TRUST SERVICES PRINCIPLES, CRITERIA, AND ILLUSTRATIONS

(To supersede the 2006 version of the Suitable Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy [AICPA,* Technical Practice Aids*, TSP sec. 100])

TSP Section 100

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

Introduction

.01 This section provides guidance to a practitioner providing attestation services, advisory services, or both that address IT-enabled systems including electronic commerce (e-commerce) systems[1] and privacy programs. The guidance is relevant when providing services with respect to system security, availability, processing integrity, confidentiality, and privacy.

.02 The guidance provided in this section includes

- trust services principles and criteria;
- examples of system descriptions; and
- illustrative practitioner reports for trust services engagements.

Trust Services

.03 The term *trust services* is defined as a set of professional attestation and advisory services based on a core set of principles and criteria that addresses the risks and opportunities of IT-enabled systems and privacy programs. Trust services principles and criteria are issued by the Assurance Services Executive Committee of the AICPA (the committee).

Attestation Services

.04 Attestation services include examination, review,[2] and agreed-upon procedures engagements. In examination and review engagements, the reporting practitioner expresses an opinion. In an examination engagement, for example, there is an opinion as to whether controls over a defined system were operating effectively to meet the criteria for systems reliability. In an agreed-upon procedures engagement, the practitioner does not express an opinion but rather performs procedures agreed upon by specified parties

---

[1] A *system* consists of five key components organized to achieve a specified objective. The five components are categorized as follows:

- *Infrastructure.* The physical and hardware components of a system (facilities, equipment, and networks)
- *Software.* The programs and operating software of a system (systems, applications, and utilities)
- *People.* The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- *Procedures.* The programmed and manual procedures involved in the operation of a system (automated and manual)
- *Data.* The information used and supported by a system (transaction streams, files, databases, and tables)

[2] A practitioner should not accept an engagement to review an entity's controls over a system related to the trust services principles and criteria.

and reports the findings. Attestation services are developed in accordance with AT section 101, *Attest Engagements* (AICPA, *Professional Standards*, vol. 1).

Advisory Services

.05 In the context of trust services, advisory services include strategic, diagnostic, implementation, sustaining, and managing services using trust services principles and criteria. Practitioners providing such services follow CS section 100, *Consulting Services: Definitions and Standards* (AICPA, *Professional Standards*, vol. 2). The practitioner does not express an opinion in these engagements.

Principles, Criteria, and Illustrative Controls

.06 The following guidance sets out (1) principles, which are broad statements of objectives, and (2) specific criteria that should be achieved to meet each principle. Criteria are benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter. The attributes of suitable criteria are objectivity, measurability, completeness, and relevance. The committee has concluded that the trust services criteria have all the attributes of suitable criteria. Furthermore, the publication of this guidance makes the criteria available to users. Trust services principles are used to describe the overall objective; however, the practitioner's opinion makes reference only to the criteria.

.07 In the trust services principles and criteria, the criteria are supported by a list of illustrative controls that, if operating effectively, enable a system to meet the criteria. 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 that the client has in place to satisfy the criteria. The choice and number of those controls would be based on such factors as the entity's management style, philosophy, size, and industry.

.08. The following are the types of engagements a practitioner may perform using the trust services principles and criteria:

- Reporting on the operating effectiveness of an entity's controls over the system.
- Reporting on the operating effectiveness of an entity's controls and the entity's compliance with its commitments related to the trust services principle(s) and criteria.
- Reporting on the suitability of the design of the entity's controls over the system to achieve the trust services principle(s) and criteria, if the controls were operating effectively. (This engagement would typically be performed prior to the system's implementation.)

When the subject matter of the engagement is an entity's privacy program, the report must cover the entity's compliance with its commitments. For purposes of brevity, this document primarily addresses engagements in which the practitioner reports on the operating effectiveness of controls over a system to achieve the trust services principles and criteria. However, the guidance is equally applicable to engagements to report on any of the subject matters listed in this paragraph, unless otherwise specified. In addition, AT section 101 permits a practitioner to report on either the subject matter or an assertion about the subject matter (see appendix C, "Management's Assertion").

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

.09 Several of the principles and criteria refer to "consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contracts." Management is responsible for identification of and compliance with laws and regulations. It is 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, when reporting on the operating effectiveness of a entity's controls, trust services engagements do not require the practitioner to test or report on an entity's compliance with applicable laws and regulations, defined commitments, service-level agreements, and other contracts but rather to report on the effectiveness of the entity's controls over monitoring compliance with them. When reporting on compliance with commitments, reference also should be made to other professional standards related to reporting on an entity's compliance with laws, regulations, and agreements.[3]

Foundation for Trust Services—Trust Services Principles and Criteria

.10 The following principles and related criteria have been developed by the AICPA and the Canadian Institute of Chartered Accountants (CICA) for use by practitioners in the performance of trust services engagements:[4]

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

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

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

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

e. *Privacy.* Personal information[5] is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and CICA (found in appendix D [paragraph .48]).

.11 The trust services principles and criteria of security, availability, processing integrity, and confidentiality are organized into four broad areas:

a. *Policies.* The entity has defined and documented its policies relevant to the particular principle. (The term *policies* as used here refer to written statements that communicate management's intent, objectives, requirements, responsibilities, and standards for a particular subject.)

b. *Communications.*[6] The entity has communicated its defined policies to responsible parties and authorized users of the system.

---

[3] See AT section 601, *Compliance Attestation* (AICPA, *Professional Standards*, vol. 1)

[4] SysTrust and WebTrust are two specific assurance services offerings developed by the AICPA and Canadian Institute of Chartered Accountants (CICA) that are based on the Trust Services Principles and Criteria. Practitioners must be licensed by the CICA to use these registered service marks. For more information on licensure, see www.webtrust.org.

[5] Personal information is information that is about or can be related to an identifiable individual.

[6] 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"

c. *Procedures.* The entity placed in operation 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.

.12 For the trust services principles and criteria of security, availability, processing integrity, and confidentiality, a two-column format has been used to present the criteria. The first column presents the criteria for each principle, and the second column provides illustrative controls.

.13 A system description is used to delineate the boundaries of the system under examination for the trust services principles and criteria of security, availability, processing integrity, and confidentiality. For engagements covering an entity's compliance with its commitments, those commitments should be included in system description or should otherwise accompany the report. Examples of system descriptions for both e-commerce and non-e-commerce systems are included in appendix A (paragraph .45) and appendix B (paragraph .46), respectively. Appendix A (paragraph .45) also includes sample disclosures related to specific principles and criteria for e-commerce systems.

.14 A reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. A practitioner may provide a report on systems reliability that addresses the trust services principles and criteria of security, availability, and processing integrity. Theses criteria are used to evaluate whether a system is reliable.

.15 The trust services principles and criteria of privacy are organized into two broad areas:

a. *Policies and communications.* Privacy policies are written statements that convey management's intent, objectives, requirements, responsibilities, and standards concerning privacy. Communications refers to the organization's communication to individuals, internal personnel, and third parties about its privacy notice and its commitments therein and other relevant information.

b. *Procedures and controls.* The other actions the organization takes to achieve the criteria.

.16 The scope of a privacy engagement can cover (1) either all personal information or only certain identified types of personal information, such as customer information or employee information, and (2) all business segments and locations for the entire entity or only certain identified segments of the business (for example, retail operations but not manufacturing operations or only operations originating on the entity's Web site or specified Web domains) or geographic locations (such as only Canadian operations). The scope of a privacy engagement should cover all of the activities in the information life cycle that consists of the collection, use, retention, disclosure and destruction, de-identification, or anonymization.

.17 For the trust services principles and criteria of privacy, a three-column format has been used to present the criteria. The first column contains the measurement 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 and procedures, which are designed to enhance the understanding of the criteria. The

---

category of the criteria in such circumstances, the policies and processes required by each of the "Communications" criteria should be disclosed on the entity's Web site. Examples of such disclosures for each of the trust services principles are contained in appendix A (paragraph .45).

illustrations are not intended to be comprehensive, nor are any of the illustrations necessary for an entity to have met the criteria. The third column presents additional considerations, including supplemental information such as good privacy practices and selected requirements of specific laws and regulations that pertain to a certain industry or country.

Effective Date

.18 The trust services principles and criteria are effective as of September 15, 2009.

Principles and Criteria

Security Principle and Criteria

.19 The *security principle* refers to the protection of the system from unauthorized access, both logical and physical. Limiting access to the system helps prevent potential abuse of the system, theft of resources, misuse of software, and improper access to, or the use, alteration, destruction, or disclosure of information. Key elements for the protection of the system include permitting authorized access based on relevant needs and preventing unauthorized access to the system in all other instances.

