2003

AICPA/CICA Privacy Framework, Including the AICPA/CICA Trust Services Privacy Principle and Criteria, November 15, 2003

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

AICPA/CICA Privacy Framework

Including the AICPA/CICA Trust Services

Privacy Principle and Criteria

November 15, 2003

Issued by the Assurance Services Executive Committee of the AICPA and the

Assurance Services Development Board of the CICA

AICPA/CICA Committees

AICPA Assurance Services Executive Committee

Thomas E. Wallace, *Chair*
Richard Dull
John Lainhart
Thomas Siders
Raymond Vicks, Jr.
Neal West

Staff Contacts:

Anthony J. Pugliese
Vice President, Member Innovation

J. Louis Matherne
Director, Business Assurance and Advisory Services

CICA Assurance Services Development Board

Doug McPhie, *Chair*
Marilyn Kuntz
Doug Timmins

Staff Contacts:

Cairine M. Wilson
Vice President, Member Services

Gregory P. Shields
Director, Assurance Services Development

AICPA/CICA Enterprise Wide Privacy Task Force

Everett C. Johnson, *Chair*
Kenneth Askelson, *Vice Chair*
Mitch Baxter
Mary Grace Davenport
Eric Federing
Linda Garvelink
Marilyn Greenstein
Don Hansen
Philip M. Juravel
Howard Mosbacher
Robert Parker
Doron Rotman
Paul E. Roy
Kerry Shackelford
Bob Shriver
Brian Tretick
Lee Zeichner

Staff Contact:

Bryan Walker, CICA
Principal
Karyn Waller, AICPA
Senior Technical Manager, Trust Services

Table of Contents

AICPA/CICA Privacy Framework

Introduction

Privacy is a risk management issue. Many organizations are looking for assistance in managing privacy risk and certified public accountants/chartered accountants (CPAs/CAs)[1] are actively helping businesses develop and implement privacy programs. The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) jointly established an Enterprise-Wide Privacy Task Force comprising a cross section of the accounting profession, including industry, large multinational firms, and small CPA/CA firms, as well as members in academia and the legal profession. Its mission is to examine the role CPAs/CAs can play in advising organizations about privacy issues and risks, and to develop a privacy framework that will serve as a benchmark for good privacy practices.

In this document, the AICPA and the CICA are introducing the AICPA/CICA Privacy Framework (the Framework) for protecting personal information.[2] It can be used by all CPAs/CAs (both in industry and in public practice) to guide and assist the organizations they serve in implementing privacy programs. The Framework incorporates concepts from significant domestic and international privacy laws, regulations, and guidelines (see Attachment D, "Comparison of International Privacy Concepts").[3] The Framework is the intellectual capital and body of knowledge that provides the foundation for CPA/CA-related privacy advisory and assurance services.

Research shows that many CPAs/CAs possess the skills necessary to implement effective privacy practices in any organization—no matter how big or small. They understand business processes, how personal information flows within an organization, and how to design privacy programs. Through a wide range of advisory and assurance services, CPAs/CAs have an opportunity to help businesses navigate the patchwork of privacy laws, regulations, and guidelines, and focus on the heart of the

---

1 The term *CPA/CA*, as used in this document, refers to a certified public accountant in the United States of America, a chartered accountant in Canada, or their equivalent in other countries, whether in public practice, private industry, government, or education. The term *practitioner* refers only to those CPAs/CAs who are in public practice.

2 The Framework and privacy-related publications are available on the AICPA and the CICA Privacy Resource Centers (see Attachment C, "Additonal Sources of Privacy-Related Information," of this document for the URLs). The publications include the booklet, *20 Questions Businesses Need to Ask About Privacy,* and the primer, *Privacy Matters: An Introduction to Personal Information Protection*. In addition, to support CPA/CAs in the delivery of privacy engagements as well as to aid them in the education of the subject matter of privacy, a privacy resource guide is available.

3 For example, the Organisation for Economic Co-operation and Development (OECD) has issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the Guidelines) and the European Union (EU) has issued Directive on Data Privacy (Directive 95/46/EC). In addition, the United States has enacted the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA). Canada has enacted the Personal Information Protection and Electronic Documents Act (PIPEDA) and Australia has enacted the Australian Privacy Act of 1988, as amended in 2001. Web site URLs for these and other privacy laws and regulations are set out in Appendix C. Compliance with the Framework criteria may not necessarily result in compliance with applicable privacy laws and regulations and entities may wish to seek appropriate legal advice regarding compliance with any laws and regulations.

matter—building trust between customers and businesses and "doing the right thing" by following good privacy practices.

CPAs/CAs in public practice will be able to offer clients a full range of services, including privacy strategic and business planning, privacy gap and risk analysis, benchmarking, privacy policy design and implementation, performance measurement, and independent verification of privacy controls, which includes attestation engagements. CPAs/CAs in industry can enhance their value to their employers by offering privacy advisory services and performing internal assessments against something they can measure—the Framework.

Online Privacy has been part of the AICPA/CICA Trust Services, which also include a core set of Principles and Criteria covering Security, Processing Integrity, Availability, and Confidentiality. The Framework criteria replace the existing Trust Services Online Privacy Principle and Criteria and will become known as the AICPA/CICA Trust Services Privacy Principle and Criteria. The Criteria have been broadened to include additional business segments and processes relating to privacy. To perform an online privacy Trust Services assurance engagement using the Framework, the entity would describe the online business segment or process in its privacy notice (see Criterion 2.2.2) and the practitioner would apply the Framework Criteria to the business segment or process that he or she is engaged to evaluate. (See Attachment E, "Transition From AICPA/CICA Trust Services Online Privacy Principle and Criteria to Transition Guidance," for additional information.)

What Is Privacy?

Privacy is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.

Personal Information

Personal information is information that is, or can be, about or 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. 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:

- Name
- Home or e-mail address
- Identification number (e.g., Social Security or Social Insurance Numbers)
- 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, sensitive information may require explicit consent rather than implicit consent.

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 "de-identified" or "anonymized." Nonpersonal information ordinarily is not subject to privacy protection because it can not be linked to an individual.

Rights and Obligations

An effective privacy program requires that organizations and individuals know and assume their rights and obligations that, in some cases, carry the force of law. The following table outlines some of these rights and obligations with respect to maintaining the privacy of personal information. Depending on the policies of the organization, specific agreements between the organization and the individual, regulations, standards, and laws, these aspects of privacy may be the right of the individual or organization, or its obligation to the other party.

	Individuals	Organizations
Rights and Obligations	• Be aware of the organization's privacy policies. • Provide accurate and appropriate information suited to the purpose for which the information is needed. • Notify the organization of inaccuracies in or changes to personal information used by the organization. • Adhere to applicable laws and regulations, and other agreements with the organization.	• Establish and communicate its privacy policies and commitments to the individual. • Provide choices or seek consent for the use of the personal information. • Collect, use, retain, and disclose personal information according to its privacy policies and commitments. • Allow the individual to update or correct personal information that is used by the organization. • Protect the personal information from unauthorized use and disclosure. • Otherwise adhere to its policies, applicable laws and regulations, and other agreements with the individual.

