TSP Section 100

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

(To supersede the 2009 version of *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP section 100A).* The privacy criteria are presented in appendix C. These criteria are the same criteria set forth in appendix D of TSP section 100A. The privacy criteria are currently under revision. The criteria in TSP section 100 are effective for periods ending on or after December 15, 2014, with earlier implementation permitted. TSP section 100A will retain the superseded material until March 31, 2016. 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, 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, [fn 1] 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 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

---

[fn 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.

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: [fn 2]

[fn 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.

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 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 [fn 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.

[fn 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.
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.
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.
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.
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.

Appendix A — Definitions

.18

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.

Appendix B — Illustrative Risks and Controls

.19 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,	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 pro-

	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*].		cess 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.
			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 prom-	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.

	ulgated and placed in operation.		
			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.
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) be-*	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.

	ing reported on: security, availability, processing integrity, or confidentiality or any combination thereof].		
			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.
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, con-

			sented, 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 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.
			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.
			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.

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.
			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 identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).	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.
		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 evalua-

			tion.
			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.
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 activi-	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.

	ties based on the operation and monitoring of those activities, and updates them as necessary.		
		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, 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.	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 system commitments and requirements.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software 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.
			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.
		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.
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.
		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 em-

			ployees 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 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).
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).
		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.
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.
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.
			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.
		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.
			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.
			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 in-	Nonpublic information is disclosed during transmission over public	VPN, SSL, secure file transfer program (SFTP), and other encryption

	formation 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*].	communication paths.	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.
			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.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduc-	Malicious or otherwise unauthorized code is used to intentionally or unintentionally compromise	The ability to install software on workstations and laptops is restricted to IT support personnel.

	tion of unauthorized or malicious software.	logical access controls or system functionality through data transmission, removable media, and portable or mobile devices.	
			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 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.	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 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
		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.
CC7.0	***Common Criteria Related to Change Management***		
CC7.1	[*Insert the principle(s) be-*	Commitments and requirements	System change requests are evalu-

	ing 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.	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.	ated 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.
			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.
		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.
			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.
		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.

		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.
			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 infra-	Environmental vulnerabilities and changing environmental conditions are not identified or addressed	Environmental protections have been installed including the following:

	structure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	through the use of environmental protections resulting in a loss of system availability.	• 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.
			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	Recovery plans are not suitably designed and backups are not suf-	Business continuity and disaster recovery plans, including restora-

	with recovery plans are periodically tested to help meet availability commitments and requirements.	ficient to permit recovery of system operation in accordance with commitments and requirements.	tion 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.
			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.
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.
			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.
		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.
			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.
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. Vari-

			ances 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.
			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.
			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.
		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 re-	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.

	quirements.		
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.
			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.
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.
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 tak-	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.

	en, 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.	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.

Appendix C — Generally Accepted Privacy Principles

.20 **[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 expec-

tations. 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/INFORMATIONTECHNOLOGY/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

Privacy—An Introduction to Generally Accepted Privacy Principles

Introduction

Many organizations find challenges in managing privacy [fn 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.
- 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

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

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, [fn 2] and good business practices. By using GAPP, or-

[fn 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.

ganizations 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. *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,	**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

	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.	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.
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 sched-	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

	ules 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.	• Updated privacy compliant forms, brochures, and contracts • Internal and external privacy awareness programs
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.	
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	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 communicat-	Privacy policies (as used herein) include security policies relevant to the protection of personal information.

	communicated to such personnel shortly after the changes are approved.	ed 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.	
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 • 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	The individual identified as being accountable for privacy should be from within the entity.

		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 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.	Corporate counsel or the legal department • determines which privacy laws and regulations are applicable in the jurisdictions in which the entity operates. • 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.	In addition to legal and regulatory requirements, some entities may elect to comply with certain standards, such as those published by International 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	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:	

	policies and procedures.	— 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	
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 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 following are used for addressing privacy impact:

- Management assesses the privacy impact of new and significantly changed products, services, business processes, and infrastructure.
- 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.

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.

- 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, 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 pri-

		vacy. Specific roles and responsibilities are assigned related to privacy.	
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 in-	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 re-	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.

ternal 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

quired by law, regulation, or policy, and (*c*) a process 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:

		— 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) • Hiring procedures (including the comprehen-

			sive 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. • 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 re-

		flect 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.