Security Principle and Criteria Table

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

	Criteria	*Illustrative Controls* [7]
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.	Written security policy, addressing both IT and physical security, has been approved by the IT standards committee and is implemented throughout the company. As part of the periodic corporate risk assessment process, the security officer identifies changes to the IT risk assessment based on new applications and infrastructure, significant changes to applications and infrastructure, new environmental security risks, changes to regulations and standards, and changes to user requirements as identified in service level agreements and other documents. The security officer then updates the security policy based on the IT risk assessment. Changes to the IT security policy are approved by the IT standards committee prior to implementation.
1.2	The entity's security policies include, but may not be limited to, the following matters: *a.* Identifying and documenting the security requirements of authorized	*An example of an illustrative control for this criterion would be an entity's documented security policy addressing the elements set out in criterion 1.2. An illustrative security policy has been omitted for brevity.*

[7] 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* [7]
users	
b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements	
c. Assessing risks on a periodic basis	
d. Preventing unauthorized access	
e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access	
f. Assigning responsibility and accountability for system security	
g. Assigning responsibility and accountability for system changes and maintenance	
h. Testing, evaluating, and authorizing system components before implementation	
i. Addressing how complaints and requests relating to security issues are resolved	
j. Identifying and mitigating security breaches and other incidents	
k. Providing for training and other resources to support its system security policies	
l. Providing for the handling of exceptions and situations not specifically addressed in its system security policies	
m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements	
n. Providing for sharing information with third parties	

	Criteria	*Illustrative Controls* [7]
1.3	Responsibility and accountability for developing and maintaining 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 security officer under the directions of the CIO. The IT standards committee of the executive committee assists in the review, update, and approval of the policy as outlined in the executive committee handbook.
2.0	**Communications: The entity communicates its defined system security policies to responsible parties and 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 A [paragraph .45]*.) For its non-e-commerce system, the entity has provided a system description to authorized users. (*For an example of a system description for a non-e-commerce based system, refer to appendix B [paragraph.46]*.)
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 to its customers and other external users are posted on the entity's Web site and 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, 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 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. Written job descriptions have been defined and are communicated to the security administration team. Written process and procedure manuals for all defined security processes are provided to security administration team personnel. The security officer updates the processes and procedures manuals based on changes to the security policy.
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 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* [7]
2.5	Changes that may affect system security are communicated to management and users who will be affected.	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. 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 and confidentiality are communicated in writing to affected customers for review and approval under the provisions of the standard services agreement before implementation of the proposed change. 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 placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.**	
3.1	Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.	A risk assessment is performed periodically. As part of this process, threats to security are identified and the risk from these threats is formally assessed. Security processes and procedures are revised by the security officer based on the assessed threats.
3.2	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:	
	a. Logical access security measures to restrict access to information resources not deemed to be public.	• Logical access to nonpublic information resources is protected through the use of native operating system security, native application and resource security, and add-on security software. • Resource specific or default access rules have been defined for all nonpublic resources. • Access to resources is granted to an authenticated user based on the user's identity.
	b. Identification and authentication of users.	• Users must establish their identity to the entity's network and application systems when accessing nonpublic resources through the use of a valid user ID that is authenticated by an associated password. • Unique user IDs are assigned to individual users. • Use of group or shared IDs is permitted only after completion of an assessment of the risk of the shared ID and written approval of the manager of the requesting business unit. • Passwords are case sensitive and must contain at least 8 characters, one of which is nonalphanumeric.

Criteria	*Illustrative Controls* [7]
	• Security configuration parameters force passwords to be changed every 90 days. • Login sessions are terminated after 3 unsuccessful login attempts.
c. 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 appropriate user ID and password. Privileges and authorizations associated with self-registered customer accounts provide specific limited system functionality. • The line-of-business supervisor authorizes access privilege change requests for employees and contractors. Access to restricted resources is authorized by the resource owner. • Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager or the resource owner. • Proper segregation of incompatible duties is considered in granting privileges based on the user's job description or role. • 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.
d. The process to make 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 made by the security administration team and require the written approval of the appropriate line-of-business supervisor or customer account manager and the resource owner. • The human resource management system provides the human resources team with a list of newly terminated employees on a weekly basis. This listing is sent to the security administration team for deactivation.
e. Distribution of output restricted to authorized users.	• Access to computer processing output is provided to authorized individuals based on the classification of the information. • Processing output is stored in an area that reflects the classification of the information. • Processing output is distributed in accordance with the security policy based on classification of the information.

	Criteria	Illustrative Controls [7]
	f. Restriction of access to offline storage, backup data, systems, and media.	• Access to offline storage, backup data, systems, and media is limited to computer operations staff through the use of physical and logical access controls.
	g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	• Hardware and operating system configuration tables are restricted to appropriate personnel through physical access controls, native operating system security, and add-on security software. • 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 in accordance with the company's IT policies. • 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.
3.3	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 physical security breaches. Offsite media are stored in locked containers in secured facilities. Physical access to these containers is restricted to facilities personnel and employees authorized by the manager of computer operations.
3.4	Procedures exist to protect against unauthorized access to system resources.	Login sessions are terminated after three unsuccessful login attempts. 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 appropri-

	Criteria	*Illustrative Controls* [7]
		ateness 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.
3.5	Procedures exist to protect against infection by computer viruses, malicious code, 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 promptly. Any viruses discovered are reported to the security team, and an alert is created for all users notifying them of a potential virus threat. The ability to install, modify, and replace operating system and other system programs is restricted to authorized personnel. Access to superuser functionality and sensitive system functions is restricted to authorized personnel.
3.6	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 industry standard encryption technology, VPN software, or other secure communication systems (consistent with its periodic IT risk assessment) for the transmission of private or confidential information over public networks, including user IDs and passwords. Users are required to upgrade their browsers to the most current version tested and approved for use by the security administration team to avoid possible security problems. Account activities, subsequent to successful login, are encrypted through industry standard encryption technology, VPN software, or other secure communication systems (consistent with its periodic IT risk assessment). Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.
	Criteria related to execution and incident management used to achieve objectives	
3.7	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 systems and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team or the network administrator via e-mail and text of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. When an incident is detected or reported, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. Procedures include a defined incident escalation process and notification mechanisms. All incidents are tracked by management until resolved.

	Criteria	*Illustrative Controls* [7]
		Closed incidents are reviewed by management for appropriate resolution. Resolution of incidents not related to security includes consideration of the effect of the incident and its resolution on security requirements.
	Criteria related to the system components used to achieve the objectives	
3.8	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary	Data owners periodically review data access rules and request modifications based on defined security requirements and risk assessments. Whenever new data are captured or created, the data are classified based on security policies, Propriety of data classification is considered as part of the change management process.
3.9	Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.	All incidents are tracked by management until resolved. Closed incidents are reviewed by management for appropriate resolution. The internal audit process includes the development of management actions plans for findings and the tracking of action plans until closed.
3.10	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software 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. The security administration team reviews and approves the architecture and design specifications for new systems development and acquisition to help 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.
3.11	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources 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.

	Criteria	*Illustrative Controls* [7]
		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.
	Change Management-related criteria applicable to the system's security	
3.12	Procedures exist to maintain system components, including configurations consistent with the defined system security policies.	Entity management receives a third-party opinion on the adequacy of security controls and routinely evaluates the level of performance it receives (in accordance with its contractual service-level agreement) from the service provider that hosts the entity's systems and Web site. The IT department maintains an up-to-date 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. 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.
3.13	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	The responsibilities for authorizing, testing, developing, and implementing changes have been segregated. 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 outstanding and closed 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).
3.14	Procedures exist to provide that emergency changes are documented and au-	Requests for changes, system maintenance, and supplier maintenance are standardized and subject to documented change manage-

	Criteria	*Illustrative Controls* [7]
	authorized timely.	ment procedures. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Emergency changes that require deviations from standard procedures are logged and reviewed by IT management daily and reported to the affected line-of-business manager. Permanent corrective measures follow the entity's change management process, including line-of-business approvals.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies.**	
4.1	The entity's system security is periodically reviewed and compared with the defined system security policies.	The information security team monitors the system and assesses the system vulnerabilities using proprietary and publicly available tools. Potential risks are evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementations are 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 either manually or by automated tools 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, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.	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

.21 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 by mutual agreement (contract) between the parties.

.22 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

.23 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.	A written availability policy has been approved by the IT standards committee and is implemented throughout the company. 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.
1.2	The entity's system availability and related security policies include, but may not be limited to, the following matters: *a.* Identifying and documenting the system availability and related security requirements of authorized users. *b.* Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements *c.* Assessing risks on a periodic basis *d.* Preventing unauthorized access. *e.* Adding new users, modifying the access levels of existing users, and removing users who no longer need access. *f.* Assigning responsibility and accountability for system availability and related security. *g.* Assigning responsibility and accountability for system changes and maintenance. *h.* Testing, evaluating, and authorizing system compo-	*An example of an illustrative control for this criterion would be an entity's documented availability policy and related security policy addressing the elements set out in criterion 1.2. Illustrative availability and securities policies have been omitted for brevity.*

	nents before implementation. *i.* Addressing how complaints and requests relating to system availability and related security issues are resolved. *j.* Identifying and mitigating system availability and related security breaches and other incidents. *k.* Providing for training and other resources to support its system availability and related security policies. *l.* Providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies. *m.* Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements. *n.* Recovering and continuing service in accordance with documented customer commitments or other agreements. *o.* Monitoring system capacity to achieve customer commitments or other agreements regarding availability	
1.3	Responsibility and accountability for developing and maintaining 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 CIO. The IT standards committee of the executive committee assists 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 are defined.
2.0	**Communications: The entity communicates the defined system availability policies to responsible parties and 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 A [paragraph .45]*.) For its non-e-commerce system, the entity has provided a system description to authorized users. (*For an example of a system de-*

		scription for a non-e-commerce based system, refer to appendix B [paragraph .46].)
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 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 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 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. Written job descriptions have been defined and are communicated to the network operations team and the security administration team. Written processes and procedures manuals for all operations and security processes are provided to personnel. Designated personnel update the processes and procedures manuals based on changes to availability requirements and security policies.
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 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 se-

		curity are communicated in writing to affected customers for review and approval under the provisions of the standard services agreement before implementation of the proposed change. Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee meetings. Changes to system components, including those that may affect system security, require the approval of the manager of network operations or the security administration team before implementation. There is periodic communication of system changes to users and customers, including changes that affect availability and system security.
3.0	**Procedures: The entity placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies.**	
3.1	Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.	A threat identification risk assessment is prepared and reviewed on a periodic 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.
3.2	Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	Management maintains measures to protect against environmental factors (for example, fire, flood, dust, power failure, and excessive heat and humidity) based on its periodic risk assessment. The entity's controlled areas are protected against fire using both smoke detectors and a fire suppression system. Water detectors are installed within the raised floor areas. The entity site is protected against a disruption in power supply to the processing environment by both uninterruptible power supplies and emergency power supplies. This equipment is tested 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.
3.3	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 IT application programs, operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on a business impact analysis. The business continuity planning coordinator reviews and updates the business impact analysis with the lines of business annually. Disaster recovery and contingency plans are tested annually in accordance with the entity's system availability policies. Testing results and change recommendations are reported to the entity's management committee. The entity's management committee reviews and approves changes to the disaster recovery plan. Contracted capacity at resumption facilities is compared to documented processing requirements on an annual basis and modified as necessary. 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.
3.4	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. An inventory of available backups and the physical location of the backups are maintained by operations personnel. 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	
3.5	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:	
	a. Logical access security measures to restrict access to information resources not deemed to be public.	• Logical access to nonpublic information resources is protected through the use of native operating system security, native application or resource security, and add-on security software. • Resource specific or default access rules have been defined for all nonpublic resources. • Access to resources granted to authenticated users based on their user profiles.