Privacy, Confidentiality, and Security

Privacy is about individuals having control over the collection, use, and disclosure of their personal information. Unlike privacy, there is not a widely accepted definition of confidentiality[4] but, in most cases, it is about keeping business information from being disclosed to unauthorized parties. Confidentiality is usually driven by agreements or contractual arrangements. Security is one of the 10 components of the Framework. The criteria for the security component of privacy are substantially equivalent to the criteria for the Trust Services Security Principle.

Why Privacy Is a Business Issue

Good privacy is good business. Good privacy practices are a key part of corporate governance and accountability. One of today's key business imperatives is maintaining the privacy of personal information. As business systems and processes become increasingly complex and sophisticated, more and more personal information is being collected. As a result, personal information may be exposed to a variety of vulnerabilities, including loss, misuse, and unauthorized access and disclosure. Those vulnerabilities raise concerns for organizations, the government, and the public in general.

Organizations are trying to strike a balance between the proper collection and use of their customers' personal information. The government is trying to protect the public interest but, at the same time, manage its own cache of personal information gathered from citizens. Consumers are very concerned about their personal information and many believe they have lost control of it. With identity theft on the rise, and fears of financial or medical records being accessed inappropriately, there is a pressing need to protect personal information.
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, privacy is a risk management issue for *all* businesses. Specific risks of having inadequate privacy policies and procedures include:

- 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

Many CPAs/CAs are skilled at examining management information systems and identifying the controls needed to effectively manage risk. As trusted business advisers, they are adept at performing comprehensive risk assessments and developing advice on risk management. Many organizations are looking to CPAs/CAs for assistance in designing, implementing, maintaining, and evaluating their privacy program. In this respect, CPAs/CAs are in a unique position to provide privacy services to help organizations mitigate privacy-related risks, protect valuable business assets, preserve and enhance an organization's brand and reputation, and maintain and enhance customer loyalty and employee

[4] AICPA/CICA Trust Services provides a Confidentiality Principle and Criteria which may be helpful for addressing confidentiality.

relationships. The Framework provides a foundation for delivering value-added privacy services. Additional information is available in the resource centers listed in Attachment C.

Solutions to Privacy Issues

CPAs/CAs can provide organizations with strategic advice on privacy risk management, help them mitigate privacy risk, and turn privacy into a competitive advantage. They build on decades of experience in providing assurance on financial and nonfinancial information. The business and professional experience, subject matter expertise, and professional characteristics needed for such services are the same key elements that enable a CPA/CA to provide solutions to privacy issues. They are the right professionals to perform objective assessments of an organization's privacy program.

If an organization collects, uses, retains, and discloses personal information, the challenge is to enhance the trust relationships with consumers, customers, employees, and third parties, as well as to comply with privacy laws and regulations and good fair information practices. A CPA/CA can help an organization address privacy issues by:

- Developing a privacy strategy and plan.
- Providing privacy advice, recommendations, and training relating to one or more of the privacy components.
- Preparing or evaluating privacy policies and procedures.
- Assessing and managing privacy risk.
- Implementing a privacy program.
- Providing assurance on whether the 10 privacy components (as measured by the criteria set out in the Framework) are met.

AICPA/CICA Privacy Framework

AICPA/CICA Trust Services Privacy Principle

Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with the AICPA/CICA Trust Services Privacy Criteria.

AICPA/CICA Trust Services Privacy Components and Criteria

The Framework contains 10 privacy components[5] and related criteria that are essential to the proper protection and management of personal information. These privacy components and criteria 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 privacy components:

5 Although some privacy regulations use the term *principle,* the term *component* is used in the Framework to represent that concept since the term principle has been previously defined in the Trust Services literature.

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 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.
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. 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 components, there are relevant, objective, complete, and measurable criteria for evaluating an entity's privacy policies, communications, and procedures and controls. *Privacy policies* are written statements that convey management's intent, objectives, requirements, responsibilities, and/or 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.

Framework Presentation

The Framework is presented in a three-column format. The first column contains the Trust Services Privacy criteria.[6] The second column, which contains illustrations and explanations, is designed to enhance the understanding of the criteria. The illustrations are not intended to be comprehensive, nor are any of the illustrations required for an entity to have met the Trust Services Privacy criteria. The third column contains additional considerations, including supplemental information such as good privacy practices and selected requirements of specific laws and regulations that pertain to a certain industry or country.

---

[6] These criteria meet the definition of "criteria established by a recognized body" described in the third general standard for attestation engagements in the United States in Chapter 1 of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Engagements: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101.24), as amended, and in the standards for assurance engagements in Canada (*CICA Handbook*, paragraph 5025.41).

The criteria identified in the 10 privacy components provide a basis for designing, implementing, maintaining, and evaluating a privacy program in order to meet an entity's needs by CPAs/CAs in public practice, industry, government, and education.

Practitioner Use of the Framework for Providing Advisory Services

Practitioners can provide a variety of advisory services to their clients, which include strategic, diagnostic, implementation, and sustaining/managing services using the Framework principle, components, and criteria. It could include, for example, advising clients on system weaknesses, assessing risk, and recommending a course of action using the Framework criteria as a benchmark.

Practitioners in the United States providing such advisory services follow Statement on Standards for Consulting Services, *Consulting Services: Definition and Standards* (AICPA, *Professional Standards*, vol. 2, CS sec. 100). Canadian practitioners are not required to comply with any specific set of standards with respect to advisory service engagements but, as noted above, are expected to meet the standards set out in Sections 5000–5900 of the CICA Handbook.

Practitioner Use of the Framework for Providing Attestation or Assurance Services

Practitioners also can use the criteria to perform an examination of an organization's privacy under Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Engagements: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended, or the *CICA Handbook—Assurance,* Section 5025, "Standards for Assurance Engagements." In addition, the practitioner guidance included in the AICPA/CICA Trust Services Criteria is applicable to these types of engagements.[7] The following key concepts apply to privacy assurance engagements:

- A privacy assurance report ordinarily covers all 10 privacy components and all of the relevant criteria in all 10 privacy components need to be met during the period covered by the report to issue an unqualified report.[8,9]
- The work should be performed at the highest level of assurance, i.e., the "examination" or equivalent level.
- 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 Web site) or geographic locations (such as only Canadian operations). In addition:
    - The scope of the engagement generally should be consistent with the description of the entities and activities covered in the privacy notice (see Criterion 2.2.2 below). The scope often could be narrower, but ordinarily not broader, than that covered by the related privacy notice.

---

[7] Chapter 10, of the *AICPA/CICA Privacy Resource Guide* also includes guidance on performing privacy assurance engagements.

[8] See Attachment B, "Illustrative Reports."

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

- 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 and destruction, de-identification or anonymization. Defining a 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 information not in the scope of the engagement, the privacy assurance 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.

