Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (Including WebTrust® and SysTrust®)

TRUST SERVICES, PRINCIPLES, CRITERIA AND ILLUSTRATIONS

Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (Including WebTrust® and SysTrust®)

May 2006

NOTICE TO READERS

The Trust Services Principles, Criteria, and Illustrations present criteria established by the Assurance Services Executive Committee of the AICPA for use by practitioners when providing attestation services on systems in the subject matters of security, availability, processing integrity, privacy, confidentiality, and certification authorities. The Assurance Services Executive Committee, in establishing and developing these criteria, followed due process procedures, including exposure of the proposed criteria for public comment. The Assurance Services Executive Committee has been designated as a senior committee and has been given authority to make public statements and publish measurement criteria without clearance from Council or the Board of Directors under Bylaw section 3.6.

Table of Contents

Introduction

.01 This section provides guidance when providing assurance services, advisory services, or both on information technology (IT)-enabled systems including electronic commerce (e-commerce) systems. It is particularly relevant when providing services with respect to security, availability, processing integrity, confidentiality, and privacy.

.02 The guidance provided in this section includes:

- Trust Services principles and criteria
- Examples of system descriptions required for these engagements
- Sample practitioner reports for Trust Services engagements

Trust Services

.03 Trust Services (including WebTrust® and SysTrust®) are defined as a set of professional assurance and advisory services based on a common framework (that is, a core set of principles and criteria) to address the risks and opportunities of IT. Trust Services principles and criteria are issued by the Assurance Services Executive Committee.

Assurance Services

.04 Assurance services are those that result in the expression of an opinion by the reporting practitioner; for example, the opinion as to whether a defined system meets the principles and criteria for systems reliability. Assurance services are developed within the framework of Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended. Only certified public accountants (CPAs) may provide the assurance services of Trust Services that result in the expression of a Trust Services, WebTrust, or SysTrust opinion.

Advisory Services

.05 In the context of Trust Services, advisory services include strategic, diagnostic, implementation and sustaining/managing services using Trust Services principles and criteria. Practitioners providing such services follow Statement on Standards for Consulting Services (AICPA, *Professional Standards*, vol. 2, CS sec. 100). There is no expression of an opinion by the practitioner under these engagements.

Principles, Criteria, and Illustrative Controls

.06 The following material sets out broad statements of principles and identifies specific criteria that should be achieved to meet each principle. Trust Services principles are broad statements of objectives. Criteria are benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. Suitable criteria are objective, measurable, complete, and relevant—they will yield information useful to intended users. It is the view of the Assurance Services Executive Committee that the Trust Services principles and supporting criteria meet the characteristics for suitable criteria. Trust

Services principles are used to describe the overall objective; however, the practitioner's opinion makes reference only to criteria.

.07 In the Trust Services Principles and Criteria, the criteria are supported by a list of illustrative controls. These illustrations are not intended to be all-inclusive and are presented as examples only. Actual controls in place at an entity may not be included in the list, and some of the listed controls may not be applicable to all systems and client circumstances. The practitioner should identify and assess the relevant controls the client has in place to satisfy the criteria. The choice and number of those controls would be based on the entity's management style, philosophy, size, and industry. In order to receive an unqualified opinion on a Trust Services engagement, all criteria must be met unless the criterion is clearly not applicable. In the context of the Trust Services Principles and Criteria, the term *policies* is used to refer to written statements that communicate management's intent, objectives, requirements, responsibilities, and/or standards for a particular subject. Such communications may be explicitly designated as policies, whereas others (such as communications with users not otherwise documented as policies, or written procedures) may be implicit. Policies may take many forms but should be in writing.

Consistency With Applicable Laws and Regulations, Defined Commitments, Service-Level Agreements, and Other Contracts

.08 Several of the principles and criteria refer to "consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contracts." Under normal circumstances, it would be beyond the scope of the engagement for the practitioner to undertake identification of *all* relevant "applicable laws and regulations, defined commitments, service-level agreements, and other contracts." Furthermore, Trust Services engagements do not require the practitioner to provide assurance of an entity's compliance with applicable laws and regulations, defined commitments, service-level agreements, and other contracts, but rather of the effectiveness of the entity's controls over monitoring compliance with them. Reference should be made to other professional standards related to providing assurance over compliance with laws, regulations, and agreements.

Foundation for Trust Services—Trust Services Principles and Criteria

.09 The Trust Services Principles and Criteria set forth herein are organized into four broad areas:

a. *Policies.* The entity has defined and documented its policies [fn 1] relevant to the particular principle.

b. *Communications.* The entity has communicated its defined policies to authorized users.

c. *Procedures.* The entity uses procedures to achieve its objectives in accordance with its defined policies.

[fn 1] As noted in paragraph .07, the term *policies* refers to written statements which communicate management's intent, objectives, requirements, responsibilities, and/or standards for a particular subject. Some policies may be explicitly described as such, being contained in policy manuals or similarly labeled documents. However, some policies may be contained in documents without such explicit labeling, including for example, notices or reports to employees or outside parties.

d. Monitoring. The entity monitors the system and takes action to maintain compliance with its defined policies.

.10 A two-column format has been used to present and discuss the criteria. The first column presents the criteria—the attributes that the entity must meet to be able to demonstrate that it has achieved the principle. The second column provides illustrative controls. These are examples of controls that the entity might have in place to conform to the criteria. Alternative and additional controls may also be appropriate. In addition, examples of system descriptions for both e-commerce and non-e-commerce systems are included in Appendix A [paragraph .42] and Appendix B [paragraph .43], respectively, and Appendix A [paragraph .42] also includes sample disclosures for e-commerce systems.

.11 The following principles and related criteria have been developed by the AICPA/CICA for use by practitioners in the performance of Trust Services engagements such as SysTrust and WebTrust.

a. Security. The system [fn 2] is protected against unauthorized access (both physical and logical).

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

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

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

e. Privacy. Personal information [fn 3] is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA/CICA (found in Appendix D [paragraph .45]).

Trust Services—Offerings of SysTrust and WebTrust

.12 SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and Criteria. The Trust Services Principles and Criteria may, however, be used to offer services other than SysTrust and WebTrust.

.13 When a practitioner intends to provide assurance from SysTrust or WebTrust engagements, he or she needs to also follow the performance and reporting standards set forth in Chapter 1, "Attest Engagements," of SSAE No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended. In order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.

[fn 2] A *system* consists of five key components organized to achieve a specified objective. The five components are categorized as follows: (*a*) infrastructure (facilities, equipment, and networks), (*b*) software (systems, applications, and utilities), (*c*) people (developers, operators, users, and managers), (*d*) procedures (automated and manual), and (*e*) data (transaction streams, files, databases, and tables).

[fn 3] *Personal information* is information that is, or can be, about or related to an identifiable individual.

Principles and Criteria

.14 The Trust Services Principles and Criteria are presented in a two-column format. The first column identifies the criteria for each principle—the attributes that the entity must meet to be able to demonstrate that it has achieved the principle. The second column provides illustrative controls. These are examples of controls that the entity might have in place to meet the criteria. Alternative and/or additional controls can also be used. Illustrative controls are presented as examples only. It is the practitioner's responsibility to identify and document the policies, procedures, and controls actually in place at the entity under examination.

.15 As discussed earlier, in certain e-commerce environments, the terms and conditions, including the rights, responsibilities, and commitments of both parties, are implicit in the user's completion of a transaction on the Web site. To meet the underlying intent of the "Communications" category of the criteria in such circumstances, the policies and processes required by each of the "Communications" criteria should be disclosed on the entity's Web site. Examples of such disclosures for each of the Trust Services principles are contained in Appendix A [paragraph .42].

Security Principle and Criteria

.16 The *security principle* refers to the protection of the system components from unauthorized access, both logical and physical. In e-commerce and other systems, the respective parties wish to ensure that information provided is available only to those individuals who need access to complete the transaction or services, or follow up on questions or issues that may arise. Information provided through these systems is susceptible to unauthorized access during transmission and while it is stored on the other party's systems. Limiting access to the system components helps prevent potential abuse of system components, theft of resources, misuse of software, and improper access to, use, alteration, destruction, or disclosure of information. Key elements for the protection of system components include permitting authorized access and preventing unauthorized access to those components.

Security Principle and Criteria Table

.17 The system is protected against unauthorized access (both physical and logical).

	Criteria	*Illustrative Controls* [fn 4]
1.0	**Policies: The entity defines and documents its policies for the security of its system.**	
1.1	The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their security requirements. User requirements are documented in service-level agreements or other documents. The security officer reviews security policies annually and submits proposed changes for approval by the information technology (IT)

[fn 4] Illustrative controls are presented as examples only. It is the practitioner's responsibility to identify and document the policies, procedures, and controls actually in place at the entity under examination.

		standards committee.
1.2	The entity's security policies include, but may not be limited to, the following matters: *a.* Identification and documentation of the security requirements of authorized users. *b.* Allowing access, the nature of that access, and who authorizes such access. *c.* Preventing unauthorized access. *d.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access. *e.* Assignment of responsibility and accountability for system security. *f.* Assignment of responsibility and accountability for system changes and maintenance. *g.* Testing, evaluating, and authorizing system components before implementation. *h.* Addressing how complaints and requests relating to security issues are resolved. *i.* The procedures to handle security breaches and other incidents. *j.* Provision for allocation for training and other resources to support its system security policies. *k.* Provision for the handling of exceptions and situations not specifically addressed in its system security policies. *l.* Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	The entity's documented security policies contain the elements set out in criterion 1.2.
1.3	Responsibility and accountability for the entity's system security policies, and changes and updates to those policies, are assigned.	Management has assigned responsibilities for the maintenance and enforcement of the entity security policy to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of the policy as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining security over such resources is defined.
2.0	**Communications: The entity communicates its defined system security policies to authorized users.**	
2.1	**The entity has prepared an objective description of the system and its boundaries and commu-**	**For its e-commerce system, the entity has posted a system description on its Web site. [***For an example of a system description for an e-commerce system, refer to Appendix A (paragraph .42).***]**

	nicated such description to authorized users.	For its non–e-commerce system, the entity has provided a system description to authorized users. [*For an example of a system description for a non–e-commerce based system, refer to Appendix B (paragraph .43).*]
2.2	The security obligations of users and the entity's security commitments to users are communicated to authorized users.	The entity's security commitments and required security obligations of its customers and other external users are posted on the entity's Web site and/or as part of the entity's standard services agreement. For its internal users (employees and contractors), the entity's policies relating to security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's security policies. Security obligations of contractors are detailed in their contracts. A security awareness program has been implemented to communicate the entity's IT security policies to employees. The entity publishes its IT security policies on its corporate intranet.
2.3	Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	The security administration team is responsible for implementing the entity's security policies under the direction of the CIO. The security administration team has custody of and is responsible for the day-to-day maintenance of the entity's security policies, and recommends changes to the CIO and the IT steering committee.
2.4	The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.	The process for customers and external users to inform the entity of possible security breaches and other incidents is posted on the entity's Web site and/or is provided as part of the new user welcome kit. The entity's security awareness program includes information concerning the identification of possible security breaches and the process for informing the security administration team. Documented procedures exist for the identification and escalation of security breaches, and other incidents.
2.5	Changes that may affect system security are communicated to management and users who will be affected.	Changes that may affect customers and users and their security obligations or the entity's security commitments are highlighted on the entity's Web site. Changes that may affect system security are reviewed and approved by affected customers under the provisions of the standard services agreement before implementation of the proposed change. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee meetings. Changes to system components, including those that may affect system security, require the approval of the security administrator before implementation. There is periodic communication of changes, including changes that affect system security. Changes that affect system security are incorporated into the entity's ongoing security awareness program.
3.0	**Procedures: The entity uses procedures to achieve its documented system security objectives in ac-**	

	cordance with its defined policies.	
3.1	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:	*a.* Registration and authorization of new users:
	a. Registration and authorization of new users.	• Customers can self-register on the entity's Web site, under a secure session in which they provide new user information and select an appropriate user identification (ID) and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality.
	b. Identification and authentication of users.	• The ability to create or modify users and user access privileges (other than the limited functionality "customer accounts") is limited to the security administration team.
	c. The process to make changes and updates to user profiles.	• The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Proper segregation of duties is considered in granting privileges.
	d. The process to grant system access privileges and permissions.	*b.* Identification and authentication of users:
	e. Distribution of output restricted to authorized users.	• Users are required to log on to the entity's network and application systems with their user ID and password before access is granted. Unique user IDs are assigned to individual users. Passwords must contain at least six characters, one of which is nonalphanumeric. Passwords are case sensitive and must be updated every 90 days.
	f. Restriction of logical access to offline storage, backup data, systems, and media.	*c.* Changes and updates to user profiles:
	g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	• Changes and updates to self-registered customer accounts can be done by the individual user at any time on the entity's Web site after the user has successfully logged onto the system. Changes are reflected immediately.
		• Unused customer accounts (no activity for six months) are purged by the system. • Changes to other accounts and profiles are restricted to the security administration team and require the approval of the appropriate line-of-business supervisor or customer account manager. • Accounts for terminated employees are deactivated upon notice of termination being received from the human resources team.
		d. The process to grant system access privileges and permissions:
		• All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles. • The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up.
		e. Distribution of output:
		• Access to computer processing output is provided to authorized individuals based on the classification of the information. • Processing outputs are stored in an area that reflects the classification of the information.
		f. Restriction of logical access to offline storage, backup data, systems, and media: • Logical access to offline storage, backup data, systems, and media is limited to computer operations staff.

		g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices: • Hardware and operating system configuration tables are restricted to appropriate personnel. • Application software configuration tables are restricted to authorized users and under the control of application change management software. • Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff. Usage is logged and monitored by the manager of computer operations. • The information security team, under the direction of the CIO, maintains access to firewall and other logs, as well as access to any storage media. Any access is logged and reviewed quarterly. • A listing of all master passwords is stored in an encrypted database and an additional copy is maintained in a sealed envelope in the entity safe.
3.2	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals by card key systems and monitored by video surveillance. Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff. Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations. Documented procedures exist for the identification and escalation of potential security breaches. Offsite backup data and media are stored at service provider facilities. Access to offsite data and media requires the approval of the manager of computer operations.
3.3	Procedures exist to protect against unauthorized logical access to the defined system.	Login sessions are terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up by the security administrator. Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and passwords. Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator. Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions. Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.4	Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized	In connection with other security monitoring, the security administration team participates in user groups and subscribes to services

	software.	relating to computer viruses. Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated at least weekly. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.
3.5	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	The entity uses 128-bit secure sockets layer (SSL) encryption for transmission of private or confidential information over public networks, including user ID and password. Users are required to upgrade their browser to the most current version tested and approved for use by the security administration team to avoid possible security problems. Account activity, subsequent to successful login, is encrypted through a 128-bit SSL session. Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.
3.6	Procedures exist to identify, report, and act upon system security breaches and other incidents.	Users are provided instructions for communicating potential security breaches to the information security team. The information security team logs incidents reported through customer hotlines and e-mail. Intrusion detection and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator via e-mail and pager of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. Documented incident identification and escalation procedures are approved by management.
3.7	Procedures exist to provide that issues of noncompliance with system security policies are promptly addressed and that corrective measures are taken on a timely basis.	Security issues are recorded and accumulated in a problem report. Corrective action is noted and monitored by management. On a routine basis, security policies, controls, and procedures are audited by the internal audit department. Results of such examinations are reviewed by management, a response is prepared, and a remediation plan is put in place.
	Criteria related to the system components used to achieve the objectives	
3.8	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to system security are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	The entity has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The SDLC methodology includes a framework for classifying data and creating standard user profiles that are established based on an assessment of the business impact of the loss of security. Users are assigned standard profiles based on needs and functional responsibilities. Owners of the information and data classify its sensitivity and determine the level of protection required to maintain an appropriate level of security. The security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's security objectives, policies, and standards. Changes to system components that may affect security require the

		approval of the security administration team. The access control and operating system facilities have been installed, including the implementation of options and parameters, to restrict access in accordance with the entity's security objectives, policies, and standards. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.9	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security are qualified to fulfill their responsibilities.	The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions. Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation. Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered. Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities. Personnel receive training and development in system security concepts and issues. Procedures are in place to provide alternate personnel for key system security functions in case of absence or departure.
	Maintainability-related criteria applicable to the system's security	
3.10	Procedures exist to maintain system components, including configurations consistent with the defined system security policies.	Entity management receives a third-party opinion on the adequacy of security controls, and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site. The IT department maintains a listing of all software and the respective level, version, and patches that have been applied. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Staffing, infrastructure, and software requirements are periodically evaluated and resources are allocated consistent with the entity's security policies. System configurations are tested annually, and evaluated against the entity's security policies and current service-level agreements. An exception report is prepared and remediation plans are developed and tracked. The IT steering committee, which includes representatives from the lines of business and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's security policies, including the potential impact of legislative changes.
3.11	Procedures exist to provide that only authorized, tested, and docu-	Senior management has implemented a division of roles and respon-

	mented changes are made to the system.	sibilities that segregates incompatible functions. The entity's documented systems development methodology describes the change initiation, software development and maintenance, and approval processes, as well as the standards and controls that are embedded in the processes. These include programming, documentation, and testing standards. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation into production. As part of the change control policies and procedures, there is a "promotion" process (for example, from "test" to "staging" to "production"). Promotion to production requires the approval of the business owner who sponsored the change and the manager of computer operations. When changes are made to key systems components, there is a "backout" plan developed for use in the event of major interruption(s).
3.12	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process, including line-of-business approvals.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies.**	
4.1	The entity's system security is periodically reviewed and compared with the defined system security policies.	The information security team monitors the system and assesses the system vulnerabilities using proprietary and other tools. Potential risk is evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementation is monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts system security reviews as part of its annual audit plan. Results and recommendations for improvement are reported to management.
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives. Monthly IT staff meetings are held to address system security concerns and trends; findings are discussed at quarterly management meetings.
4.3	Environmental and technological	Senior management, as part of its annual IT planning process, con-

	changes are monitored and their effect on system security is assessed on a timely basis.	siders developments in technology and the impact of applicable laws or regulations on the entity's security policies. The entity's IT security group monitors the security impact of emerging technologies. Users are proactively invited to contribute to initiatives to improve system security through the use of new technologies.

Availability Principle and Criteria

.18 The *availability principle* refers to the accessibility to the system, products, or services as advertised or committed by contract, service-level, or other agreements. It should be noted that this principle does not, in itself, set a minimum acceptable performance level for system availability. The minimum performance level is established through commitments made or by mutual agreement (contract) between the parties.

.19 Although there is a connection between system availability, system functionality, and system usability, the availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to specific tasks or problems). It does address system availability, which relates to whether the system is accessible for processing, monitoring, and maintenance.