b.	Identification and authentication of users.	• Users must establish their identity to the entity's network and application systems when accessing nonpublic resources through the use of a valid user ID that is authenticated by an associated password. • Unique user IDs are assigned to individual users. • Use of group or shared IDs is permitted only after completion of an assessment of the risk of the shared ID and written approval of the manager of the requesting business unit. • Passwords are case sensitive must contain at least 8 characters, one of which is nonalphanumeric. • Security configuration parameters force passwords to be changed every 90 days. • Login sessions are terminated after 3 unsuccessful login attempts.
c.	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 appropriate user 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. Access to restricted resources is authorized by the resource owner. • Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. Proper segregation of duties is considered in granting privileges.
d.	The process to make 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. • The human resource management system provides the human resources team with a list of newly terminated employees on a weekly basis. This listing is sent to the security administration team for deactivation.
e.	Restriction of access to offline storage, backup data, systems	• Access to offline storage, backup data, systems, and media is limited to computer operations staff through the use of physical

	and media.	and logical access controls.
	f. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	• 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 in accordance with the company's IT policies. • 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, 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 physical 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 access to system resources.	Login sessions are terminated after three unsuccessful login attempts. 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 promptly. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat. The ability to install, modify, and replace operating system and other system programs is restricted to authorized personnel Access to superuser functionality and sensitive system functions is restricted to authorized personnel.
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 industry standard encryption technology, VPN software or other secure communication systems (consistent with its periodic IT risk assessment) for the transmission of private or confidential information over public networks, including user IDs and passwords. Users are required to upgrade their browsers to the most current versions tested and approved for use by the security administration team to avoid possible security problems. Account activities, subsequent to successful login, are encrypted through industry standard encryption technology, VPN software, or other secure communication systems (consistent with its periodic IT risk assessment). Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.
	Criteria related to execution and incident management used to achieve objectives	
3.10	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 system and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and the network administrator via e-mail and text 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 and include a defined incident escalation process and notification mechanisms. Network performance, system availability, and security incident statistics and comparisons to approved targets are accumulated and reported to the IT steering committee monthly. System performance and capacity analysis and projections are com-

		pleted annually as part of the IT planning and budgeting process. System and network operations are actively monitored by operations personnel. When a system disruption is detected or reported, a defined incident management process in initiated by systems and network operations personnel. Corrective actions are implemented in accordance with defined policies and procedures. All incidents are tracked by operations management until resolved. Closed incidents are reviewed by operations personnel for appropriate resolution.
	Criteria related to the system components used to achieve the objectives	
3.11	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.	Data owners periodically review data access rules and request modifications based on defined security and availability requirements and risk assessments Whenever new data are captured or created, the data are classified based on security and availability policies. Propriety of data classification is considered as part of the change management process.
3.12	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.	All incidents are tracked by management until resolved. Closed incidents are reviewed by management for appropriate resolution. The internal audit process includes the development of management actions plans for findings and the tracking of action plans until closed.
3.13	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software 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. • developing "backout" plans before implementation of changes. The security administration team reviews and approves the architecture and design specifications for new systems development and acquisition to ensure consistency with the entity's 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 entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.
3.14	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources 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 and security functions in case of absence or departure.
	Change management-related criteria applicable to the system's availability	
3.15	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 an up-to-date 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, security policies, and current service-level agreements. An exception report is prepared, and remediation plans are developed and tracked.
3.16	Procedures exist to provide that only authorized, tested, and documented changes are made to the	The responsibilities for authorizing, testing, developing, and implementing changes have been segregated.

	system.	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 outstanding and closed 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).
3.17	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 publicly available tools. Potential risks are evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed, and implementations are monitored. The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. The internal audit function conducts system availability and system security reviews as part of its annual audit plan. Results and recommendations for improve-

		ment 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 either manually or by automated tools 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, regulatory, and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis; policies are updated for that assessment.	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

.24 The *processing integrity principle* refers to the completeness, accuracy, validity, 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 are processed or all services are performed without exception. Validity means that transactions and services are not processed more than once and that they are in accordance with business values and expectations. Accuracy means that key information associated with the submitted transaction remains accurate throughout the processing of the transaction and that the transaction or service is processed or performed as intended. The timeliness of the provision of services or the delivery of goods is addressed in the context of commitments made for such delivery. Authorization means that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing.

.25 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 and effective processing integrity controls, the user may not receive the information, goods, or services requested. For example, a 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 operate effectively, there is a greater likelihood that the user will receive the information, goods, or services requested in the correct quantity, at the correct price, and when promised. Processing integrity addresses all of the system components including procedures to initiate, record, process, and report the information related to the 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 paragraph .27 identify some of these differences.

.26 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. Even in a case when the information stored by the system is explicitly included in the description of the system that defines the engagement, it is still possible that the system exhibits high processing integrity without exhibiting high data integrity. For example, an address stored in the system may have passed all appropriate edit checks and other processing controls when it was added to the system, but it may no longer be current (if a person or company relocated) or it may be incomplete (if an apartment number or mailing location is omitted from the address).

Processing Integrity Principle and Criteria Table

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

	Criteria	*Illustrative Controls*
1.0	**Policies: The entity defines and documents its policies for the processing integrity of its system.**	
1.1	The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.	Written policies addressing processing integrity have been approved by the executive committee and are implemented throughout the company. As part of the periodic corporate risk assessment process, management identifies changes to the risk assessment based on: new applications and infrastructure, significant changes to applications and infrastructure, new environmental risks, changes to regulations and standards, and changes to user requirements as identified in service level agreements and other documents. Management then updates the policies based on the risk assessment. User requirements are documented in service-level agreements or other documents. Changes to policies are approved by leadership prior to implementation
1.2	The entity's system processing integrity and related security policies include, but may not be limited to, the following matters: *a.* Identifying and documenting the system processing integrity and related security requirements of authorized users *b.* Classifying data based on their criticality and sensitivity; that	*An example of an illustrative control for this criterion would be an entity's documented processing integrity policy and security policy addressing the elements set out in criterion 1.2. Illustrative process integrity and security policies have been omitted for brevity.*

	classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements	
	c. Assessing risks on a periodic basis	
	d. Preventing unauthorized access	
	e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access	
	f. Assigning responsibility and accountability for system processing integrity and related security	
	g. Assigning responsibility and accountability for system changes and maintenance	
	h. Testing, evaluating, and authorizing system components before implementation	
	i. Addressing how complaints and requests relating to system processing integrity and related security issues are resolved	
	j. Identifying and mitigating errors and omissions and other system processing integrity and related security breaches and other incidents	
	k. Providing for training and other resources to support its system processing integrity and related system security policies	
	l. Providing for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies	
	m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements	
1.3	Responsibility and accountability for developing and maintaining entity's	Management has assigned responsibilities for the implementation of the entity's processing integrity and related security policies to indi-

	system processing integrity and related system security policies; changes, updates, and exceptions to those policies are assigned.	vidual members of management. Others on the executive committee assist in the review, update, and approval of the policies as outlined in the executive committee handbook.
2.0	**Communications: The entity communicates its documented system processing integrity policies to responsible parties and 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 (whether they are new, used, or reconditioned). — description of services (or service contract). — sources of information (where it was obtained and how it was compiled). *b.* The terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following matters: — Time frame for completion of transactions (*transaction* means fulfillment of orders where goods are being sold and delivery of service where a service is being provided) — Time frame and process for informing customers of exceptions to normal processing of orders or service requests — Normal method of delivery of goods or services, including customer options, where applicable	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 A [paragraph .45]*.) For its non-e-commerce system, the entity has provided a system description to authorized users. (*For an example of a system description for a non-e-commerce based system, refer to appendix B [paragraph .46]*.)

		— 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, as part of the entity's standard services agreement, or in both places. 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 contracts. A security awareness program has been implemented to communicate the entity's processing integrity and related security policies to employees. The entity publishes its IT security policies on its corporate intranet.
2.3	Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Management has assigned responsibilities for the enforcement of the entity's processing integrity policies to the COO. 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. Written job descriptions have been defined and are communicated to the security administration team. Written process and procedure manuals for all defined security processes are provided to security administration team personnel. The security officer updates the processes and procedures manuals based on changes to the security policy.
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, is provided as part of the new user welcome kit, or is in both places. 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.	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. 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 communicated in writing to affected customers for review and approval by affected customers under the provisions of the standard services agreement before implementation of the proposed change. There is periodic communication of changes that affect system security, including changes to users and customers. Changes are incorporated into the entity's ongoing user training and security awareness programs.
3.0	**Procedures: The entity placed in operation procedures to achieve its documented system processing integrity objectives in accordance with its defined policies.**	
3.1	Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair processing integrity commitments and (2) assess the risks associated with the identified threats.	A risk assessment is performed periodically. As part of this process, threats to processing integrity are identified and the risks from these threats are formally assessed. Processes and procedures are revised by management based on the assessed threats.
3.2	The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integ-	The entity has established data preparation procedures to be followed by user departments. Data entry screens contain field edits and range checks, and input

	rity policies. If the system is an e-commerce system, the entity's procedures include, but may not be limited to, the following matters:	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.
	a. The entity checks each request or transaction for accuracy and completeness.	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.
	b. Positive acknowledgment is received from the customer before the transaction is processed.	Logical access controls restrict data entry capability to authorized personnel. (See item 3.6 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 item 3.1 may take somewhat different forms, such as • account activity, subsequent to successful login, is encrypted through industry standard encryption software. • 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.
3.3	The procedures related to complete-	Responsibilities for order processing, application of credits and cash

	ness, 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:	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.
a.	The correct goods are shipped in the correct quantities in the time frame agreed upon, or services and information are provided to the customer as requested.	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.
b.	Transaction exceptions are promptly communicated to the customer.	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.
c.	Incoming messages are processed and delivered accurately and completely to the correct IP address.	The following additional controls are included in the entity's e-commerce system:
d.	Outgoing messages are processed and delivered accurately and completely to the service provider's (SP's) Internet access point.	• Packing slips are created from the customer sales order and checked by warehouse staff as the order is packed.
e.	Messages remain intact while in transit within the confines of the SP's network.	• 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.