Trust Services Privacy Components and Criteria

Management

Reference	Criteria	Illustrations and Explanations of Criteria	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: • Notice (See 2.1.0) • Choice and Consent (See 3.1.0) • Collection (See 4.1.0) • Use and Retention (See 5.1.0) • Access (See 6.1.0) • Onward Transfer and Disclosure (See 7.1.0) • Security (See 8.1.0) • Quality (See 9.1.0) • 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	The entity: • Periodically communicates to internal personnel (for example, on a network or a Web site) relevant information about the entity's privacy policies and	Privacy policies encompass security policies relevant to the protection of personal information.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	changes to its privacy policies. • Requires internal personnel to confirm (initially and periodically) their understanding of an agreement to comply with the entity's privacy policies. • Educates and trains internal personnel (initially and periodically) who have access to personal information or are charged with the security of personal information about privacy awareness, concepts, and issues.	
1.1.2	**Responsibility and Accountability for Policies** Responsibility and accountability are assigned to a person or group for 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 authority and accountability of the designated person or group are clearly documented. Responsibilities include: • Establishing standards 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	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		• Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices The Board periodically includes privacy in its regular review of corporate governance. The entity requires users, management, and third parties to confirm (initially and annually) their understanding of and agreement to comply with the entity's privacy policies and procedures related to the security of personal information.	
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 there are changes to such laws and regulations. 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. • Reviews the entity's privacy policies and procedures to ensure they are consistent with the applicable laws and regulations.	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
1.2.3	**Consistency of Commitments With Privacy Policies and Procedures** Entity personnel or advisors review contracts for consistency with privacy policies and procedures and address any inconsistencies.	Management and the corporate counsel or the legal department review all contracts and service-level agreements for consistency with the entity's privacy policies and procedures.	
1.2.4	**Infrastructure and Systems Management** Entity personnel or advisors review the design, acquisition, implementation, configuration, and management of the infrastructure, systems, and procedures and changes thereto for consistency with the entity's privacy policies and procedures and address any inconsistencies.	Procedures are in place to: • Govern the development, acquisition, implementation, and maintenance of information systems and the related technology used to collect, use, retain, and disclose personal information. • Ensure that the entity's backup and disaster-recovery planning processes are consistent with its privacy policies and procedures. • Classify the sensitivity of classes of data, and determine the classes of users who should have access to each class of data. Users are assigned user-access profiles based on their need for access and their functional responsibilities as they relate to personal information. • Assess planned changes to systems and procedures for their potential effect on privacy. • Test changes to system components to minimize the risk of an adverse effect on the systems that process personal	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		information. All test data are anonymized. • Require the documentation and approval by the privacy officer and business unit manager before implementing the changes to systems and procedures that handle personal information, including those that may affect security. Emergency changes may be documented and approved on an after-the-fact basis. The Information Technology (IT) department maintains a listing of all software 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.	
1.2.5	**Supporting Resources** Resources are provided by the entity to implement and support its privacy policies.	Management reviews annually the assignment of personnel, budgets, and allocation of other resources to its privacy program.	
1.2.6	**Qualifications of 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: • Formal job descriptions (including responsibilities, educational and professional requirements and organizational reporting for key privacy management positions)	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		• Hiring procedures (including the comprehensive screening of credentials, background checks, and reference checking) • Training programs related to privacy and security matters • Performance appraisals (performed by supervisors, including assessments of professional development activities)	
1.2.7	**Changes in Business and Regulatory Environments** For each jurisdiction in which the entity operates, the effect on privacy of changes in the following factors is identified and addressed: • Business operations and processes • People • Technology • Legal • Contracts, including service-level agreements Privacy policies and procedures are updated for such changes.	The entity has an ongoing process in place to monitor, assess, and address the effect on privacy of changes in: • Business operations and processes • People assigned responsibility for privacy and security matters • Technology (prior to implementation) • Legal and regulatory environments • 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 corporate counsel before they are executed.)	

Notice

Reference	Criteria	Illustrations and Explanations of Criteria	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: • Purpose for collecting personal information • Choice and Consent (See 3.1.1) • Collection (See 4.1.1) • Use and Retention (See 5.1.1) • Access (See 6.1.1) • Onward Transfer and Disclosure (See 7.1.1) • Security (See 8.1.1) • Quality (See 9.1.1) • 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 purposes for which personal information is collected. • Indicates that the purpose for collecting sensitive personal information is part of a legal requirement. • May be provided in various ways (for example, in a face-to-face interview, a telephone interview, an application form or questionnaire, or electronically). Written notice is the preferred method.	Notice also may describe situations in which personal information will be disclosed, such as: • 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**	Privacy notice is:	Some regulatory requirements indicate

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	Notice is provided to the individual about the entity's privacy policies and procedures: • At or before the time personal information is collected, or as soon as practical thereafter. • At or before the entity changes its privacy policies and procedures, or as soon as practical thereafter • Before personal information is used for new purposes not previously identified (See 3.2.2, "Consent for New Purposes and Uses.")	• Readily accessible and available when personal information is first collected from the individual. • Provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal information to the entity. • Clearly dated to allow individuals to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. In addition, the entity: • Tracks previous iterations of the entity's privacy policies and procedures. • Informs individuals of a change to a previously communicated privacy notice, for example, by posting the notification on the entity's Web site, by sending written notice via the mail, or by sending an e-mail. • Documents that changes to privacy policies and procedures were communicated to individuals.	that a privacy notice is to be provided on a periodic basis, for example, annually in the Gramm-Leach-Bliley Act (GLBA).

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
2.2.2	**Entities and Activities Covered** An objective description of the entities and activities covered by the privacy policies and procedures is included in the entity's privacy notice.	The privacy notice describes the particular entities, business segments, locations, and types of information covered, for example: • 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 leave the Web site and are no longer covered by the entity's privacy policies and procedures.	
2.2.3	**Clear and Conspicuous** Clear and conspicuous language is used in the entity's privacy notice.	The privacy notice is: • In plain and simple language. • Appropriately labeled, easy to see, and not in fine print. • Linked to or displayed on the Web site at points of data collection.	If multiple notices are used for different subsidiaries or segments of an entity, similar formats should be encouraged to avoid consumer confusion and clarify their understanding of any differences. Some regulations, such as GLBA, may contain specific information that a disclosure must contain. Illustrative notices are often available for

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
			certain industries and types of collection, use, retention, and disclosure.

Choice and Consent

Reference	Criteria	Illustrations and Explanations of Criteria	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 the choices available to them with respect to the collection, use, and disclosure of personal information. • That implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise.	The entity's privacy notice describes, in a clear and concise manner: • 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 consequences of failing to provide personal information Individuals are advised that: • Personal information not essential to the purposes identified in the privacy notice need not be provided. • Preferences may be changed and	Some laws and regulations (such as Principle 11, Limits on the 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 recordkeeper 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.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		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.	The entity informs individuals at the time of collection: • 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 or before the time personal information is collected or as	The entity: • Obtains and documents an individual's consent in a timely manner (that is, at or before the time	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	soon as practical thereafter. The individual's preferences expressed in his or her consent are confirmed and implemented.	personal information is collected, or as soon as practical thereafter). • 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. • Addresses conflicts in the records about an individual's 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.	If policies are changed but do not constitute new purposes or uses, the organization may wish to consult with legal counsel.
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	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	The 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.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	specifically requires otherwise. .	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.	Most jurisdictions referenced to in Attachment D, "Comparison of International Privacy Concepts," prohibit the collection of sensitive data, unless specifically allowed. For example, in the European Union (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 that "The collection and processing of sensitive data is forbidden." However, a permit to collect and process sensitive data may be obtained.
3.2.4	**Consent for Online Data Transfers to/from an Individual's Computer** Consent is obtained before personal information is transferred to/from an individual's computer.	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. The entity requests customer permission to store, alter, or copy personal information (other than cookies) in the customer's computer. Organizations will not download software that will transfer personal information without obtaining permission.	Consideration should be given to software that is designed to mine or extract information from a computer and therefore may be used to extract personal information, e.g., spyware.

