University of Mississippi

eGrove

AICPA Professional Standards

American Institute of Certified Public Accountants (AICPA) Historical Collection

2003

Suitable Trust Services Criteria and Illustrations for Security, Availability, Processing Integrity, Online Privacy, and Confidentiality

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_prof

 Part of the Accounting Commons, and the Taxation Commons

Suitable Trust Services Criteria and Illustrations

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

Supersedes version 2.0 of the SysTrust Principles and Criteria and version 3.0 of the WebTrust Principles and Criteria. Effective for engagements beginning on or after April 1, 2003. Earlier implementation is encouraged.

Copyright © 2003 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants.
Permission is granted to make copies of this work provided that such copies are for personal, intraorganizational, or educational use only and are not sold or disseminated and provided further that each copy bears the following credit line: "Copyright © 2003 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. Used with permission."

This document is available on AICPA Online at www.aicpa.org.

Notice to Readers

The Suitable Trust Services 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, online 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, online privacy, and confidentiality.

.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 services in which a practitioner is engaged to issue an opinion, a review or an agreed upon procedures report on subject matter or an assertion about the subject matter; for example, an opinion as to whether a defined system meets the principles and criteria for system 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. Accordingly, a practitioner would be expected to be aware of the professional requirements established by the relevant professional standards. 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. Under these standards, an independent objective, knowledgeable practitioner will perform tests of either management's assertion or the subject matter to which the assertion relates. The practitioner will gather evidence about the assertion's conformity with the criteria in the same way as is commonly done in other audit engagements, by performing procedures such as inquiry, observation, inspection, and reperformance to verify the achievement of specified Trust Services criteria. The practitioner will express an opinion on management's assertion or on the subject matter to which it relates. The practitioner's report provides value to management because it increases the credibility of management's assertion and helps distinguish the entity from other service providers.

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. It would include, for example, advising clients on system weaknesses, assessing risk and

recommending a course of action using the Trust Services developed principles and criteria as a benchmark. 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 are organized into four broad areas:

a. *Policies***.** The entity has defined and documented its policies[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.

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 B and Appendix C, respectively, and Appendix B 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[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. *Online privacy.*[3] Personal information[4] obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.

---

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.

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).

3 The Enterprise Wide Privacy Task Force is in the process of developing criteria and other guidance on enterprise wide privacy. It is expected that that criteria will replace the online privacy criteria in this document upon issuance.

4 The term *personal information* includes personally identifiable information and other sensitive information for which the entity has legal or other privacy obligations and commitments.

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

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 Statement on Standards for Attestation Engagements (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.

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 B.

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[5]
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) 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	The entity's documented security policies contain the elements set out in criterion 1.2.

[5] 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.

	Criteria	Illustrative Controls[5]
	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 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 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 B.*] 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 C.*]
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.

	Criteria	Illustrative Controls[5]
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 accordance 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. 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. 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).	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 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

	Criteria	Illustrative Controls[5]
		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

	Criteria	Illustrative Controls[5]
		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 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.
3.5	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

	Criteria	Illustrative Controls[5]
		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	Entity management receives a third-party opinion on the adequacy of

	Criteria	Illustrative Controls[5]
	system components, including configurations consistent with the defined system security policies.	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 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).
3.12	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

	Criteria	Illustrative Controls[5]
		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 changes are monitored and their effect on system security is assessed on a timely basis.	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 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. 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	The entity's documented availability and related security policies contain the elements set out in criterion 1.2.

	Criteria	Illustrative controls
	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 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 B.*] 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*

	Criteria	Illustrative controls
		C.]
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

	Criteria	Illustrative controls
		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

	Criteria	Illustrative controls
		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 utilities, and security devices (for example, firewalls).	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 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.

	Criteria	Illustrative controls
		• 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.

	Criteria	Illustrative controls
		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

	Criteria	Illustrative controls
		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 determine the level of protection required to maintain an appropriate level of security. The security administration team reviews and approves the

	Criteria	Illustrative controls
		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

	Criteria	Illustrative controls
		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

	Criteria	Illustrative controls
		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	The entity's documented systems development and acquisition process includes procedures to identify and document authorized

	Criteria	Illustrative controls
	established and periodically reviewed and approved by a designated individual or group.	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. 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.	The entity's documented processing integrity and related security policies contain the elements set out in criterion 1.2.

	Criteria	Illustrative controls
	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 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	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 for an e-commerce system, refer to Appendix B.*] 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 C.*]

	Criteria	Illustrative controls
	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.	
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	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

	Criteria	Illustrative controls
	policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	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	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

	Criteria	Illustrative controls
	completeness. • Positive acknowledgment is received from the customer before the transaction is processed.	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: • The correct goods are shipped in the correct quantities in the time frame agreed upon, or	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. 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.