3.4	The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies.	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.
	If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters:	The following additional controls are included in the entity's e-commerce system:
	• The entity displays sales prices and all other costs and fees to the customer before processing the transaction.	• 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.
	• Transactions are billed and electronically settled as agreed.	• Customers have the option of printing, before an online order is processed, an "order confirmation" for future verification with payment records (such as credit card statement) detailing information about the order (such as item(s) ordered, sales prices, costs, sales taxes, and shipping charges).
	• Billing or settlement errors are promptly corrected.	• 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.
3.5	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 3 years and is available for immediate access by customer service representatives. After 3 years, this information is maintained in offline storage. Original source documents are retained on image management systems for a minimum of 7 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	
3.6	Procedures exist to restrict logical access to the defined system including, but not limited to, the following mat-	

ters:

a. Logical access security measures to access information not deemed to be public	• Logical access to nonpublic information resources is protected through the use of native operating system security, native application and resource security, and add-on security software. • Resource specific or default access rules have been defined for all nonpublic resources. • Access to resources is granted to an authenticated user based on the user's identity.
b. Identification and authentication of authorized users	• Users must establish their identity to the entity's network and application systems when accessing nonpublic resources through the use of a valid user ID that is authenticated by an associated password. • Unique user IDs are assigned to individual users. • Use of group or shared IDs is permitted only after completion of an assessment of the risk of the shared ID and written approval of the manager of the requesting business unit. • Passwords are case sensitive must contain at least 8 characters, one of which is nonalphanumeric. • Security configuration parameters force passwords to be changed every 90 days. • The login sessions are terminated after 3 unsuccessful login attempts.
c. 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 appropriate user 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. Access to restricted resources is authorized by the resource owner. • Customer access privileges beyond the default privileges granted during self-registration are approved by the customer account manager. • Proper segregation of duties is considered in granting privileges.
d. The process to make 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 secu-

		rity administration team and require the approval of the appropriate line-of-business supervisor or customer account manager. • The human resource management system provides the human resources team with a list of newly terminated employees on a weekly basis. This listing is sent to the security administration team for deactivation.
	e. Distribution of output restricted to authorized users	• 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 access to offline storage, backup data, systems, and media	• 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 (for example, firewalls)	• 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 in accordance with the company's IT policies. • 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.
3.7	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 is 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 physical 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.
3.8	Procedures exist to protect against unauthorized access to system resources.	Login sessions are terminated after three unsuccessful login attempts.

		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.
3.9	Procedures exist to protect against infection by computer viruses, malicious code, 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 promptly. Any viruses discovered are reported to the security team, and an alert is created for all users notifying them of a potential virus threat. The ability to install, modify, and replace operating systems and other system programs is restricted to authorized personnel. Access to superuser functionality and sensitive system functions is restricted to authorized personnel.
3.10	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 industry standard encryption technology, VPN software, or other secure communication systems (consistent with its periodic IT risk assessment) for the transmission of private or confidential information over public networks, including user IDs and passwords. Users are required to upgrade their browsers 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 industry standard encryption technology, VPN software, or other secure communication systems (consistent with its periodic IT risk assessment). Users are logged out on request (by selecting the "Sign-out" button on the Web site) or after 10 minutes of inactivity.
	Criteria related to execution and incident management used to achieve objectives	
3.11	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 systems and other tools are used to identify, log,

		and report potential security breaches and other incidents. The system notifies the security administration team, the network administrator, or both via e-mail and text of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. When an incident is detected or reported, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. Procedures include a defined incident escalation process and notification mechanisms. All incidents are tracked by management until resolved. Closed incidents are reviewed by management for appropriate resolution. Resolution of incidents not related to security includes consideration of the impact of the incident and its resolution on security requirements.
	Criteria related to the system components used to achieve the objectives	
3.12	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary	The entity has a data quality assurance function. The data quality assurance group reviews data usage and ensures that metadata is documented. including, but not limited to, the following matters: *a.* Purpose *b.* Origin/Ownership, both internal and external *c.* Used by *d.* Custodian/Steward *e.* Standards governing *f.* Classification for security/privacy *g.* Access privileges *h.* Location (for searchability) *i.* Version *j.* Timestamp *k.* Retention/Disposal Requirements *l.* Source; Owner/responsible party/Lineage/Audit trail *m.* Assurance Whenever new data are captured or created, the data are classified based on security and process integrity policies. Propriety of data classification is considered as part of the change

		management process.
3.13	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.	The entity requires procedures to be consistent with policies and there is a process to check that procedures are consistent with policies. The entity monitors changes to policies and promptly updates procedures affected by those changes. 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.
3.14	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software 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. The security administration team reviews and approves the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's processing integrity and related security objectives, policies, and standards. Process owner review, approval of test results, and authorization are required for implementation of changes. Changes to system components that may affect security require the approval of the security administration team.
3.15	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security have qualifications and resources 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. Outsourced activities are included in assessments of personnel qualifications and resource adequacy. 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. Procedures are in place for allocating the number of personnel and other resources commensurate with the processing integrity and related security requirements.
	Change management-related criteria applicable to the system's processing integrity	
3.16	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 an up-to-date 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. 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 entity monitors changes to policies and promptly updates procedures affected by those changes.
3.17	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	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 outstanding and closed 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).
3.18	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	
3.19	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 periodic 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 periodic risk assessment. The entity's controlled areas are protected against fire using both smoke detectors and a fire suppression system. Water detectors are installed within the raised floor areas. The entity site is protected against a disruption in power supply to the processing environment by both uninterruptible power supplies and emergency power supplies. This equipment is tested semiannually. Preventive maintenance agreements and scheduled maintenance procedures are in place for key system hardware components. Vendor warranty specifications are complied with and tested to determine if the system is properly configured. Procedures to address minor processing errors, outages, and destruction of records are documented. Procedures exist for the identification, documentation, escalation, resolution, and review of problems. Physical and logical security controls are implemented to reduce the opportunity for unauthorized actions that could impair system processing integrity.
3.20	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 IT 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 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.
3.21	Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.	Automated backup processes include procedures for testing the integrity of the backup data. Backups are performed in accordance with the entity's defined backup strategy, and usability of backups is verified at least annually. Backup systems and data are stored offsite at the facilities of a third-party service provider. Under the terms of its service provider agreement, the entity performs an annual verification of media stored at the offsite storage facility. As part of the verification, media at the offsite location are matched to the appropriate media management system. The storage site is reviewed biannually for physical access security and security of data files and other items. Backup systems and data are tested as part of the annual disaster recovery test.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.**	
4.1	System processing integrity and security performance are 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 publicly available tools. Potential risks are evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed and implementations are 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 either manually or by automated tools 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, regulatory, and technological changes are monitored, their impact on system processing integrity and security is assessed on a timely basis, and policies are updated for that assessment.	The entity's data center facilities include climate and environmental monitoring devices. Deviations from optimal performance ranges are escalated and resolved. Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's processing integrity and related security policies. The entity's customer service group monitors the impact of emerging technologies, customer requirements, and competitive activities.

Confidentiality Principle and Criteria

.28 The *confidentiality principle* refers to the system's ability to protect the information designated as confidential, as committed or agreed. Unlike personal information, which is defined by regulation in a number of countries worldwide and is subject to the privacy principles (see paragraph .33), there is no widely recognized definition of what constitutes 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 that information to complete the transaction or to resolve any questions that may arise. To enhance business partner confidence, it is important that the business partner be informed about the entity's system and information confidentiality policies, procedures, and practices. The entity needs to disclose its system and information confidentiality policies, procedures, and practices relating to the manner in which it provides for authorized access to its system and uses and shares information designated as confidential.

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

- transaction details,
- engineering drawings,

- business plans,
- banking information about businesses,
- intellectual property,
- inventory availability,
- bid or ask prices,
- price lists,
- legal documents,
- client and customer lists, and
- revenue by client and industry.

.30 What is considered to be confidential information can vary significantly from business to business and is determined by contractual arrangements or regulations. It is important to understand and agree upon what information is to be maintained in the system on a confidential basis and what, if any, rights of access will be provided.

.31 Confidential 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 the information is being transmitted. Controls such as encryption can be used to protect the confidentiality of this information during its transmission. Firewalls and rigorous access controls can also be used to help protect the information while it is processed or stored on computer systems.

Confidentiality Principle and Criteria Table

.32 Information designated as confidential is protected by the system as committed or agreed.

	Criteria	*Illustrative Controls*
1.0	**Policies: The entity defines and documents its policies related to the system protecting confidential information, as committed or agreed.**	
1.1	The entity's system confidentiality and related security policies are established and periodically reviewed and approved by a designated individual or group.	Written system confidentiality and security policies, addressing both IT and physical security, have been approved by the IT standards committee and are implemented throughout the company. As part of the periodic corporate risk assessment process, the security officer identifies changes to the IT risk assessment based on • new applications and infrastructure changes, • significant changes to applications and infrastructure components, • new environmental based confidentiality and security risks, • changes to regulations and standards, and • changes to user requirements as identified in service level agreements and other documents.