Collection

Reference	Criteria	Illustrations and Explanations of Criteria	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 and the methods used to collect personal information.	
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.	Examples of the types of personal information collected are: • Financial (for example, financial account information) • Health (for example, information about physical or mental status or history) • Demographic (for example, age, income range, social geo-codes). Examples of methods of collecting and third-party sources of personal information are: • Credit reporting agencies • Over the telephone • Via the Internet using forms, cookies, or Web beacons The entity's privacy notice discloses that it uses cookies and Web beacons and how they are used. The notice also describes	Some jurisdictions, such as those in the EU, require that individuals have the opportunity to decline the use of cookies.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		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 there are changes to the program or service). • Obtain explicit consent when sensitive personal information is collected (see 3.2.3, "Explicit Consent for Sensitive Information.") • Monitor that the collection of personal information is limited to that necessary for the purposes identified in the privacy notice and that all optional data is identified as such.	
4.2.2	**Collection by Fair and Lawful Means** Methods of collecting personal information are reviewed by management, legal counsel, or both before they are implemented to confirm that personal information is obtained: • Fairly, without intimidation or deception, and • Lawfully, adhering to all relevant rules of law, whether derived from statute or common law,	The entity's legal counsel reviews the methods of collection and any changes thereto.	It may be considered a deceptive practice: • To use tools, such as cookies and Web beacons, on the entity's Web site to collect personal information without providing notice to the individual. • To link information collected during an individual's visit to a Web site with personal information from other sources without providing notice to the individual. • To use a third party to collect

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	relating to the collection of personal information		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 there are unfair or unlawful practices. .
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 and collection methods of third parties before accepting personal information from third-party data sources.	Contracts include provisions requiring personal information to be collected fairly and lawfully and from reliable sources. If information collected from third parties is to be combined with information collected from the individual, consideration should be given to providing notice to such individuals.

Use and Retention

Reference	Criteria	Illustrations and Explanations of Criteria	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.**		

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
5.1	**Policies and Communications**		
5.1.0	**Privacy Policies** The entity's privacy policies address the use and retention of personal information.		
5.1.1	**Communication to Individuals** Individuals are informed that 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. • Retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation.	The entity's privacy notice describes the 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 Web sites 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.	
5.2	**Procedures and Controls**		
5.2.1	**Use of Personal Information** Personal information is used only for the	Systems and procedures are in place to monitor the use of personal information to	Some regulations have specific provisions concerning the use of personal

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.	ensure: • Use in conformity with the purposes identified in the entity's privacy notice. • Use in agreement with the consent received from the individual • Compliance with applicable laws and regulations	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. Personal information no longer retained is disposed and destroyed of in a manner that prevents loss, misuse, or unauthorized access.	The entity: • Documents its retention policies and disposal procedures. • Erases or destroy records in accordance with the retention policies, regardless of the method of storage (for example, electronic or paper-based). • Retains, stores, and disposes of archived and backup copies of records in accordance with its retention policies. • Ensures that personal information is not kept beyond the standard retention time unless there is a justified business reason for doing so. • Locates and removes 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	Some laws specify the retention period for personal information; for example, HIPAA has a six-year retention period from the date of creation or last in effect for personal information. There may be other statutory record retention requirements; for example, certain data may need to be retained for tax purposes or in accordance with employment laws.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		fulfill the identified purposes or required by laws and regulations. Contractual requirements should be considered when establishing retention practices.	

Access

Reference	Criteria	Illustrations and Explanations of Criteria	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 Web site).	
6.2	**Procedures and Controls**		
6.2.1	**Access by Individuals to Their**	Procedures are in place to:	Some laws and regulations specify:

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	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, 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: • Access to their personal information • Requests to change sensitive or other personal information (for example, to update information such as address or bank details). The entity: • Does not use government-issued identifiers (for example, Social Security numbers or Social Insurance numbers) for authentication. • Mails information about a change request only to the address of record or, in the case of a change of address,	The extent of authentication considers the type and sensitivity of personal information that is made available. Different techniques may be considered for the different channels: • Web • Interactive voice response system • Call center • In person

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		to both the old and new addresses. • Requires that a user identification (ID) 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 time frame, 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 time frame that is similar to the entity's normal response times for other business transactions, or as permitted or required by law. • Provides access to personal information in archived or backup systems and media. • Informs individuals of the cost of	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		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, that 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 as to why access to personal information is denied. • Provides a formal escalation and review process if access to personal information is denied. (See 6.2.7, "Escalation of Complaints and Disputes.") • Conveys the entity's legal rights and the individual's right to challenge, if applicable.	Some laws and regulations (for example, Principle 5, "Information Relating to Records Kept by Record-Keeper," point 2 of the Australian Privacy Act of 1988) cover situations in which the individual cannot review the reasons for denial of access.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
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 Web site). • 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** Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.	If an individual and an entity disagree about whether personal information is complete and accurate, the individual may ask the entity to accept a statement claiming that the personal information is not complete and accurate. The entity: • Documents instances where an	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

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		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.	having access to the information in question.
6.2.7	**Escalation of Complaints and Disputes** Complaints and other disputes are escalated until they are resolved.	The entity has established a formal escalation process to address complaints and disputes that are not resolved. The entity: • Trains employees responsible for handling individuals' complaints and disputes about the escalation process. • Documents unresolved complaints and disputes. • Escalates complaints and disputes for review by management. • Resolves complaints and disputes on a	Some laws (for example, PIPEDA) permit escalation through the court system up to the most senior court.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		timely basis. • Engages an external, third-party dispute resolution service (for example, an arbitrator), when appropriate, to assist in the resolution of complaints and disputes.	