	Criteria	Illustrative controls
	services and information are provided to the customer as requested. • Transaction exceptions are promptly communicated to the customer. • 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 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. 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 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.	Written procedures exist for the distribution of output reports that conform to the system processing integrity objectives, policies, and standards. 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

	Criteria	Illustrative controls
		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. 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).	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 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:

	Criteria	Illustrative controls
		• 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.

	Criteria	Illustrative controls
		• 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 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

	Criteria	Illustrative controls
		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

	Criteria	Illustrative controls
		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.

	Criteria	Illustrative controls
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.

	Criteria	Illustrative controls
		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.

	Criteria	Illustrative controls
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.

Online Privacy Principle and Criteria

.25 The *online privacy principle* focuses on protecting the personal information an organization may collect from its customers through its e-commerce systems. Even though the controls an organization may have in place to protect such information may extend beyond its Web-based systems and may even include its service providers, it is not the intent of this principle to address protection of the privacy of all personal information an entity may collect, from all sources. The AICPA and CICA have established a separate task force to consider principles and criteria relevant to enterprise-wide privacy.

.26 E-commerce facilitates the gathering of information from and about individuals and its subsequent exchange with other entities. Some consumers like this because it allows them to receive targeted marketing materials that focus on their needs. On the other hand, many consumers consider such uses of information about them to be an invasion of their privacy. For this reason, it is important that entities inform their customers about the kinds of information that are collected about them, the uses of such information, customer options, and related matters. In addition, many countries have implemented laws and regulations covering the privacy of information obtained through e-commerce.

.27 Privacy can have many aspects, but for purposes of this principle and the corresponding criteria, *privacy* is defined as the rights and obligations of individuals and entities with respect to the collection, use, disclosure, and retention of personal information. *Personal information* is defined as any information relating to an identified or identifiable individual. Such information includes but is not limited to the customer's name; address; telephone number; Social Security, insurance, or other government identification numbers; employer; credit card numbers; personal or family financial information; personal or family medical information; employment history; history of purchases or other transactions; credit records; and similar information. *Sensitive information* is defined as personal information specifying 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.[6]

.28 It is important for consumers to have confidence that an entity takes appropriate steps to protect personal information. Although it can be relatively easy to establish an e-commerce system, the underlying technology can be complex and can entail a multitude of information protection and related security issues. The privacy of information transmitted over the Internet or other public networks can be compromised relatively easily. Without the use of basic encryption techniques, for example, consumer credit card numbers can be intercepted and stolen during transmission. Without appropriate firewalls and other security practices, personal information residing on an entity's e-commerce computer system can be intentionally or unintentionally provided to third parties not related to the entity's business.

Privacy Concepts

.29 The AICPA/CICA Privacy Framework consists of nine privacy practices that are key to the proper management of personal information and are based on internationally known fair information practices. Many of these practices are required by privacy laws and regulations from various jurisdictions around the world. Although they may not be widely known, these nine privacy practices appear in most comprehensive privacy laws worldwide. They include:

---

[6] This is the meaning of the term as defined by the European Union (EU) directives, and the United States Safe Harbor Privacy Principles, July 21, 2000.

a. *Notice.* The entity provides notice about its privacy policies and practices to the individual at or before the time information is collected, or as soon as practicable thereafter. The notice describes the purpose for which personal information is collected and how it will be used.

b. *Choice and consent.* The entity describes the choices available to the individual and obtains consent from the individual with respect to the collection, use, disclosure, and retention of personal information.

c. *Collection.* The entity limits the collection of personal information to that which is necessary for the purposes described in the notice.

d. *Use and retention.* The entity limits the use of personal information to the purposes described in the notice and for which the individual has provided either implicit or explicit consent. The entity retains personal information for only as long as necessary for the fulfillment of the stated purposes, or as required by laws and regulations.

e. *Access.* The entity provides access to the individual to review, update, block further use, or erase his or her personal information.

f. *Onward transfer and disclosure.* The entity discloses personal information to third parties only for purposes described in the notice and for which the individual has provided either implicit or explicit consent, or as permitted by laws or regulations. The entity discloses personal information only to third parties who provide substantially equivalent privacy protection as the entity.

g. *Security.* The entity takes reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction based on the sensitivity and value of the information.

h. *Integrity.* The entity maintains accurate, complete, current, relevant, and reliable personal information for the purposes for which it is to be used.

i. *Management and enforcement.* The entity designates one or more individuals who are accountable for the entity's compliance with its privacy policies. The entity has a periodic process in place to assess and verify compliance with its privacy policies. The entity has procedures to address privacy-related inquiries and disputes.

Global Impact of Privacy Criteria

.30 E-commerce by its nature is global. As companies cross international boundaries, they are faced with the challenges of meeting standards and complying with laws regarding privacy. Organizations that wish to tap into the global marketplace without adequate privacy standards and disclosures may face prohibitions or restrictions on how they do business.