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 pri-

The privacy notice is

- readily accessible and available when personal information is first collected from the individual.
- provided in a timely man-

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).

vacy policies and procedures, or as soon as practical thereafter, or (*c*) before personal information is used for new purposes not previously identified.

ner (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.

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.

- 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)

3.2 Procedures and Controls

3.2.1 **Implicit or Explicit Consent**

Implicit or explicit consent is obtained from the individual at

The entity

- obtains and documents an individual's consent in a

		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.	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.
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. 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.	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.

		Entities will not download software that will transfer personal information without obtaining permission.	

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.
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	Some jurisdictions, such as those in the EU, require that individuals have the opportunity to decline the use of cookies.

		• 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.	
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**	The entity's management, privacy officer, and legal counsel, review the methods of collection and any	The following may be considered deceptive practices:

	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.	changes thereto.	• 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 • 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	Contracts include provisions requiring personal information to be collected fairly and lawfully and from reliable sources.

		from third-party data 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.	

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 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 ac-	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 none-

		cordance 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.	lectronic 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.
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 regula-	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.

		tions. Contractual requirements are considered when establishing disposal, destruction, and redaction practices if they may result in exception to the entity's normal policies.	

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**	Procedures are in place to	Some laws and regulations specify the following:

	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.	• 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. • 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.	• Provisions and requirements for providing access to personal information (for example, HIPAA) • Requirements that requests for access to personal information be submitted in writing
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.	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

		• 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.	
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	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.

		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.	
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.	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.

		• 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.	
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. • 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.	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.
6.2.6	**Statement of Disagreement**	If an individual and an entity dis-	See 10.1.1, "Communications to

Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.	agree 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.	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.	
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	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

		a designated privacy executive, such as a corporate privacy officer. • 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 on-site evaluation of the third party. • The entity receives an audit or similar report provided by an independent auditor.	to transfer. 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 en-	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 reg-

		tity 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.	ulatory agencies. • in another country and may be subject to other requirements.
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).	

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.
8.2	**Procedures and Controls**		
8.2.1	**Information Security Pro-**	The entity's security program	Safeguards employed may con-

gram

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[fn 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]

g. Communications and operations management [sections 1, 7, and 10]

h. Access control [sections 1, 8.2, and 10]

i. Information systems acquisition, development, 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
- Assignment of responsibility and accountability

sider 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
  - — exercising appropriate due diligence in the selection of service providers.
  - — requiring service providers by con-

[fn 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.

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]	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	tract 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.	

		addressed in its system processing integrity and related system security policies • 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).	
8.2.2	**Logical Access Controls** Logical access to personal in-	Systems and procedures are in place to	User authorization processes consider the following:

formation 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, mali-

- 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.

- 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.

	cious 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.
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 sup-	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.

		pression system. In addition, the entity maintains physical and other safeguards to prevent accidental disclosure of personal information in the event of an environmental incident.	
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.
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 per-	Consideration should be given to the protection needed for any personal information provided to, for example, regulators and auditors.

		sonal 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.	
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 in-	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

formation.

- 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.

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).
- indicate how to verify the accuracy and completeness of personal information obtained directly from an individual, re-

			ceived 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 re-	

		solving complaints about the entity. • action that will be taken with respect to the disputed information until the complaint is satisfactorily resolved. • 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 com-	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.

		plaints and disputes for review by management. • identify trends and the potential need to change the entity's privacy policies and procedures. • 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,	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.

			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).
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.	
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. On-	*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.

going monitoring activities would include a review of human resource files of selected employees to determine that they contain the appropriate evidence of course completion.

- 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 con-

sistency 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. [fn 1] [fn 2]

- 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:

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

[fn 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 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. [fn 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. [fn 4] When the practitioner reports on the subject matter, the practitioner may want 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

---

[fn 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.

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

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, [fn 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. [fn 6] In this type of engagement, the practitioner's report is in

---

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

[fn 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 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.

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* [fn 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.

Appendix C — Illustrative Privacy Examination and Audit Reports

[fn 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.

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*]