). • provides relevant contact information to which the individual can direct complaints (for example, name, telephone number, mailing address, and e-mail address of the individual or office responsible for handling complaints).	
10.2	**Procedures and Controls**		
10.2.1	**Inquiry, Complaint, and Dispute Process** A process is in place to address inquiries, complaints, and disputes.	The corporate privacy officer or other designated individual is authorized to address privacy related complaints, disputes, and other problems. Systems and procedures are in place that allow for • procedures to be followed in communicating and resolving complaints about the entity. • action that will be taken with respect to the disputed information until the complaint is satisfactorily resolved.	

(continued)

Ref.	*Monitoring and Enforcement Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• remedies to be available in case of a breach of personal information and how to communicate this information to an individual. • recourse and a formal escalation process to be in place to review and approve any recourse offered to individuals. • contact information and procedures to be followed with any designated third party dispute resolution or similar service (if offered).	
10.2.2	**Dispute Resolution and Recourse** Each complaint is addressed, and the resolution is documented and communicated to the individual.	The entity has a formally documented process in place to • train employees responsible for handling individuals' complaints and disputes about the resolution and escalation processes. • document and respond to all complaints in a timely manner. • periodically review unresolved disputes and complaints to ensure they are resolved in a timely manner. • escalate unresolved complaints and disputes for review by management. • identify trends and the potential need to change the entity's privacy policies and procedures.	Some regulations (for example HIPAA and COPPA) have specific procedures and requirements. Some laws (for example, PIPEDA) permit escalation through the court system up to the most senior court.

Ref.	*Monitoring and Enforcement Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
		• use specified independent third-party dispute resolution services or other processes mandated by regulatory bodies in the event the individual is not satisfied with the entity's proposed resolution, together with a commitment from such third parties to handle such recourses. If the entity offers a third-party dispute resolution process for complaints that cannot be resolved directly with the entity, an explanation is provided about how an individual can use that process.	
10.2.3	**Compliance Review** Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts is reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.	Systems and procedures are in place to • annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, standards adopted by the entity, and other contracts. • document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign offs. • report the results of the compliance review and recommendations for improvement to management, and implement a remediation plan. • monitor the resolution of issues and vulnerabilities noted in the compliance review to ensure that appropriate corrective action is taken on a timely basis (that is, privacy policies and procedures are revised, as necessary).	In addition to legal, regulatory and contractual requirements, some entities may elect to comply with certain standards, such as those published by ISO, or may be required to comply with certain standards, such as those published by the payment card industry, as a condition of doing business.

(continued)

Ref.	*Monitoring and Enforcement Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
10.2.4	**Instances of Noncompliance** Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.	Systems and procedures are in place to • notify employees of the need to report privacy breaches and security vulnerabilities in a timely manner. • inform employees of the appropriate channels to report security vulnerabilities and privacy breaches. • document instances of noncompliance with privacy policies and procedures. • monitor the resolution of security vulnerabilities and privacy breaches to ensure appropriate corrective measures are taken on a timely basis. • discipline employees and others, as appropriate, who cause privacy incidents or breaches. • mitigate, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures (for example, notify individuals affected, attempt to recover information disclosed to others, void affected account numbers and reissue new numbers). • identify trends that may require revisions to privacy policies and procedures.	

Ref.	*Monitoring and Enforcement Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
10.2.5	**Ongoing Monitoring** Ongoing procedures are performed for monitoring the effectiveness of controls over personal information, based on a risk assessment [1.2.4], and for taking timely corrective actions where necessary.	The entity uses the following: • Control reports • Trend analysis • Training attendance and evaluations • Complaint resolutions • Regular internal reviews • Internal audit reports • Independent audit reports covering controls at service organizations • Other evidence of control effectiveness The selection of controls to be monitored, and the frequency with which they are monitored are based on the sensitivity of the information and the risks of possible exposure of the information. Examples of such controls are as follows: • Policies require that all employees take initial privacy training within 30 days of employment. Ongoing monitoring activities would include a review of human resource files of selected employees to determine that they contain the appropriate evidence of course completion.	*Guidance on Monitoring Internal Control Systems*, published by COSO (the Committee of Sponsoring Organizations of the Treadway Commission), provides helpful guidance for monitoring the effectiveness of controls.