.31 Consumers from around the world are concerned about how their information will be used, how it is protected, what process is in place that will allow them to correct erroneous information, and who will have access to this information. Without proper controls and without proper related disclosure, these consumers may choose to do business elsewhere, where there are adequate controls.

Consumer Recourse

.32 Because of the unique nature of e-commerce, customers are concerned about how their complaints are addressed. If a Web site is unwilling or unable to address a consumer's concerns, what recourse does the consumer have? If the consumer is in one country and the business is in another, how will the consumer's rights be protected? Some governments already require consumer recourse procedures to ensure consumer protection. Traditional dispute resolution through the court system can be time-consuming and expensive.

.33 A third-party dispute mechanism (such as those offered by the National Arbitration Forum) can provide an effective means for consumer recourse. All such mechanisms should conform to the principles of arbitration in Appendix A, "Consumer Arbitration." For entities in countries that have programs mandated by regulatory bodies, each program would be followed and disclosed on the site's e-commerce systems.

.34 The online privacy criteria require the entity to:

a. Commit to the use of a third-party dispute resolution mechanism that conforms to the principles of arbitration in Appendix A. Such third-party dispute resolution may be provided by any organization or governmental function offering such service.

b. Disclose its procedures for consumer recourse for issues not resolved by the entity.[7]

Online Privacy Principle and Criteria Table

.35 Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.

	Criteria	Illustrative controls
1.0	**Policies: The entity defines and documents its policies regarding the protection of personal information obtained as a result of e-commerce.**	
1.1	The entity's privacy 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 online privacy requirements. User requirements are documented in service-level agreements or other documents. The chief privacy officer (CPO) reviews the entity's privacy and related security policies annually and submits proposed changes as needed for approval by the executive committee.
1.2	The entity's online privacy and related security policies include, but may not be limited to, the following matters: a. Identification and documentation of the online privacy and related security requirements of authorized users. b. Allowing access, the nature of	The entity's documented online privacy and related security policies contain the elements set out in criterion 1.2.

[7] In some countries around the world, third-party arbitration is not an accepted means for the handling of consumer complaints. In those countries, the entity should follow customary laws and regulations. Such practices should be disclosed on its e-commerce systems.

	Criteria	Illustrative controls
	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 online privacy 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 online privacy and related security issues are resolved, and use of a third-party dispute resolution process that conforms to the principles of arbitration. [*See Appendix A*.] i. The procedures to handle online privacy and related security breaches and other incidents. j. Provision for allocation for training and other resources to support its online privacy and related system security policies. k. Provision for the handling of exceptions and situations not specifically addressed in its online privacy 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. m. Providing notice to the customer regarding the information collected. n. Providing choice to the customer regarding the type(s) of information gathered and any options the customer has regarding the collection of this information. o. Permitting access by the customer to his or her personal	

	Criteria	Illustrative controls
	information for update and corrective purposes. p. Record retention and destruction practices.	
1.3	Responsibility and accountability for the entity's online privacy and related system security policies, and changes and updates to those policies, are assigned.	Management has assigned responsibilities for the maintenance and enforcement of the entity's online privacy and related system security policies to the CPO. 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 the online privacy of and related security over such resources is defined.
2.0	**Communications: The entity communicates its defined policies regarding the protection of personal 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.	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 B*.]
2.2	The online privacy and related security obligations of users and the entity's online privacy and related security commitments to users are communicated to authorized users and disclosed on the entity's Web site. These disclosures include, but are not limited to, the following matters: a. The specific kinds and sources of information being collected and maintained, the use of that information, and possible third-party distribution of that information. If information is provided to third parties, disclosure includes any limitation on the reliance on the third party's privacy practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's privacy practices and controls that meet or exceed those of the entity. Such third-parties might include: • Parties who participate in completing the transaction (for example, credit card processors, delivery services, and fulfillment organizations). • Parties not related to the transaction (for example, marketing organizations to	The entity's disclosed user obligations and privacy and related security commitments contain the elements set out in criterion 2.2. For its internal users (employees and contractors), the entity's policies relating to online privacy 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. Security and privacy obligations of contractors are detailed in their contract. A privacy awareness program has been implemented to communicate the entity's online privacy and related security policies to employees. The entity publishes its online privacy and related security policies on its corporate intranet.