Availability Principle and Criteria Table

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

	Criteria	*Illustrative Controls*
1.0	**Policies: The entity defines and documents its policies for the availability of its system.**	
1.1	The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their availability and related security requirements. User requirements are documented in service-level agreements or other documents. Management reviews the entity's availability and related security policies annually. Proposed changes are submitted as needed for approval by the information technology (IT) standards committee, which includes representation from the customer service department.
1.2	The entity's system availability and related security policies include, but may not be limited to, the following matters: *a.* Identification and documentation of the system availability and related security requirements of authorized users. *b.* Allowing access, the nature of that access, and who authorizes such access.	The entity's documented availability and related security policies contain the elements set out in criterion 1.2.

	c. Preventing unauthorized access. *d.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access. *e.* Assignment of responsibility and accountability for system availability and related security. *f.* Assignment of responsibility and accountability for system changes and maintenance. *g.* Testing, evaluating, and authorizing system components before implementation. *h.* Addressing how complaints and requests relating to system availability and related security issues are resolved. *i.* The procedures to handle system availability and related security breaches and other incidents. *j.* Provision for allocation for training and other resources to support its system availability and related security policies. *k.* Provision for the handling of exceptions and situations not specifically addressed in its system availability and related security policies. *l.* Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts. *m.* Recovery and continuity of service in accordance with documented customer commitments or other agreements. *n.* Monitoring system capacity to achieve customer commitments or other agreements regarding availability.	
1.3	Responsibility and accountability for the entity's system availability and related security policies, and changes and updates to those policies, are assigned.	Management has assigned responsibilities for the maintenance and enforcement of the entity's availability policies to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of these policies as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining the system availability of and related security over such resources is defined.
2.0	**Communications: The entity communicates the defined system availability policies to authorized users.**	
2.1	The entity has prepared an objective description of the system and its boundaries and communicated	For its e-commerce system, the entity has posted a system description on its Web site. [*For an example of a system description for an*

	such description to authorized users.	*e-commerce system, refer to Appendix A(paragraph .42).*] For its non–e-commerce system, the entity has provided a system description to authorized users. [*For an example of a system description for a non–e-commerce based system, refer to Appendix B (paragraph .43).*]
2.2	The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	The entity's system availability and related security commitments and required system availability and related security obligations of its customers and other external users are posted on the entity's Web site and/or as part of the entity's standard services agreement. Service-level agreements are reviewed with the customer annually. For its internal users (employees and contractors), the entity's policies relating to system availability and security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's policies. Obligations of contractors are detailed in their contract. A security awareness program has been implemented to communicate the entity's IT security policies to employees. The entity publishes its IT security policies on its corporate intranet.
2.3	Responsibility and accountability for the entity's system availability and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	The network operations team is responsible for implementing the entity's availability policies under the direction of the chief information officer (CIO). The security administration team is responsible for implementing the related security policies. The network operations team has custody of and is responsible for the day-to-day maintenance of the entity's availability policies, and recommends changes to the CIO and the IT steering committee. The security administration team is responsible for the related security policies. Availability and related security commitments are reviewed with the customer account managers as part of the annual IT planning process.
2.4	The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.	The process for customers and external users to inform the entity of system availability issues, possible security breaches, and other incidents is posted on the entity's Web site and/or is provided as part of the new user welcome kit. The entity's user training program includes modules dealing with the identification and reporting of system availability issues, security breaches, and other incidents. The entity's security awareness program includes information concerning the identification of possible security breaches and the process for informing the security administration team. Documented procedures exist for the identification and escalation of system availability issues, security breaches, and other incidents.
2.5	Changes that may affect system availability and system security are communicated to management and users who will be affected.	Changes that may affect system availability, customers and users and their security obligations, or the entity's security commitments are highlighted on the entity's Web site. Changes that may affect system availability and related system security are reviewed and approved by affected customers under the

		provisions of the standard services agreement before implementation of the proposed change. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee meetings. Changes to system components, including those that may affect system security, require the approval of the manager of network operations and/or the security administration team, before implementation. There is periodic communication of system changes, including changes that affect availability and system security. Changes that affect system security are incorporated into the entity's ongoing security awareness program.
3.0	**Procedures: The entity uses procedures to achieve its documented system availability objectives in accordance with its defined policies.**	
3.1	Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, labor disputes, and routine operational errors and omissions) that might disrupt system operations and impair system availability.	A risk assessment is prepared and reviewed on a regular basis or when a significant change occurs in either the internal or external physical environment. Threats such as fire, flood, dust, power failure, excessive heat and humidity, and labor problems have been considered. Management maintains measures to protect against environmental factors (for example, fire, flood, dust, power failure, and excessive heat and humidity) based on its risk assessment. The entity's controlled areas are protected against fire using both smoke detectors and a fire suppression system. 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 (UPS) and emergency power supplies (EPS). This equipment is tested semiannually. Preventive maintenance agreements and scheduled maintenance procedures are in place for key system hardware components. Vendor warranty specifications are complied with and tested to determine if the system is properly configured. Procedures to address minor processing errors, outages, and destruction of records are documented. Procedures exist for the identification, documentation, escalation, resolution, and review of problems. Physical and logical security controls are implemented to reduce the opportunity for unauthorized actions that could impair system availability.
3.2	Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.	Management has implemented a comprehensive strategy for backup and restoration based on a review of business requirements. Backup procedures for the entity are documented and include redundant servers, daily incremental backups of each server, and a complete backup of the entire week's changes on a weekly basis. Daily and weekly backups are stored offsite in accordance with the entity's system availability policies. Disaster recovery and contingency plans are documented. The disaster recovery plan defines the roles and responsibilities and identifies the critical information technology application programs,

		operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on the business impact analysis. The business continuity planning (BCP) coordinator reviews and updates the business impact analysis with the lines of business annually. Disaster recovery and contingency plans are tested annually in accordance with the entity's system availability policies. Testing results and change recommendations are reported to the entity's management committee. The entity's management committee reviews and approves changes to the disaster recovery plan. All critical personnel identified in the business continuity plan hold current versions of the plan, both onsite and offsite. An electronic version is stored offsite.
3.3	Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.	Automated backup processes include procedures for testing the integrity of the backup data. Backups are performed in accordance with the entity's defined backup strategy, and usability of backups is verified at least annually. Backup systems and data are stored offsite at the facilities of a third-party service provider. Under the terms of its service provider agreement, the entity performs an annual verification of media stored at the offsite storage facility. As part of the verification, media at the offsite location are matched to the appropriate media management system. The storage site is reviewed biannually for physical access security and security of data files and other items. Backup systems and data are tested as part of the annual disaster recovery test.
	Security-related criteria relevant to the system's availability	
3.4	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: *a.* Registration and authorization of new users. *b.* Identification and authentication of users. *c.* The process to make changes and updates to user profiles. *d.* The process to grant system access privileges and permissions. *e.* Restriction of access to system configurations, superuser functionality, master passwords, powerful	*a.* Registration and authorization of new users: • Customers can self-register on the entity's Web site, under a secure session in which they provide new user information and select an appropriate user identification (ID) and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality. • The ability to create or modify users and user access privileges (other than the limited functionality "customer accounts") is limited to the security administration team. • The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Proper segregation of duties is considered in granting privileges. *b.* Identification and authentication of users: • Users are required to log on to the entity's network and application systems with their user ID and password before access is granted. Unique user IDs are assigned to individual users. Passwords must

	utilities, and security devices (for example, firewalls).	contain at least six characters, one of which is nonalphanumeric. Passwords are case sensitive and must be updated every 90 days. *c.* Changes and updates to user profiles: • Changes and updates to self-registered customer accounts can be done by the individual user at any time on the entity's Web site after the user has successfully logged onto the system. Changes are reflected immediately. • Unused customer accounts (no activity for six months) are purged by the system. • Changes to other accounts and profiles are restricted to the security administration team and require the approval of the appropriate line-of-business supervisor or customer account manager. • Accounts for terminated employees are deactivated upon notice of termination being received from the human resources team. *d.* The process to grant system access privileges and permissions: • All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles. • The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up. *e.* Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices: • Hardware and operating system configuration tables are restricted to appropriate personnel. • Application software configuration tables are restricted to authorized users and under the control of application change management software. • Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff. Usage is logged and monitored by the manager of computer operations. • The information security team, under the direction of the CIO, maintains access to firewall and other logs, as well as access to any storage media. Any access is logged and reviewed quarterly. • A listing of all master passwords is stored in an encrypted database and an additional copy is maintained in a sealed envelope in the entity safe.
3.5	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals by card key systems and monitored by video surveillance. Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff. Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations. Documented procedures exist for the identification and escalation of potential security breaches. Offsite backup data and media are stored at service provider facilities. Access to offsite data and media requires the approval of the manager of computer operations.
3.6	Procedures exist to protect against unauthorized logical access to the defined system.	Login sessions are terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up by the

		security administrator. Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and passwords. Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator. Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions. Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.7	Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	In connection with other security monitoring, the security administration team participates in user groups and subscribes to services relating to computer viruses. Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated at least weekly. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.
3.8	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	The entity uses 128-bit secure sockets layer (SSL) encryption for transmission of private or confidential information over public networks, including user ID and password. Users are required to upgrade their browser to the most current version tested and approved for use by the security administration team to avoid possible security problems. Account activity, subsequent to successful login, is encrypted through a 128-bit SSL session. Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.
3.9	Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.	Users are provided instructions for communicating system availability issues, potential security breaches, and other issues to the help desk or customer service center. Documented procedures exist for the escalation of system availability issues and potential security breaches that cannot be resolved by the help desk. Network performance and system processing are monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Documented procedures exist for the escalation and resolution of performance and processing availability issues. Intrusion detection and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator via e-mail and pager of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily.

		Documented incident identification and escalation procedures are approved by management. Network performance, system availability, and security incident statistics and comparisons to approved targets are accumulated and reported to the IT steering committee monthly. System performance and capacity analysis and projections are completed annually as part of the IT planning and budgeting process.
3.10	Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	System processing and security-related issues are recorded and accumulated in a problem report. Corrective action is noted and monitored by management. As a part of the monthly monitoring of the site, availability and site usage reports are compared to the disclosed availability levels. This analysis is used to forecast future capacity, reveal any performance issues, and provide a means of fine-tuning the system. Standard procedures exist for the documentation, escalation, resolution, and review of problems. On a routine basis, security policies, controls, and procedures are audited by the internal audit department. Results of such examinations are reviewed by management, a response is prepared, and a remediation plan is put in place. Entity management evaluates the level of performance it receives from the Internet service provider (ISP) which hosts the entity Web site. This evaluation is done by evaluating the provider's actual performance as compared to agreed service-level commitments including measures for system processing performance levels, availability, and security controls the ISP has in place. Management receives an annual independent third-party report on the adequacy of internal controls from its Web-hosting service provider. Management reviews these reports and follows up with the service provider management on any open items or causes for concern.
	Criteria related to the system components used to achieve the objectives	
3.11	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to system availability and security are consistent with defined system availability and related security policies.	The entity has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The SDLC methodology includes a framework for: • Establishing performance level and system availability requirements based on user needs. • Maintaining the entity's backup and disaster recovery planning processes in accordance with user requirements. • Classifying data and creating standard user profiles that are established based on an assessment of the business impact of the loss of security; assigning standard profiles to users based on needs and functional responsibilities. • Testing changes to system components to minimize the risk of an adverse impact to system performance and availability. • Development of "backout" plans before implementation of changes. Owners of the information and data establish processing performance and availability benchmarks, classify its sensitivity, and deter-

		mine the level of protection required to maintain an appropriate level of security.
		The security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's availability and related security policies.
		Changes to system components that may affect systems processing performance, availability, and security require the approval of the security administration team.
		The access control and operating system facilities have been installed, including the implementation of options and parameters, to restrict access in accordance with the entity's security objectives, policies, and standards.
		The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.12	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security are qualified to fulfill their responsibilities.	The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions.
		Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation.
		Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered.
		Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities.
		Personnel receive training and development in system availability concepts and issues.
		Procedures are in place to provide alternate personnel for key system availability functions in case of absence or departure.
	Maintainability-related criteria applicable to the system's availability	
3.13	Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies.	Entity management receives a third-party opinion on the adequacy of security controls, and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site.
		The IT department maintains a listing of all software and the respective level, version, and patches that have been applied.
		Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests.
		Staffing, infrastructure, and software requirements are periodically evaluated and resources are allocated consistent with the entity's availability and related security policies.

		System configurations are tested annually and evaluated against the entity's processing performance, availability, and security policies, and current service-level agreements. An exception report is prepared and remediation plans are developed and tracked. The IT steering committee, which includes representatives from the lines of business and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's availability and related security policies, including the potential impact of legislative changes.
3.14	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Senior management has implemented a division of roles and responsibilities that segregates incompatible functions. The entity's documented systems development methodology describes the change initiation, software development and maintenance, and approval processes, as well as the standards and controls that are embedded in the processes. These include programming, documentation, and testing standards. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation into production. As part of the change control policies and procedures, there is a "promotion" process (for example, from "test" to "staging" to "production"). Promotion to production requires the approval of the business owner who sponsored the change and the manager of computer operations. When changes are made to key systems components, there is a "backout" plan developed for use in the event of major interruption(s).
3.15	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process, including line-of-business approvals.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system availability policies.**	
4.1	The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.	Network performance and system processing are monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Network performance, system availability, and security incident statistics and comparisons to approved targets are accumulated and reported to the IT steering committee monthly. The customer service group monitors system availability and related customer complaints. It provides a monthly report of such matters

		together with recommendations for improvement, which are considered and acted on at the monthly IT steering committee meetings. The information security team monitors the system and assesses the system vulnerabilities using proprietary and other tools. Potential risk is evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementation is monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts system availability and system security reviews as part of its annual audit plan. Results and recommendations for improvement are reported to management.
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.	Network performance and system processing are monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Network performance, system availability, and security incident statistics and comparisons to approved targets are accumulated and reported to the IT steering committee monthly. Future system performance, availability, and capacity requirements are projected and analyzed as part of the annual IT planning and budgeting process. Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its system availability and related security objectives. Monthly IT staff meetings are held to address system performance, availability, capacity, and security concerns and trends; findings are discussed at quarterly management meetings.
4.3	Environmental and technological changes are monitored and their effect on system availability and security is assessed on a timely basis.	The entity's data center facilities include climate and environmental monitoring devices. Deviations from optimal performance ranges are escalated and resolved. Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's availability and related security policies. The entity's customer service group monitors the impact of emerging technologies, customer requirements, and competitive activities.

Processing Integrity Principle and Criteria

.21 The *processing integrity principle* refers to the completeness, accuracy, timeliness, and authorization of system processing. Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Completeness generally indicates that all transactions and services are processed or performed without exception, and that transactions and services are not processed more than once. Accuracy includes assurances that key information associated with the submitted transaction will remain accurate throughout the processing of the transaction and the transaction or services are processed or performed as intended. The timeliness of the provision of services or the delivery of goods is addressed in the context of commitments made for such delivery. Authorization includes assurances that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing.

.22 The risks associated with processing integrity are that the party initiating the transaction will not have the transaction completed or the service provided correctly, and in accordance with the desired or specified request. Without appropriate processing integrity controls, the buyer may not receive the goods or services ordered, receive more than requested, or receive the wrong goods or services altogether. However, if appropriate processing integrity controls exist and are operational within the system, the buyer can be reasonably assured that the correct goods and services in the correct quantity at the correct price are received when promised. Processing integrity addresses all of the system components including procedures to initiate, record, process, and report the information, product, or service that is the subject of the engagement. The nature of data input in e-commerce systems typically involves the user entering data directly over Web-enabled input screens or forms, whereas in other systems, the nature of data input can vary significantly. Because of this difference in data input processes, the nature of controls over the completeness and accuracy of data input in e-commerce systems may be somewhat different than for other systems. The illustrative controls outlined in the following table identify some of these differences.

.23 Processing integrity differs from data integrity. Processing integrity does not automatically imply that the information stored by the system is complete, accurate, current, and authorized. If a system processes information inputs from sources outside of the system's boundaries, an entity can establish only limited controls over the completeness, accuracy, authorization, and timeliness of the information submitted for processing. Errors that may have been introduced into the information and the control procedures at external sites are typically beyond the entity's control. When the information source is explicitly excluded from the description of the system that defines the engagement, it is important to describe that exclusion in the system description. In other situations, the data source may be an inherent part of the system being examined, and controls over the completeness, accuracy, authorization, and timeliness of information submitted for processing would be included in the scope of the system as described.

Processing Integrity Principle and Criteria Table

.24 System processing is complete, accurate, timely, and authorized.

	Criteria	*Illustrative Controls*
1.0	**Policies: The entity defines and documents its policies for the processing integrity of its system.**	
1.1	The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their processing integrity and related security requirements. User requirements are documented in service-level agreements or other documents. The security officer reviews security policies annually and submits proposed changes as needed for approval by the information technology (IT) standards committee.
1.2	The entity's system processing integrity and related security policies include, but may not be limited to, the following matters: *a.* Identification and documentation of the system processing integrity and related security requirements of authorized users.	The entity's documented processing integrity and related security policies contain the elements set out in criterion 1.2.

	b. Allowing access, the nature of that access, and who authorizes such access. *c.* Preventing unauthorized access. *d.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access. *e.* Assignment of responsibility and accountability for system processing integrity and related security. *f.* Assignment of responsibility and accountability for system changes and maintenance. *g.* Testing, evaluating, and authorizing system components before implementation. *h.* Addressing how complaints and requests relating to system processing integrity and related security issues are resolved. *i.* The procedures to handle errors and omissions and other system processing integrity and related security breaches and other incidents. *j.* Provision for allocation for training and other resources to support its system processing integrity and related system security policies. *k.* Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies. *l.* Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	
1.3	Responsibility and accountability for the entity's system processing integrity and related system security policies, and changes, updates, and exceptions to those policies, are assigned.	Management has assigned responsibilities for the implementation of the entity's processing integrity and related security policies to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of the policies as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining system processing integrity and related security over such resources is defined.
2.0	**Communications: The entity communicates its documented system processing integrity policies to authorized users.**	
2.1	The entity has prepared an objective description of the system and its boundaries and communicated	For its e-commerce system, the entity has posted a system description including the elements set out in criterion 2.1 on its Web site. [*For an example of a system description and additional disclosures*

such description to authorized users.

If the system is an e-commerce system, additional information provided on its Web-site includes, but may not be limited to, the following matters:

a. Descriptive information about the nature of the goods or services that will be provided, including, where appropriate:
- Condition of goods (meaning, whether they are new, used, or reconditioned).
- Description of services (or service contract).
- Sources of information (meaning, where it was obtained and how it was compiled).

b. The terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following matters:
- Time frame for completion of transactions (*transaction* means fulfillment of orders where goods are being sold and delivery of service where a service is being provided).
- Time frame and process for informing customers of exceptions to normal processing of orders or service requests.
- Normal method of delivery of goods or services, including customer options, where applicable.
- Payment terms, including customer options, if any.
- Electronic settlement practices and related charges to customers.
- How customers may cancel recurring charges, if any.
- Product return policies and limited liability, where applicable.

c. Where customers can obtain warranty, repair service, and support related to the goods and services purchased on its Web site.

d. Procedures for resolution of issues regarding processing integrity. These may relate to any part of a customer's e-commerce transaction, including complaints related to the quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints.

for an e-commerce system, refer to Appendix A (paragraph .42).]