Disclosure to Third Parties

Reference	Criteria	Illustrations and Explanations of Criteria	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. Disclosure includes any limitation on the third party's privacy practices and controls. Lack of such disclosure indicates that the third party's privacy practices and	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 (1) identified in the notice and (2) for	The entity's privacy notice may disclose: • 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.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	controls meet or exceed those of the entity.	which the individual has provided implicit or explicit consent, or as specifically allowed or required by law or regulation. Individuals are informed if third parties provide lower levels of protection.	
7.1.2	**Communication to Third Parties** Privacy policies 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 to and obtains a written agreement from the third party that its practices are substantially equivalent to the entity's.	
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 allows or requires 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 while 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	Systems and procedures are in place to: • Provide a level of protection of personal information equivalent to that of the entity when information is	The entity is responsible for personal information in its possession or custody, including information that has been transferred to a third party.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	from loss, misuse, unauthorized access, disclosure, alteration, and destruction.	provided to a third party (that is, by contract or agreement). • Affirm that the level of protection of personal information by third parties is equivalent to that of the entity, for example, by obtaining assurance (for example, an auditor's report), contractual obligation, or other representation (for example, written annual confirmation). • Limit the third party's use of personal information to purposes necessary to fulfill the contract. • Communicate the individual's preferences to the third party. • Refer any requests for access or complaints about the personal information transferred by the entity to the privacy officer. • Specify how and when third parties are to dispose of or return any personal information provided by the entity.	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. The EU requires substantially equivalent privacy protection before transferring personal information to a third party. Some jurisdictions, including some countries in Europe, require entities that transfer personal information to register with their regulatory body prior to transfer. PIPEDA requires a comparable level of protection while the personal information is being processed by a third party. Article 25 of the U.S./EU's Safe Harbor requires that such transfers take place only where the third party ensures an adequate level of protection.
7.2.3	**New Purposes and Uses** Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.	Systems and procedures are in place to: • Notify individuals and obtain their consent prior to disclosing personal information to a third party for purposes not identified in the privacy notice. • Document whether the entity has	Other types of onward transfers include transfers to third parties who are: • Subsidiaries or affiliates. • Providing a service requested by the individual. • Law enforcement or regulatory agencies.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		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.	• 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: • Monitors 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. • Takes remedial action in the event that a third party misuses personal information. (For example, contractual clauses address the ramification of misuse of personal information.)	

Security

Reference	Criteria	Illustrations and Explanations of Criteria	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 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. • Special 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.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
8.2	**Procedures and Controls**		
8.2.1	**Information Security Program** A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.	The entity's security program addresses the following matters related to protection of personal information: *a.* Periodic risk assessments *b.* Identification and documentation of the security requirements of authorized users *c.* Allowing access, the nature of that access, and who authorizes such access *d.* Preventing unauthorized access by using effective physical and logical access controls *e.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access *f.* Assignment of responsibility and accountability for security *g.* Assignment of responsibility and accountability for system changes and maintenance *h.* Implementing system software upgrades and patches *i.* Testing, evaluating, and authorizing system components before implementation *j.* Addressing how complaints and requests relating to security issues are	Safeguards employed may consider the nature and sensitivity of the data, as well as the size and complexity of the entity's operations. For example, the entity may protect personal information and other sensitive information to a level greater than it applies for other information. Some regulations (for example, HIPAA) provide a greater level of detail and guidance on specific security measures to be considered and implemented. Some security rules (for example, GLBA-related rules for safeguarding information) require: • 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 contract to implement and maintain appropriate safeguards for the

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		resolved *k.* Handling errors and omissions, security breaches, and other incidents *l.* Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing) *m.* Allocating training and other resources to support its security policies *n.* Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies *o.* Disaster recovery plans and related testing *p.* Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts *q.* A requirement that users, management, and third parties confirm (initially and annually) their understanding of and agreement to comply with the entity's privacy policies and procedures related to the security of personal information The entity's security program prevents access to personal information in computers, media and paper-based	personal information at issue. Some security laws (for example, California SB1386) require entities to notify individuals if the protection of their personal information is compromised.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		information that are no longer in active use by the organization (e.g. computers, media and paper-based information in storage, sold or otherwise disposed of).	
8.2.2	**Logical Access Controls** Logical access to personal information is restricted by procedures that address the following matters: *a.* Authorizing and registering internal personnel and individuals *b.* Identifying and authenticating internal personnel and individuals *c.* Making changes and updating access profiles *d.* Granting system access privileges and permissions *e.* Preventing individuals from accessing other than their own personal or sensitive information *f.* Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities *g.* Distributing output only to authorized internal personnel *h.* Restricting logical access to offline storage, backup data, systems, and media	Systems and procedures are in place to: • Establish the level and nature of access that will be provided to users based on the sensitivity of the data and the user's legitimate business need to access the personal information. • Authenticate users, for example, by user name and password, certificate, external token, or biometrics. • Require the user to provide a valid ID and password to be authenticated by the system before access is granted to systems handling personal information. • Require enhanced security measures for remote access, such as additional or dynamic passwords, dial-back controls, digital certificates, or secure ID cards, virtual private network (VPN), properly configured firewalls. • Implement intrusion detection and monitoring systems.	User authorization processes consider: • 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.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls) *j.* Preventing the introduction of viruses, malicious code, and unauthorized software		
8.2.3	**Physical Access Controls** Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).	Systems and procedures are in place to: • Manage logical and physical access to personal information, including hard copy, archival, and backup copies. • Log and monitor access to personal information. • Prevent the unauthorized or accidental destruction or loss of personal information. • Investigate breaches and attempts to gain unauthorized access. • 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 unlawful destruction, accidental loss, 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	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		using both smoke detectors and a fire suppression system. Water detectors are installed within the raised floor areas. The entity site is protected against a disruption in power supply to the processing environment by both uninterruptible power supplies and emergency power supplies. This equipment is tested semiannually.	
8.2.5	**Transmitted Personal Information** Personal information is protected when transmitted by mail and over the Internet and public networks by deploying industry standard encryption technology for transferring and receiving personal information.	Systems and procedures are in place to: • Address the confidentiality of information and communication, and the appropriate protection of personal information transmitted over the Internet or other public networks. • Define minimum levels of encryption and controls. • Employ industry standard encryption technology, for example, 128 bit secure socket layer (SSL), for transferring and receiving personal information. • Approve external network connections. • Protect personal information sent by mail, courier, or other physical means.	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 SSL encryption, including user IDs and passwords).
8.2.6	**Testing Security Safeguards** Tests of the effectiveness of the key administrative, technical, and physical	Systems and procedures are in place to: • Regularly test the effectiveness of the key administrative, technical, and	The frequency and nature of the testing of security safeguards will vary with the entity's size and complexity, the nature

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	safeguards protecting personal information are conducted at least annually.	physical safeguards protecting personal information. • Periodically undertake independent audits of security controls using either internal or external auditors. • Test card access systems and other physical security devices at least annually. • Document and test disaster recovery and contingency plans at least annually to ensure their viability. • Periodically undertake threat and vulnerability testing, including security penetration reviews 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.	and scope of its activities, and the sensitivity of personal information. Some security regulations (for example, GLBA-related rules for safeguarding information) require an entity to: • Conduct regular tests of key controls, systems, and procedures by independent third parties or by staff independent of those that develop or maintain security (or at least have these independent parties review results of testing). • Assess and possibly adjust its information security at least annually.

Quality

Reference	Criteria	Illustrations and Explanations of Criteria	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 the extent to which personal information is kept accurate and complete depends on the use of the information.	
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 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	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Consideration
		information obtained directly from an individual, received from a third party (see 4.2.3, "Collection From Third Parties"), or disclosed to a third party (see 7.2.2, "Protection of Personal Information"). • Ensure personal information used on an ongoing basis is sufficiently accurate and complete to make decisions, unless there are clear limits to 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.	
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	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Consideration
		minimize the use of inappropriate data for decision making.	