(continued)

Ref.	*Monitoring and Enforcement Criteria*	*Illustrative Controls and Procedures*	*Additional Considerations*
10.2.5		• Policies require that whenever an employee changes job responsibilities or is terminated, such employee's access to personal information be reviewed and appropriately modified or terminated within 24 hours (or immediately in the case of employee termination). This is controlled by an automated process within the human resource system which produces a report of employee status changes, which requires supervisor action to avoid automatic termination of access. This is monitored by the security group which receives copies of these reports and the related supervisor actions. • Policies state that confirmation of a privacy-related complaint is provided to the complainant within 72 hours, and if not resolved within 10 working days, then the issue is escalated to the CPO. The control is a log used to record privacy complaints, including complaint date, and subsequent activities through to resolution. The monitoring activity is the monthly review of such logs for consistency with this policy.	

Appendix A—Glossary

affiliate. An entity that controls, is controlled by, or is under common control with another entity.

anonymize. The removal of any person-related information that could be used to identify a specific individual.

confidentiality. The protection of nonpersonal information and data from unauthorized disclosure.

consent. Agreement by the individual for the entity to collect, use, and disclose personal information in accordance with the privacy notice. Such agreement can be explicit or implied. *Explicit consent* is given orally, electronically, or in writing, is unequivocal and does not require any inference on the part of the entity seeking consent. *Implicit consent* may reasonably be inferred from the action or inaction of the individual such as not having *opted out*, or providing credit card information to complete a transaction. (see opt in and opt out).

cookies. Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. The information can then be used to identify the user when returning to the website, to personalize Web content, and suggest items of potential interest based on previous buying habits. Certain advertisers use tracking methods, including cookies, to analyze the patterns and paths through a site.

encryption. The process of transforming information to make it unreadable to anyone except those possessing special key (to decrypt).

entity. An organization that collects, uses, retains, and discloses personal information.

individual. The person about whom the personal information is being collected (sometimes referred to as the *data subject*).

internal personnel. Employees, contractors, agents, and others acting on behalf of the entity and its affiliates.

opt in. Personal information may not be collected, used, retained and disclosed by the entity without the explicit consent of the individual.

opt out. Implied consent exists for the entity to collect, use, retain, and disclose personal information unless the individual explicitly denies permission.

outsourcing. The use and handling of personal information by a third party that performs a business function for the entity.

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

personal information cycle. The collection, use, retention, disclosure, disposal, or anonymization of personal information.

policy. A written statement that communicates management's intent, objectives, requirements, responsibilities, and standards.

privacy. The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information.

privacy breach. A privacy breach occurs when personal information is collected, retained, accessed, used, or disclosed in ways that are not in accordance with the provisions of the enterprise's policies, applicable privacy laws, or regulations.

privacy program. The policies, communications, procedures, and controls in place to manage and protect personal information in accordance with business and compliance risks and requirements.

purpose. The reason personal information is collected by the entity.

redact. To delete or black out personal information from a document or file.

sensitive personal information. Personal information that requires an extra level of protection and a higher duty of care, for example, information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

third party. An entity that is not affiliated with the entity that collects personal information or any affiliated entity not covered by the entity's privacy notice.

Web beacon. Web beacons, also known as Web bugs, are small strings of code that provide a method for delivering a graphic image on a Web page or in an e-mail message for the purpose of transferring data. Businesses use Web beacons for many purposes, including site traffic reporting, unique visitor counts, advertising and e-mail auditing and reporting, and personalization. For example, a Web beacon can gather a user's IP address, collect the referrer, and track the sites visited by users.

Appendix B—CPA and CA Practitioner Services Using Generally Accepted Privacy Principles

This appendix provides a high level overview of the services that CPAs and CAs in public practice (practitioners) can provide using *Generally Accepted Privacy Principles* (GAPP). Additional guidance for practitioners is available from both the AICPA and Canadian Institute of Chartered Accountants (CICA) (see www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/Pages/default.aspx and www.cica.ca).

Privacy Advisory Engagements

Practitioners can provide a variety of advisory services to their clients, which include strategic, diagnostic, implementation, and sustaining and managing services using GAPP criteria. These services could include advising clients on system weaknesses, assessing risk, and recommending a course of action using GAPP criteria as a benchmark.

Practitioners in the United States providing such advisory services follow CS section 100 of Statement on Standards for Consulting Services, *Consulting Services: Definition and Standards* (AICPA, *Professional Standards*). No standards for Canadian practitioners exist in the CICA Handbook covering the performance of consulting services.