For its non–e-commerce system, the entity has provided a system description to authorized users. [*For an example of a system description for a non–e-commerce based system, refer to Appendix B (paragraph .43).*]

2.2	The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.	The entity's processing integrity and related security commitments and required processing integrity and related security obligations of its customers and other external users are posted on the entity's Web site and/or as part of the entity's standard services agreement. For its internal users (employees and contractors), the entity's policies relating to processing integrity and security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's processing integrity and security policies. Obligations of contractors are detailed in their contract. A security awareness program has been implemented to communicate the entity's processing integrity and related security policies to employees. The entity publishes its IT security policies on its corporate intranet.
2.3	Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Management has assigned responsibilities for the enforcement of the entity's processing integrity policies to the chief financial officer (CFO). The security administration team is responsible for implementing the entity's security policies under the direction of the CIO. Others on the executive committee assist in the review and update of the policy as outlined in the executive committee handbook. The security administration team has custody of and is responsible for the day-to-day maintenance of the entity's security policies, and recommends changes to the CIO and the IT steering committee. Processing integrity and related security commitments are reviewed with the customer account managers as part of the annual IT planning process.
2.4	The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.	The process for customers and external users to inform the entity of possible processing integrity issues, security breaches, and other incidents is posted on the entity's Web site and/or is provided as part of the new user welcome kit. The entity's user training and security awareness programs include information concerning the identification of processing integrity issues and possible security breaches, and the process for informing the security administration team. Documented procedures exist for the identification and escalation of system processing integrity issues, security breaches, and other incidents.
2.5	Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.	Changes that may affect customers and users and their processing integrity and related security obligations or the entity's processing integrity and related security commitments are highlighted on the entity's Web site. Changes that may affect processing integrity and related system security are reviewed and approved by affected customers under the provisions of the standard services agreement before implementation of the proposed change. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee

		meetings. Changes to system components, including those that may affect system security, require the approval of the security administrator and the sponsor of the change before implementation. There is periodic communication of changes, including changes that affect system security. Changes are incorporated into the entity's ongoing user training and security awareness programs.
3.0	**Procedures: The entity uses procedures to achieve its documented system processing integrity objectives in accordance with its defined policies.**	
3.1	The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies. If the system is an e-commerce system, the entity's procedures include, but may not be limited to, the following matters: • The entity checks each request or transaction for accuracy and completeness. • Positive acknowledgment is received from the customer before the transaction is processed.	The entity has established data preparation procedures to be followed by user departments. Data entry screens contain field edits and range checks, and input forms are designed to reduce errors and omissions. Source documents are reviewed for appropriate authorizations before input. Error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected. Original source documents are retained on image management systems for a minimum of seven years, to facilitate the retrieval or reconstruction of data as well as to satisfy legal requirements. Logical access controls restrict data entry capability to authorized personnel. (See 3.5 in this table.) The customer account manager performs a regular review of customer complaints, back-order logs, and other transactional analysis. This information is compared to customer service agreements. The entity protects information from unauthorized access, modification, and misaddressing during transmission and transport using a variety of methods including: • Encryption of transmission information. • Batch header and control total reconciliations. • Message authentication codes and hash totals. • Private leased lines or virtual private networking connections with authorized users. • Bonded couriers and tamper-resistant packaging. Because of the Web-based nature of the input process, the nature of the controls to achieve the criterion set out in 3.1 may take somewhat different forms, such as: • Account activity, subsequent to successful login, is encrypted through a 128-bit secure sockets layer (SSL) session. • Web scripts contain error checking for invalid inputs. • The entity's order processing system contains edits, validity, and range checks, which are applied to each order to check for accuracy and completeness of information before processing. • Before a transaction is processed by the entity, the customer is presented with a request to confirm the intended transaction and the customer is required to click on the "Yes, please process this order" button before the transaction is processed. The entity e-mails an order confirmation to the customer-supplied e-

		mail address. The order confirmation contains order details, shipping and delivery information, and a link to an online customer order tracking service. Returned e-mails are investigated by customer service.
3.2	The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters:	Responsibility for order processing, application of credits and cash receipts, custody of inventory, user account management, and database management have been segregated. The entity's documented systems development life cycle (SDLC) methodology is used in the development of new applications and the maintenance of existing applications. The methodology contains required procedures for user involvement, testing, conversion, and management approvals of system processing integrity features.
	• The correct goods are shipped in the correct quantities in the time frame agreed upon, or services and information are provided to the customer as requested. • Transaction exceptions are promptly communicated to the customer.	Computer operations and job scheduling procedures exist, are documented, and contain procedures and instructions for operations personnel regarding system processing integrity objectives, policies, and standards. Exceptions require the approval of the manager of computer operations. The entity's application systems contain edit and validation routines to check for incomplete or inaccurate data. Errors are logged, investigated, corrected, and resubmitted for input. Management reviews error logs daily to ensure that errors are corrected on a timely basis. End-of-day reconciliation procedures include the reconciliation of the number of records accepted to the number of records processed to the number of records output.
	• Incoming messages are processed and delivered accurately and completely to the correct IP address. • Outgoing messages are processed and delivered accurately and completely to the service provider's (SP's) Internet access point. • Messages remain intact while in transit within the confines of the SP's network.	The following additional controls are included in the entity's e-commerce system: • Packing slips are created from the customer sales order and checked by warehouse staff as the order is packed. • Commercial delivery methods are used that reliably meet expected delivery schedules. Vendor performance is monitored and assessed periodically. • Service delivery targets are maintained and actual services provided are monitored against such targets. • The entity uses a feedback questionnaire to confirm customer satisfaction with completion of service or delivery of information to the customer. • Computerized back-order records are maintained and are designed to notify customers of back orders within 24 hours. Customers are given the option to cancel a back order or have an alternate item delivered. • Monitoring tools are used to continuously monitor latency, packet loss, hops, and network performance. • The organization maintains network integrity software and has documented network management policies. • Appropriately documented escalation procedures are in place to initiate corrective actions to unfavorable network performance.
3.3	The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented	Written procedures exist for the distribution of output reports that conform to the system processing integrity objectives, policies, and standards.

	system processing integrity policies. If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters: • The entity displays sales prices and all other costs and fees to the customer before processing the transaction. • Transactions are billed and electronically settled as agreed. • Billing or settlement errors are promptly corrected.	Control clerks reconcile control totals of transaction input to output reports daily, on both a system-wide and an individual customer basis. Exceptions are logged, investigated, and resolved. The customer service department logs calls and customer complaints. An analysis of customer calls, complaints, Back-order logs, and other transactional analysis and comparison to the entity's processing integrity policies are reviewed at monthly management meetings, and action plans are developed and implemented as necessary. The following additional controls are included in the entity's e-commerce system: • All costs, including taxes, shipping, and duty costs, and the currency used, are displayed to the customer. Customer accepts the order, by clicking on the "yes" button, before the order is processed. • Customers have the option of printing, before an online order is processed, an "order confirmation" for future verification with payment records (such as credit card statement) detailing information about the order (such as item(s) ordered, sales prices, costs, sales taxes, and shipping charges). • All foreign exchange rates are displayed to the customer before performing a transaction involving foreign currency. • Billing or settlement errors are followed up and corrected within 24 hours of reporting by the customer.
3.4	There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.	Input transactions are date and time stamped by the system and identified with the submitting source (user, terminal, IP address). Each order has a unique identifier that can be used to access order and related shipment and payment settlement information. This information can also be accessed by customer name and dates of order, shipping, or billing. The entity maintains transaction histories for a minimum of 10 years. Order history information is maintained online for three years and is available for immediate access by customer service representatives. After three years, this information is maintained in offline storage. Original source documents are retained on image management systems for a minimum of seven years, to facilitate the retrieval or reconstruction of data as well as to satisfy legal requirements. The entity performs an annual audit of tapes stored at the offsite storage facility. As part of the audit, tapes at the offsite location are matched to the appropriate tape management system.
	Security-related criteria relevant to the system's processing integrity	
3.5	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: *a*. Registration and authorization of new users. *b*. Identification and authentication of authorized users.	*a*. Registration and authorization of new users: • Customers can self-register on the entity's Web site, under a secure session in which they provide new user information and select an appropriate user identification (ID) and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality. • The ability to create or modify users and user access privileges (other than the limited functionality "customer accounts") is limited to the security administration team.

c. The process to make changes and updates to user profiles.

d. The process to grant system access privileges and permissions.

e. Distribution of output restricted to authorized users.

f. Restriction of logical access to offline storage, backup data, systems, and media.

g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

• The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Proper segregation of duties is considered in granting privileges.

b. Identification and authentication of users:

• Users are required to log on to the entity's network and application systems with their user ID and password before access is granted. Unique user IDs are assigned to individual users. Passwords must contain at least six characters, one of which is nonalphanumeric. Passwords are case sensitive and must be updated every 90 days.

c. Changes and updates to user profiles:

• Changes and updates to self-registered customer accounts can be done by the individual user at any time on the entity's Web site after the user has successfully logged onto the system. Changes are reflected immediately.

• Unused customer accounts (no activity for six months) are purged by the system.

• Changes to other accounts and profiles are restricted to the security administration team and require the approval of the appropriate line-of-business supervisor or customer account manager.

• Accounts for terminated employees are deactivated upon notice of termination being received from the human resources team.

d. The process to grant system access privileges and permissions:

• All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles.

• The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up.

e. Distribution of output:

• Access to computer processing output is provided to authorized individuals based on the classification of the information.

• Processing outputs are stored in an area that reflects the classification of the information.

f. Restriction of logical access to offline storage, backup data, systems, and media:

• Logical access to offline storage, backup data, systems, and media is limited to computer operations staff.

g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices:

• Hardware and operating system configuration tables are restricted to appropriate personnel.

• Application software configuration tables are restricted to authorized users and under the control of application change management software.

• Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff. Usage is logged and monitored by the manager of computer operations.

• The information security team, under the direction of the CIO, maintains access to firewall and other logs, as well as access to any storage media. Any access is logged and reviewed quarterly.

		• A listing of all master passwords is stored in an encrypted database and an additional copy is maintained in a sealed envelope in the entity safe.
3.6	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, offline storage media, backup media and systems, and other system components such as firewalls, routers, and servers.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals by card key systems and monitored by video surveillance. Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff. Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations. Documented procedures exist for the identification and escalation of potential security breaches. Offsite backup data and media are stored at service provider facilities. Access to offsite data and media requires the approval of the manager of computer operations.
3.7	Procedures exist to protect against unauthorized logical access to the defined system.	Login sessions are terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up by the security administrator. Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and passwords. Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator. Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions. Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.8	Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	In connection with other security monitoring, the security administration team participates in user groups and subscribes to services relating to computer viruses. Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated at least weekly. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.
3.9	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet	The entity uses 128-bit secure sockets layer (SSL) encryption for transmission of private or confidential information over public networks, including user ID and password. Users are required to upgrade their browser to the most current version tested and approved for use by the security administration team to avoid possible security

	or other public networks.	problems. Account activity, subsequent to successful login, is encrypted through a 128-bit SSL session. Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.
3.10	Procedures exist to identify, report, and act upon system processing integrity issues and related security breaches and other incidents.	Users are provided instructions for communicating system processing integrity issues and potential security breaches to the IT hotline. Processing integrity issues are escalated to the manager of computer operations. The information security team investigates security-related incidents reported through customer hotlines and e-mail. Production run and automated batch job scheduler logs are reviewed each morning and processing issues are identified, escalated, and resolved. Intrusion detection and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator via e-mail and pager of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. Documented incident identification and escalation procedures are approved by management.
3.11	Procedures exist to provide that issues of noncompliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	Computer operations team meetings are held each morning to review the previous day's processing. Processing issues are discussed, remedial action is taken, and additional action plans are developed, where necessary, and implemented. Standard procedures exist for the review, documentation, escalation, and resolution of system processing problems. Entity management routinely evaluates the level of performance it receives from the Internet service provider (ISP) which hosts the entity's Web site. This includes evaluating the security controls the ISP has in place by an independent third party as well as following up with the ISP management on any open items or causes for concern. Processing integrity and related security issues are recorded and accumulated in a problem report. Corrective action is noted and monitored by management. On a routine basis, processing integrity and related security policies, controls, and procedures are audited by the internal audit department. Results of such examinations are reviewed by management, a response is prepared, and a remediation plan is put in place.
	Criteria related to the system components used to achieve the objectives	
3.12	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to processing integrity and security are consistent with defined processing integrity and related security policies.	The entity has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The SDLC methodology includes a framework for assigning ownership of systems and classifying data. Process owners are involved in development of user specifications, solution selection, testing, conversion, and implementation. Owners of the information and data classify its sensitivity and determine the level of protection required to maintain an appropriate

		level of security. The security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's processing integrity and related security objectives, policies, and standards. Process owner review, approval of test results, and authorization are required for implementation of changes.
3.13	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security are qualified to fulfill their responsibilities.	A separate systems quality assurance group reporting to the CIO has been established. The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions. Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation. Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered. Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities. Personnel receive training and development in computer operations, system design and development, testing, and security concepts and issues. Procedures are in place to provide alternate personnel for key system processing functions in case of absence or departure.
	Maintainability-related criteria applicable to the system's processing integrity	
3.14	Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies.	Entity management receives a third-party opinion on the adequacy of security controls, and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site. The IT department maintains a listing of all software and the respective level, version, and patches that have been applied. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Staffing, infrastructure, and software requirements are periodically evaluated and resources are allocated consistent with the entity's processing integrity and related security policies. System configurations are tested annually, and evaluated against the entity's processing integrity and security policies and current service-level agreements. An exception report is prepared and remediation plans are developed and tracked. The IT steering committee, which includes representatives from the lines of business and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's processing integrity and related security policies, including the potential

		impact of legislative changes.
3.15	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Senior management has implemented a division of roles and responsibilities that segregates incompatible functions. The entity's documented systems development methodology describes the change initiation, software development and maintenance, and testing and approval processes, as well as the standards and controls that are embedded in the processes. These include programming, documentation, and testing standards. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Changes to system infrastructure and software are developed and tested in a separate development and test environment before implementation into production. As part of the change control policies and procedures, there is a "promotion" process (for example, from "test" to "staging" to "production"). Promotion to production requires the approval of the business owner who sponsored the change and the manager of computer operations. When changes are made to key systems components, there is a "backout" plan developed for use in the event of major interruption(s).
3.16	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process, including line-of-business approvals.
	Availability-related criteria applicable to the system's processing integrity	
3.17	Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.	A risk assessment is prepared and reviewed on a regular basis or when a significant change occurs in either the internal or external physical environment. Threats such as fire, flood, dust, power failure, excessive heat and humidity, and labor problems have been considered. Management maintains measures to protect against environmental factors (for example, fire, dust, power failure, and excessive heat and humidity) based on its risk assessment. The entity's controlled areas are protected against fire using both smoke detectors and a fire suppression system. 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 (UPS) and emergency power supplies (EPS). This equipment is tested semiannually.

		Preventive maintenance agreements and scheduled maintenance procedures are in place for key system hardware components. Vendor warranty specifications are complied with and tested to determine if the system is properly configured. Procedures to address minor processing errors, outages, and destruction of records are documented. Procedures exist for the identification, documentation, escalation, resolution, and review of problems. Physical and logical security controls are implemented to reduce the opportunity for unauthorized actions that could impair system processing integrity.
3.18	Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.	Management has implemented a comprehensive strategy for backup and restoration based on a review of business requirements. Backup procedures for the entity are documented and include redundant servers, daily incremental backups of each server, and a complete backup of the entire week's changes on a weekly basis. Daily and weekly backups are stored offsite in accordance with the entity's system policies. Disaster recovery and contingency plans are documented. The disaster recovery plan defines the roles and responsibilities and identifies the critical information technology application programs, operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on the business impact analysis. The business continuity planning (BCP) coordinator reviews and updates the business impact analysis with the lines of business annually. Disaster recovery and contingency plans are tested annually in accordance with the entity's system policies. Testing results and change recommendations are reported to the entity's management committee. The entity's management committee reviews and approves changes to the disaster recovery plan. All critical personnel identified in the business continuity plan hold current versions of the plan, both onsite and offsite. An electronic version is stored offsite.
3.19	Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.	Automated backup processes include procedures for testing the integrity of the backup data. Backups are performed in accordance with the entity's defined backup strategy, and usability of backups is verified at least annually. Backup systems and data are stored offsite at the facilities of a third-party service provider. Under the terms of its service provider agreement, the entity performs an annual verification of media stored at the offsite storage facility. As part of the verification, media at the offsite location are matched to the appropriate media management system. The storage site is reviewed biannually for physical access security and security of data files and other items. Backup systems and data are tested as part of the annual disaster recovery test.

4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.**	
4.1	System processing integrity and security performance is periodically reviewed and compared with the defined system processing integrity and related security policies.	System processing is monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Processing logs, performance and security incident statistics, and comparisons to approved targets are reviewed by the operations team daily and are accumulated and reported to the IT steering committee monthly. The customer service group monitors system processing and related customer complaints. It provides a monthly report of such matters together with recommendations for improvement, which are considered and acted on at the monthly IT steering committee meetings. The information security team monitors the system and assesses the system vulnerabilities using proprietary and other tools. Potential risk is evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementation is monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts processing integrity and system security reviews as part of its annual audit plan. Results and recommendations for improvement are reported to management.
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.	System processing is monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Processing logs and performance and security incident statistics and comparisons to approved targets are reviewed by the operations team daily and are accumulated and reported to the IT steering committee monthly. Future system processing performance and capacity requirements are projected and analyzed as part of the annual IT planning and budgeting process. Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its system processing integrity and related security objectives. Monthly IT staff meetings are held to address system processing, capacity, and security concerns and trends; findings are discussed at quarterly management meetings.
4.3	Environmental and technological changes are monitored and their impact on system processing integrity and security is assessed on a timely basis.	The entity's data center facilities include climate and environmental monitoring devices. Deviations from optimal performance ranges are escalated and resolved. Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's processing integrity and related security policies. The entity's customer service group monitors the impact of emerging technologies, customer requirements, and competitive activities.

Confidentiality Principle and Criteria

.25 The *confidentiality principle* focuses on information designated as confidential. Unlike personal information, which is being defined by regulation in a number of countries worldwide and is subject to the pri-

vacy principles (see paragraph .30), there is no widely recognized definition of confidential information. In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis. In most instances, the respective parties wish to ensure that the information they provide is available only to those individuals who need access to complete the transaction or resolution on any questions that arise. To enhance business partner confidence, it is important that the business partner is informed about the entity's confidentiality practices. The entity needs to disclose its practices relating to the manner in which it provides for authorized access to and uses and shares information designated as confidential.

.26 Examples of the kinds of information that may be subject to confidentiality include:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Client and customer lists
- Revenue by client and industry

.27 Also, unlike personal information, there are no defined rights of access to confidential information to ensure its accuracy and completeness. As a result, interpretations of what is considered to be confidential information can vary significantly from business to business and in most cases are driven by contractual arrangements. As a result, it is important for those engaged or expecting to be engaged in business relationships to understand and to accept what information is to be maintained on a confidential basis and what, if any, rights of access or other expectations an entity might have to update that information to ensure its accuracy and completeness.