Monitoring and Enforcement

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
10.0	**The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related 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 complaints.	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 Web site 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	**Complaint Process** A process is in place to address complaints.	The corporate privacy officer or other designated individual is authorized to address privacy-related complaints, disputes, and other problems.	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		Systems and procedures are in place that set out: • Procedures to be followed in communicating and resolving complaints about the entity • Action that will be taken with respect to the disputed information until the complaint is satisfactorily resolved • Remedies available in case of a breach of personal information and how to communicate this information to an individual • Recourse available and formal escalation process 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** Every complaint is addressed and the resolution is documented and communicated to the individual.	The entity has a formally documented process in place to: • Record and respond to all complaints in a timely manner. • Periodically review unresolved disputes and complaints to ensure they are resolved in a timely manner. • Identify trends and the potential need to change the entity's privacy policies and procedures. • Address complaints that cannot be resolved.	Some regulations (for example HIPAA and COPPA) have specific procedures and requirements.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		• Use specified independent third-party dispute resolution services or other process 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, the entity's privacy policies and procedures are enforced.	Systems and procedures are in place to: • Annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts. • Document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign-off, are maintained. • Report the results of the compliance review and recommendations for improvement to management, and implement a remediation plan. • Monitor the resolution of issues and vulnerabilities noted in the compliance review to ensure that appropriate corrective action is taken	

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		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 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. • Identify trends that may require revisions to privacy policies and procedures.	

Attachment A

Glossary

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

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 either orally or in writing, is unequivocal and does not require any inference on the part of the entity seeking consent. Implied consent may reasonably be inferred from the action or inaction of the individual.

Cookies. Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. This information can then be used to identify the user when returning to the Web site, 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.

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 out. There is implied consent for the entity to collect, use, retain, and disclose personal information unless the individual explicitly denies permission.

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

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

Policy. A written statement that communicates management’s intent, objectives, requirements, responsibilities, and/or standards.

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

Privacy Program. The policies, communications, procedures, and controls in place to manage and protect personal information in accordance with the AICPA/CICA Trust Services Privacy Principle, Components and Criteria in the AICPA/CICA Privacy Framework.

Purpose. The reason why personal information is collected by the entity.

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, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

System. A system consists of five key components organized to achieve a specified objective. The five components are categorized as infrastructure (facilities, equipment, and networks); software (systems, applications, and utilities); people (developers, operators, users, and managers); procedures (automated and manual); and data (transaction streams, files, databases, and tables).

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. The Web beacon may be controlled by the organization that is responsible for the Web site being visited, or by another party that has been given permission to place the Web beacon on the site. Primarily, they are used in conjunction with cookies to transmit data online. When third parties use Web beacons, users have no knowledge that their personal information is being collected. Furthermore, third parties are not legally required to abide by the privacy policy set by the original Web site.

Attachment B

Illustrative Reports

Illustration 1--Reporting Directly on the Subject Matter Under A.I.C.P.A. 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, and disclosed based on its commitments in the privacy notice and on the AICPA/CICA Trust Services Privacy Criteria, and (2) ABC Company's compliance with its commitments in the privacy notice related to the Business during the period Xxxx xx, 2003 through Yyyy yy, 2003. ABC Company's management is responsible for maintaining the effectiveness of these controls and for compliance with its commitments in the 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 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 the Company's commitments in the 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, 2003 through Yyyy yy, 2003, 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, and disclosed based on its commitments in the privacy notice and on the AICPA/CICA Trust Services Privacy Criteria; and (2) complied with its commitments in the privacy notice.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

Illustration 2—Reporting on Management's Assertion Under A.I.C.P.A. 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, 2003 through Yyyy yy, 2003, 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, and disclosed based on its commitments in the privacy notice related to the Business and on the AICPA/CICA Trust Services Privacy Criteria, and
- Complied with its commitments in the privacy notice.

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 the Company's commitments in the 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, 2003 through Yyyy yy, 2003, ABC Company:

- Maintained effective controls over privacy of personal information collected in the Business to provide reasonable assurance that the personal information was collected, used, retained and disclosed based on its commitments in the privacy notice and on the AICPA/CICA Trust Services Privacy Criteria; and
- Complied with its commitments in the privacy notice,

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, based on ABC Company's privacy notice and on the AICPA/CICA Trust Services Privacy Criteria.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

Illustrative Management Assertion

During the period Xxxx xx, 2003 through Yyyy yy, 2003, 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 and disclosed based on our commitments in the privacy notice related to the Business and on the AICPA/CICA Trust Services Privacy Criteria, and
- Complied with our commitments in the privacy notice.

Illustration 3--Reporting Directly on the Subject Matter Under CICA Assurance Standards

Auditor's Privacy Report

To the Management of ABC Company, Ltd.:

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, and disclosed in accordance with its commitments in the privacy notice and with the AICPA/CICA Trust Services Privacy Criteria, and (2) ABC Company's compliance with its commitments in the privacy notice related to the Business during the period Xxxx xx, 2003 through Yyyy yy, 2003. ABC Company's management is responsible for maintaining the effectiveness of these controls and for compliance with its commitments in the 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 Canadian Institute of Chartered Accountants (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 the Company's commitments in the 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, 2003 through Yyyy yy, 2003, 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, and disclosed in accordance with its commitments in the privacy notice and with the AICPA/CICA Trust Services Privacy Criteria; and (2) complied with its commitments in the privacy notice.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

[*Name of CA firm*] [*City, Province*]
Chartered Accountants [*Date*]

Illustration 4--Reporting on Management's Assertion Under CICA Assurance Standards

Auditor's Privacy Report

To the Management of ABC Company, Ltd.:

We have audited ABC Company, Inc.'s (ABC Company) management assertion that, during the period Xxxx xx, 2003 through Yyyy yy, 2003, 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, and disclosed in accordance with its commitments in the privacy notice related to the Business and with the AICPA/CICA Trust Services Privacy Criteria, and

- Complied with its commitments in the privacy notice.

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 Canadian Institute of Chartered Accountants (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 the Company's commitments in the 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, 2003 through Yyyy yy, 2003, ABC Company:

- Maintained effective controls over privacy of personal information collected in the Business to provide reasonable assurance that the personal information was collected, used, retained and disclosed in accordance with its commitments in the privacy notice and with the AICPA/CICA Trust Services Privacy Criteria; and
- Complied with its commitments in the privacy notice,

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 accordance with ABC Company's privacy notice and the AICPA/CICA Trust Services Privacy Criteria.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

[*Name of CA firm*] [*City, Province*]
Chartered Accountants [*Date*]

Illustrative Management Assertion

During the period Xxxx xx, 2003 through Yyyy yy, 2003, 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 and disclosed in accordance with our commitments in the privacy notice related to the Business and with the AICPA/CICA Trust Services Privacy Criteria, and

- Complied with our commitments in the privacy notice.