	Criteria	Illustrative controls
	whom information is provided). b. Choices regarding how personal information collected from an individual online may be used and/or distributed. Individuals are given the opportunity to opt out of such use, by either not providing such information or denying its distribution to parties not involved with the transaction. c. Sensitive information needed for the e-commerce transaction. Individuals must opt in before this information is gathered and transmitted. d. The consequences, if any, of an individual's refusal to provide information or of an individual's decision to opt out of (or not opt in to) a particular use of such information. e. How personal information collected can be reviewed and, if necessary, corrected or removed.	
2.3	If the entity's Web site uses cookies or other tracking methods (for example, Web bugs and middleware), the entity discloses how they are used. If the customer refuses cookies, the consequences, if any, of such refusal are disclosed.	The entity discloses its use of cookies on its Web site.
2.4	The process for obtaining support and informing the entity about breaches of online privacy and systems security is communicated to authorized users.	The process for customers and external users to inform the entity of possible privacy and related security breaches and other incidents is posted on the entity's Web site. The entity's privacy 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 privacy and security breaches and other incidents.
2.5	The entity discloses its procedures for consumer recourse for issues regarding privacy that are not resolved by the entity. These complaints may relate to collection, use, and distribution of personal information, and the consequences for failure to resolve such complaints. This resolution process has the following attributes: a. Management's commitment to use a specified third-party dispute resolution service or other process mandated by	The entity discloses its consumer recourse procedures on its Web site.

	Criteria	Illustrative controls
	regulatory bodies in the event the customer is not satisfied with the entity's proposed resolution of such a complaint together with a commitment from such third party to handle such unresolved complaints. b. Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party. c. What use or other action will be taken with respect to the personal information which is the subject of the complaint until the complaint is satisfactorily resolved.	
2.6	The entity discloses any additional privacy practices needed to comply with applicable laws or regulations or any self-regulatory programs in which the entity participates.	The entity discloses additional privacy practices on its Web site.
2.7	In the event that a disclosed online privacy policy is discontinued or changed to be less restrictive, the entity provides clear and conspicuous customer notification of the revised policy.	Changes to the entity's online privacy policies are disclosed on its Web site for a minimum period of three months from the effective date of the change.
2.8	The entity notifies users when they have left the site covered by the entity's online privacy policies.	The entity uses pop-up windows to notify users that they are leaving the site covered by the entity's online privacy policies. Use of pop-up windows for this purpose is disclosed on the entity's Web site.
2.9	Responsibility and accountability for the entity's online privacy and related system security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Management has assigned responsibility and accountability for the entity's privacy policies to the CPO. Responsibility and accountability for the entity's security policies is assigned to the chief information officer (CIO). The CPO has custody of and is responsible for the day-to-day maintenance of the entity's online privacy policies, and recommends changes to the management committee.
2.10	Changes that may affect online privacy and system security are communicated to management and users who will be affected.	Changes that may affect customers and users and their online privacy or related security obligations or the entity's online privacy or related security commitments are highlighted on the entity's Web site. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly information technology (IT) steering committee meetings. Changes to system components that may affect online privacy require the approval of the CPO before implementation. There is periodic communication of changes, including changes that may affect online privacy and system security. Changes that affect online privacy or system security are incorporated into the entity's ongoing privacy and security awareness programs.

	Criteria	Illustrative controls
3.0	**Procedures - The entity uses procedures to achieve its documented privacy objectives in accordance with its defined policies.**	
3.1	The entity's procedures provide that personal information is disclosed only to parties essential to the transaction, unless customers are clearly notified before providing such information. If the customer was not clearly notified when he or she submitted the information, customer permission is obtained before such information is released to third parties.	Entity procedures require that customers are given the clear and conspicuous option about sharing their information with other parties not associated with the transaction and that there are controls in place to track those options within the entity's database.
3.2	The entity's procedures provide that personal information obtained as a result of e-commerce is used by employees only in ways associated with the entity's business.	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits disclosures of information and other data to which the employee has access to other individuals or entities. Appropriate access controls are in place that limit access to sensitive, confidential, or personal information based on job function and need.
3.3	The entity has procedures to edit and validate personal information as it is collected, created, or maintained.	The entity accepts data only from the customer or other reliable sources and uses reliable collection methods. Before completing the transaction, customers are prompted by the system to check the personal data they have entered. Customers have the opportunity to correct any personal data entered before completing the transaction.
3.4	The entity has procedures to obtain assurance or representation that the information protection and privacy policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's disclosed privacy policies.	The entity outsources technology support or service and transfers data to the outsource provider. 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.
3.5	Customer permission is obtained before downloading files and information to be stored, altered, or copied on a customer's computer. a. 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. b. The entity requests customer permission to store, alter, or copy information (other than cookies) in the customer's computer.	The entity requests the customer's permission before it intentionally stores, alters, or copies information in the customer's computer. The entity requests the customer's permission before it performs any diagnostic or inventory on the customer's computer. The consumer registration page notifies and requests permission from consumers to use cookies to expedite site registration and logon. Customers are prompted when files are to be downloaded as part of the service.
3.6	In the event that a disclosed privacy practice is discontinued or changed to be less restrictive, the entity has procedures to protect personal information in accordance with the privacy practices in place when	Data collected before and after each privacy policy change are tracked in the entity's database. When changes to a less restrictive policy are made, the entity sends notification of such changes and deletions to affected customers and requests that the customers opt in to the new policy. Customers who do not opt in to the new policy will continue to be protected under the

	Criteria	Illustrative controls
	such information was collected, or obtains customer consent to follow the new privacy practice with respect to the customer's personal information.	old policy.
	Security-related criteria relevant to online privacy	
3.7	Procedures exist to restrict logical access to personal information obtained through e-commerce 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. Procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information. f. Procedures to limit access to personal information to only authorized employees based upon their assigned roles and responsibilities. g. Distribution of output restricted to authorized users. 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).	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 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.