.28 Information that is provided to another party is susceptible to unauthorized access during transmission and while it is stored on the other party's computer systems. For example, an unauthorized party may intercept business partner profile information and transaction and settlement instructions while they are being transmitted. Controls such as encryption can be used to protect the confidentiality of this information during transmission, whereas firewalls and rigorous access controls can help protect the information while it is stored on computer systems.

Confidentiality Principle and Criteria Table

.29 Information designated as confidential is protected as committed or agreed.

	Criteria	*Illustrative Controls*
1.0	**Policies: The entity defines and documents its policies related to the protection of confidential information.**	
1.1	The entity's system confidentiality and related security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their confidentiality and related security requirements. User requirements are documented in service-level agreements, nondisclosure agreements, or other documents. The security officer reviews the entity's confidentiality and related security policies annually and proposed changes as needed for the approval by the information technology (IT) standards committee, which includes representation from the customer service department.
1.2	The entity's policies related to the protection of confidential information and security include, but are not limited to, the following matters: *a.* Identification and documentation of the confidentiality and related security requirements of authorized users. *b.* Allowing access, the nature of that access, and who authorizes such access. *c.* Preventing unauthorized access. *d.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access. *e.* Assignment of responsibility and accountability for confidentiality and related security. *f.* Assignment of responsibility and accountability for system changes and maintenance. *g.* Testing, evaluating, and authorizing system components before implementation. *h.* Addressing how complaints and requests relating to confidentiality and related security issues are resolved. *i.* The procedures to handle confidentiality and related security breaches and other incidents. *j.* Provision for allocation for training and other resources to support its system confidentiality and related security policies. *k.* Provision for the handling of exceptions and situations not specifically addressed in its system confidentiality and related security	The entity's documented confidentiality and related security policies contain the elements set out in criterion 1.2.

	policies.	
	l. Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	
1.3	Responsibility and accountability for the entity's confidentiality and related security policies, and changes and updates to those polices, are assigned.	Management has assigned responsibilities for implementation of the entity's confidentiality policies to the vice president, human resources team. Responsibility for implementation of the entity's security policies has been assigned to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of the policies as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining confidentiality of and related security over such resources is defined.
2.0	**Communications: The entity communicates its defined policies related to the protection of confidential information to internal and external users.**	
2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	For its e-commerce system, the entity has posted a system description on its Web site. [*For an example of a system description for an e-commerce system, refer to Appendix A (paragraph .42).*] For its non–e-commerce system, the entity has provided a system description to authorized users. [*For an example of a system description for a non–e-commerce based system, refer to Appendix B (paragraph .43).*]
2.2	The confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters:	The entity's confidentiality and related security commitments and required confidentiality and security obligations of its customers and other external users are posted on the entity's Web site; or the entity's confidentiality policies and practices are outlined in its customer contracts, service-level agreements, vendor contract terms and conditions, and its standard nondisclosure agreement.
	a. How information is designated as confidential and ceases to be confidential.	Signed nondisclosure agreements are required before sharing information designated as confidential with third parties. Customer contracts, service-level agreements, and vendor contracts are negotiated before performance or receipt of service. Changes to the standard confidentiality provisions in these contracts require the approval of executive management.
	b. How access to confidential information is authorized.	For its internal users (employees and contractors), the entity's policies relating to confidentiality and security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's security policies. Confidentiality and security obligations of contractors are detailed in their contract.
	c. How confidential information is used.	A security awareness program has been implemented to communicate the entity's confidentiality and security policies to employees.
	d. How confidential information is shared.	The entity publishes its confidentiality and related security policies on its corporate intranet.

	e. If information is provided to third parties, disclosures include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity. *f.* Confidentiality practices needed to comply with applicable laws and regulations.	
2.3	Responsibility and accountability for the entity's confidentiality and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	The security administration team is responsible for implementing the entity's confidentiality and related security policies under the direction of the CIO. The security administration team has custody of and is responsible for the day-to-day maintenance of the entity's confidentiality and related security policies, and recommends changes to the CIO and the IT steering committee. Confidentiality and related security commitments are reviewed with the customer account managers as part of the annual IT planning process.
2.4	The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.	The process for customers and external users to inform the entity of possible confidentiality or security breaches and other incidents is posted on the entity's Web site and/or is provided as part of the new user welcome kit. The entity's security awareness program includes information concerning the identification of possible confidentiality and security breaches and the process for informing the security administration team. Documented procedures exist for the identification and escalation of possible confidentiality or security breaches and other incidents.
2.5	Changes that may affect confidentiality and system security are communicated to management and users who will be affected.	Changes that may affect customers and users and their confidentiality and related security obligations or the entity's confidentiality and security commitments are highlighted on the entity's Web site. Changes that may affect confidentiality and system security are reviewed and approved by affected customers under the provisions of the standard services agreement before implementation of the proposed change. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee meetings. Changes to system components, including those that may affect system security, require the approval of the security administrator before implementation. There is periodic communication of changes, including changes that may affect confidentiality and system security. Changes that affect confidentiality or system security are incorporated into the entity's ongoing security awareness program.
3.0	**Procedures: The entity uses procedures to achieve its documented confidentiality objectives in ac-**	

	cordance with its defined policies.	
3.1	The entity's procedures provide that confidential information is disclosed to parties only in accordance with its defined confidentiality and related security policies.	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has access. Logical access controls are in place that limit access to confidential information based on job function and need. Requests for access privileges to confidential data require the approval of the data owner. Business partners are subject to nondisclosure agreements (NDAs) or other contractual confidentiality provisions.
3.2	The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined confidentiality and related security policies, and that the third party is in compliance with its policies.	The entity outsources technology support or service and transfers data to an outsource provider. The requirements of the service provider with respect to confidentiality of information provided by the entity are included in the service contract. Legal counsel reviews third-party service contracts to assess conformity of the service provider's confidentiality provisions with the entity's confidentiality policies. The entity obtains representation about the controls that are followed by the outsource provider and obtains a report on the effectiveness of such controls from the outsource provider's independent auditor.
3.3	In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, the entity has procedures to protect confidential information in accordance with the confidentiality practices in place when such information was received, or obtains customer consent to follow the new confidentiality practice with respect to the customer's confidential information.	Changes to confidentiality provisions in business partner contracts are renegotiated with the business partner. When changes to a less restrictive policy are made, the entity attempts to obtain the agreement of its customers to the new policy. Confidential information for those customers who do not agree to the new policy is either removed from the system and destroyed or isolated and receives continued protection under the old policy.
	Security-related criteria relevant to confidentiality	
3.4	Procedures exist to restrict logical access to confidential information including, but not limited to, the following matters: *a.* Registration and authorization of new users. *b.* Identification and authentication of all users. *c.* The process to make changes and updates to user profiles. *d.* The process to grant system access privileges and permissions.	*a.* Registration and authorization of new users: • Customers can self-register on the entity's Web site, under a secure session in which they provide new user information and select an appropriate user identification (ID) and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality. • The ability to create or modify users and user access privileges (other than the limited functionality "customer accounts") is limited to the security administration team. • The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Confidentiality and proper segregation of duties are considered in granting privileges. *b.* Identification and authentication of users:

e. Procedures to prevent customers, groups of individuals, or other entities from accessing other than their own confidential information.	• Users are required to log on to the entity's network and application systems with their user ID and password before access is granted. Unique user IDs are assigned to individual users. Passwords must contain at least six characters, one of which is nonalphanumeric. Passwords are case sensitive and must be updated every 90 days. *c.* Changes and updates to user profiles:
f. Procedures to limit access to confidential information to only authorized employees based upon their assigned roles and responsibilities.	
g. Distribution of output containing confidential information restricted to authorized users.	• Changes and updates to self-registered customer accounts can be done by the individual user at any time on the entity's Web site after the user has successfully logged onto the system. Changes are reflected immediately. • Unused customer accounts (no activity for six months) are purged by the system.
h. Restriction of logical access to offline storage, backup data, systems, and media.	
i. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	• Changes to other accounts and profiles are restricted to the security administration team and require the approval of the appropriate line-of-business supervisor or customer account manager.
	• Accounts for terminated employees are deactivated upon notice of termination being received from the human resources team. *d.* The process to grant system access privileges and permissions: • All paths that allow access to significant information resources are controlled by the access control system and operating system facilities. Access requires users to provide their user ID and password. Privileges are granted to authenticated users based on their user profiles. • The login session is terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up. *e.* Restriction of access to information of other customers: • Corporate customers are assigned a unique company identifier that is required as part of the login process. Logical access software is used to restrict user access based on the company identifier used at login. • Individual customers are restricted to their own information based on their unique user ID. *f.* Restriction of access to confidential information: • Requests for privileges to access confidential customer information require the approval of the customer account manager. • Simulated customer data is used for system development and testing purposes. Confidential customer information is not used for this purpose. *g.* Distribution of output: • Access to computer processing output is provided to authorized individuals based on the classification of the information. • Processing outputs are stored in an area that reflects the classification of the information. *h.* Restriction of logical access to offline storage, backup data, systems, and media: • Logical access to offline storage, backup data, systems, and media is limited to computer operations staff. *i.* Restriction of access to system configurations, superuser

		functionality, master passwords, powerful utilities, and security devices: • Hardware and operating system configuration tables are restricted to appropriate personnel. • Application software configuration tables are restricted to authorized users and under the control of application change management software. • Utility programs that can read, add, change, or delete data or programs are restricted to authorized technical services staff. Usage is logged and monitored by the manager of computer operations. • The information security team, under the direction of the CIO, maintains access to firewall and other logs, as well as access to any storage media. Any access is logged and reviewed quarterly. • A listing of all master passwords is stored in an encrypted database and an additional copy is maintained in a sealed envelope in the entity safe.
3.5	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware such as firewalls and routers, is restricted to authorized individuals by card key systems and monitored by video surveillance. Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff. Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations. Documented procedures exist for the identification and escalation of potential security breaches. Offsite backup data and media are stored at service provider facilities. Access to offsite data and media requires the approval of the manager of computer operations.
3.6	Procedures exist to protect against unauthorized logical access to the defined system.	Login sessions are terminated after three unsuccessful login attempts. Terminated login sessions are logged for follow-up by the security administrator. Virtual private networking (VPN) software is used to permit remote access by authorized users. Users are authenticated by the VPN server through specific "client" software and user ID and passwords. Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator. Unneeded network services (for example, telnet, ftp, and http) are deactivated on the entity's servers. A listing of the required and authorized services is maintained by the IT department. This list is reviewed by entity management on a routine basis for its appropriateness for the current operating conditions. Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.

3.7	Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	In connection with other security monitoring, the security administration team participates in user groups and subscribes to services relating to computer viruses. Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated at least weekly. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.
3.8	A minimum of 128-bit encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks.	The entity uses 128-bit secure sockets layer (SSL) encryption for transmission of private or confidential information over public networks, including user ID and password. Users are required to upgrade their browser to the most current version tested and approved for use by the security administration team to avoid possible security problems. Account activity, subsequent to successful login, is encrypted through a 128-bit SSL session. Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity. Confidential information submitted to the entity over its trading partner extranet is encrypted using 128-bit SSL. Transmission of confidential customer information to third-party service providers is done over leased lines.
3.9	Procedures exist to identify, report, and act upon confidentiality and security breaches and other incidents.	Users are provided instructions for communicating potential confidentiality and security breaches to the information security team. The information security team logs incidents reported through customer hotlines and e-mail. Intrusion detection and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator via e-mail and pager of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. Documented incident identification and escalation procedures are approved by management.
3.10	Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	Security and confidentiality problems are reported immediately to the customer account manager, recorded, and accumulated in a problem report. Corrective action, decided upon in conjunction with the customer account manager, is noted and monitored by management. The vice president, customer services is responsible for assessing the customer service impact of potential confidentiality breaches and coordinating response activities. On a routine basis, security policies, controls, and procedures are audited by the internal audit department. Results of such examinations are reviewed by management, a response is prepared, and a remediation plan is put in place.
	Criteria related to the system components used to achieve the objectives	
3.11	Design, acquisition, implementation, configuration, modification, and management of infrastructure	The entity has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information

	and software related to confidentiality and security are consistent with defined confidentiality and related security policies.	systems and related technology. The SDLC methodology includes a framework for classifying data, including customer confidentiality requirements. Standard user profiles are established based on customer confidentiality requirements and an assessment of the business impact of the loss of security. Users are assigned standard profiles based on needs and functional responsibilities. Internal information is assigned to an owner based on its classification and use. Customer account managers are assigned as custodians of customer data. Owners of internal information and custodians of customer information and data classify its sensitivity and determine the level of protection required to maintain an appropriate level of confidentiality and security. The security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's confidentiality and related security policies. Changes to system components that may affect security require the approval of the security administration team. The access control and operating system facilities have been installed, including the implementation of options and parameters, to restrict access in accordance with the entity's confidentiality and related security policies. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.12	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting confidentiality and security are qualified to fulfill their responsibilities.	The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions. Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are offered employment subject to background checks and reference validation. Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered. Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities. Personnel receive training and development in system confidentiality and security concepts and issues. Procedures are in place to provide alternate personnel for key system confidentiality and security functions in case of absence or departure.
	Maintainability-related criteria relevant to confidentiality	
3.13	Procedures exist to maintain system components, including configurations consistent with the defined system confidentiality and related security policies.	Entity management receives a third-party opinion on the adequacy of security controls, and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site. The IT department maintains a listing of all software and the re-

		spective level, version, and patches that have been applied. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Staffing, infrastructure, and software requirements are periodically evaluated and resources are allocated consistent with the entity's confidentiality and related security policies. System configurations are tested annually, and evaluated against the entity's security policies and current service-level agreements. An exception report is prepared and remediation plans are developed and tracked. The IT steering committee, which includes representatives from the lines of business and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's confidentiality and related security policies, including the potential impact of legislative changes.
3.14	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Senior management has implemented a division of roles and responsibilities that segregates incompatible functions. The entity's documented systems development methodology describes the change initiation, software development and maintenance, and approval processes, as well as the standards and controls that are embedded in the processes. These include programming, documentation, and testing standards. Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation into production. As part of the change control policies and procedures, there is a "promotion" process (for example, from "test" to "staging" to "production"). Promotion to production requires the approval of the business owner who sponsored the change and the manager of computer operations. When changes are made to key systems components, there is a "backout" plan developed for use in the event of major interruption(s).
3.15	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change management procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process,

		including line-of-business approvals.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with its defined confidentiality policies.**	
4.1	The entity's confidentiality and security performance is periodically reviewed and compared with the defined confidentiality and related security policies.	The information security team monitors the system and assesses the system's vulnerabilities using proprietary and other tools. Potential risk is evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementation is monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts system security reviews as part of its annual audit plan. Results and recommendations for improvement are reported to management.
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its confidentiality and related security policies.	Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its system confidentiality and related security objectives. Monthly IT staff meetings are held to address system security concerns and trends; findings are discussed at quarterly management meetings.
4.3	Environmental and technological changes are monitored and their impact on confidentiality and security is assessed on a timely basis.	Trends and emerging technologies and their potential impact on customer confidentiality requirements are reviewed with corporate customers as part of the annual performance review meeting. Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's confidentiality and related security policies. The entity's customer service group monitors the impact of emerging technologies, customer requirements, and competitive activities.

Privacy Principles and Criteria

.30 This section provides a brief overview and privacy concepts, objectives and principles. The complete set of privacy principles is contained in *Generally Accepted Privacy Principles—A Global Privacy Framework* (GAPP) found in Appendix D [paragraph .45].

.31 The *privacy principles*, which are included in GAPP, focus on protecting the personal information an organization may collect about its customers, employees and other individuals. Generally Accepted Privacy Principles have been developed from a business perspective, referencing significant domestic and international privacy regulations. GAPP operationalizes complex privacy requirements into a single privacy objective that is supported by ten privacy principles.

Privacy Concepts

Privacy Definition

.32 Under Generally Accepted Privacy Principles, 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

.33 *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., a Social Security or Social Insurance Number)
- Physical characteristics
- Consumer purchase history

.34 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

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

.36 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 cannot be linked to an individual.

Privacy or Confidentiality?

.37 As discussed in the Confidentiality Principle, personal information is different from confidential information. Unlike personally identifiable information, which is often defined by regulation in a number of

countries worldwide, there is no single definition of confidential information that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires to be maintained on a "need to know" basis.

Generally Accepted Privacy Principles

Overall Privacy Objective

.38 Generally Accepted Privacy Principles are founded on the following privacy objective:

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

The Privacy Principles

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

The following are the 10 Generally Accepted Privacy Principles:

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

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

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

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

5. Use 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 for Privacy. The entity protects personal information against unauthorized access (both physical and logical).

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

10. Monitoring and Enforcement. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

For each of the 10 privacy principles, relevant, objective, complete, and measurable criteria have been developed for evaluating an entity's privacy policies, communications, and procedures and controls.

.40 These criteria are set forth in a separate publication *Generally Accepted Privacy Principles—A Global Privacy Framework.*

Online Privacy Engagements

.41 When the privacy engagement relates to an online segment, an entity may choose to display a WebTrust Online Privacy seal. For these engagements, the scope needs to include, as a minimum, an online business segment of the entity. For additional considerations see Appendix C of the GAPP document.

Appendix A

Illustrative Disclosures for E-Commerce Systems

This appendix sets out illustrative disclosures for electronic commerce (e-commerce) systems that are required to meet the Trust Services principles. The disclosures are set out separately by Trust Services principles; they are illustrative only and should be tailored according to the particular organization's system.

System Description

Rather than addressing the components of a system (used for describing non–e-commerce systems), an organization may describe the functionality of the system covered by the WebTrust examination, as follows:

> Example System Description
>
> Our site (abc-xyz.org) enables users to create and manage their own online store (myABC-xyz.org). It also covers the back-end fulfillment and settlement systems that integrate with abc-xyx.org to facilitate ordering from customer sites created on our site and the use of third-party service providers with which we have contracted to provide various services related to our site.
>
> Entrepreneurs and small business owners can use the abc-xyz.org suite of business services to take advantage of the online world. abc-xyz.org's Web browser interface can be used to create your own online store (complete with product ordering). You design the site and control the customer experience.
>
> The WebTrust seal covers the functionality set out in our abc-xyz.org site that allows users to create and manage their own online store. It also covers the back-end fulfillment and settlement systems that integrate with abc-xyz.org to facilitate ordering from customer sites created on abc-xyz.org, myABC-xyz.org – e-commerce and Web publishing made easy. Entrepreneurs and small business owners can use the abc-xyz.org suite of business services to take advantage of the convenience, reach, and speed of the online world. myABC-xyz.org's simple Web browser interface can be used to create your own online store (complete with secure ordering) within minutes. You design the site, control the customer experience, list the products, and fulfill orders in a secure environment.

Disclosures Related to Specific Principles and Criteria

The following tables set out illustrative disclosures for e-commerce systems.