		The security officer then updates the confidentiality and security policies based on the IT risk assessment. Changes to the IT security policy are approved by the IT standards committee prior to implementation. User confidentiality requirements are documented in service-level agreements, nondisclosure agreements, or other documents.
1.2	The entity's policies related to the system's protection of confidential information and security include, but are not limited to, the following matters:	*An example of an illustrative control for this criterion would be an entity's documented confidentiality policy and related security policy addressing the elements set out in criterion 1.2. Illustrative confidentiality policies and security policies have been omitted for brevity.*
	a. Identifying and documenting the confidentiality and related security requirements of authorized users	
	b. Classifying data based on its criticality and sensitivity that is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements	
	c. Assessing risk on a periodic basis	
	d. Preventing unauthorized access	
	e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access	
	f. Assigning responsibility and accountability for confidentiality and related security	
	g. Assigning responsibility and accountability for system changes and maintenance	
	h. Testing, evaluating, and authorizing system components before implementation	
	i. Addressing how complaints and requests relating to confidentiality and related security issues are resolved	
	j. Handling confidentiality and related security breaches and other incidents	
	k. Providing for training and other resources to support its system confidentiality and related secu-	

	rity policies	
	l. Providing for the handling of exceptions and situations not specifically addressed in its system confidentiality and related security policies	
	m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements	
	n. Sharing information with third parties	
1.3	Responsibility and accountability for developing and maintaining the entity's system 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 human resources team. Responsibility for implementation of the entity's security policies has been assigned to the security officer under the direction of the CIO. The IT standards committee of the executive committee assists in the review, update, and approval of the policies as outlined in the executive committee handbook.
2.0	**Communications: The entity communicates its defined policies related to the system's protection of confidential information to responsible parties and 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 A [paragraph .45]*.) For its non-e-commerce system, the entity has provided a system description to authorized users. (*For an example of a system description for a non-e-commerce based system, refer to appendix B [paragraph .46]*.)
2.2	The system confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters:	The entity's confidentiality and related security commitments and required confidentiality and security obligations of its customers and other external users are posted on the entity's Web site. The entity's confidentiality policies and practices can also be outlined in its customer contracts, service-level agreements, vendor contract terms and conditions, and standard nondisclosure agreement.
	a. How information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, back-up, and distribution or transmission of confidential information.	Signed nondisclosure agreements are required before sharing information designated as confidential with third parties. Customer contracts, service-level agreements, and vendor contracts are negotiated before performance or receipt of service. Changes to the standard confidentiality provisions in these contracts require the approval of executive management.
	b. How access to confidential information is authorized and how such authorization is rescinded.	For its internal users (employees and contractors), the entity's policies relating to confidentiality and security are reviewed with new employees and contractors as part of their orientation, and the key elements of the policies and their impact on the employee are discussed. New employees must sign a statement signifying that they have read, understand, and will follow these policies. Each

		year, as part of their performance review, employees must reconfirm their understanding of and compliance with the entity's security policies. Confidentiality and security obligations of contractors are detailed in their contract.
	c. How confidential information is used.	A security awareness program has been implemented to communicate the entity's confidentiality and security policies to employees.
	d. How confidential information is shared.	The entity publishes its confidentiality and related security policies on its corporate intranet.
	e. If information is provided to third parties, disclosures include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity.	Signed nondisclosure agreements are required before sharing information designated as confidential with third parties.
	f. Practices to comply with applicable laws and regulations addressing confidentiality.	
2.3	Responsibility and accountability for the entity's system 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 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 and legal department representatives as part of the annual IT planning process. Written job descriptions have been defined and are communicated to the responsible personnel. Written process and procedure manuals for defined confidentiality processes are provided to responsible personnel. The security officer updates the processes and procedures manuals based on changes to the confidentiality policy.
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, provided as part of the new user welcome kit, or both. 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.	Planned changes to system components and the scheduling of those changes are reviewed as part of 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. 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 communicated in writing to affected customers for review and approval under the provisions of the standard services agreement before implementation of the proposed change. 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 placed in operation procedures to achieve its documented system confidentiality objectives in accordance with its defined policies.**	
3.1	Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair system confidentiality commitments and (2) assess the risks associated with the identified threats.	A risk assessment is performed periodically. As part of this process, threats to confidentiality are identified, and the risk from these threats is formally assessed. Confidentiality processes and procedures are revised by the security officer based on the assessed threats.
3.2	The system procedures related to confidentiality of inputs are consistent with the documented confidentiality policies.	Confidentiality processes are established to help ensure that all inputs have been authorized, have been accepted for processing, and are accounted for. Any missing or unaccounted source documents or input files have been identified and investigated. These processes require that exceptions be resolved within a specified time period but before data processing occurs or is completed. Confidentiality processes are implemented to limit access to input routines and physical input media (blank and completed) to authorized individuals. Confidentiality processes exist to restrict the capability to input information to only authorized individuals. This should include limitations based on specific operational or project roles and responsibilities. Error messages are revealed to authorized personnel. Error messages do not reveal potentially harmful information that could be used by others, and sensitive information (for example, e-mail content and financial data) is not listed in error logs or associated administrative messages.
3.3	The system procedures related to confidentiality of data processing are consistent with the documented confidentiality policies.	Confidentiality processes use transaction logs to reasonably ensure that all transactions are processed and to identify transactions that were not completely processed. Processes are in place to identify and review the incomplete execution of transactions, analyze them, and take appropriate action. Confidentiality processes exist to monitor, in a timely manner, unauthorized attempts to access data for any purposes, or for purposes beyond the authorization level of the person accessing the data, including inappropriate or unusual actions, overrides, or bypasses applied to data and transaction processing.

3.4	The system procedures related to confidentiality of outputs are consistent with the documented confidentiality policies.	Management has developed a reporting strategy that includes the sensitivity and confidentiality of data and appropriateness of user access to output data. Management has processes in place to monitor the replication or production of confidential output data used in reports or other communications within or outside the entity. User access to output data is appropriately aligned with the user's role and confidentiality of information. Access to reports is restricted to those users with a legitimate business need for the information. Users should have appropriate authorization for accessing reports containing confidential information.
3.5	The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's 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 been granted access. Logical access controls are in place that limit access to confidential information based on job function and need. Requests for access privileges to confidential data require the approval of the data owner. Business partners are subject to nondisclosure agreements or other contractual confidentiality provisions.
3.6	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 system 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 representations and assurances 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.
3.7	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 system 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 resulting in 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 to receive continued protection under the old policy.

System security-related criteria relevant to confidentiality

3.8	Procedures exist to restrict logical access to the system and the confidential information resources maintained in the system including, but not limited to, the following matters:	

a.	Logical access security measures to restrict access to information resources not deemed to be public	• Logical access to nonpublic confidential information resources is protected through the use of native operating system security, native application and resource security, and add-on security software. • Resource specific or default access rules have been defined for all nonpublic resources. • Access to resources is granted to an authenticated user based on the user's identity.
b.	Identification and authentication of all users.	• Users must establish their identity to the entity's network and application systems when accessing nonpublic confidential information resources through the use of a valid user ID that is authenticated by an associated password. • Unique user IDs are assigned to individual users. • Use of group or shared IDs is permitted only after completion of an assessment of the risk of the shared ID and written approval of the manager of the requesting business unit. • Passwords are case sensitive and must contain at least 8 characters, one of which is nonalphanumeric. • Security configuration parameters force passwords to be changed every 90 days. • Login sessions are terminated after 3 unsuccessful login attempts.
c.	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 appropriate user ID or user account and password. Privileges and authorizations associated with self-registered customer accounts provide access to specific limited system functionalities. • 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. Access to restricted resources is authorized by the resource owner. • 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.
d.	The process to make 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 • The human resource management system provides the human resources team with a list of newly terminated employees on a weekly basis. This listing is sent to the security administration team for deactivation.
e.	Procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.	• Corporate customers are assigned a unique company identifier that is required as part of the login process. Access software is used to restrict user access based on the company identifier used at login. • Individual customers have their access restricted to their own confidential information resources based on their unique user IDs.
f.	Procedures to limit access to confidential information to only authorized employees based upon their assigned roles and responsibilities.	• Requests for privileges to access confidential customer information resources require the approval of the customer account manager. • Simulated customer data are used for system development and testing purposes. Confidential customer information is not used for this purpose.
g.	Distribution of output containing confidential information restricted to authorized users.	• 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 access to offline storage, backup data, systems, and media.	• Access to offline storage, backup data, systems, and media is limited to computer operations staff through the use of physical and logical access controls.
i.	Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	• 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 other programs are restricted to authorized technical services staff. Usage of such programs are logged and monitored by the manager of computer operations. • The information security team, under the direction of the CIO, maintains access controls over firewall and other logs, as well as access to any storage media. Such access is logged and reviewed in accordance with the entity's IT policies.

		• The 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.
3.9	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 physical 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.
3.10	Procedures exist to protect against unauthorized access to system resources.	Login sessions are terminated after three unsuccessful login attempts. 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 the 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.
3.11	Procedures exist to protect against infection by computer viruses, malicious code, 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 promptly. Any viruses discovered are reported to the security team, and an alert is created for all users notifying them of a potential virus threat.
3.12	Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the In-	The entity employs industry standard encryption technology, VPN software, or other secure communication systems (consistent with its periodic IT risk assessment) for the transmission of private or confidential information over public networks, including user IDs

	ternet or other public networks.	and passwords. Users are required to upgrade their browsers to the most current version tested and approved for use by the security administration team to avoid possible security problems. Account activities, subsequent to successful login, are encrypted through industry standard encryption technology, VPN software, or other secure communication systems (consistent with the entity's periodic IT risk assessment). 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. Transmission of confidential customer information to third-party service providers is done over leased lines.
	Criteria related to execution and incident management used to achieve the objectives	
3.13	Procedures exist to identify, report, and act upon system 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, the network administrator, or both via e-mail and pager of potential incidents in progress. Incident logs are monitored and evaluated by the information security team daily. When an incident is detected or reported, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures. Procedures include a defined incident escalation process and notification mechanisms. All incidents are tracked by management until resolved. Closed incidents are reviewed by management for appropriate resolution. Resolution of incidents not related to security includes consideration of the impact of the incident and its resolution on security requirements.
	Criteria related to the system components used to achieve the objectives	
3.14	Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies.	Data owners periodically review data access rules and request modifications based on defined security requirements and risk assessments. Whenever new data are captured or created, the data are classified based on security and confidentiality policies. Propriety of data classification is considered as part of change management process.
3.15	Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective	All incidents are tracked by management until resolved. Closed incidents are reviewed by management for appropriate resolution.

	measures are taken on a timely basis.	The internal audit process includes the development of management actions plans for findings and the tracking of action plans until closed.
3.16	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software 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 protection mechanisms required to maintain an appropriate level of confidentiality and security. The security administration team reviews and approves the architecture and design specifications for new systems development or acquisition to help ensure consistency with the entity's confidentiality and related security policies. Changes to system components that may affect security or the confidentiality of information 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.
3.17	Procedures exist to help ensure that personnel responsible for the design, development, implementation, and operation of systems affecting confidentiality and security have the qualifications and resources 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 candidates' verified credentials are commensurate with the proposed position. New personnel are offered conditional 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.