	Criteria	Illustrative controls
		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 personal information: • Requests for privileges to access information designated as private require the approval of the assigned data owner. 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.
3.8	Procedures exist to restrict physical access to the components of the entity's system(s) that contain or protect personal information obtained through e-commerce 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.

	Criteria	Illustrative controls
		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.
3.9	Procedures exist to protect against unauthorized logical access to e-commerce system(s).	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.
3.10	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.
3.11	A minimum of 128-bit encryption or other equivalent security techniques are used to protect transmissions of user authentication and other personal 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. Transmission of private customer information to third-party service providers for processing is done over leased lines.
3.12	Procedures exist to identify, report, and act upon privacy and related security breaches and other incidents.	Customers are directed to an area of the Web site with instructions to enable the customer to contact the incident response hotline by telephoning or to post a message about security breaches or possible online privacy breaches as soon as they become concerned. These customer comments are followed up within 24 hours for evaluation, and a report is issued to the customer and CPO. 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.

	Criteria	Illustrative controls
		Documented incident identification and escalation procedures are approved by management.
3.13	Procedures exist to provide that issues of noncompliance with online privacy and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	Privacy and related security breaches or other incidents are reported immediately to the IT security team and the CPO. Corrective action, decided upon in conjunction with the CPO, is noted and monitored by management. Security policies, controls, and procedures are audited by the internal audit department as part of its ongoing internal audit plan. 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	
3.14	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software related to online privacy and security are consistent with defined online privacy 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 classifying data, including customer and regulatory privacy requirements. Standard user profiles are established based on privacy requirements and an assessment of the business impact of the loss of security. Users are assigned standard profiles based on needs and functional responsibilities. Owners and custodians of personal information collected through the entity's e-commerce systems classify its sensitivity and determine the level of protection required to maintain an appropriate level of privacy. The CPO and/or 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 online privacy and related security policies. Changes to system components that may affect security require the approval of the CPO and/or 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 online privacy and related security policies. The entity contracts with third parties to conduct periodic privacy and security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management. Periodic assessments are conducted by the internal audit team to compare existing online privacy and system security features to documented online privacy and system security policies and to regulatory requirements.
3.15	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting online privacy 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

	Criteria	Illustrative controls
		development activities. Personnel receive training and development in privacy and system security concepts and issues. Attendance and execution of these programs is monitored by the CPO. Procedures are in place to provide alternate personnel for key privacy and system security functions in case of absence or departure.
	Maintainability-related criteria relevant to online privacy	
3.16	Procedures exist to maintain system components, including configurations consistent with the defined online privacy and related security policies.	Entity management receives a third-party opinion on the adequacy of privacy procedures and related 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 online privacy and related security policies. System configurations are tested annually, and evaluated against the entity's online privacy and related 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 the CPO, representatives from the lines of business, and customer support, meets monthly and reviews anticipated, planned, or recommended changes to the entity's online privacy and related security policies, including the potential impact of legislative changes.
3.17	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. Simulated data is used for software development and testing. Personal information is not used for this purpose. 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.

	Criteria	Illustrative controls
3.18	Procedures exist to require 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 policies regarding the protection of personal information.**	
4.1	The entity's privacy and security performance is periodically reviewed and compared with the entity's defined online privacy and related 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 privacy assessment and related 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 online privacy and related security policies.	Logs are analyzed to identify trends that may have a potential impact on the entity's ability to achieve its privacy and related system security objectives. Monthly IT staff meetings are held to address privacy and related system security concerns and trends; findings are discussed at quarterly management meetings.
4.3	Environmental and technological changes are monitored and their impact on the entity's online privacy and security is assessed on a timely basis.	The CPO, in conjunction with outside legal counsel, monitors legislative privacy requirements and evolving industry privacy practices in the key markets which the entity serves. 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 online privacy 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

.36 The *confidentiality principle* focuses on information designated as confidential. Unlike personally identifiable information, which is being defined by regulation in a number of countries worldwide, 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.

.37 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

.38 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.

.39 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

.40 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.	The entity's documented confidentiality and related security policies contain the elements set out in criterion 1.2.

	Criteria	Illustrative controls
	k. Provision for the handling of exceptions and situations not specifically addressed in its system confidentiality 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.	
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 B.*] 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 C.*]
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: a. How information is designated as confidential and ceases to be confidential. b. How access to confidential information is authorized. c. How confidential information is used. d. How confidential information is shared. 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'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. 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. 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. A security awareness program has been implemented to communicate the entity's confidentiality and security policies to employees.