Criteria Reference		*Illustrative Disclosures*
Security		
2.2	The security obligations of users and the entity's security commitments to users are communicated to authorized users.	Even though we strive to protect the information you provide through ABC.com, no data transmission over the Internet can be guaranteed to be 100 percent secure. As a result, even though we strive to protect your information, we cannot ensure or warrant the security of any information you transmit to or receive from us through our Web site and online services. We review our security policies on a regular basis, and changes

		are made as necessary. They undergo an intense review on an annual basis by the information technology (IT) department. These defined security policies detail access privileges, information collection needs, accountability, and other such matters. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service-level agreements. For example, only a select group of authorized individuals within ABC have access to user information. A complete policy with details regarding access, scripting, updates, and remote access is available for review by qualified personnel within the organization. This document is not available to the general public for study. ABC.com operates secure data networks that are password-protected and are not available to the public. When transmitting information between you and ABC.com, data security is handled through a security protocol called secured sockets layer (SSL). SSL is an Internet security standard using data encryption and Web server authentication. Encryption strength is measured by the length of the key used to encrypt the data; that is, the longer the key, the more effective the encryption. Using the SSL protocol, data transmission between you and the ABC.com server is performed at a 128-bit level of encryption strength.
2.4	The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.	Should you feel that there has been a breach to the security of this site, please contact us *immediately* at (800) 123-1234.
2.5	Changes that may affect system security are communicated to management and users who will be affected.	Any changes that affect the security of our Web site as it affects you as a site user will be communicated to you by posting the highlight of the change to the Web page that summarizes our security policies and significant controls.
Availability		
2.2	The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	To allow sufficient time for file maintenance and backup, the maximum number of hours per day that our network will be made available is 22 hours per day, 7 days a week. In the event of a disaster or other prolonged service interruption, the entity has arranged for the use of alternative service sites to allow for full business resumption within 24 hours. Our company's defined security policies detail access privileges, information collection needs, accountability, and other such matters. They are reviewed and updated at quarterly management meetings and undergo an intense review on an annual basis by the information technology (IT) department. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service-level agreements. For example, current policy prohibits shared identifications (IDs); each support person has his or her own unique ID to log on and maintain network equipment. A complete policy with details regarding access, scripting, updates, and remote access is available for review by qualified personnel. This document will not be released to the general public for study.
2.4	The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communi-	Management has in place a consumer hotline to allow customers to telephone in any comments, complaints, or concerns regarding the security of the site and availability of the system. If you are unable to obtain access to this site, please contact our customer

	cated to authorized users.	support personnel at (800) 123-2345. Should you believe that there has been a breach to the security of this site please contact us *immediately* at (800) 123-1234.
2.5	Changes that may affect system availability and system security are communicated to management and users who will be affected.	Highlights of any changes that affect the security of our Web site and availability of the system as it affects you as a site user will be communicated to you by e-mail seven days in advance of the anticipated change. The highlights of the change will be posted to the Web page that summarizes our availability and security policies.
Processing Integrity		
2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users. If the system is an e-commerce system, additional information provided on its Web-site includes, but may not be limited to, the following matters:	You can purchase new and used books on our site; used books are clearly labeled as such. The mortgage rate information we obtain for your brokerage transaction is gathered from 12 different lending institutions on a daily basis. A complete listing of these lending institutions can be obtained by clicking here [*insert hot link/URL*]. ABC's Online RFQ Brokerage is the online clearing house for requests for quotes (RFQ) on custom-made parts. Through our unique service, OEM manufacturers looking for parts will be connected to contract manufacturers looking for work.
	a. Descriptive information about the nature of the goods or services that will be provided, including, where appropriate:	RFQs published on our online brokerage undergo an intensive review process to ensure that contract manufacturers get all the information needed to compose a quote. ABC's trained personnel will work closely with OEM manufacturers new to the outsourcing market to ease their fears.
	• Condition of goods (meaning, whether they are new, used, or reconditioned).	Contract manufacturers participating in the RFQ bidding process are members of ABC's BizTrust program. New members are subjected to an assortment of checks such as credit checks and reference checks to ensure that they are qualified to bid on RFQs. The results from these checks are organized into an easy-to-read BizTrust Report accessible by all members of ABC.
	• Description of services (or service contract).	The nationwide survey, conducted by the compensation-research firm of Dowden & Co., presents data on 20X2 compensation gathered from among more than 900 employers of information systems professionals, including corporations of all sizes, in every industry group, and from every U.S. region. The survey was completed July 20X1.
	• Sources of information (meaning, where it was obtained and how it was compiled).	Our policy is to ship orders within one week of receipt of a customer-approved order. Our experience is that over 90 percent of our orders are shipped within 48 hours; the remainder is shipped within one week.
	b. The terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following matters: • Time frame for completion of transactions (*transaction* means fulfillment of orders where goods are being sold and delivery of service where a service is being provided).	We will notify you by e-mail within 24 hours if we cannot fulfill your order as specified at the time you placed it and will provide you the option of canceling the order without further obligation. You will not be billed until the order is shipped. You have the option of downloading the requested information now or we will send it to you on CD-ROM by UPS two-day or Federal Express overnight delivery. Credit approval is required before shipment. All goods will be invoiced on shipment according to either our normal terms of settlement (net 30 days), or where alternative contractual arrangements are in place, those arrangements shall prevail.
	• Time frame and process for informing customers of exceptions to normal processing of orders or ser-	We require an electronic funds transfer of fees and costs at the end of the transaction. For new customers, a deposit may be required.

	vice requests.	To cancel your monthly service fee, send us an e-mail at Subscriber@ABC.com or call us at (800) 555-1212. Be sure to include your account number.
	• Normal method of delivery of goods or services, including customer options, where applicable.	Purchases can be returned for a full refund within 30 days of receipt of shipment. Call our toll-free number or e-mail us for a return authorization number, which should be written clearly on the outside of the return package.
	• Payment terms, including customer options, if any.	Warranty and other service can be obtained at any one of our 249 locations worldwide that are listed on this Web site. A list of these locations is also provided with delivery of all of our products.
	• Electronic settlement practices and related charges to customers.	Transactions at this site are covered by binding arbitration conducted through our designated arbitrator [*name of arbitrator*]. They can be reached at www.name.org or by calling toll-free (800) 111-2222. For the details of the terms and conditions of arbitration, click here [*insert hot link/URL*].
	• How customers may cancel recurring charges, if any.	Our process for consumer dispute resolution requires that you contact our customer toll-free hotline at (800) 555-1234 or contact us via e-mail at custhelp@ourcompany.com. If your problem has not been resolved to your satisfaction you may contact the Cyber Complaint Dispute Resolution Association, which can be reached at (877) 123-4321 during normal business hours (8:00 a.m. – 5:00 p.m. central time) or via their Web site at www.ccomplaint.com.
	• Product return policies and limited liability, where applicable.	For the details of the terms and conditions of arbitration, click here [*insert hot link/URL*]. For transactions at this site, should you, our customer, require follow-up or response to your questions or complaints, you may contact us at www.xxxquestions.org. If your follow-up or your complaint is not handled to your satisfaction, you should contact the e-commerce ombudsman who handles consumer complaints for e-commerce in this country. He or she can be reached at www.ecommercombud.org or by calling toll-free at (800) XXX-XXXX.
	c. Where customers can obtain warranty, repair service, and support related to the goods and services purchased on its Web site. *d.* Procedures for resolution of issues regarding processing integrity. These may relate to any part of a customer's e-commerce transaction, including complaints related to the quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints.	
2.2	The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.	Our company's defined processing integrity policies and related security policies are communicated to all authorized users of the company. The security policies detail access privileges, information collection needs, accountability, and other such matters. They are reviewed and updated at quarterly management meetings and undergo an intense review on an annual basis by the information technology (IT) department. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service-level agreements. For example, current policy prohibits shared identifications (IDs); each support person has his or her own unique ID to log on and maintain network equipment. A complete policy with

		details regarding access, scripting, updates, and remote access is available for review by qualified personnel. This document will not be released to the general public for study.
2.4	The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.	For service and other information, contact one of our customer service representatives at (800) 555-1212 between 7:00 a.m. and 8:00 p.m. (central standard time) or you can write to us as follows: Customer Service Department ABC Company 1234 Anystreet Anytown, Illinois 60000 or CustServ@ABC.com Should you believe that there has been a breach to the integrity or security of this site, please contact us *immediately* at (800) 123-1234.
2.5	Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.	Highlights of any changes that affect the security of our Web site and processing integrity of the system as it affects you as a site user will be communicated to you by e-mail seven days in advance of the anticipated change. The highlights of the change will be posted to the Web page that summarizes our processing integrity and security policies.
Confidentiality		
2.2	The confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters:	XYZ manufacturing.com is a high-quality custom manufacturer of electronic components. Customers and potential customers can submit engineering drawings, specifications, and requests for manufacturing price quotes through our Web site or e-mail.
	a. How information is designated as confidential and ceases to be confidential.	Access to your information is limited to our employees and any third-party subcontractors we may elect to use in preparing our quote. We will not use any information you provide for any purpose other than a price quote and subsequent manufacturing and order fulfillment on your behalf. However, access may need to be provided in response to subpoenas, court orders, legal process, or other needs to comply with applicable laws and regulations.
	b. How access to confidential information is authorized.	Using our encryption software, you may designate information as confidential by checking the "Confidential Treatment" box. This software can be downloaded from our site and will accept information in most formats. Such information will automatically be encrypted using our public key before transmission over the Internet. You may transmit such information to us through our Web site or by e-mail.
	c. How confidential information is used.	Access to information designated as confidential will be restricted only to our employees with a need to know. We will not provide such information to third parties without your prior permission.
	d. How confidential information is shared.	When we provide information to third parties, we do not provide your company name. However, we make no representation regarding third-party confidential treatment of such information.
	e. If information is provided to third parties, disclosures include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity.	Our confidentiality protection is for a period of two years, after which we will cease to provide such protection. In addition, should such information become public through your actions or other means, our confidentiality protection ceases.

	f. Confidentiality practices needed to comply with applicable laws and regulations.	If you are not a customer at the time of submitting such information, you will be provided with an account number and password. You may use this account number and password to access the information you have submitted, plus any related price quote information provided by us. You may also set up an additional 10 subaccounts and passwords so others in your organization can also access this information. Our services and the protection of confidential information are subject to third-party dispute resolution. This process is described under "Arbitration Process" elsewhere on our Web site
2.4	The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.	If you have any questions about our organization or our policies on confidentiality as stated at this site, please contact CustServ@XYZ-manufacturing.com. Should you feel that there has been a breach to the security of this site, please contact us *immediately* at (800) 123-1234.
2.5	Changes that may affect confidentiality and system security are communicated to management and users who will be affected.	Effective January 200X, we eliminated our "secret" category of information. Information submitted under such secret category will continue to be protected in accordance with our commitments at that time.

Privacy

See Generally Accepted Privacy Principles in Appendix D [paragraph .45] for related criteria.

Appendix B

Example System Description for Non-E-Commerce Systems

The purpose of a system description is to delineate the boundaries of the system covered by management's assertion or the subject matter of the practitioner's report (in this example, a pension processing service). The system description should be an integrated part of the entity's communication of policies related to the specific principles subject to the practitioner's attestation. In all cases, the system description should accompany the practitioner's report.

Background

XYZ Co. Pension Services (XPS), based in New York, New York, with offices across North America, manages and operates the Pension Administration System (PAS) on behalf of pension plan sponsors who are XPS Co.'s customers. The plan members are the employees of XPS Co.'s customers who are enrolled in the pension plan. XPS uses PAS for recordkeeping of pension-related activities.

Infrastructure

PAS uses a three-tier architecture, including proprietary client software, application servers, and database servers.

Various peripheral devices, such as tape cartridge silos, disk drives, and laser and impact printers, are also used.

Software

The PAS application was developed by programming staff in XITD's (XYZ Co.'s Information Technology Department) Systems Development and Application Support area. PAS enables the processing of contributions to members' pension plans and withdrawals at retirement, based on plan rules. PAS generates all the required reports for members, plan sponsors, and tax authorities. PAS also provides a facility to record investments and related transactions (purchases, sales, dividends, interest, and other miscellaneous transactions). Batch processing of transactions is performed nightly.

PAS provides a facility for online data input and report requests. In addition, PAS accepts input from plan sponsors in the form of digital or magnetic media or files transmitted via the telecommunications infrastructure.

People

XPS has a staff of approximately 200 employees organized in the following functional areas:

- Pension administration includes a team of specialists for set-up of pension rules, maintenance of master files, processing of contributions to PAS, reporting to plan sponsors and members, and assistance with inquiries from plan members;

- Financial operations is responsible for processing of withdrawals, deposit of contributions and investment accounting;

- Trust accounting is responsible for bank reconciliation; and

- Investment services is responsible for processing purchases of stocks, bonds, certificates of deposits, and other financial instruments.

XITD has a staff of approximately 50 employees who are dedicated to PAS and related infrastructure and are organized in the following functional areas:

- The help desk provides technical assistance to users of PAS and other infrastructure, as well as plan sponsors.

- Systems development and application support provides application software development and testing for enhancements and modifications to PAS.

- Product support specialists prepare documentation manuals and training material.

- Quality assurance monitors compliance with standards, and manages and controls the change migration process.

- Information security and risk is responsible for security administration, intrusion detection, security monitoring, and business-recovery planning.

- Operational services performs day-to-day operation of servers and related peripherals.

- System software services installs and tests system software releases, monitors daily system performance, and resolves system software problems.

- Technical delivery services maintains job scheduling and report distribution software, manages security administration, and maintains policies and procedures manuals for the PAS processing environment.

Voice and data communications maintains the communication environment, monitors the network and provides assistance to users and plan sponsors in resolving communication problems and network planning.

Procedures

The pension administration services covered by this system description include:

- Pension master file maintenance.

- Contributions.

- Withdrawals.

- Investment accounting.

- Reporting to members.

These services are supported by XYZ Co.'s Information Technology Department (XITD), which supports PAS 24 hours a day, 7 days a week. The key support services provided by XITD include:

- Systems development and maintenance.
- Security administration and auditing.
- Intrusion detection and incident response.
- Data center operations and performance monitoring.
- Change controls.
- Business recovery planning.

Data

Data, as defined for the PAS, constitutes the following:

- Master file data.
- Transaction data.
- Error and suspense logs.
- Output reports.
- Transmission records.
- System and security files.

Transaction processing is initiated by the receipt of paper documents, electronic media, or calls to XYZ's call center. Transaction data are processed by PAS in either online or batch modes of processing, and are used to update master files. Output reports are available either in hard copy or through a report-viewing facility to authorized users based on their job functions. Pension statement and transaction notices are mailed to plan sponsors and members.

Appendix C

Practitioner Guidance on Scoping and Reporting Issues

This appendix deals with issues related to engagement planning, performance, and reporting using the Trust Services principles and criteria. It does not deal with reporting issues under the WebTrust® Program for Certification Authorities. This has been separately considered and issued. [fn 1]

Specifically, this section deals with:

- Engagement elements
- The practitioner's report.
- Reporting on multiple principles
- Additional reporting guidance
- Agreed-upon procedure engagements
- Other matters

As Trust Services attestation or audit reports are issued under Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended, the practitioner should be familiar with the relevant standards.

Engagement Elements

Trust Services Principles

Trust Services provides for a modular approach using five different principles—security, availability, processing integrity, confidentiality, and privacy. It is possible for the client to request a separate Trust Services examination that covers one or any combination of the principles. Principles provide the basis for describing various aspects of the system under examination with logical groupings of suitable criteria.

Trust Services Criteria

Criteria are the benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter.

Under the U.S. attestation standards, [fn 2] suitable criteria must have each of the following attributes:

[fn 1] Audit reporting for certification authorities is dealt with in TSP section 200, *Trust Services Principles, Criteria, and Illustrations for WebTrust® for Certification Authorities*.

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

The Trust Services criteria meet the requirement for being suitable criteria and are the result of a public exposure and comment process.

Management's Assertion

Under AICPA attestation standards, management must provide the practitioner with a written assertion or the practitioner will be required to modify his or her report. [fn 3] Specifically, management asserts that, during the period covered by the report and based on the AICPA/CICA Trust Services criteria, it maintained effective controls over the system under examination to satisfy the stated Trust Services principle(s). For engagements covering only certain principles, management's assertion should only address the principles covered by the engagement.

In a WebTrust engagement, the practitioner is engaged to examine both that an entity complied with the Trust Services criteria and that it maintained effective controls over the system based on the Trust Services criteria. In order to receive a WebTrust seal, both compliance and operating effectiveness must be addressed. This differs from a SysTrust® engagement in which the practitioner is engaged to examine only that an entity maintained effective controls over the system under examination based on the Trust Services criteria.

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

[fn 2] See Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10: *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101.24).

[fn 3] See Chapter 1 of SSAE No. 10 (AT sec. 101.58) for a description of a practitioner's options, if a written assertion is not obtained.

[fn 4] See Chapter 1 of SSAE No. 10 (AT sec. 101.64).

If one or more criteria have not been achieved, the practitioner issues a qualified or adverse report. Under AICPA attestation standards, when issuing a qualified or adverse report the practitioner should report directly on the subject matter rather than on the assertion.

Period of Coverage

The practitioner's report and management's assertion (when required) always should specify the time period covered by the report and assertion, respectively. A practitioner may issue a report for a period of time or at a point in time. The determination of an appropriate period should be at the discretion of the practitioner and the entity.

Factors to be considered in establishing the reporting period may include the following:

- The anticipated users of the report and their needs.
- The need to support a "continuous" audit model.
- The degree and frequency of change in each of the system components.
- The cyclical nature of processing within the system.
- Historical information about the system.

For WebTrust or SysTrust seals on Web sites, the report must be refreshed at least every 12 months. A three-month grace period is permitted from the end of the reporting period to allow for the practitioner to complete the fieldwork and prepare the report. For example, if the current report is for the period ending December 31, 20X2, the next report must be for a period ending no later than December 31, 20X3, and must be posted no later than March 31, 20X4. In this example, the first report may continue to be posted to the client's Web site until March 31, 20X4.

The Practitioner's Report

There are a variety of reporting alternatives that are discussed below.

Reporting on the Entity's Controls to Achieve the Criteria

This reporting alternative provides an opinion on the operating effectiveness of controls based on one or more Trust Services principle(s) and criteria. The practitioner can issue either a SysTrust report (and corresponding seal), if applicable, or a Trust Services report. A WebTrust report (and corresponding seal) cannot be issued for this type of engagement since the practitioner is not also reporting on whether the entity has complied with the criteria.

Reporting on the Entity's Having Complied With the Criteria

This reporting alternative provides an opinion on the operating effectiveness of controls based on one or more Trust Services principle(s) and criteria and whether the entity complied with the criteria. In this type of engagement, the practitioner can issue either a WebTrust or a SysTrust report (and corresponding seal) as appropriate.

Reporting on the Suitability of the Design of Control Procedures

A practitioner may be asked to conduct a Trust Services engagement addressing the suitability of design of controls for a system, prior to the system's implementation. In such an engagement, the practitioner can issue a Trust Services report, but cannot issue a WebTrust or SysTrust report or corresponding seal.

Reporting on Multiple Principles

In most cases, a practitioner will be asked to report on one or more Trust Services principles and related criteria, rather than on the entire set of five principles. The practitioner, in the introductory paragraph, makes reference to the principles included in the scope of examination but makes no further statement that the entire set of principles was not included in the scope of the examination.

When the client asks the practitioner to examine and report on its conformity with two or more Trust Services principles and related criteria, there are a number of issues that the practitioner should consider, which are discussed in this section.