Privacy Attestation and Assurance Engagements

Practitioners also can use GAPP to provide attestation and assurance services to their clients, which typically result in a report for use by third parties. The nature of these services, the relevant professional standards, and the types of reports that may be issued for each are described subsequently.

Privacy Examination and Audit Engagements

Relevant U.S. standards for attestation engagements are contained in the Statements on Standards for Attestation Engagements. Relevant Canadian standards for assurance engagements are contained in Section 5025 of the CICA Handbook. Privacy attestation and assurance engagements are defined within the context of these standards. A practitioner is expected to comply with the requirements established by the relevant professional standards.

Examination and audit engagements are designed to provide a high, though not absolute, level of assurance on the subject matter or assertion. With that objective, the practitioner develops audit procedures that, in the practitioner's professional judgment, reduce to a low level the risk that the practitioner will reach an inappropriate conclusion. Illustrative privacy examination and audit reports are included in appendix C.

The following key concepts apply to privacy examination and audit engagements:

- Privacy examination and audit reports ordinarily cover all 10 principles. All of the relevant criteria for each principle need to be met during the period covered by the report to issue an unqualified report.[1,2]

---

[1] See appendix C, "Illustrative Privacy Examination and Audit Reports."

[2] In certain circumstances (such as a report on a third-party service provider), special purpose privacy reports covering some of the 10 principles could be issued. It is recommended that such reports contain language that indicates that the privacy principles not covered are essential for overall assurance of privacy and be "restricted use" reports.

- The work should be performed at the examination or equivalent level of assurance.
- The scope of the engagement can cover (1) either all personal information or only certain identified types of personal information, such as customer information or employee information, and (2) all business segments and locations for the entire entity or only certain identified segments of the business (retail operations, but not manufacturing operations or only operations originating on the entity's website or specified web domains) or geographic locations (such as only Canadian operations). In addition:
  - The privacy notice either should (1) be readily available to the users of the auditor's report and be clearly described in management's assertion and the report, or (2) accompany management's assertion and the auditor's report.
  - The scope of the engagement should generally be consistent with the description of the entities and activities covered in the privacy notice (see criterion 2.2.2). The scope often could be narrower, but ordinarily not broader, than that covered by the related privacy notice.
  - The scope of the engagement should cover all of the activities in the information cycle for the relevant personal information. These should include collection, use, retention, disclosure, disposal, or anonymization. Defining a business segment that does not include this entire cycle could be misleading to the user of the practitioner's report.
  - If the identified personal information included in the scope of the examination is commingled with other personal information not in the scope of the engagement, the scope of the engagement needs to cover controls over all of the information from the point of commingling forward.
  - The practitioner's report should ordinarily cover a period of time (not less than two months); however, the practitioner's initial report can be a point in time report.

Management's Assertion

Under AICPA attestation standards, in an examination engagement, the practitioner should ordinarily obtain a written assertion. If management will not provide the practitioner with a written assertion, the practitioner may still report on the subject matter; however, the form of the report will vary depending on the circumstances.[3]

Under AICPA standards, the practitioner may report on either management's assertion or the subject matter of the engagement. When the practitioner reports on the assertion, the assertion should accompany the practitioner's report, or the first paragraph of the report should contain a statement of the assertion.[4] When the practitioner reports on the subject matter, the practitioner may want

[3] See paragraph .58 of AT section 101, *Attest Engagements* (AICPA, *Professional Standards*) for a description of a practitioner's options, if a written assertion is not obtained.

[4] See paragraph .64 of AT section 101.

to request that management make an assertion available to the users of the practitioner's report.

Under CICA assurance standards, the practitioner may report on either management's assertion regarding the subject matter of the engagement, or directly on the subject matter. When the practitioner reports on management's assertion, the assertion should accompany the practitioner's report. When the practitioner reports directly on the subject matter, the practitioner is not required to obtain a written assertion of management. However, when the practitioner has not obtained such assertion, the practitioner is required to establish by other means that management is responsible for the subject matter—this is fundamental to performing the engagement.

For a privacy examination or audit, it is believed that an assertion-based engagement is more appropriate than an engagement to report directly on the subject matter. By providing a publicly available assertion, management explicitly acknowledges its responsibility for the matters addressed in its assertion.