	Criteria	Illustrative controls
	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.	The entity publishes its confidentiality and related security policies on its corporate intranet.
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 accordance 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

	Criteria	Illustrative controls
		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. e. Procedures to prevent customers, groups of individuals, or other entities from accessing other than their own confidential information. 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. h. Restriction of logical access to	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: • 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

	Criteria	Illustrative controls
	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).	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 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

	Criteria	Illustrative controls
		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

	Criteria	Illustrative controls
		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 and software related to confidentiality and security are consistent with defined confidentiality 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 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

	Criteria	Illustrative controls
		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 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 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

	Criteria	Illustrative controls
		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.

	Criteria	Illustrative controls
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.

APPENDIX A

CONSUMER ARBITRATION

This appendix applies to engagements that use an arbitration program. Should a program mandated by a regulatory body be in effect, that program would be followed and disclosed. This appendix provides additional information about the arbitration process.

Before arbitration can take place, two parties must agree to it. An agreement may take many forms other than a written contract. Both parties show their agreement by some reasonable, affirmative act. An organization's Web site may invite acceptance by conduct, such as a check box or other means, and may propose limitations on the kind of conduct that constitutes acceptance. For example, consumers may find the following language at a Web site, which would constitute acceptance of an agreement:

> By accessing this Web site or ordering products described on this site, you agree to be bound by certain terms and conditions. Please read these terms and conditions carefully.

The terms and conditions would elaborate on arbitration, consumer recourse, and other issues for both the consumer and the Web site.

PRINCIPLES OF ARBITRATION

Under the model adopted for Trust Services, arbitration must be based on the rules of law, applied consistently. Outlined below, as an example, are the 12 principles identified by the National Arbitration Forum (NAF).

1. *Fundamentally fair process.* All parties in an arbitration process are entitled to fundamental fairness.
2. *Access to information.* Information about arbitration should be reasonably accessible before the parties commit to an arbitration contract.
3. *Competent and impartial arbitrators.* The arbitrators should be both skilled and neutral.
4. *Independent administration.* An arbitration should be administered by someone other than the arbitrator or the parties themselves.
5. *Contracts for dispute resolution.* An agreement to resolve disputes through arbitration is a contract and should conform to the legal principles of contract and statutory law. Arbitration contracts drafted by a fiduciary party should be accompanied by an accurate explanation of the advantages and disadvantages of arbitration.
6. *Reasonable costs.* The cost of an arbitration should be proportionate to the claim and reasonably within the means of the parties, as required by applicable law.
7. *Reasonable time limits.* A dispute should be resolved with reasonable promptness.

8. *Right to representation.* All parties have the right to be represented in an arbitration, if they wish, for example, by an attorney or other representative.
9. *Settlement and mediation.* The preferable process is for the parties themselves to resolve the dispute.
10. *Hearings.* Hearings should be convenient, efficient, and fair for all.
11. *Reasonable discovery.* The parties should have access to the information they need to make a reasonable presentation of their case to the arbitrator.
12. *Award and remedies.* The remedies resulting from arbitration must conform to the law.

APPENDIX B

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.

Security

Criteria Reference		Illustrative Disclosures
2.2	The security obligations of users and	Even though we strive to protect the information you provide through

	the entity's security commitments to users are communicated to authorized users.	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

Criteria Reference		Illustrative Disclosures
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 communicated to authorized users.	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 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

Criteria Reference		Illustrative Disclosures
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: 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).	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. 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. 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. 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. 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. 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. We will notify you by e-mail within 24 hours if we cannot fulfill your

	• 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.	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. We require an electronic funds transfer of fees and costs at the end of the transaction. For new customers, a deposit may be required. 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. 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. 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. 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. 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. For the details of the terms and conditions of arbitration, click here. 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.
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.

Online Privacy

Criteria Reference		Illustrative Disclosures
2.2	The online privacy and related security obligations of users and the entity's online privacy and related security commitments to users are communicated to authorized users and disclosed on the entity's Web site. These disclosures include, but are not limited to, the following matters: a. The specific kinds and sources of information being collected and maintained, the use of that information, and possible third-party distribution of that information. If information is provided to third parties, disclosure includes any limitation on the reliance on the third party's privacy practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's privacy practices and controls that meet or exceed those of the entity. Such third-parties might include: ▪ Parties who participate in completing the transaction (for example, credit card processors, delivery	We will need certain information—such as name, Internet address or screen name, billing address, type of computer, and credit card number—to provide our service to you. Your e-mail address is used to send information about our company. Your credit card number is used for billing purposes for the products you order. We may also use this information, along with information such as your age, income level, and postal code, to keep you informed about additional products and services from our company, and to send promotional material that may be of interest to you from some of our partners. Your age, income level, and postal code are also used to tailor the content displayed to correspond to your preferences. We do not provide information gathered from you to any other third parties except as required by law.