Individual or Combined Report

When engaged to perform a Trust Services examination for multiple principles, the practitioner can, depending on the needs of the client, issue either a combined report or individual reports for each of the principles. For the purpose of this discussion, it is assumed that the practitioner has been asked to report on the client's conformity with three sets of principles and criteria: security, privacy, and confidentiality.

The first issue is to decide whether this represents (1) one engagement to examine three principles or (2) three engagements that examine one principle each. This can affect, among other matters, the engagement letter, the content and number of representation letters, and whether one audit report or multiple audit reports will be issued.

A Trust Services examination for multiple principles can be performed either as a single engagement involving those three principles or as three separate engagements involving one principle each. In either case, the practitioner's report(s) should clearly communicate the nature of the engagement(s).

There can be reporting complications when a qualified report is appropriate for one or more, but not all three, of the principles. In certain instances, the practitioner may decide not to issue such a report. In order to ensure a clear understanding with the client on this matter, the engagement letter might include language indicating that "a report may or may not be issued."

Failure to Meet Criteria

There may be instances, with a multiple principle engagement, in which the entity fails to meet the relevant criteria for one or more of the multiple principles. If one or more relevant criteria have not been met, the practitioner cannot issue an unqualified report. Under AICPA attestation standards, when issuing a qualified or adverse report, the practitioner should report directly on the subject matter rather than on the assertion.

In the situation where, for example, the entity did not meet the confidentiality criteria but met all of the security and privacy criteria, the practitioner, depending upon how the engagement was structured, has the following options available:

1. Issue one report that deals with all three principles. Because the report would be qualified, no seal would be issued. Since this option would most likely not accomplish the client's objective of obtaining a seal, the practitioner should consider the next option.

2. Issue multiple reports (for example, two reports), with segregation of the confidentiality principle into a separate report. The other two principles would have an unqualified report, thereby enabling the entity to obtain the seal.[fn 5] The practitioner may then either issue a separate qualified report for confidentiality or withdraw from the confidentiality engagement. In either case, the practitioner may wish to issue recommendations to management on how the deficiencies can be corrected. The impact of the deficiency for confidentiality would need to be assessed to ascertain its effect, if any, on the other principles.[fn 6]

In the situation where the practitioner treats each principle as a separate engagement with separate engagement letters, option (2) would be the most appropriate.

Different Examination Periods

There may be situations where the entity requests that more than one principle be examined, but due to various reasons the principles will have different reporting periods (either the length of the reporting period, the date that the various reporting periods begin, or both). Ideally, it would be more efficient for the practitioner to have such periods coincide. When different reporting periods exist, the practitioner should consider whether to issue separate or combined reports. Separate reports covering the separate principles are less complex to prepare than a combined report. If a combined report is issued, the different reporting periods would need to be detailed in the introductory and opinion paragraphs of the report to ensure that the different examination periods are highlighted.

Additional Reporting Guidance

Special Issues for Initial Reports

Typically, an initial report would need to cover a period of two months or more. However, an initial report covering a period of less than two months (including a point-in-time report) can be issued in any of the following circumstances:

- When the conditions dictate (see Table 1).
- When an entity wishes to restore a Trust Services seal following a significant event that caused the entity to no longer comply with the criteria (that necessitated removal of the practitioner's report and the Trust Services seal from the entity's site).
- When an entity requests a Trust Services engagement for a system that is in the pre-implementation stage. The report would be a point in time rather than a period in time. Such a report would indicate that the system has not been placed in operation.

[fn 5] In determining whether a WebTrust seal would be issued in such circumstances, the practitioner should consider the guidance under the section "Responsibility for Communicating Lack of Compliance in Other Principle(s)."

[fn 6] Chapter 1 of SSAE No. 10 (AT secs. 501.34 and 601.53).

Similar to any attest engagement, before a practitioner can render an opinion, sufficient and competent evidential matter needs to be obtained. [fn 7] For all criteria, there needs to be sufficient client transaction volumes and other procedure and control evidence to provide the practitioner with the necessary evidential matter. Therefore, in accepting an engagement that will result in the issuance of a report on a period of less than two months (including a point-in-time report) the practitioner should consider, as it relates to management's assertion about compliance with the criteria and the operating effectiveness of its controls, whether there will be an appropriate testing period ("look-back period") to provide sufficient evidence to enable the practitioner to issue such a report. The period over which a practitioner should perform tests is a matter of judgment.

The period of time over which the practitioner would need to perform tests of controls to determine that such controls were operating effectively will vary with the nature of the controls being tested and the frequency with which the specific controls operate and specific policies are applied. Some controls operate continuously while others operate only at certain times.

If it is concluded that there will be an appropriate "look-back period" to provide sufficient evidential matter, the practitioner may undertake the engagement to issue a report covering a period of less than two months, or a point-in-time report. If the practitioner decides to issue a point-in-time report, the report should indicate that the firm has examined management's assertion as of [*Month, day, year*], rather than during a period.

The Trust Services practitioner should, in addition to considering the guidance herein, consider the relevant attest standards [fn 8] with respect to the wording of such a report, to assure that he or she is complying with such attest standards.

The length of the relevant initial period should be determined by the practitioner's professional judgment based on factors such as those set out in Table 1.

Table 1

Considerations for Use of a Shorter Initial Period	*Considerations for Use of a Longer Initial Period*
• Clients for whom other control examinations have already been performed	• Start-up operation that has not generated, during pre-implementation stages, sufficient transaction volume and conditions typical of expected normal operations
• Established site, with little transaction volatility	• Operations that experience volatile transaction volumes
• Operations that experience infrequent changes to disclosures, policies, and related controls	• Complex operations
• Start-up operation with significant transaction volumes and operating conditions (typical of expected normal operations) during the practitioner's pre-	• Operations that experience frequent changes to disclosures, policies, and related controls or significant instances that lack compliance with disclosures,

[fn 7] Chapter 1 of SSAE No. 10 (AT sec. 101.51).

[fn 8] See Chapter 1 of SSAE No. 10 (AT sec. 101.84–.87) and Appendix A (AT sec. 101.110) for additional reporting guidance.

implementation testing period and a transition to a live operational site that expects infrequent changes in policies and controls once it is operational	policies, and related controls

Use of Third-Party Service Providers

The practitioner may encounter situations where the entity under examination uses a third-party service provider to accomplish some of the Trust Services criteria. The AICPA/CICA *Effects of a Third-Party Service Provider in a WebTrust or Similar Engagement* provides applicable guidance for these situations and is available for download at www.webtrust.org.

Considerations When Restoring a Removed Seal

The following guidance applies when an entity wishes to restore the seal following a significant event that caused the entity to no longer comply with the criteria (that necessitated removal of the practitioner's report and the Seal from the entity's site). It is important that the entity consider disclosing to its users the nature of the significant event that created the "out of compliance" situation and the steps taken to remedy the situation. The entity should consider disclosing the event on its Web site or as part of its management assertion. Likewise, before issuing a new report, the practitioner should consider the significance of the event, the related corrective actions, and whether appropriate disclosure has been made. The practitioner also should consider whether this matter should be (1) disclosed as part of management's assertion, (2) emphasized in a separate explanatory paragraph in the practitioner's report, or (3) both.

Responsibility for Communicating Lack of Compliance in Other Principle(s)

During an examination of a client's conformity with a Trust Services principle, information about compliance or control deficiencies related to principles and criteria that are not within the defined scope of the engagement may come to the practitioner's attention. For example, while engaged only to report on controls related to the security principle, a practitioner may become aware that the entity is not complying with its privacy policy as stated on its Web site (for example, it is disclosing personal information to selected third parties). Although the practitioner is not responsible for detecting information outside the scope of his or her examination, the practitioner should consider such information when it comes to his or her attention and evaluate whether the identified deficiencies are significant (that is, whether such deficiencies could materially mislead users of the system).

If the practitioner determines that such deficiencies are significant, they should be communicated in writing to management. Management should be asked either to correct the deficiency (in this case, cease providing the information to third parties) or to properly disclose their actual practices publicly so that users are aware of actual policies (in this case, the privacy statement would be amended to reflect the fact that they do provide information to third parties).

If the practitioner concludes that omission of this information would be significant and if management is unwilling to either correct the deficiency or to disclose the information, the practitioner should consider withdrawing from the engagement.

Cumulative Reporting

Under Trust Services reporting guidelines, the period reported upon by a practitioner is limited to the current period under examination and shall not exceed 12 months. A cumulative report that covers the current examination period and prior periods that were subject to similar examinations by the practitioner is not recommended. The relevance of a cumulative reporting period has been questioned given the significant pace of growth and change in technological systems, especially those for electronic commerce.

Qualified or Adverse Opinions

Under the AICPA attestation standards, reservations about the subject matter or the assertion refers to any unresolved reservation about the assertion or about the conformity of the subject matter with the criteria, including the adequacy of the disclosure of material matters. They can result in either a qualified or an adverse opinion, depending on the materiality of the departure from the criteria against which the subject matter was evaluated.

Subsequent Events

Events or transactions sometimes occur subsequent to the point in time or period of time of the subject matter being tested but prior to the date of the practitioner's report that have a material effect on the subject matter and therefore require adjustment or disclosure in the presentation of the subject matter or assertion. These occurrences are referred to as *subsequent events*. In performing an attest engagement, a practitioner should consider information about subsequent events that comes to his or her attention. Two types of subsequent events require consideration by the practitioner.

The first type consists of events that provide additional information with respect to conditions that existed at the point in time or during the period of time of the subject matter being tested. This information should be used by the practitioner in considering whether the subject matter is presented in conformity with the criteria and may affect the presentation of the subject matter, the assertion, or the practitioner's report.

The second type consists of those events that provide information with respect to conditions that arose subsequent to the point in time or period of time of the subject matter being tested that are of such a nature and significance that their disclosure is necessary to keep the subject matter from being misleading. This type of information will not normally affect the practitioner's report if the information is appropriately disclosed.

While the practitioner has no responsibility to detect subsequent events, the practitioner should inquire of the responsible party (and his or her client if the client is not the responsible party) as to whether they are aware of any subsequent events, through the date of the practitioner's report, that would have a material effect on the subject matter or assertion. [fn 9] The representation letter ordinarily would include a representation concerning subsequent events.

[fn 9] For certain subject matter, specific subsequent event standards have been developed to provide additional requirements for engagement performance and reporting. Additionally, a practitioner engaged to examine the design or effectiveness of internal control over items not covered by Chapter 5, "Reporting on an Entity's Internal Control Over Financial Reporting," or Chapter 6, "Compliance Attestation," of SSAE No. 10, as amended, should consider the subsequent events guidance set forth in Chapter 5 (AT sec. 501.65–.68), and Chapter 6 (AT sec. 601.50–.52).

The practitioner has no responsibility to keep informed of events subsequent to the date of his or her report; however, the practitioner may later become aware of conditions that existed at that date that might have affected the practitioner's report had he or she been aware of them. In such circumstances, the practitioner may wish to consider the guidance in Statement on Auditing Standards (SAS) No. 1, section 561, *Subsequent Discovery of Facts Existing at the Date of the Auditor's Report* (AICPA, *Professional Standards*, vol. 1, AU sec. 561). [fn 10]

Agreed-Upon Procedures Engagements

A client may request that a practitioner perform an agreed-upon procedures engagement related to the Trust Services principles and criteria. In such an engagement, the practitioner performs specified procedures agreed to by the specified parties, [fn 11] and reports his or her findings. Because the needs of the parties may vary widely, the nature, timing, and extent of the agreed-upon procedures may vary as well; consequently, the specified parties assume responsibility for the sufficiency of the procedures since they best understand their own needs. In an agreed-upon procedures engagement, the practitioner does not perform an examination or review of an assertion or subject matter or express an opinion or negative assurance about the assertion or subject matter. The practitioner's report on agreed-upon procedures is a presentation of procedures and findings. [fn 12] The use of an agreed-upon procedures report is restricted to the specified parties who agreed upon the procedures. In such engagements, issuance of a seal is not appropriate.

Other Matters

All Trust Services engagements should be performed in accordance with the applicable professional standards and the Trust Services license agreement. Because users are seeking a high level of assurance, WebTrust and SysTrust are examination level engagements. Accordingly, it is not appropriate to provide these services with the intent of providing a moderate level or a review report. Although permissible, a moderate assurance or review level Trust Services engagement may not provide the desired degree of usefulness for the intended users.

Illustrative Reports

The following illustrative reports are for both SysTrust and WebTrust engagements. Illustrations 1 through 2 are period-of-time report examples. Illustration 3 is a point-in-time report example.

[fn 10] Chapter 1 of SSAE No. 10 (AT sec. 101.95–.99).

[fn 11] The specified users and the practitioner agree upon the procedures to be performed by the practitioner.

[fn 12] Agreed-upon procedures engagements are performed under Chapter 2, “Agreed-Upon Procedures Engagements,” of SSAE No. 10 (AT sec. 201).

Under the SSAEs, the first paragraph of the practitioner's report will state that the practitioner has performed an examination of management's assertion about compliance with the Trust Services criteria or, alternatively, that the practitioner has examined the subject matter. The practitioner may opine (1) on management's assertion or (2) directly on the subject matter. Both alternatives are covered in the illustrative reports.

These reports are for illustrative purposes and should be modified in accordance with the applicable professional standards as the specific engagement facts and circumstances warrant.

Illustration 1—SysTrust Report for Systems Reliability—Reporting Directly on the Subject Matter (Period-of-Time Report)

Independent Practitioner's SysTrust Report on System Reliability

To the Management of ABC Company, Inc.:

We have examined the effectiveness of ABC Company, Inc.'s (ABC Company) controls over the reliability of its _____ [*system under examination*] System during the period [*Month, day, year*] through [*Month, day, year*], based on the AICPA/CICA Trust Services Criteria for systems reliability. Maintaining the effectiveness of these controls is the responsibility of ABC Company's management. Our responsibility is to express an opinion based on our examination.

A reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. The AICPA/CICA Trust Services Availability, Security, and Processing Integrity Criteria [*hot link to applicable principles and criteria*] are used to evaluate whether ABC Company's controls over the reliability of its _____ [*system under examination*] System are effective.

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 relevant system availability, security, and processing integrity controls; (2) testing and evaluating the operating effectiveness of the controls; and (3) 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 maintained, in all material respects, effective controls over the reliability of the _____[*system under examination*] System to provide reasonable assurance that:

- The System was available for operation and use, as committed or agreed;
- The System was protected against unauthorized access (both physical and logical); and
- The System processing was complete, accurate, timely, and authorized during the period [*Month, day, year*] through [*Month, day, year*], based on the AICPA/CICA Trust Services Criteria for systems reliability.

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 fail-

ure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

The SysTrust seal on ABC Company's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

[*See Notes to Illustrative Reports prepared under AICPA standards.*]

Illustration 2—Report for One Principle—Reporting Directly on the Subject Matter (Period-of-Time Report Including Schedule Describing Controls)

Independent Practitioner's SysTrust Report

To the Management of ABC Company, Inc.:

We have examined the effectiveness of ABC Company, Inc.'s (ABC Company) controls, described in Schedule X, over the security of its _____ [*system under examination*] System during the period [*Month, day, year*] through [*Month, day, year*], based on the AICPA/CICA Trust Services Security Criteria. Maintaining the effectiveness of these controls 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 relevant security controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) 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 maintained, in all material respects, effective controls, described in Schedule X, over the security of the _____[*system under examination*] System to provide reasonable assurance that the _____ [*system under examination*] System was protected against unauthorized access (both physical and logical) during the period [*Month, day, year*] through [*Month, day, year*], based on the AICPA/CICA Trust Services Security 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.

The SysTrust seal on ABC Company's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

[*See Notes to Illustrative Reports prepared under AICPA standards.*]

Schedule X—Controls Examined Supporting AICPA/CICA Trust Services Security Criteria

The system is protected against unauthorized access (both physical and logical).

1.0	**Policies: The entity defines and documents its policies for the security of its system.**	**Controls**
1.1	The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	The company's documented systems development and acquisition process includes procedures to identify and document authorized users of the system and their security requirements. User requirements are documented in service-level agreements or other documents. The security officer reviews security policies annually and submits proposed changes for the approval by the information technology standards committee.
1.2	The entity's security policies include, but may not be limited to, the following matters: *a.* Identification and documentation of the security requirements of authorized users. *b.* Allowing access, the nature of that access, and who authorizes such access. *c.* Preventing unauthorized access. *d.* The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access. *e.* Assignment of responsibility and accountability for system security. *f.* Assignment of responsibility and accountability for system changes and maintenance. *g.* Testing, evaluating, and authorizing system components before implementation. *h.* Addressing how complaints and requests relating to security issues are resolved. *i.* The procedures to handle security breaches and other incidents. *j.* Provision for allocation for training and other resources to support its system security policies. *k.* Provision for the handling of exceptions and situations not specifically addressed in its system security policies. *l.* Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts.	The company's documented security policies contain the elements set out in criterion 1.2.

1.3	Responsibility and accountability for the entity's system security policies, and changes and updates to those policies, are assigned.	Management has assigned responsibilities for the maintenance and enforcement of the company security policy to the chief information officer (CIO). Others on the executive committee assist in the review, update, and approval of the policy as outlined in the executive committee handbook. Ownership and custody of significant information resources (for example, data, programs, and transactions) and responsibility for establishing and maintaining security over such resources is defined.

This schedule is for illustrative purposes only and does not contain all the criteria for the security principle. When the practitioner is reporting on more than one principle, a similar format would be used to detail the appropriate criteria and controls. The practitioner is not bound by this presentation format and may utilize other alternative presentation styles.

Illustration 3—Report for One Principle—Reporting on Management's Assertion (Point-in-Time Report)

Independent Practitioner's WebTrust Report

To the Management of ABC Company, Inc.:

We have examined management's assertion [*hot link to management's assertion*] that ABC Company, Inc. (ABC Company) as of [*Month, day, year*] complied with the AICPA/CICA Trust Services Security Criteria and, based on these Criteria, maintained effective controls to provide reasonable assurance the _____ [*system under examination*] System was protected against unauthorized access (both physical and logical). 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 relevant security controls, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with the Security Criteria and (3) 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, management's assertion that ABC Company complied with AICPA/CICA Trust Services Security Criteria and, based on these Criteria, maintained effective controls to provide reasonable assurance that the _____ [*system under examination*] System was protected against unauthorized access (both physical and logical) as of [*Month, day, year*] is fairly stated, in all material respects.

OR

In our opinion, ABC Company's management's assertion referred to above is fairly stated, in all material respects, based on the AICPA/CICA Trust Services Security 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 fail-

ure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

The WebTrust seal of assurance on ABC Company's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

[*See Notes to Illustrative Reports prepared under AICPA standards.*]

Appendix D

Generally Accepted Privacy Principles—A Global Privacy Framework

May 2006

Acknowledgments:

The AICPA and CICA appreciate the contribution of the volunteers who devoted significant time and effort to this project. The institutes also acknowledge the support the following organizations have provided to the development of Generally Accepted Privacy Principles:

- ISACA
- The Institute of Internal Auditors

NOTICE TO READERS

This CPA/CA practitioner version is identical to "Generally Accepted Privacy Principles—A Global Privacy Framework" with the exception of Appendix C, "Practitioner Services Using Generally Accepted Privacy Principles," and Appendix D, "Illustrative Privacy Examination/Audit Reports." These additional appendices are intended primarily to assist CPAs and CAs in public practice in providing privacy services to their clients. Effective for Reports issued after June 30, 2006. Early adoption is encouraged.