Attachment C

Additional Sources of Privacy-Related Information

Privacy Resource Centers

- American Institute of Certified Public Accountants AICPA overview (www.aicpa.org/privacy) and resource center (www.cpa2biz.com/ResourceCenters/Information+Security/Privacy/default.htm)
- Canadian Institute of Chartered Accountants CICA (www.cica.ca/privacy)
- *WebTrust for Online Privacy* AICPA/CICA (www.aicpa.org/trustservices and www.cica.ca/webtrust)

Privacy Legislation and Regulations

- *Children's Online Privacy Protection Act* (COPPA) United States (www.ftc.gov/privacy), online privacy rule (www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm), and consumer guide (www.consumerprivacyguide.org/law)
- *Data Protection Act* United Kingdom (www.dataprotection.gov.uk)
- *Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* European Union (www.europa.eu.int/comm/internal_market/en/dataprot/law/index.htm)
- European Union (EU) Directive on Data Protection (95/46/EC) (http://www.dataprivacy.ie/6aii.htm)
- EU Directive on Privacy and Electronic Communications (2002/58/EC) (http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf
- *Freedom of Information Act* (FOIA) United States (www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm)
- *Gramm-Leach-Bliley Act* (GLBA) United States (www.ftc.gov/privacy)
- *Greece's Data Protection Law (Unofficial English Translation of Law 2472/1997 on the Protection of Individuals With Regard to the Processing of Personal Data)* (http://www.dpa.gr/legal_eng.htm)
- *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Organisation for Economic Co-operation and Development [OECD]) (www.oecd.org/EN/document/0,,EN-document-43-1-no-24-10255-43,00.html)
- *Health Insurance Portability and Accountability Act* (HIPAA) United States (http://aspe.os.dhhs.gov/admnsimp/pl104191.htm), resource centre (http://aspe.os.dhhs.gov/admnsimp/) and consumer guide (www.consumerprivacyguide.org/law)
- *Model Code for the Protection of Personal Information* (Canadian Standards Association, now CSA International, CAN/CSA-Q830-96) (www.csa.ca/standards/privacy/default.asp?load=code)
- *Personal Information Protection and Electronic Documents Act* (PIPEDA) Canada (www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html)
- *Privacy Act* United States (www.usdoj.gov/foia/privstat.htm) and consumer guide (www.consumerprivacyguide.org/law)
- *Privacy Act* Australia (www.austlii.edu.au/au/legis/cth/consol_act/pa1988108)
- *Privacy Act* New Zealand (www.privacy.org.nz/comply/comptop.html)
- Privacy International and the Electronic Privacy Information Center Annual review of privacy laws in over 50 countries around the world (www.privacyinternational.org/survey)

- Safe Harbor Privacy Principles United States (www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm) and overview (www.export.gov/safeharbor/sh_overview.html)
- Universal Declaration of Human Rights United Nations General Assembly (www.unhchr.ch/udhr/index.htm)

Privacy Commissioners

- Australia Privacy Commissioner (www.privacy.gov.au)
- Canada Privacy Commissioner (www.privcom.gc.ca)
- European Union National Data Protection Commissioners (http://europa.eu.int/comm/internal_market/en/dataprot/links.htm)
- Federal Trade Commission United States (www.ftc.gov/privacy/index.html)
- New Zealand Privacy Commissioner (www.privacy.org.nz)
- Ontario Information and Privacy Commissioner (www.ipc.on.ca)
- United Kingdom Information Commissioner (www.dataprotection.gov.uk)

Privacy Information Web Sites

- Access to justice network (www.acjnet.org)
- American Civil Liberties Union (www.aclu.org)
- Canadian Marketing Association (www.the-cma.org)
- Center for Democracy & Technology (www.cdt.org/privacy)
- Center for Media Education (www.cme.org)
- Computer Professionals for Social Responsibility (www.cpsr.org)
- Consumer Project on Technology (www.cptech.org/privacy)
- Consumer Protection Association (www.consumerpro.com)
- Identity theft U.S. government central Web site (www.consumer.gov/idtheft)
- Consumer.net - Consumer Information Organization (www.consumer.net)
- Cookie Central (www.cookiecentral.com)
- Cyber-Rights & Cyber-Liberties (www.cyber-rights.org)
- Direct Marketing Association (www.the-dma.org)
- Electronic Frontier Canada (http://insight.mcmaster.ca/org/efc/efc.html)
- Electronic Frontier Foundation (www.eff.org)
- Electronic Privacy Information Center (www.epic.org)
- European Union (http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm)
- Health Privacy Project (www.healthprivacy.org)
- HIPAA Central Siemens Health Services (www.smed.com/hipaa/index.php)
- Industry Canada E-Commerce Task Force (http://e-com.ic.gc.ca/english/privacy/index.html)
- Internet Law and Policy Forum (www.ilpf.org)
- International Security, Trust and Privacy Alliance (www.istpa.org)
- JunkBusters (www.junkbusters.com)
- Media Awareness Network (www.media-awareness.ca)
- National Small Business Poll – Privacy and National Small Business Poll – Advice and Advisors National Federation of Independent Business (NFIB) Research Foundation (www.nfib.com)

- Office for Civil Rights (www.hhs.gov/ocr/hipaa)
- Online Privacy Alliance (www.privacyalliance.org)
- Privacy & American Business (www.pandab.org)
- Privacy Exchange (www.privacyexchange.org)
- Privacy Forum (www.vortex.com/privacy.html)
- International Association of Privacy Professionals (www.privacyassociation.org)
- Privacy Page (www.privacy.org)
- Privacy Rights Clearinghouse (www.privacyrights.org)
- Public Interest Advocacy Centre (www.piac.ca)

Attachment D

Comparison of International Privacy Concepts

The table below presents a comparison of privacy concepts set out in some domestic and international privacy regulations, laws, and guidelines in relation to the 10 components of the AICPA/CICA Privacy Framework (the Framework). This is for illustrative purposes only and not meant to be comprehensive. Column 1 lists the 10 components of the Framework. Columns 2 through 10 lists the significant principles discussed in specific laws and regulations. The "Key to Column and Source," that follows the table identifies the source of each law and regulation compared:

(1) ***AICPA/CICA Privacy Framework***	*(2)* ***U.S. FTC***	*(3)* ***Canada PIPEDA***	*(4)* ***Australia Privacy Act***	*(5)* ***U.S. Safe Harbor***	*(6)* ***E.U. Directive***	*(7)* ***OECD Guidelines***	*(8)* ***U.S. HIPAA***	*(9)* ***U.S. GLBA***	*(10)* ***U.S. COPPA***
Management		Accountability			Notification	Accountability	Administrative requirements		
Notice	Notice	Identifying Purposes, Openness	Openness	Notice	Information to be Given to the Data Subject	Purpose Specification, Openness	Notice	Privacy and Opt Out Notices, Exceptions	Notice
Choice and Consent	Choice	Consent	Use and Disclosure	Choice	Criteria for Making Data Processing Legitimate, Data Subject's Right to Object	Collection Limitation	Consent, Uses and Disclosures	Privacy and Opt Out Notices	Parental Consent
Collection		Limiting Collection	Collection, Sensitive Information, Anonymity	Data Integrity	Principles Relating to Data Quality, Exemptions and Restrictions	Collection (including consent) Limitation			Parental Consent, Prohibition Against Conditioning a Child's Participation on Collection of Personal Information
Use and Retention		Limiting Use, Disclosure, and	Identifiers, Use and Disclosure	(implied but not specified in the	Making Data Processing	Use Limitation (including	Uses and Disclosures	Limits on Disclosures	Right of Parent to Review