Privacy Review Engagements

A *review engagement* is a type of attestation or assurance engagement. However, the term *privacy review* is often misused to refer either to a privacy examination or to certain types of privacy advisory engagements, such as a privacy diagnostic engagement or an engagement to develop findings and recommendations related to privacy. To reduce the risk that either the practitioner or the client may misinterpret the needs or expectations of the other party, the practitioner should establish an understanding with the client regarding the specifics of services to be performed and type of report to be issued.

A review engagement, as defined in professional standards, is a type of attestation or assurance engagement in which the practitioner reports on whether any information came to his or her attention, on the basis of the work performed, that indicates that the subject matter is not based on (or in conformity with) the criteria, or the assertion is not presented (or fairly stated) in all material respects based on the criteria. The procedures performed to provide a basis for the practitioner's review engagement report generally are limited to inquiry, analytical review procedures, and discussion. In the view of the AICPA and CICA Privacy Task Force, these types of procedures and the limited assurance provided from a review engagement would not be adequate to meet the needs of most parties affected by privacy requirements and expectations when the reporting entity is expected to demonstrate compliance with generally accepted privacy principles and criteria. Accordingly, no guidance is provided on the performance of privacy review engagements.

Agreed-Upon (Specified Auditing) Procedures Engagements

In an agreed-upon or specified procedures engagement, the practitioner performs specified procedures, agreed to by the parties,[5] and reports his or her findings. The practitioner does not perform an audit or review of an assertion or subject matter nor does the practitioner express an opinion or negative assurance about the assertion or subject matter.[6] In this type of engagement, the

[5] The specified users of the report and the practitioner agree upon the procedures to be performed by the practitioner.

[6] In the United States, agreed-upon procedures engagements are performed under paragraph .15 of AT section 201, *Agreed-Upon Procedures Engagements* (AICPA, *Professional Standards*). In Canada

(continued)

practitioner's report is in the form of a description of procedures and findings. Generally accepted privacy principles and criteria may be used in such engagements. This type of work would not lead to an examination or audit report, but rather to a report presenting the agreed-upon or specified procedures and the corresponding findings for each procedure. Agreed-upon or specified procedures could be undertaken to address a subset of an entity's system or a subset of the generally accepted privacy principles and criteria, or both. For example, an entity may request that a practitioner complete agreed-upon or specified procedures using selected criteria from generally accepted privacy principles and report the findings. In Canada, specified procedures engagements are permitted, although they are not considered to be assurance engagements under CICA Handbook section 5025.

Because users' needs may vary widely, the nature, timing, and extent of the agreed-upon and specified procedures may vary as well. Consequently, the specified users and the client assume responsibility for the sufficiency of the procedures since they best understand their own needs. The use of such a report is restricted to the specified parties who agreed upon the procedures.

Relationship Between Generally Accepted Privacy Principles and the Trust Services Principles and Criteria

Generally accepted privacy principles are part of the AICPA and CICA *Trust Services Principles and Criteria* that are based upon a common framework (that is, a core set of principles and criteria) to provide professional attestation or assurance and consulting or advisory services. The *Trust Services Principles and Criteria*[7] were developed by volunteer task forces under the auspices of the AICPA and CICA. The other *trust services principles and criteria* are:

- *Security.* The system is protected against unauthorized access (both physical and logical).
- *Availability.* The system is available for operation and use as committed or agreed.
- *Processing integrity.* System processing is complete, accurate, timely, and authorized.
- *Confidentiality.* Information designated as confidential is protected as committed or agreed.

These are discussed more fully at www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/TRUSTSERVICES/Pages/default.aspx.

(footnote continued)

there are no general standards for agreed-upon procedures/specified procedures. A practitioner could, however, look to the guidance provided by the Canadian Institute of Chartered Accountants (CICA) handbook section 9100 that contains standards for performing Specified Procedures on Financial Information Other Than Financial Statements. In specified auditing procedures engagements, the practitioner is engaged to report to specific users the results of applying specified procedures. In applying such procedures, the practitioner does not express a conclusion concerning the subject matter because he or she does not necessarily perform all of the procedures that, in the practitioner's judgment, would be necessary to provide a high level of assurance. Rather, the practitioner's report sets out the factual results of the procedures applied, including any exceptions found.

[7] WebTrust and SysTrust are two specific attestation or assurance services offerings developed by the AICPA and the CICA that are based on the *Trust Services Principles and Criteria*. Practitioners must be licensed by the CICA to use either the WebTrust or SysTrust seals. When the privacy engagement incorporates an online segment and the entity has received an examination or audit report that does not include a qualification or scope limitation, an entity may choose to display a WebTrust Online Privacy seal. For more information on licensure and Online Privacy Engagements see www.webtrust.org.