Foreword

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) believe strongly that privacy is a business issue. In considering what organizations face when trying to address privacy issues, we quickly concluded that businesses did not have a comprehensive framework to manage their privacy risks effectively. The institutes decided that they could contribute significantly by developing a privacy framework that would address the needs and expectations of all of the parties affected by privacy requirements or expectations. Therefore, the institutes developed the initial AICPA/CICA Privacy Framework. This framework has been updated to reflect that the principles included have now become more widely accepted. Accordingly, the framework has now been renamed as Generally Accepted Privacy Principles. The institutes are making these principles and criteria widely available to all parties interested in addressing privacy issues.

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

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

For organizations operating in a multijurisdictional environment, managing privacy risk can be even a more significant challenge. Organizations need to be aware of the significant privacy requirements in all the jurisdictions in which the organization does business.

With these issues in mind, the AICPA and CICA developed Generally Accepted Privacy Principles to be used as an operational framework to help management address privacy in a manner that takes into consideration local, national, or international requirements. The primary objective is to facilitate privacy compliance and effective privacy management. The secondary objective is to provide suitable criteria against which a privacy examination (which is usually referred to as a "privacy audit") can be performed.

Generally Accepted Privacy Principles represent the AICPA and CICA contribution to the effective management of privacy risk, recognizing the needs of organizations while reflecting the public interest. Additional history about the development and additional privacy resources can be found at www.aicpa.org/privacy and www.cica.ca/privacy. *Generally Accepted Privacy Principles—A Global Privacy Framework* can be downloaded from the AICPA and the CICA Web sites. [fn *]

[fn *] The respective URLs are http://infotech.aicpa.org/Resources/Privacy/ and www.cica.ca/index.cfm/ci_id/258/la_id/1.htm.

The development and maintenance of Generally Accepted Privacy Principles is a dynamic process; as a result, please forward any comments about this document to the AICPA (ncohen@aicpa.org) or the CICA (privacy@cica.ca).

AICPA CICA

May 2006

AICPA/CICA Privacy Task Force

Chair

Everett C. Johnson, CPA

Deloitte & Touche LLP (retired)

Vice Chair

Kenneth D. Askelson,

CPA/CITP, CIA

Eric Federing

KPMG LLP

Don H. Hansen, CPA

Moss Adams LLP

Philip M. Juravel, CPA

Juravel & Company, LLC

Sagi Leizerov, Ph.D.

Ernst & Young LLP

Marilyn Prosch, Ph.D.

Arizona State University

Doron M. Rotman, CPA (Israel),

CISA, CIA, CISM, CIPP

KPMG LLP

Kerry Shackelford, CPA

KLS Consulting LLC

Donald E. Sheehy, CA·CISA

Deloitte & Touche LLP

Staff Contact:

Bryan Walker, CA, CICA *Principal, Assurance Services Development*

Nancy A. Cohen, CPA

Senior Technical Manager, InfoTechnology Communities

Generally Accepted Privacy Principles—A Global Privacy Framework was approved by the AICPA Board of Directors.

Introduction

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

Generally Accepted Privacy Principles have been developed from a business perspective, referencing significant domestic and international privacy regulations. Generally Accepted Privacy Principles operationalize complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by objective, measurable criteria that need to be met. Illustrative policy requirements, communications, and controls, including monitoring controls, are provided as support for the criteria.

This document sets out Generally Accepted Privacy Principles that can be used by any organization as part of its privacy program. Generally Accepted Privacy Principles have been developed to help management create an effective privacy program that addresses privacy risks and obligations and business opportunities. This introduction includes a definition of privacy and an explanation of why privacy is a business issue and not solely a compliance issue. Also illustrated is how these principles can be applied to outsourcing scenarios and the potential types of privacy initiatives that can be undertaken for the benefit of the organizations and their customers.

This introduction and the set of Generally Accepted Privacy Principles and Criteria will be useful to those who:

- Oversee and monitor privacy and security programs
- Implement and manage privacy in an organization
- Implement and manage security in an organization
- Assess compliance and audit privacy and security programs
- Regulate privacy

Why Privacy Is a Business Issue

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

[fn 1] The first occurrence of each word contained in Appendix A—Glossary is underlined in the introduction section and in the Generally Accepted Privacy Principles and Criteria tables.

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

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

International Privacy Considerations

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

For example, the global nature of the Internet and business means that regulatory actions in one country may affect the rights and obligations of users around the world. Many countries have laws regulating transborder data flow, including the European Union's 1995 and 1997 directives on data protection and privacy with which an organization must comply if it wants to do business in those jurisdictions. Therefore, organizations need to comply with changing privacy requirements around the world. Further, different jurisdictions have different privacy philosophies, making international compliance a complex task. To illustrate this, some countries view personal information as belonging to the individual and take the position that the enterprise has a fiduciary-like relationship when collecting and maintaining such information. Alternatively, other countries view personal information as belonging to the enterprise that collects it.

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

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

Outsourcing and Privacy

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

The Generally Accepted Privacy Principles and supporting Criteria set out in this document can assist an organization in completing assessments (including independent examinations) about the privacy policies, procedures, and practices of the entity performing the outsourcing to which part of its privacy responsibility has been transferred.

The fact that these principles have global application can provide comfort to an outsourcer that privacy assessments can be undertaken using a consistent measurement based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized as good privacy practices.

What Is Privacy?

Privacy Definition

Under Generally Accepted Privacy Principles, 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., a Social Security or Social Insurance Number)
- Physical characteristics
- Consumer purchase history

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

- Information on medical or health conditions
- Financial information

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, the use of 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 cannot be linked to an individual.

Privacy or Confidentiality?

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

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Revenue by client and industry

Also, unlike personal information, rights of access to confidential information to ensure its accuracy and completeness are not clearly defined. As a result, interpretations of what is considered to be confidential

information can vary significantly from organization to organization and in most cases are driven by contractual arrangements. The AICPA/CICA Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (including WebTrust® and SysTrust®) provides a set of criteria for confidentiality (see www.webtrust.org).

Introducing Generally Accepted Privacy Principles

Generally Accepted Privacy Principles are designed to assist management in creating an effective privacy program that addresses their privacy risks and business opportunities.

The set of Generally Accepted Privacy Principles is founded on key concepts from significant domestic and international privacy laws, regulations, and guidelines (see Appendix B, "Comparison of International Privacy Concepts")[fn 2] and good business practices. By using these Generally Accepted Privacy Principles, organizations can proactively address the significant challenges that they face in establishing and managing their privacy programs and risks from a business perspective. The use of Generally Accepted Privacy Principles also facilitates management of privacy risk on a multijurisdictional basis.

Overall Privacy Objective

Generally Accepted Privacy Principles are founded on the following privacy objective.

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

Generally Accepted Privacy Principles

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

The following are the 10 Generally Accepted Privacy Principles:

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

[fn 2] 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 B. Compliance with this set or Generally Accepted Privacy Principles and 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.

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

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

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

For each of the 10 privacy principles, relevant, objective, complete, and measurable criteria have been developed 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.

Using Generally Accepted Privacy Principles

Generally Accepted Privacy Principles can be used by organizations for:

- Privacy policy design and implementation
- Performance measurement
- Benchmarking
- Monitoring and auditing privacy programs

Management of a privacy program entails the following activities:

- Strategizing—Performing privacy strategic and business planning

- Diagnosing—Performing privacy gap and risk analysis
- Implementing—Introducing and institutionalizing solutions
- Sustaining/Managing—Monitoring activities of a privacy program
- Auditing—Internal or external auditors evaluating the organization's privacy program

The following table summarizes and illustrates how Generally Accepted Privacy Principles can be used by an organization to address these business activities.

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

	ment, identifying opportunities where weaknesses, vulnerability, and threats exist. The most common initial engagement for an organization is an assessment. The purpose of an assessment is to evaluate the entity against its privacy goals and objectives and determine to what extent the organization is achieving those goals and objectives.	needs, privacy policy and practices, competitive pressures, and the requirements of the relevant laws and regulations to which the entity is subject. Generally Accepted Privacy Principles provides a legislative-neutral benchmark to allow the entity to assess the current state of privacy against the desired state.
Implementing	At this point, an action plan is mobilized and/or a diagnostic recommendation is put into effect. Implementing involves the execution of all planned and other tasks necessary to make the action plan operational. It includes the definition of who will perform what tasks, assigning responsibilities, and establishing schedules/milestones. This involves the planning and implementation of a series of planned projects to provide guidance, direction, methodology, and tools to the organization in developing its initiatives.	Generally Accepted Privacy Principles can assist the entity in meeting its implementation goals. At the completion of the implementation phase, the entity should have developed the following deliverables: • Converted systems, procedures, and processes to address the privacy requirements • Updated privacy compliant forms, brochures, and contracts • Internal and external privacy awareness programs
Sustaining/Managing	Sustaining/Managing involves monitoring the work to identify how progress differs from the action plan in time to initiate corrective action. Monitoring refers to the management policies, processes, and supporting technology to ensure compliance with organizational privacy policies and procedures and the ability to exhibit due diligence.	The entity can use Generally Accepted Privacy Principles, for example, to develop appropriate reporting criteria for monitoring requests for information, the sources used to compile the information and the information actually disclosed. It can also be used for determining validation procedures to ensure that the parties to whom the information was disclosed are entitled to receive that information.
Internal privacy audit	Internal auditors provide objective assurance and consulting services designed to add value and improve an entity's operations. They help an entity accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.	Internal auditors can evaluate an entity's privacy program using Generally Accepted Privacy Principles as a benchmark and provide useful information and reporting to management.

External privacy audit	External auditors, notably CAs and CPAs, can perform assurance services. Generally, an external audit of financial and nonfinancial information builds trust and confidence for individuals, management, customers, business partners, and other users.	An external auditor can evaluate an entity's privacy program in accordance with Generally Accepted Privacy Principles and provide reports useful to individuals, management, customers, business partners, and other users.

Presentation of Generally Accepted Privacy Principles and Criteria

Under each principle, the Criteria are presented in a three-column format. The first column contains the measurement criteria. The second column contains illustrations and explanations, which are 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 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.

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

Management

Ref.	*Management 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	The entity: • Periodically communicates to in-	Privacy policies encompass security policies relevant to the protection of personal information.

	communicated at least annually to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	ternal personnel (for example, on a network or a Web site) relevant information about the entity's privacy policies and 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 and security concepts, and issues; and promotes ongoing awareness.	
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 responsibility, authority, and accountability of the designated person or group are clearly documented. Responsibilities include: • Establishing with management standards to classify the sensitivity of personal information and to de-	The individual identified as being accountable for privacy should be from within the entity.

		termine the level of protection required • Formulating and maintaining the entity's privacy policies • Monitoring and updating the entity's privacy policies • Delegating authority for enforcing the entity's privacy policies • Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices The board periodically includes privacy in its regular review of corporate governance. The entity requires and documents users, management, and third-party confirmations (initially and annually) of their understanding and agreement to comply with the entity's privacy policies and procedures.	
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.	
1.2.3	**Consistency of Commitments With Privacy Policies and Procedures** Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.	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** Internal personnel or advisers review the design, acquisition, development, implementation, configuration, and management of: • Infrastructure, • Systems, • Applications,	Procedures are in place to: • Govern the development, acquisition, implementation, and maintenance of information systems and the related technology used to collect, use, retain, disclose and destroy personal information. • Ensure that the entity's business continuity management processes are consistent with its privacy policies and procedures.	

	• Web sites, and • Procedures, and changes thereto for consistency with the entity's privacy policies and procedures and address any inconsistencies.	• 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 information. All test data are anonymized. • Require the documentation and approval by the privacy officer, business unit manager and IT management 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 au-	

		thorized, 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 Internal Personnel** The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.	The qualifications of internal personnel responsible for protecting the privacy and security of personal information are ensured by procedures such as: • Formal job descriptions (including responsibilities, educational and professional requirements, and organizational reporting for key privacy management positions) • 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	The entity has an ongoing process in place to monitor, assess, and address the effect on privacy of changes in:	

	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.	• 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

Ref.	*Notice 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	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. The use of "short notice" privacy statements is becoming more common. A short

	10.1.1) If personal information is collected from sources other than the individual, such sources are described in the notice.		notice privacy statement is a separate page that succinctly highlights the scope, collection, use, choice, contact details, and other information relative to the information being collected in the particular business activity to which it is attached.
2.2	**Procedures and Controls**		
2.2.1	**Provision of Notice** Notice is provided to the individual about the entity's privacy policies and procedures: • 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.	Privacy notice is: • Readily accessible and available when personal information is first collected from the individual. • Provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal information to the entity. • Clearly dated to allow individuals to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to the entity. In addition, the entity: • Tracks previous iterations of the entity's privacy policies and procedures. • Informs individuals of a change to	See 3.2.2, "Consent for New Purposes and Uses." Some regulatory requirements indicate that a privacy notice is to be provided on a periodic basis, for example, annually in the Gramm-Leach-Bliley Act (GLBA).

		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.	
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 might assume that they are covered by the	

		entity's privacy policies but in fact are no longer covered (for example linking to another Web site that is similar to the entity's, or using services on the entity's premises provided by third parties).	
2.2.3	**Clear and Conspicuous** The entity's privacy notice is conspicuous and uses clear language.	The privacy notice is: • In plain and simple language. • Appropriately labeled, easy to see, and not in 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 are encouraged to avoid consumer confusion and allow consumers to identify any differences. Some regulations, such as GLBA, may contain specific information that a disclosure must contain. Illustrative notices are often available for certain industries and types of collection, use, retention, and disclosure.

Choice and Consent

Ref.	*Choice and Consent Criteria*	*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 ability of and process for an individual to change contact preferences. • The consequences of failing to provide personal information required for a transaction or service. Individuals are advised that:	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.

		• Personal information not essential to the purposes identified in the privacy notice need not be provided. • Preferences may be changed and consent may be withdrawn at a later time, subject to legal or contractual restrictions and reasonable notice. The type of consent required depends on the nature of the personal information and the method of collection (for example, an individual subscribing to a newsletter gives implied consent to receive communications from the entity).	
3.1.2	**Consequences of Denying or Withdrawing Consent** When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.	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 per-	

		sonal 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 soon as practical thereafter. The individual's preferences expressed in his or her consent are confirmed and implemented.	The entity: • Obtains and documents an individual's consent in a timely manner (that is, at or before the time personal information is collected, or 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 in a timely fashion. • Addresses conflicts in the records about an individual's preferences by providing a process for users to notify and challenge a vendor's interpretation of their contact preferences. • Ensures that the use of personal information, throughout the entity	

		and by third parties, is in accordance with an individual's preferences.	
3.2.2	**Consent for New Purposes and Uses** If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified, and implicit or explicit consent is obtained prior to such new use or purpose.	When personal information is to be used for a purpose not previously specified, the entity: • Notifies the individual and documents the new purpose. • Obtains and documents consent or withdrawal of consent to use the personal information for the new purpose. • Ensures that personal information is being used in accordance with the new purpose or, if consent was withdrawn, not so used.	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 specifically requires otherwise.	The entity collects sensitive information only if the individual provides explicit consent. *Explicit consent* requires that the individual affirmatively agree, through some action, to the use or disclosure of the sensitive information. Explicit consent is obtained directly from the individual and documented, for example, by requiring the individual to check a box or sign a form. This is sometimes referred to as opt in.	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. Most jurisdictions referenced to in Appendix B, "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, "The collection and processing of sensitive data is forbidden." However, a permit to collect and process sensitive data may be obtained. Some jurisdictions consider government-issued personal identifiers for example, Social Security numbers or Social Insurance numbers, to be sensitive information.
3.2.4	**Consent for Online Data Transfers** to/From an Individual's Computer Consent is obtained before personal information is transferred to/from an individual's computer.	The entity requests customer permission to store, alter, or copy personal information (other than cookies) in the customer'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. 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

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

		• Over the telephone • Via the Internet using forms, cookies, or Web beacons. The entity's privacy notice discloses that it uses cookies and Web beacons and how they are used. The notice also describes the consequences if the cookie is refused.	
4.2	**Procedures and Controls**		
4.2.1	**Collection Limited to Identified Purpose** The collection of personal information is limited to that necessary for the purposes identified in the notice.	Systems and procedures are in place to: • Specify the personal information essential for the purposes identified in the notice and differentiate it from optional personal information. • Periodically review the entity's program or service needs for personal information (for example, once every five years or when 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, relating to the collection of personal information.	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 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 indi-	The entity: • Performs due diligence before establishing a relationship with a	Contracts include provisions requiring personal information to be collected fairly and lawfully and from reliable sources. If information collected from third parties

	vidual) are reliable sources that collect information fairly and lawfully.	third-party data provider. • Reviews the privacy policies and collection methods of third parties before accepting personal information from third-party data sources.	is to be combined with information collected from the individual, consideration should be given to providing notice to such individuals.

Use and Retention

Ref.	*Use and Retention 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.**		
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 purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.	Systems and procedures are in place to ensure that personal information is used in: • Conformity with the purposes identified in the entity's privacy notice • Agreement with the consent received from the individual • Compliance with applicable laws and regulations.	Some regulations have specific provisions concerning the use of personal information. Examples are the GLBA, the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA).
5.2.2	**Retention of Personal Information** Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise. 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 pa-	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

		per-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 fulfill the identified purposes or as required by laws and regulations. Contractual requirements should be considered when establishing retention practices.	laws.

Access

Ref.	*Access 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 Personal Information** Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.	Procedures are in place to: • Determine whether the entity holds or controls personal information about an individual. • Communicate the steps to be taken to gain access to the personal in-	Some laws and regulations specify: • Provisions and requirements for providing access to personal information (for example, HIPAA). • Requirements that requests for access to personal information be

		formation. • 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.	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	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

		request only to the address of record or, in the case of a change of address, to both the old and new addresses. • Requires that a 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 re-	Entities may provide individuals with access to their personal information at no cost or at a minimal cost because of the potential business and customer-relationship benefits as well as the opportunity to enhance the quality of the information.

		sponse times for other business transactions, or as permitted or required by law. • Provides access to personal information in archived or backup systems and media. • Informs individuals of the cost of access at the time the access request is made or as soon as practicable thereafter. • Charges the individual for access to personal information at an amount, if any, which is not excessive in relation to the entity's cost of providing access. • Provides an appropriate physical space to inspect personal information.	
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 per-	Some laws and regulations (for example, Principle 5, "Information Relating to Records Kept by Record-Keeper," point 2 of the Australian Privacy Act of 1988 and PIPEDA, Sections 8.(4), 8.(5), 8.(7), 9, 10 and 28) specify the situations in which access can be denied, the process to be followed (such as notifying the customer of the denial in writing within 30 days), and potential penalties or sanctions for lack of compliance.

		sonal 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.	
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	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.