Change management-related criteria relevant to confidentiality

3.18	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 an up-to-date 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 outstanding and closed requests. 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.
3.19	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	The responsibilities for authorizing, testing, developing, and implementing changes have been segregated. 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 outstanding and closed 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).
3.20	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 cor-

		rective measures follow the entity's change management process, including the requirements for obtaining line-of-business approvals.
3.21	Procedures exist to provide that confidential information is protected during the system development, testing, and change processes in accordance with defined system confidentiality and related security policies.	Information designated as confidential is not stored, processed, or maintained in test or development systems and environments. Test or development systems and environments that must contain information designated as confidential use data encryption, masking, and sanitization techniques to protect the confidentiality of the information.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with its defined confidentiality policies.**	
4.1	The entity's system confidentiality and security performance is periodically reviewed and compared with the defined system confidentiality and related security policies.	The information security team monitors the system and assesses the system's vulnerabilities using proprietary and publicly available tools. Potential risks are evaluated and compared to service-level agreements and other obligations of the entity. Remediation plans are proposed, and implementations are 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 system confidentiality and related security policies.	Logs are analyzed, either manually or by automated tools, to identify trends that may have a potential impact on the entity's ability to achieve its system confidentiality and related security objectives. Monthly IT staff meetings are held to address system security concerns and trends; findings are discussed at quarterly management meetings.
4.3	Environmental, regulatory, and technological changes are monitored, and their impact on system confidentiality and security is assessed on a timely basis. System confidentiality policies and procedures are updated for such changes as required.	Trends and emerging technologies and their potential impact on customer confidentiality requirements are reviewed with corporate customers as part of the annual performance review meeting. Senior management, as part of its annual IT planning process, considers developments in technology and the impact of applicable laws or regulations on the entity's confidentiality and related security policies. The entity's customer service group monitors the impact of emerging technologies, customer requirements, and competitive activities.

Privacy Principles and Criteria

.33 This section provides a brief overview of privacy concepts, objectives, and principles. The complete set of privacy principles is contained in generally accepted privacy principles (GAPP) found in appendix D (paragraph .48).

.34 The *privacy principles*, which are included in GAPP, focus on protecting the personal information an organization may collect about its customers, employees, and other individuals. GAPP have been developed from a business perspective, referencing significant domestic and international privacy regulations.

GAPP operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles.

Privacy Concepts

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

.36 *Personal information* is information that is about or can be related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are

- name,
- home or e-mail address,
- identification number (for example, a Social Security or Social Insurance Number),
- physical characteristics, and
- consumer purchase history.

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

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

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

.39 Some information about or related to people cannot be associated with specific individuals. Such information is referred to as *nonpersonal information*. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains because the information is "de-identified" or "anonymized." Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual.

Privacy or Confidentiality?

.40 As discussed in the confidentiality principle, personal information is different from confidential information. Unlike personally identifiable information, which is often defined by regulation in a number of countries worldwide, there is no single definition of confidential information that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires be maintained on a "need to know" basis.

Generally Accepted Privacy Principles

Overall Privacy Objective

.41 GAPP are founded on the following privacy objective:

> Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CICA.

The Privacy Principles

.42 GAPP are essential to the proper protection and management of personal information. They are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices. The following are the 10 GAPP:

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

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

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

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

5. *Use and retention.* The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.

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

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

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

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

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

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

.43 These criteria are set forth in the separate publication *Generally Accepted Privacy Principles*.

Online Privacy Engagements

.44 When the privacy engagement relates to an online segment, an entity may choose to display a privacy seal. For these engagements, the scope needs to include, as a minimum, an online business segment of the entity. For additional considerations, see appendix C of *Generally Accepted Privacy Principles*.

Appendix A

Illustrative Disclosures for E-Commerce Systems

This appendix sets out illustrative disclosures for e-commerce systems that are required to meet the trust services principles and criteria. The required disclosures are identified separately in the trust services principles (security, availability, processing integrity, and confidentiality). The following disclosures are illustrative only and should be tailored 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 as follows:

> Illustrative System Description
>
> Our site (abc-xyz.org) enables entrepreneurs and small business owners to create and manage their own online store (myABC-xyz.org) using the abc-xyz.org suite of business services. It also covers the fulfillment and settlement systems that integrate with abc-xyx.org to facilitate ordering from these online stores and the use of third-party service providers with which we have contracted to provide various services related to our site.
>
> The description covers the functionality in our abc-xyz.org site that allows users to create and manage their own online store. It also covers the fulfillment and settlement systems that integrate with abc-xyz.org to facilitate ordering from customer sites created on abc-xyz.org.

Disclosures Related to Specific Principles and Criteria

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

Criteria Reference		*Illustrative Disclosures*
Security		
2.2	The security obligations of users and the entity's security commitments to users are communicated to authorized users.	Even though we strive to protect the information you provide through ABC.com, no data transmission over the Internet can be guaranteed to be 100 percent secure. As a result, even though we strive to protect your information, we cannot guarantee 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 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 has 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 industry standard 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.	If you feel that there has been a breach to the security of this site, please contact us *immediately* at (800) XXX-XXXX.
2.5	Changes that may affect system security are communicated to management and users who will be affected.	Any changes that affect the security of our Web site as it affects you as a site user will be communicated to you by posting the highlight of the change to the Web page that summarizes our security policies and significant controls.
Availability		
2.2	The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	To allow sufficient time for file maintenance and backup, the maximum number of hours per day that our network will be made available is 22 hours per day, 7 days a week. In the event of a disaster or other prolonged service interruption, the entity has arranged for the use of alternative service sites to allow for full business resumption within 24 hours. Our company's defined security policies detail access privileges, information collection needs, accountability, and other such matters. They are reviewed and updated at quarterly management meetings and undergo an intense review on an annual basis by the 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 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) XXX-XXXX. If you believe that there has been a breach to the security of this site, please contact us *immediately* at (800) XXX-XXXX.
2.5	Changes that may affect system availability and system security are communicated to management and users who will be affected.	Highlights of any changes that affect the security of our Web site and availability of the system as it affects you as a site user will be communicated to you by e-mail seven days in advance of the anticipated change. The highlights of the change will be posted to the Web page that summarizes our availability and security policies.

Processing Integrity

2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users. If the system is an e-commerce system, additional information provided on its Web site includes, but may not be limited to, the following matters:	You can purchase new and used books on our site; used books are clearly labeled as such. The mortgage rate information we obtain for your brokerage transaction is gathered from 12 different lending institutions on a daily basis. A complete listing of these lending institutions can be obtained by clicking here [*insert hot link/URL*]. ABC's Online RFQ Brokerage is the online clearing house for requests for quotes (RFQ) on custom-made parts. Through our unique service, Original Equipment Manufacturers (OEM) looking for parts will be connected to contract manufacturers looking for work.
	a. Descriptive information about the nature of the goods or services that will be provided, including, where appropriate	RFQs published on our online brokerage undergo an intensive review process to ensure that contract manufacturers get all the information needed to compose a quote. ABC's trained personnel will work closely with OEM manufacturers new to the outsourcing market to ease their fears.
	• condition of goods (whether they are new, used, or reconditioned).	Contract manufacturers participating in the RFQ bidding process are members of ABC's BizTrust program. New members are subjected to an assortment of checks such as credit checks and reference checks to ensure that they are qualified to bid on RFQs. The results from these checks are organized into an easy-to-read BizTrust Report accessible by all members of ABC.
	• description of services (or service contract).	The nationwide survey, conducted by the compensation-research firm of Dowden & Co., presents data on 20X2 compensation that was gathered from among more than 900 employers of information systems professionals, including corporations of all sizes, in every industry group, and from every U.S. region. The survey was completed July 20X1.
	• sources of information (where it was obtained and how it was compiled).	Our policy is to ship orders within 1 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 1 week.
	b. The terms and conditions by which it conducts its e-	We will notify you by e-mail within 24 hours if we cannot fulfill your order as specified at the time you placed it and will provide