Appendix C—Illustrative Privacy Examination and Audit Reports

The following appendix includes examples of examination and audit reports under AICPA or Canadian Institute of Chartered Accountants (CICA) professional reporting standards, respectively:

Under AICPA Attestation Standards	*Under CICA Assurance Standards*
Illustration 1—Reporting on Management's Assertion and Sample Management Assertion	Illustration 3—Reporting on Management's Assertion and Sample Management Assertion
Illustration 2—Reporting Directly on the Subject Matter	Illustration 4—Reporting Directly on the Subject Matter

Illustration 1—Reporting on Management's Assertion Under AICPA Attestation Standards

Independent Practitioner's Privacy Report

To the Management of ABC Company, Inc.:

We have examined ABC Company, Inc.'s (ABC Company) management assertion that, during the period Xxxx xx, 2009 through Yyyy yy, 2009, it:

- Maintained effective controls over the privacy of personal information collected in its _____ [*description of the entities and activities covered, for example "the mail-order catalog-sales operations"*] business (the Business) to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with its commitments in its privacy notice related to the Business and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants, and
- Complied with its commitments in its privacy notice, which is dated xxxx xx, 2009 and [is available at www.ABC-Company/privacy or accompanies this report].

This assertion is the responsibility of ABC Company's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of ABC Company's controls over the privacy of personal information, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with ABC Company's commitments in its privacy notice, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, ABC Company's management assertion that, during the period Xxxx xx, 2009 through Yyyy yy, 2009, ABC Company:

- Maintained effective controls over the privacy of personal information collected in the Business to provide reasonable assurance that the personal information was collected, used, retained, disclosed and disposed of in conformity with its commitments in its

privacy notice and with criteria set forth in Generally Accepted Privacy Principles; and

- Complied with its commitments in its privacy notice referred to above,

is, in all material respects, fairly stated.

OR

In our opinion, ABC Company's management assertion referred to above is fairly stated, in all material respects, in conformity with ABC Company's privacy notice referred to above and with criteria set forth in Generally Accepted Privacy Principles.

Because of the nature and inherent limitations of controls, ABC Company's ability to meet the aforementioned criteria and the commitments in its privacy notice may be affected. For example, fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements may not be prevented or detected. Also, the projection of any conclusions, based on our findings, to future periods is subject to the risk that any changes or future events may alter the validity of such conclusions.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

Sample Management Assertion for Illustration 1

During the period Xxxx xx, 2009 through Yyyy yy, 2009, ABC Company, in all material respects:

- Maintained effective controls over the privacy of personal information collected in our _____ [*description of the entities and activities covered, for example "the mail-order catalog-sales operations"*] business (the Business) to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with our commitments in our privacy notice related to the Business and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants, and
- Complied with our commitments in our privacy notice, which is dated xxxx xx, 2009 and [is available at www.ABC-Company/privacy or accompanies this report].

Illustration 2—Reporting Directly on the Subject Matter Under AICPA Attestation Standards

Independent Practitioner's Privacy Report

To the Management of ABC Company, Inc.:

We have examined (1) the effectiveness of ABC Company, Inc.'s (ABC Company) controls over the personal information collected in its _____ [*description of the entities and activities covered, for example "the mail-order catalog-sales operations"*] business (the Business) to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with its commitments in its privacy notice and with criteria set forth

in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants, and (2) ABC Company's compliance with its commitments in its privacy notice, which is dated xxxx xx, 2009 and [is available at www.ABC-Company/privacy or accompanies this report], related to the Business during the period Xxxx xx, 2009 through Yyyy yy, 2009. ABC Company's management is responsible for maintaining the effectiveness of these controls and for compliance with its commitments in its privacy notice. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of ABC Company's controls over the privacy of personal information, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with ABC Company's commitments in its privacy notice, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, during the period Xxxx xx, 2009 through Yyyy yy, 2009, ABC Company, in all material respects (1) maintained effective controls over privacy of personal information collected in the Business to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles; and (2) complied with its commitments in its privacy notice referred to above.