		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.	
6.2.6	**Statement of Disagreement** Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.	If an individual and an entity disagree about whether personal information is complete and accurate, the individual may ask the entity to accept a statement claiming that the personal information is not complete and accurate. The entity: • Documents instances where an individual and the entity disagree about whether personal information is complete and accurate. • Informs the individual, in writing, of the reason a request for correction of personal information is denied, citing the individual's right to appeal. • Informs the individual, when access to personal information is requested or when access is actually provided, that the statement of disagreement may include infor-	Some regulations (for example, HIPAA) have specific requirements for denial of requests and handling of disagreements from individuals. If a challenge is not resolved to the satisfaction of the individual, when appropriate, the existence of such challenge is communicated to third parties having access to the information in question.

		mation 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.	
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 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.	See 10.1.1, "Communications to Individuals", 10.2.1, "Complaint Process", and 10.2.2, "Dispute Resolution and Recourse." Some laws (for example, PIPEDA) permit escalation through the court system up to the most senior court.

Disclosure to Third Parties

Ref.	*Disclosure to Third Parties 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.	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 which the individual has provided implicit or explicit consent, or as specifically allowed or required by law or regulation.	The entity's privacy notice may disclose: • The process used to assure the privacy and security of personal information that has been disclosed to a third party. • How personal information shared with a third party will be kept up-to-date, so that outdated or incorrect information shared with a third party will be changed if the individual has changed his or her information.
7.1.2	**Communication to Third Parties** Privacy policies are communicated to	Prior to sharing personal information with a third party, the entity communicates its privacy policies to and obtains a written	

	third parties to whom personal information is disclosed.	agreement from the third party that its data protection 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 in a manner consistent with the relevant aspects of the entity's privacy policies.	Systems and procedures are in place to: • Provide a level of protection of personal information equivalent to that of the entity when information is 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	The entity is responsible for personal information in its possession or custody, including information that has been transferred to a third party. Some regulations (for example, from the U.S. federal financial regulatory agencies) require that an entity take reasonable steps to oversee appropriate service providers by exercising appropriate due diligence in the selection of service providers. Some jurisdictions, including some coun-

		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 a designated privacy executive, such as a corporate privacy officer. • Specify how and when third parties are to dispose of or return any personal information provided by the entity.	tries 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 EU's Directive requires that such transfers take place only where the third party ensures an adequate level of protection.
7.2.3	**New Purposes and Uses** Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.	Systems and procedures are in place to: • Notify individuals and obtain their consent prior to disclosing personal information to a third party for purposes not identified in the privacy notice. • Document whether the entity has notified the individual and re-	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.

		ceived 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: • Reviews complaints to identify indications of any misuse of personal information by third parties. • Responds to any knowledge of a third party using or disclosing personal information in variance with the entity's privacy policies and procedures or contractual arrangements. • Mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures (For example, notify individuals affected, attempt to recover information disclosed to others, void and reissue new account numbers). • Takes remedial action in the event that a third party misuses personal information (for example, contractual clauses address the ramification of misuse of personal infor-	

		mation).	

Security for Privacy

Ref.	*Security for Privacy 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.

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: • Periodic risk assessments • Identification and documentation of the security requirements of authorized users • Allowing access, the nature of that access, and who authorizes such access • Preventing unauthorized access by using effective physical and logical access controls • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access • Assignment of responsibility and accountability for security • Assignment of responsibility and accountability for system changes and maintenance • Implementing system software upgrades and patches • Testing, evaluating, and authorizing system principles before im-	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 personal information at is-

		plementation • Addressing how complaints and requests relating to security issues are resolved • Handling errors and omissions, security breaches, and other incidents • Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing) • Allocating training and other resources to support its security policies • Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies • Disaster recovery plans and related testing • Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts • A requirement that users, man-	sue. Some security laws (for example, California SB1386) require entities to notify individuals if the protection of their personal information is compromised. Payment card issuers have established security and privacy requirements.

		agement, 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 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: • Authorizing and registering internal personnel and individuals • Identifying and authenticating internal personnel and individuals • Making changes and updating access profiles • Granting system access privileges and permissions • Preventing individuals from accessing other than their own per-	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 meas-	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.

	sonal or sensitive information • Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities • Distributing output only to authorized internal personnel • Restricting logical access to offline storage, backup data, systems, and media • Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls) • Preventing the introduction of viruses, malicious code, and unauthorized software	ures for remote access, such as additional or dynamic passwords, dial-back controls, digital certificates, secure ID cards, virtual private network (VPN), or properly configured firewalls. • Implement intrusion detection and monitoring systems.	
8.2.3	**Physical Access Controls** Physical access is restricted to personal information in any form (including the principles 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 per-	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.

		sonal information. • Investigate breaches and attempts to gain unauthorized access. • Communicate investigation results to appropriate designated privacy executive. • Maintain physical control over the distribution of reports containing personal information. • Securely dispose of waste containing confidential information (for example, shredding).	
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 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 semi-annually.	
8.2.5	**Transmitted Personal Information** Personal information is protected when	Systems and procedures are in place to: • Address the confidentiality of in-	Some regulations (for example, HIPAA) have specific provisions for the electronic transmission and authentication of signa-

	transmitted by mail and over the Internet and public networks by deploying industry standard encryption technology for transferring and receiving personal information.	formation 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.	tures 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 safeguards protecting personal information are conducted at least annually.	Systems and procedures are in place to: • Regularly test the effectiveness of the key administrative, technical, and physical safeguards protecting personal information. • Periodically undertake independent audits of security controls using either internal or external auditors. • Test card access systems and other physical security devices at least	The frequency and nature of the testing of security safeguards will vary with the entity's size and complexity, the nature and scope of its activities, and the sensitivity of personal information. Some security regulations (for example, GLBA-related rules for safeguarding information) require an entity to: • Conduct regular tests of key controls, systems, and procedures by independent third parties or by staff independent of those that de-

		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.	velop or maintain security (or at least have these independent parties review results of testing). • Assess and possibly adjust its information security at least annually.

Quality

Ref.	*Quality Criteria*	*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. Accurate directions are presented by the entity to inform individuals as to what information is needed to complete a transaction and what information is optional.	
9.2	**Procedures and Controls**		
9.2.1	**Accuracy and Completeness of Personal Information** Personal information is accurate and complete for the purposes for which it is to be used.	Systems and procedures are in place to: • Edit and validate personal information as it is collected, created, maintained, and updated. • Record the date when the personal information is obtained or updated. • Specify when the personal information is no longer valid. • Specify when and how the per-	

		sonal information is to be updated and the source for the update (for example, annual reconfirmation of information held and methods for individuals to proactively update personal information). • Indicate how to verify the accuracy and completeness of personal information obtained directly from an individual, 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 minimize the use of inappropriate data for decision making.	

Monitoring and Enforcement

Ref.	*Monitoring and Enforcement 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. 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 man-	Some regulations (for example HIPAA and COPPA) have specific procedures and requirements.

		ner. • Identify trends and the potential need to change the entity's privacy policies and procedures. • Address complaints that cannot be resolved. • 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 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.	

		• Mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the entity's privacy policies and procedures (for example, notify individuals affected, attempt to recover information disclosed to others, void and reissue new account numbers). • Identify trends that may require revisions to privacy policies and procedures.	

Appendix A

Glossary

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

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

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

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

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

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

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

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

Privacy Program. The policies, communications, procedures, and controls in place to manage and protect personal information in accordance with Generally Accepted Privacy Principle and Criteria.

Purpose. The reason 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.

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

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

Appendix B

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 Generally Accepted Privacy Principles. This is for illustrative purposes only and not meant to be comprehensive. Column 1 lists the 10 principles of Generally Accepted Privacy Principles. Columns 2 through 9 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)Generally Accepted Privacy Principles	***(2)Australia Privacy Act***	***(3)Canada PIPEDA***	***(4)E.U. Directive***	***(5)OECD Guidelines***	***(6)U.S. FTC***	***(7)U.S. Safe Harbor***	***(8)U.S. HIPAA***	***(9)U.S. GLBA***
Management		Accountability	Notification	Accountability			Administrative requirements	
Notice	Openness	Identifying Purposes, Openness	Information to Be Given to the Data Subject	Purpose Specification, Openness	Notice	Notice	Notice	Privacy and Opt Out Notices, Exceptions
Choice and Consent	Use and Disclosure	Consent	Criteria for Making Data Processing Legitimate, Data Subject's Right to Object	Collection Limitation	Choice	Choice	Consent, Uses and Disclosures	Privacy and Opt Out Notices
Collection	Collection, Sensitive Information, Anonymity	Limiting Collection	Principles Relating to Data Quality, Exemptions and Restrictions	Collection (including consent) Limitation		Data Integrity		
Use and Retention	Identifiers, Use and Disclosure	Limiting Use, Disclosure, and Retention	Making Data Processing	Use Limitation (including disclosure		(Implied but not specified in the princi-	Uses and Disclosures	Limits on Disclosures

			Legitimate, Special Categories of Processing, Principles Relating to Data Quality, Exemptions and Restrictions, The Data Subject's Right to Object	limitation)		ples)		
Access	Access and Correction	Individual Access	The Data Subject's Right of Access to Data	Individual Participation		Access	Access	
Disclosure to Third Parties	Use and Disclosure, Transborder Data Flows	Limiting Use, Disclosure, and Retention	Transfer of Personal Data to Third Countries	Use Limitation (including disclosure limitation)		Onward Transfer	Uses and Disclosures, Accounting of Disclosures	Limits on Disclosures
Security for Privacy	Data Security	Safeguards	Confidentiality and Security of Processing	Security Safeguards	Security	Security	Security Rule	Security Guidelines mandated by section 501(b) of GLBA
Quality	Data Quality	Accuracy	Principles Relating to Data Quality	Data Quality	Integrity	Data Integrity	Amendment	
Monitoring and Enforcement	Enforcement by the Office of the Privacy	Challenging Compliance	Judicial Remedies, Liability and	Individual Participation (including	Enforcement	Enforcement	Compliance and Enforcement by the	Enforcement by financial services in-

	Commis-sioner		Sanctions, Codes of Conduct, Supervisory Authority and Working Party on the Protection of Individuals with Regard to the Processing of Personal Data	challenging compliance)			Department of Health and Human Services	dustry regulators, the FTC, and SEC

Key to Column and Source

(1) AICPA/CICA Generally Accepted Privacy Principles, May 2006.

(2) Australia Privacy Act 1988, *Privacy Act 1988*, as amended, effective December 21, 2001.

(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) 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.

(5) OECD Guidelines, *Organisation for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980.

(6) 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.

(7) 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.

(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.

Appendix C

CPA/CA Practitioner Services Using Generally Accepted Privacy Principles

This appendix provides a high-level overview of the services that CPAs and CAs in public practice (practitioners) can provide using Generally Accepted Privacy Principles. Detailed guidance in "*Understanding and Implementing Privacy Services—A CPA's Resource*" has been developed by the task force and is available from both the AICPA and CICA (see www.aicpa.org/privacy and www.cica.ca). This detailed guidance is viewed as an essential resource for practitioners who intend to provide any of the services discussed in this appendix.

Privacy Advisory Engagements

Practitioners can provide a variety of advisory services to their clients, which include strategic, diagnostic, implementation, and sustaining/managing services using the Generally Accepted Privacy Principles criteria. These services could include, for example, advising clients on system weaknesses, assessing risk, and recommending a course of action using the Generally Accepted Privacy Principles 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 expected to meet the standards set out in Sections 5000–5900 of the CICA Handbook.

Privacy Attestation /Assurance Engagements

Privacy attestation/assurance engagements include services in which a practitioner is engaged to:

- Issue an opinion (examination/audit),
- Conduct a review, or
- In the United States, conduct agreed-upon procedures on a defined privacy-related subject matter or an assertion thereon.

Privacy Examination/Audit Engagements

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

In an examination/audit engagement, the practitioner provides a high, though not absolute, level of assurance on a subject matter or assertion. With that objective, the practitioner develops examination/audit procedures that, in the practitioner's professional judgment, reduce the risk that the practitioner will reach an inappropriate conclusion to a low level. Illustrative privacy examination/audit reports are included in Appendix D.

The following key concepts apply to privacy assurance engagements. [fn 1]

- A privacy assurance report ordinarily covers all 10 principles. All of their relevant criteria need to be met during the period covered by the report to issue an unqualified report. [fn 2], [fn 3]

- The work should be performed at the highest level of assurance, that is, 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 specified web domains) 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). The scope often could be narrower, but ordinarily not broader, than that covered by the related privacy notice.

  — The scope of the engagement should cover all of the activities in the "information cycle" for the relevant personal information. These should include collection, use, retention, disclosure 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.

Privacy Review Engagements

[fn 1] Chapter 10 of the AICPA Guide "Understanding and Implementing Privacy Services—A CPA's Resource" and Chapters 10 and 11 of the CICA Guide "Solutions for Today's Privacy Issues" include guidance on performing privacy assurance engagements.

[fn 2] See Appendix D, "Illustrative Privacy Examination/Audit Reports."

[fn 3] In certain circumstances (such as a report on a third-party service provider), special purpose privacy reports covering some of the 10 Principles could be issued. The Privacy Task Force recommends that such reports contain language that indicates that the privacy principles not covered are essential for overall assurance of privacy and be "restricted use" reports.

Under professional standards, a review engagement is a form of an attestation/assurance engagement. However, the term "privacy review" is often misused to mean a privacy examination or certain types of privacy advisory engagements, such as a privacy diagnostic engagement. Because review engagements, as defined in professional standards, are susceptible to misunderstanding by third-party users, the Privacy Task Force does not recommend their use.

Agreed-Upon (Specified Auditing) Procedures Engagements

In an agreed-upon/specified procedures engagement, the practitioner performs specified procedures, agreed to by the parties [fn 4], and reports his or her findings. The practitioner does not perform an audit or review of an assertion or subject matter or express an opinion or negative assurance about the assertion or subject matter. [fn 5] In this type of engagement, the practitioner's report is in the form of a description of procedures and findings. Generally Accepted Privacy Principles may be used in such engagements. This type of work would not lead to an assurance report, but rather to a report presenting the agreed-upon/specified procedures and the corresponding findings. Agreed-upon/specified procedures could be undertaken relative to a subset of an entity's system with reference to a subset of the Generally Accepted Privacy Principles. For example, an entity may request that a practitioner complete agreed-upon/specified procedures using a sub-set of Generally Accepted Privacy Principles and report the findings. In Canada, specified procedures engagements are permitted, although they are not considered to be assurance engagements under CICA Handbook Section 5025.

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

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

Generally Accepted Privacy Principles are part of the AICPA/CICA Trust Services Principles and Criteria—a set of professional assurance and advisory services based on a common framework (i.e., a core set of principles and criteria). The Trust Services Principles and Criteria were developed by volunteer task forces under the auspices of the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). The AICPA and the CICA are referred to in this document as "the Institutes." The other Trust Services Principles and Criteria are:

[fn 4] The specified users of the report and the practitioner agree upon the procedures to be performed by the practitioner.

[fn 5] In the U.S., agreed-upon procedures engagements are performed under SSAE No. 10, Chapter 2, *Agreed-Upon Procedures Engagements*. In Canada there are no general standards for agreed-upon procedures/specified procedures. A practitioner could, however, look to the guidance provided by CICA Handbook section 9100 that contains standards for performing Specified Procedures on Financial Information Other Than Financial Statements. In specified auditing procedures engagements, the practitioner is engaged to report to specific users the results of applying specified procedures. In applying such procedures, the practitioner does not express a conclusion concerning the subject matter because he or she does not necessarily perform all of the procedures that, in the practitioner's judgment, would be necessary to provide a high level of assurance. Rather, the practitioner's report sets out the factual results of the procedures applied, including any exceptions found.

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

These are discussed more fully at www.webtrust.org. Additional information about Trust Services is set out in the Guide, "*Understanding and Implementing Trust Services*," which is available from the AICPA and CICA.

Online Privacy Engagements

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

- The scope of the engagement needs to include, as a minimum, 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.
    - The entity must agree to certain conditions governing the use of the WebTrust seal (generally included in the practitioner's engagement letter).
    - 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."

Appendix D

Illustrative Privacy Examination/Audit Reports

The following appendix includes examples of examination/audit reports under professional reporting standards:

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

Illustration 1—Reporting Directly on the Subject Matter Under AICPA Attestation Standards

Independent Practitioner's Privacy Report

To the Management of ABC Company, Inc.:

We have examined (1) the effectiveness of ABC Company, Inc.'s (ABC Company) controls over the personal information collected in its _____ [*description of the entities and activities covered, for example "the mail-order catalog-sales operations"*] business (the Business) to provide reasonable assurance that the personal information was collected, used, retained, and disclosed in conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants, and (2) ABC Company's compliance with its commitments in its privacy notice related to the Business during the period Xxxx xx, 2006 through Yyyy yy, 2006. ABC Company's management is responsible for maintaining the effectiveness of these controls and for compliance with its commitments in its privacy notice. Our responsibility is to express an opinion based on our examination.

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

In our opinion, during the period Xxxx xx, 2006 through Yyyy yy, 2006, 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 conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles; and (2) complied with its commitments in its privacy notice.

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 fail-

ure 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 AICPA Attestation Standards

Independent Practitioner's Privacy Report

To the Management of ABC Company, Inc.:

We have examined ABC Company, Inc.'s (ABC Company) management assertion that, during the period Xxxx xx, 2006 through Yyyy yy, 2006, 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 conformity with its commitments in its privacy notice related to the Business and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants, and

- Complied with its commitments in its privacy notice.

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

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

In our opinion, ABC Company's management assertion that, during the period Xxxx xx, 2006 through Yyyy yy, 2006, 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 conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles; and

- Complied with its commitments in its privacy notice,

is, in all material respects, fairly stated.

OR

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

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, 2006 through Yyyy yy, 2006, 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 in conformity with our commitments in our privacy notice related to the Business and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants , and

- Complied with our commitments in our privacy notice.

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 conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (CICA), and (2) ABC Company's compliance with its commitments in its privacy notice related to the Business during the period Xxxx xx, 2006 through Yyyy yy, 2006. ABC Company's management is responsible for maintaining the effectiveness of these controls and for compliance with its commitments in its privacy notice. Our responsibility is to express an opinion based on our audit.

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

In our opinion, during the period Xxxx xx, 2006 through Yyyy yy, 2006, 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 conformity with its commitments in its privacy notice and with criteria set forth in the Generally Accepted Privacy Principles; and (2) complied with its commitments in its privacy notice.

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, 2006 through Yyyy yy, 2006, 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 conformity with its commitments in its privacy notice related to the Business and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (CICA), and

- Complied with its commitments in its privacy notice.

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

Our audit was conducted in accordance with standards for assurance engagements established by the CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of ABC Company's controls over the privacy of personal information, (2) testing and evaluating the operating effectiveness of the

controls, (3) testing compliance with ABC Company's commitments in its privacy notice and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, ABC Company's management assertion that, during the period Xxxx xx, 2006 through Yyyy yy, 2006, 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 conformity with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles; and

- Complied with its commitments in its privacy notice,

is, in all material respects, fairly stated.

OR

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

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, 2006 through Yyyy yy, 2006, 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 criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants , and

- Complied with our commitments in our privacy notice.