	commerce transactions including, but not limited to, the following matters:	you the option of canceling the order without further obligation. You will not be billed until the order is shipped.
	• 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 have the option of downloading the requested information now, or we will send it to you on CD-ROM by UPS 2-day or Federal Express overnight delivery. Credit approval is required before shipment. All goods will be invoiced on shipment according to either our normal terms of settlement (net 30 days), or where alternative contractual arrangements are in place, those arrangements shall prevail.
	• Time frame and process for informing customers of exceptions to normal processing of orders or service requests	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) XXX-XXXX. Be sure to include your account number or have it ready when you call.
	• Normal method of delivery of goods or services, including customer options, where applicable	Purchases can be returned for a full refund within 30 days of receipt of shipment. Call our toll-free number or e-mail us for a return authorization number, which should be written clearly on the outside of the return package.
	• Payment terms, including customer options, if any	Warranty and other service can be obtained at any one of our 249 locations worldwide that are listed on this Web site. A list of these locations is also provided with delivery of all of our products.
	• Electronic settlement practices and related charges to customers	Transactions at this site are covered by binding arbitration conducted through our designated arbitrator [*name of arbitrator*]. They can be reached at www.name.org or by calling toll-free (800) XXX-XXXX. For the details of the terms and conditions of arbitration, click here [*insert hot link/URL*].
	• How customers may cancel recurring charges, if any	Our process for consumer dispute resolution requires that you contact our customer toll-free hotline at (800) XXX-XXXX or contact us via e-mail at custhelp@ourcompany.com.
	• Product return policies and limited liability, where applicable	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) XXX-XXXX during normal business hours (8:00 a.m. to 5:00 p.m. central time) or via their Web site at www.ccomplaint.com.
c.	Where customers can obtain warranty, repair service, and support related to the goods and services purchased on its Web site.	For the details of the terms and conditions of arbitration, click here [*insert hot link/URL*].
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	If you, our customer, require follow-up or response to your questions or complaints regarding transactions at this site, 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

	quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints.	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 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 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) XXX-XXXX between 7:00 a.m. and 8:00 p.m. (central standard time), or you can write to us at CustServ@ABC.com or at the following address: Customer Service Department ABC Company 1234 Anystreet Anytown, Illinois 60000 If you believe that there has been a breach to the integrity or security of this site, please contact us *immediately* at (800) 123-1234.
2.5	Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.	Highlights of any changes that affect the security of our Web site and processing integrity of the system as it affects you as a site user will be communicated to you by e-mail seven days in advance of the anticipated change. The highlights of the change will be posted to the Web page that summarizes our processing integrity and security policies.
Confidentiality		
2.2	The confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters:	XYZ manufacturing.com is a high quality custom manufacturer of electronic components. Customers and potential customers can submit engineering drawings, specifications, and requests for manufacturing price quotes through our Web site or e-mail.
	a. How information is designated as confidential and ceases to be confidential; the handling, destruction, back-up, and distribution or transmission of confidential information.	Access to your information is limited to our employees and any third-party subcontractors we may elect to use in preparing our quote. We will not use any information you provide for any purpose other than a price quote and subsequent manufacturing and order fulfillment on your behalf. However, access may need to be provided in response to subpoenas, court orders, legal process, or other needs to comply with applicable laws and regulations.

	b. How access to confidential information is authorized and how such authorization is rescinded.	Using our encryption software, you may designate information as confidential by checking the "Confidential Treatment" box. This software can be downloaded from our site and will accept information in most formats. Such information will automatically be encrypted using our public key before transmission over the Internet. You may transmit such information to us through our Web site or by e-mail.
	c. How confidential information is used.	Access to information designated as confidential will be restricted only to our employees with a need to know. We will not provide such information to third parties without your prior permission.
	d. How confidential information is shared.	When we provide information to third parties, we do not provide your company name. However, we make no representation regarding third-party confidential treatment of such information.
	e. If information is provided to third parties, disclosures include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity.	Our confidentiality protection is for a period of two years, after which any confidential information will be returned to you, upon request, or destroyed.
	f. Practices to comply with applicable laws and regulations addressing confidentiality.	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 in addition to 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. If you feel that there has been a breach to the security of this site, please contact us *immediately* at (800) XXX-XXXX.
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 the secret category will continue to be protected in accordance with our commitments at that time.

Privacy

See generally accepted privacy principles in appendix D (paragraph .48) for related criteria.

Appendix B

Illustrative System Description of a Non-E-Commerce System

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's customers. The plan members are the employees of XPS'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 XYZ Co.'s Information Technology Department (XITD) 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 that set up pension rules, maintain master files, process contributions to PAS, report to plan sponsors and members, and assist with inquiries from plan members.
- Financial operations is responsible for processing withdrawals, depositing contributions, and investment accounting.

- Trust accounting is responsible for bank reconciliation.
- 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 its 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, and
- reporting to members.

These services are supported by 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, and
- business recovery planning.

Data

PAS data consist of 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 Co.'s call center. Transaction data are processed by PAS in either online or batch modes of processing and are used to update master files. Output reports are available either in hard copy or through a report-viewing facility to authorized users based on their job functions. Pension statement and transaction notices are mailed to plan sponsors and members.

Appendix C

Practitioner Guidance on Scoping and Reporting Issues

This appendix deals with issues related to engagement planning, performance, and reporting using the trust services principles and criteria. This section deals with

- engagement components,
- the practitioner's report,
- review engagements,
- agreed-upon procedures engagements, and
- other matters.

Trust services engagements are attest engagements performed under the AICPA Statements of Standards for Attestation Engagements.

Engagement Components

Trust Services Principles

Trust services provides for a modular approach using five different principles—security, availability, processing integrity, confidentiality, and privacy. A practitioner may perform a trust services examination that covers only one or any combination of the principles. Each principle describes an attribute of a system (for example, availability) and is followed by criteria for evaluating the system with respect to that attribute.

Trust Services Criteria

Criteria are the benchmarks used to measure and present the subject matter. The practitioner evaluates the subject matter against these criteria.

AT section 101, *Attest Engagements* (AICPA, *Professional Standards*, vol. 1), of the attestation standards,[8] states that 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

AT section 101 states that the practitioner should ordinarily obtain a written assertion[9] from management, or the practitioner will be required to modify his or her report.[10] Specifically, management asserts that, during the period covered by the report and based on the AICPA and CICA trust services criteria, it maintained effective controls over the system under examination to satisfy the stated trust services principle(s) and criteria. For engagements covering only certain principles, management's assertion should only address the principles covered by the engagement. In addition, for engagements covering an entity's compliance with its commitments, those commitments covered by the report should be indentified in management's assertion.

---

[8] See AT section 101, *Attest Engagements* (AICPA, *Professional Standards,* vol. 1), paragraph .24.

[9] See AT section 101 paragraph .09.

[10] See AT section 101 paragraph .58 for a description of a practitioner's options if a written assertion is not obtained.

Under AT section 101, the practitioner may report on either management's assertion or on the subject matter of the engagement. When the practitioner reports on the assertion, the assertion should accompany the practitioner's report or be included in the first paragraph of the practitioner's report.[11] 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 deviations from the criteria exist, the practitioner should modify the report. When issuing a modified report, the practitioner should report directly on the subject matter rather than on the assertion.[12]

Period of Coverage

AT section 101 provides that the practitioner's report and management's assertion should specify the time period covered by the report and the 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.

The committee has identified the following factors that the practitioner may want to consider in establishing the reporting period:

- The anticipated users of the report and their needs
- The need for contiguous coverage between reports
- 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

The Practitioner's Report

The committee has identified the following items that the practitioner may want to consider when reporting on trust services principles and criteria.

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. In the introductory paragraph of the report, the practitioner should identify the principles included in the scope of the examination.

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 three principles and related criteria: security, privacy, and confidentiality.

---

[11] See AT section 101 paragraph .64.
[12] See AT section 101 paragraph .66.

The first issue is to decide whether this represents (1) one engagement to examine three principles or (2) three engagements to examine one principle each. This decision can affect, among other matters, the engagement letter, the content and number of representation letters, and whether one report or multiple reports will be issued. In either case, the practitioner's report(s) should clearly communicate the scope and nature of the engagement(s).

Failure to Meet Criteria

If one or more relevant criteria have not been met, the practitioner cannot issue an unqualified report. Under AT section 101, when issuing a modified report, the practitioner should report directly on the subject matter rather than on the assertion.[13]

Different Examination Periods

There may be situations in which the entity requests that more than one principle be examined, but due to various reasons, the principles will have different reporting periods (for example, differences in the length of the reporting period or the date that the various reporting periods begin). Ideally, it would be more efficient for the practitioner to have such periods coincide. When different reporting periods exist, the practitioner may 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.

Use of Third-Party Service Providers

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

Responsibility for Communicating Departures From the Criteria Related to Other Principles

During a trust services examination, information about departures from the criteria, such as noncompliance or control deficiencies related to principles and criteria that are not within the 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 about departures from the criteria that are outside the scope of his or her examination, the practitioner may want to evaluate whether such information that comes to his or her attention is significant (that is, whether the effects of such departures could materially mislead users of the system).

If the practitioner determines that the effects of such departures are significant, the committee believes that the practitioner should communicate in writing to management. Management should be asked either to correct the control deficiency or noncompliance (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

[13] See AT section 101 paragraph .66.

(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 departure or disclose the information, the practitioner may consider withdrawing from the engagement.

Subsequent Events

Events or transactions sometimes occur subsequent to the point in time or period of time covered by the practitioner's report but prior to the date of the practitioner's report that have a material effect on the subject matter or assertion 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 covered by the practitioner's report. This information should be used by the practitioner in considering whether the subject matter or assertion 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 covered by the practitioner's report 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.

Although 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.[14] 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 AU section 561, *Subsequent Discovery of Facts Existing at the Date of the Auditor's Report* (AICPA, *Professional Standards*, vol. 1).[15]

Review Engagements

A review engagement performed in accordance with Statements on Standards for Attestation Engagements is a type of attestation engagement in which the practitioner reports on whether any information came to his or her attention on the basis of the work performed that indicates that the subject matter is not based on (or in conformity with) the criteria, or the assertion is not presented (or fairly stated) in all

[14] Certain attestation standards include requirements regarding the practitioner's consideration of subsequent events, for example, AT section 601 paragraphs .50–.51 and .129–.134

[15] See AT 101 paragraphs .95–.99.

material respects based on the criteria. Such review engagements generally are limited to inquiry and analytical review procedures. Accordingly, the committee has determined that review engagements should not be performed when reporting on controls over a system in accordance with trust services principles and criteria.

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,[16] 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 of an assertion or subject matter or express an opinion about the assertion or subject matter. The practitioner's report on agreed-upon procedures is a presentation of procedures and findings.[17] The use of an agreed-upon procedures report is restricted to the specified parties who agreed upon the procedures.