(1) ***AICPA/CICA Privacy Framework***	*(2)* ***U.S. FTC***	*(3)* ***Canada PIPEDA***	*(4)* ***Australia Privacy Act***	*(5)* ***U.S. Safe Harbor***	*(6)* ***E.U. Directive***	*(7)* ***OECD Guidelines***	*(8)* ***U.S. HIPAA***	*(9)* ***U.S. GLBA***	*(10)* ***U.S. COPPA***
		Retention		principles)	Legitimate, Special Categories of Processing, Principles Relating to Data Quality, Exemptions and Restrictions, The Data Subject's Right to Object	disclosure limitation)			Personal Information Provided by a Child
Access		Individual Access	Access and Correction	Access	The Data Subject's Right of Access to Data	Individual Participation	Access		Right of Parent to Review Personal Information Provided by a Child

(1) ***AICPA/CICA Privacy Framework***	*(2)* ***U.S. FTC***	*(3)* ***Canada PIPEDA***	*(4)* ***Australia Privacy Act***	*(5)* ***U.S. Safe Harbor***	*(6)* ***E.U. Directive***	*(7)* ***OECD Guidelines***	*(8)* ***U.S. HIPAA***	*(9)* ***U.S. GLBA***	*(10)* ***U.S. COPPA***
Disclosure to Third Parties		Limiting Use, Disclosure, and Retention	Use and Disclosure, Transborder Data Flows	Onward Transfer	Transfer of Personal Data to Third Countries	Use Limitation (including disclosure limitation)	Uses and Disclosures, Accounting of Disclosures	Limits on Disclosures	Parental Consent
Security	Security	Safeguards	Data Security	Security	Confidentiality and Security of Processing	Security Safeguards	Security Rule	Security Guidelines mandated by section 501(b) of GLBA	Confidentiality, Security, and Integrity of Personal Information Collected From Children
Quality	Integrity	Accuracy	Data Quality	Data Integrity	Principles Relating to Data Quality	Data Quality	Amendment		Confidentiality, Security, and Integrity of Personal Information Collected From Children
Monitoring and Enforcement	Enforcement	Challenging Compliance	(Enforcement by the Office of the Privacy Commissioner)	Enforcement	Judicial Remedies, Liability and Sanctions, Codes of Conduct, Supervisory Authority and Working Party on the Protection of Individuals with Regard to the Processing of Personal Data	Individual Participation (including challenging compliance)	(Compliance and Enforcement by the Department of Health and Human Services)	(Enforcement by financial services industry regulators, the FTC and SEC)	Enforcement

Key to Column and Source

(2) U.S. FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*, United States (U.S.) Federal Trade Commission (FTC), May 2000.
(3) Canada *Personal Information Protection and Electronic Documents Act* (PIPEDA), also referred to as. Bill C-6, Second Session, Thirty-sixth Parliament, 48-49 Elizabeth II, 1999-2000, assented to April 13, 2000, effective January 1, 2001.
(4) Australia Privacy Act 1988, *Privacy Act 1988*, as amended, effective December 21, 2001.
(5) U.S. Safe Harbor, an agreement between the U.S. Department of Commerce and the European Commission's Internal Market Directorate, approved by the European Commission July 27, 2000, open for use November 1, 2000.
(6) EU Directive, European Union (EU), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, October 24, 1995, effective October 25, 1998, as implemented in EU country-specific laws and regulations.
(7) OECD Guidelines, Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980.
(8) U.S. United States Health Insurance Portability and Accountability Act of 1996 (HIPAA), Privacy Rule (compliance deadline April 16, 2003), Security Rule (compliance deadline April 21, 2005).
(9) U.S. Financial Services Modernization Act, also referred to as the Gramm-Leach-Bliley Act (GLBA), Title V – Privacy, Subtitle A, enacted November 12, 1999, effective November 13, 2000, Compliance by July 1, 2001. The Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision (collectively, the Agencies) published final Guidelines establishing standards for safeguarding customer information that implement sections 501 and 505(b) of GLBA.
(10) U.S. Children's Online Privacy Protection Act of 1998 (COPPA), effective April 21, 2000.

Attachment E

Transition from AICPA/CICA Trust Services Online Privacy Principle and Criteria to the AICPA/CICA Trust Services Privacy Principle and Criteria

Transition Guidance

For Trust Services assurance privacy engagements with reporting periods beginning on or after April 1, 2004, the AICPA/CICA Privacy Framework Principle and Criteria are to be used in place of the AICPA/CICA Trust Services Online Privacy Principle and Criteria and will become known as the AICPA/CICA Trust Services Privacy Principle and Criteria. Earlier application is encouraged.

WebTrust Online Privacy Seal or WebTrust Consumer Protection Seal[10]

Existing WebTrust Online Privacy Engagements

For those entities wishing to continue to display a WebTrust Online Privacy seal or a WebTrust Consumer Protection seal (both seals require an attestation or assurance report based on the AICPA/CICA Trust Services Online Privacy Principle and Criteria), a new unqualified report must be issued using the new AICPA/CICA Trust Services Privacy Principle and Criteria when the examination to renew the seal covers a period beginning on or after April 1, 2004.

New Online Privacy Engagements

When the privacy engagement relates to an online segment, an entity may choose to display a WebTrust Online Privacy seal or a WebTrust Consumer Protection seal. For these engagements:

- The scope of the engagement needs to include, but is not limited to, an online business segment of the entity. Use of the WebTrust Seal is only permitted in circumstances where the online business segment is included in the scope of the practitioner's examination.

- WebTrust seals are trademarked and service-marked graphic images and their use is subject to the Trust Services License agreement. The Trust Services license agreement and the guidance established for the Trust Services program permit the images to be displayed on a client's Web site or electronically, subject to certain requirements:

  — The practitioner must be licensed under the Trust Services license agreement.

  — The entity must have received a report from the practitioner that does not include a qualification or scope limitation.

---

[10] Currently, the use of a seal for other types of privacy assurance/attestation reports is under consideration. Please contact Karyn Waller at the AICPA (kwaller@aicpa.org) or Bryan Walker at the CICA (bryan.walker@cica.ca) for additional information.

— The seal must be issued using the AICPA/CICA processes and be listed on the Institutes' server.

— Fees as established by the Trust Services license agreement for the use of the seal must be paid to the Institutes.

When the WebTrust Seal is used, the Task Force recommends that the practitioner's report includes language such as the following: "The WebTrust Online Privacy Seal constitutes a symbolic representation of the contents of the independent auditor's report and it is not intended, nor should it be construed, to update that report or provide any additional assurance."