Because of the nature and inherent limitations of controls, ABC Company's ability to meet the aforementioned criteria and the commitments in its privacy notice may be affected. For example, fraud, unauthorized access to systems and information, and failure to comply with internal or external policies or requirements may not be prevented or detected. Also, the projection of any conclusions, based on our findings, to future periods is subject to the risk that any changes or future events may alter the validity of such conclusions.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

Illustration 3—Reporting on Management's Assertion Under CICA Assurance Standards

Auditor's Privacy Report

To the Management of ABC Company, Inc.:

We have audited ABC Company, Inc.'s (ABC Company) management assertion that, during the period Xxxx xx, 2009 through Yyyy yy, 2009, it:

- Maintained effective controls over the privacy of personal information collected in its _____ [*description of the entities and activities covered, for example "the mail-order catalog-sales operations*"] business (the Business) to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with its commitments in its privacy notice related to the Business and with criteria set forth in Generally Accepted Privacy Principles, issued by the American

Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (CICA), and

- Complied with its commitments in its privacy notice, which is dated xxxx xx, 2009 and [is available at www.ABC-Company/privacy or accompanies this report].

This assertion is the responsibility of management. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with standards for assurance engagements established by the CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of ABC Company's controls over the privacy of personal information, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with ABC Company's commitments in its privacy notice and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, ABC Company's management assertion that, during the period Xxxx xx, 2009 through Yyyy yy, 2009, ABC Company:

- Maintained effective controls over the privacy of personal information collected in the Business to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles; and

- Complied with its commitments in its privacy notice referred to above,

is, in all material respects, fairly stated.

OR

In our opinion, ABC Company management's assertion referred to above is fairly stated, in all material respects, in conformity with ABC Company's privacy notice referred to above and with criteria set forth in Generally Accepted Privacy Principles.

Because of the nature and inherent limitations of controls, ABC Company's ability to meet the aforementioned criteria and the commitments in its privacy notice may be affected. For example, fraud, unauthorized access to systems and information, failure to comply with internal and external policies and requirements may not be prevented or detected. Also, the projection of any conclusions, based on our findings, to future periods is subject to the risk that any changes or future events may alter the validity of such conclusions.

[*Name of CA firm*]

[*City, Province*]

Chartered Accountants

[*Date*]

Sample Management Assertion for Illustration 3

During the period Xxxx xx, 2009 through Yyyy yy, 2009, ABC Company, in all material respects:

- Maintained effective controls over the privacy of personal information collected in our _____ business [*description of the entities and activities covered, for example "the mail-order catalog-sales operations*"] (the Business) to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in accordance with our commitments in the privacy notice related to the Business and with the criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants, and
- Complied with our commitments in our privacy notice which is dated xxxx xx, 2009 and [is available at www.ABC-Company/privacy or accompanies this report].

Illustration 4—Reporting Directly on the Subject Matter Under CICA Assurance Standards

Auditor's Privacy Report

To the Management of ABC Company, Inc.:

We have audited (1) the effectiveness of ABC Company, Inc.'s (ABC Company) controls over the personal information collected in its _____ [*description of the entities and activities covered, for example "the mail-order catalog-sales operations*"] business (the Business) to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (CICA), and (2) ABC Company's compliance with its commitments in its privacy notice, which is dated xxxx xx, 2009 and [is available at www.ABC-Company/privacy or accompanies this report], related to the Business during the period Xxxx xx, 2009 through Yyyy yy, 2009. ABC Company's management is responsible for maintaining the effectiveness of these controls and for compliance with its commitments in its privacy notice. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with standards for assurance engagements established by the CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of ABC Company's controls over the privacy of personal information, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with ABC Company's commitments in its privacy notice, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, during the period Xxxx xx, 2009 through Yyyy yy, 2009, ABC Company, in all material respects (1) maintained effective controls over privacy of personal information collected in the Business to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with its commitments in its privacy notice and with

criteria set forth in the Generally Accepted Privacy Principles; and (2) complied with its commitments in its privacy notice referred to above.

Because of the nature and inherent limitations of controls, ABC Company's ability to meet the aforementioned criteria and the commitments in its privacy notice may be affected. For example, fraud, unauthorized access to systems and information, and failure to comply with internal or external policies or requirements may not be prevented or detected. Also, the projection of any conclusions, based on our findings, to future periods is subject to the risk that any changes or future events may alter the validity of such conclusions.

[*Name of CA firm*]

[*City, Province*]

Chartered Accountants

[*Date*]

AICPA®

888.777.7077 | aicpa.org

19496-349