Illustrative Reports

The following are illustrative reports for trust services examination engagements. Illustrations 1, 2, and 3 are examples of reports in which the practitioner is reporting on management's assertion. Illustrations 4 and 5 are examples of reports in which the practitioner is reporting directly on the subject matter. The first paragraph of the practitioner's report will indicate whether the practitioner is reporting on management's assertion or directly on the subject matter.

The trust services principles and criteria for *system reliability* include availability, security, and processing integrity. There is also a fourth principle and set of criteria related to confidentiality that a practitioner may report on.

The trust services principles and criteria related to availability, processing integrity and confidentiality include criteria that refer to commitments the entity has made to customers. For those principles and criteria, the client may request that the practitioner (1) report on controls over commitments (in which case the report will make no special reference to commitments) or (2) report on controls over commitments *and* on whether the entity has complied with those commitments (in which case the report will make reference to the commitments, as shown in illustration 3).

A client may include a list of its controls over the system related to the principles and criteria being reported on. An illustrative report for that option is shown in illustration 5.

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.

---

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

[17] See AT section 201, *Agreed-Upon Procedures Engagements* (AICPA, *Professional Standards*, vol. 1), for guidance on agreed-upon procedures engagements.

Illustration 1—Trust Services Report on Management's Assertion about the Effectiveness of Controls Related to Four Principles (Availability, Security, Process Integrity, and Confidentiality) (Period-of-Time Report)

Independent Practitioner's Trust Services Report

To the management of ABC Company, Inc.:

We have examined management's assertion that during the period [*month, day, and year*] through [*month, day, and year*], ABC Company, Inc. (ABC Company) maintained effective controls over the _____ [*type or name of system*] system based on the AICPA and CICA trust services availability, security, processing integrity, and confidentiality criteria 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);
- the system processing was complete, accurate, timely, and authorized; and
- information designated as confidential was protected by the system as committed or agreed

based on the AICPA and CICA trust services security, availability, processing integrity, and confidentiality criteria.

ABC Company's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the _____ [*type or name of system*] system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

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 controls over the availability, security, processing integrity, and confidentiality of the _____ [*type or name of system*] system; (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.

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

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA and CICA trust services security, availability, processing integrity, and confidentiality criteria.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

[*See notes to illustrative reports prepared under AICPA standards.*]

Illustration 2—Trust Services Report on Management's Assertion about the Effectiveness of Controls over System Reliability (Availability, Security, and Processing Integrity (Period-of-Time Report)

Independent Practitioner's Trust Services Report on System Reliability

To the management of ABC Company, Inc.:

We have examined the assertion made by management of ABC Company, Inc. (ABC Company) about its controls over the reliability of the _____ [*type or name of system*] system during the period [*month, day, year*] through [*month, day, year*] based on the AICPA and CICA trust services availability, security, and processing integrity criteria for systems reliability. A reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. Management's assertion is included in the accompanying document titled "ABC Company's Assertion Regarding the Effectiveness of Its Controls Over the _____ [*type or name of system]* System" and states that:

> During the period [*month, day, year*] through [*month, day, year*], ABC Company maintained effective controls over the availability, security and processing integrity of the _____ [*type or name of system*] 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
>
> based on the AICPA and CICA trust services availability, security, and processing integrity criteria for systems reliability.
>
> The attached system description of ABC Company's _____ [*type or name of system*] system identifies the aspects of the_____ [*type or name of system*] system covered by the assertion.

ABC Company's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the _____ [*type or name of system*] system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

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 controls over the availability, security, and processing integrity of the _____ [*type or name of system*] system; (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.

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

In our opinion, management's assertion referred to above is fairly stated in all material respects, based on the AICPA and CICA trust services availability, security, and processing integrity criteria for systems reliability.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

[*See notes to illustrative reports prepared under AICPA standards.*]

Illustration 3—Trust Services Report on Management's Assertion About the Effectiveness of Controls and Compliance With the Criteria for One Principle (Confidentiality) (Point-in-Time Report)

Independent Practitioner's Trust Services Report

To the management of ABC Company, Inc.:

We have examined management's assertion [*hot link to management's assertion*] that as of [*month, day, year*] ABC Company, Inc. (ABC Company) maintained effective controls over the _____ [*type or name of system*] system to provide reasonable assurance that the _____ [*type or name of system*] system protected information designated as confidential, as committed or agreed upon and complied with its commitments regarding the protection of information designated as confidential [*hot link to management's commitments*] based on the AICPA and CICA trust services confidentiality criteria.

ABC Company's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the _____ [*type or name of system*] system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

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 the controls over the protection of information designated as confidential in ABC Company's_____ [*type or name of system*] system; (2) testing and evaluating the operating effectiveness of those controls; (3) testing compliance with ABC Company's commitments regarding the protection of information designated as confidential, 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.

Because of the nature and inherent limitations of controls, ABC Company's ability to meet the aforementioned criteria and its commitments may be affected. For example, controls may not prevent or de-

tect and correct error or fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, ABC Company's management's assertion referred to above is fairly stated, in all material respects, based on the AICPA and CICA trust services confidentiality criteria.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

[*See notes to illustrative reports prepared under AICPA standards.*]

Illustration 4—Trust Services Report on System Reliability (Availability, Security, and Processing Integrity)—Reporting Directly on the Subject Matter (Period-of-Time Report)

Independent Practitioner's Trust Services 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 _____ [*type or name of system*] system during the period [*month, day, year*] through [*month, day, year*] based on the AICPA and CICA trust services availability, security, and processing integrity criteria for systems reliability. A reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. ABC Company's management is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion based on our examination.

Management's description of the aspects of the _____ [*type or name of system*] system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

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 controls over availability, security, and processing integrity; (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.

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

In our opinion, ABC Company maintained, in all material respects, effective controls over the reliability of ABC Company's _____[*type or name of system*] 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 and CICA trust services availability, security, and processing integrity criteria for systems reliability.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

[*See notes to illustrative reports prepared under AICPA standards.*]

Illustration 5—Trust Services Report on the Effectiveness of Controls Related to One Principle (Security)—Reporting Directly on the Subject Matter (Period-of-Time Report Including Schedule Describing Controls)

Independent Practitioner's Trust Services 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 _____ [*type or name of system*] system during the period [*month, day, year*] through [*month, day, year*] based on the AICPA and CICA trust services security criteria. ABC Company's management is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion based on our examination.

Management's description of the aspects of the _____ [*type or name of system*] system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

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 the ABC Company's controls over the security of_____ [*type or name of system*] system; (2) testing and evaluating the operating effectiveness of those 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.

Because of the nature and inherent limitations of controls, ABC Company's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, and failure to comply with internal and external

policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, ABC Company maintained, in all material respects, effective controls, described in schedule X, over the security of ABC Company's _____ [*type or name of system*] system to provide reasonable assurance that the ABC Company's _____ [*type or name of system*] system was protected against unauthorized access (both physical and logical) during the period [*month, day, year*] through [*month, day, year*], based on the AICPA and CICA trust services security criteria.

[*Name of CPA firm*]

Certified Public Accountants

[*City, State*]

[*Date*]

[*See notes to illustrative reports prepared under AICPA standards.*]

Schedule X—Controls Over the Security of ABC Company's _____ [type or name of system] System Supporting the AICPA and CICA Trust Services Security Criteria

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

	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 IT standards committee.
1.2	The entity's security policies include, but may not be limited to, the following matters: *a.* Identifying and documenting the security requirements of authorized users. *b.* Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access right and access restrictions, and retention and destruction requirements. *c.* Assessing risks on a periodic basis *d.* Preventing unauthorized access.	The company's documented security policies contain the elements set out in criterion 1.2.

	e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access.	
	f. Assigning responsibility and accountability for system security.	
	g. Assigning responsibility and accountability for system changes and maintenance.	
	h. Testing, evaluating, and authorizing system components before implementation.	
	i. Addressing how complaints and requests relating to security issues are resolved.	
	j. Identifying and mitigating security breaches and other incidents.	
	k. Providing for training and other resources to support its system security policies.	
	l. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.	
	m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	
	n. Providing for sharing information with third parties.	
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 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 of 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 use other alternative presentation styles.

Appendix D

Generally Accepted Privacy Principles

At time of press of this publication, the generally accepted privacy principles (GAPP) were under revision. For the current version of GAPP, go to http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/.

ASSURANCE SERVICES EXECUTIVE COMMITTEE

(2008/09)

Alan Anderson, Chair
Suzanne Christensen
Robert Dohrer
Clarence R. Ebersole
Olivia Kirtley
Mike Krzus
Glenn Stastny
Jorge Asef-Sargent
Robert M. Tarola
Bill Titera
Miklos Vasarhelyi
David Sharpe

TRUST/DATA INTEGRITY TASK FORCE

Chris Halterman, Chair
Efrim Boritz
Mark Eich
Sheri Fedokovitz
Thomas E. Festing
Tim Krick
John Lainhart
Dave Palmer
Tom Patterson
Dan Schroeder
Jerry Trites
Miklos Vasarhelyi

PRIVACY TASK FORCE

Everett C. Johnson, Chair
Kenneth D. Askelson, Vice Chair
Eric Federing
Philip M. Juravel
Sagi Leizerov
Rena Mears
Robert Parker
Marilyn Prosch
Doron M. Rotman
Kerry Shackelford
Donald E. Sheehy

AICPA/CICA Staff

Amy Pawlicki
Director
AICPA Business Reporting, Assurance, and Advisory Services

Bryan Walker
Director
CICA Practitioner Support

Stephen L. Winters
Director
AICPA Specialized Communities and Practice Management

Erin Mackler
Senior Manager
AICPA Business Reporting, Assurance, and Advisory Services

Nancy A. Cohen
Senior Technical Manager
AICPA Specialized Communities and Practice Management

Nicholas F. Cheung
Principal
CICA Assurance Services Development