	services, and fulfillment organizations). ▪ Parties not related to the transaction (for example, marketing organizations to whom information is provided). b. Choices regarding how personal information collected from an individual online may be used and/or distributed. Individuals are given the opportunity to opt out of such use, by either not providing such information or denying its distribution to parties not involved with the transaction. c. Sensitive information needed for the e-commerce transaction. Individuals must opt in before this information is gathered and transmitted. d. The consequences, if any, of an individual's refusal to provide information or of an individual's decision to opt out of (or not opt in to) a particular use of such information. e. How personal information collected can be reviewed and, if necessary, corrected or removed.	You can choose not to receive information and promotional material from us and/or our partners by letting us know on the registration screen when you sign up for the product or service. If you subsequently wish to change your preference to opt in or opt out, go to the xxx screen, or send an e-mail to xxx@domain.com with the message opt in or opt out in the subscribe field. Before we can process your insurance application, we require that you click here to give us your permission to submit your medical history to the various insurance companies we use. This is your explicit permission for us to process your request. If you do not wish to have this information transmitted, we will be unable to process your application. You may call our customer service department for additional information or assistance. The minimum information you need to provide to complete the transaction is highlighted on the Web page. You will be unable to place an order without providing this minimum information. This site provides you with the ability to correct, update, or remove your information by e-mailing CustServ@ABC.com.
2.3	If the entity's Web site uses cookies or other tracking methods (for example, Web bugs and middleware), the entity discloses how they are used. If the customer refuses cookies, the consequences, if any, of such refusal are disclosed.	Cookies are used to personalize Web content and suggest items of potential interest based on your previous buying habits. This cookie can be read only by us. If you do not accept this cookie, you may be asked to re-enter your name and account number several times during a visit to our Web site or if you return to the site later. By accepting a cookie, certain information [*disclose information*] will be tracked and used for marketing purposes. Our cookies expire in 30 days. Certain advertisers on our site use tracking methods, including cookies, to analyze patterns and paths through this site. To opt out of this practice, refer to their privacy policy at www.domain.com/privacy/opt-out.html.
2.4	The process for obtaining support and informing the entity about breaches of online privacy and systems security 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. If you have any questions about our organization or our policies on privacy as stated at this site, please contact CustServ@ABC.com. Access to your customer data file is made available to our customer support representatives to fully service your inquiries. After hours, our customer support inquiries are managed by our service provider xxx, who is contractually required to comply with our privacy policy.
2.5	The entity discloses its procedures for	Transactions at this site, with respect to privacy, are covered by

	consumer recourse for issues regarding privacy that are not resolved by the entity. These complaints may relate to collection, use, and distribution of personal information, and the consequences for failure to resolve such complaints. This resolution process has the following attributes: a. Management's commitment to use a specified third-party dispute resolution service or other process mandated by regulatory bodies in the event the customer is not satisfied with the entity's proposed resolution of such a complaint together with a commitment from such third party to handle such unresolved complaints. b. Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party. c. What use or other action will be taken with respect to the personal information which is the subject of the complaint until the complaint is satisfactorily resolved.	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. For transactions at this site with respect to privacy, 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, then 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.
2.6	The entity discloses any additional privacy practices needed to comply with applicable laws or regulations or any self-regulatory programs in which the entity participates.	Federal law requires that all personal information be removed from the system after three years of inactivity.
2.7	In the event that a disclosed online privacy policy is discontinued or changed to be less restrictive, the entity provides clear and conspicuous customer notification of the revised policy.	During the period from May 31 to August 31, 20XX, we collected customer telephone numbers. Starting September 1, we no longer require this information for the processing of your transaction. On September 30, 20XX, we were acquired by XYZ Co. Accordingly, we adopted the privacy policies of XYZ Co., which allow the distribution of collected personal information to third parties. Because our previous policy did not allow for the distribution of such personal information, we will obtain your permission before the distribution of such information collected before September 30, 20XX.
2.8	The entity notifies users when they have left the site covered by the entity's online privacy policies.	Many of our partners have pages that look and navigate like our site. We will notify you via a one-time pop-up window to let you know that you are leaving our site and are no longer covered by our privacy practices. We strive to protect your information and suggest that you read the privacy policies of the site to which you are redirected *before* supplying any personal information. In accordance with our privacy policy we will not pass any information to these sites without your express consent.
2.10	Changes that may affect online privacy 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 online privacy 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 online privacy and security policies.

Confidentiality

Criteria Reference		Illustrative Disclosures
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: a. How information is designated as confidential and ceases to be confidential. b. How access to confidential information is authorized. c. How confidential information is used. d. How confidential information is shared. 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.	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. 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. 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. 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. 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. 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. 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 sub-accounts 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.

APPENDIX C:

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 D

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.[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, online privacy, and confidentiality. 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.

---

[1] Audit reporting for certification authorities is dealt with in *Suitable Trust Services Criteria and Illustrations for WebTrust® for Certification Authorities* in the Suitable Trust Services Criteria and Illustrations section of *Technical Practice Aids*.

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

- *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.[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.[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.

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.

---

[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).

[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.

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

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, online 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 online 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.[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.[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.

Similar to any attest engagement, before a practitioner can render an opinion, sufficient and competent evidential matter needs to be obtained.[7] For all criteria, there needs to be sufficient client transaction volumes and other procedure and control evidence to provide the practitioner

---

[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)."

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

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

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[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 • Established site, with little transaction volatility • Operations that experience infrequent changes to disclosures, policies, and related controls • Start-up operation with significant transaction volumes and operating conditions (typical of expected normal operations) during the practitioner's pre-implementation testing period and a transition to a live operational site that expects infrequent changes in policies and controls once it is operational	• Start-up operation that has not generated, during pre-implementation stages, sufficient transaction volume and conditions typical of expected normal operations • Operations that experience volatile transaction volumes • Complex operations • Operations that experience frequent changes to disclosures, policies, and related controls or significant instances that lack compliance with disclosures, policies, and related controls

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

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.aicpa.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.[9] The representation letter ordinarily would include a representation concerning subsequent events.

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, *Codification of Auditing Standards and Procedures* (AICPA, *Professional Standards,* vol. 1, AU sec. 561, "Subsequent Discovery of Facts Existing at the Date of the Auditor's Report").[10]

---

[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).

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

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,[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.[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 3 are period-of-time report examples. Illustration 4 is a point-in-time report example.

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.

---

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

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

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 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.*]

Illustration 2—WebTrust Report for Consumer Protection—Reporting Directly on the Subject Matter (Period-of-Time Report)

Independent Practitioner's WebTrust Report on Consumer Protection

To the Management of ABC Company, Inc.:

We have examined ABC Company, Inc.'s (ABC Company) compliance with the AICPA/CICA Trust Services Criteria for consumer protection, and based on these Criteria, the effectiveness of controls over the Online Privacy and Processing Integrity of the _____ (*system under examination*) System during the period {*Month, day, year*] through [*Month, day, year*]. The compliance with these criteria and 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.

Within the context of AICPA/CICA Trust Services, consumer protection addresses the controls over personally identifiable information and the processing of electronic commerce transactions. The AICPA/CICA Trust Services Online Privacy and Processing Integrity Criteria are used to evaluate whether ABC Company's controls over consumer protection of its [*system under examination*] System are effective. Consumer protection does not address the quality of ABC Company's goods [*information or services*] nor their suitability for any customer's intended purpose.

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 online privacy and processing integrity controls; (2) testing and evaluating the operating effectiveness of the controls; (3) testing compliance with the Online Privacy and Processing Integrity Criteria; 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 complied, in all material respects, with the criteria for consumer protection and maintained, in all material respects, effective controls over the -_____[*system under examination*] System to provide reasonable assurance that:

- Personal information obtained as a result of electronic commerce was collected, used, disclosed, and retained as committed or agreed, and
- 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 consumer protection.

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 WebTrust 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.

This report does not include any representation as to the quality of the ABC Company's goods [*information or services*] nor their suitability for any customer's intended purpose.

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

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

Illustration 3—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 4—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 failure 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.*]

AICPA
Assurance Services Executive Committee
Susan Rucker, *Chair*
Gari Fails
Everett C. Johnson, Jr.
John Lainhart
Thomas Siders
Mike Starr
Keith Vance
Thomas Wallace
Neal West

CICA
Assurance Services Development Board
Doug McPhie, *Chair*
Marilyn Kuntz
Doug Timmins

Staff Contacts:
Anthony J. Pugliese
Vice President, Member Innovation

J. Louis Matherne
Direction, Business Assurance and Advisory Services

Staff Contacts:
Cairine M. Wilson,
Vice President, Innovation

Gregory P. Shields,
Director, Assurance Services Development

AICPA / CICA Trust Services Task Force

Thomas E. Wallace, *Chair*
Gary Baker
Bruce R. Barrick
Efrim Boritz
Joseph G. Griffin
Arturo Lopez
Emil Ragones
Donald E. Sheehy
Christian R. Stormer
Alfred F. Van Ranst, Jr.
Miklos Vasarhelyi
Jeff Ward

The AICPA and CICA are extremely grateful to Chris Leach for co chairing this task force at its inception and to Robert Parker, Robert Reimer, David Ross and Kerry Shackelford for their technical assistance with this document.

Staff Contacts:

Bryan Walker, CICA

Principal, Assurance Services Development

For issues related to this release, please email assure@aicpa.org.

Karyn Waller, AICPA

Senior Technical Manager, Trust Services