

Trust Services Principles and Criteria - An Overview

Published January 29, 2009

Trust Services are 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 document, Trust Services Principles, Criteria, and Illustrations provides guidance when providing assurance services, advisory services, or both on information technology (IT)-enabled systems including electronic commerce (e-commerce) systems. It is particularly relevant when providing services with respect to security, availability, processing integrity, online privacy, and confidentiality.

The increased use of technology, the increased use of third-party service providers for significant components of information processing systems, and the advent of new technologies have created more complex systems and new business processes to increase productivity and efficiency. With the more complex systems and new processes, issues of trustworthiness, such as reliability, privacy, and security, have become paramount. With these changes, there are increased business opportunities and risks.

Trust Services helps differentiate entities from their competitors by demonstrating to stakeholders that the entities are attuned to the risks posed by their environment and equipped with the controls that address those risks. Therefore, the potential beneficiaries of Trust Services assurance reports are consumers, business partners, creditors, bankers and other creditors, regulators, outsourcers and those using outsourced services, and any other stakeholders who in some way rely on electronic commerce (e-commerce) and IT systems.

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.

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^[1]:

- *Security.* The system is protected against unauthorized access (both physical and logical).
- *Availability.* The system is available for operation and use as committed or agreed.
- *Processing integrity.* System processing is complete, accurate, timely, and authorized.
- *Confidentiality.* Information designated as confidential is protected as committed or agreed.
- *Privacy.* 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 trust services principles and criteria of security, availability, processing integrity, and confidentiality are organized in four broad areas:

- *Policies.* The entity has defined and documented its policies relevant to the particular principle.
- *Communications.* The entity has communicated its defined policies to responsible parties and authorized users of the system.
- *Procedures.* The entity placed in operation procedures to achieve its objectives in accordance with its defined policies.
- *Monitoring.* The entity monitors the system and takes action to maintain compliance with its defined policies.

[Download Trust Services Principles and Criteria.](#) For more details and to access the full illustration, [click here](#) to purchase the Technical Practice Aid available on www.CPA2Biz.com.

The Trust Services Principles and Criteria are effective as of September 15, 2009.

[1] SysTrust and WebTrust are two specific assurance services offerings developed by the AICPA and 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 or contact Bryan Walker at Bryan.Walker@cica.ca or 416.204.3278.

Trust Services Principles and Criteria

Security Principle and Criteria

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

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

<i>Criteria</i>	<i>Illustrative Controls</i> ¹
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.	<p>Written security policy, addressing both IT and physical security, has been approved by the IT standards committee and is implemented throughout the company.</p> <p>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.</p> <p>Changes to the IT security policy are approved by the IT standards committee prior to implementation.</p>
1.2 The entity's security policies include, but may not be limited to, the following matters:	<p><i>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.</i></p>
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 rights and access restrictions, and retention and destruction requirements	

¹ 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.

<ul style="list-style-type: none"> 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 	
<p>1.3 Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned.</p>	<p>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.</p>

2.0 Communications: The entity communicates its defined system security policies to responsible parties and authorized users.

Criteria	Illustrative Controls ¹
2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	<p>For its e-commerce system, the entity has posted a system description on its Web site. <i>(For an example of a system description for an e-commerce system, refer to appendix A [paragraph .45].)</i></p> <p>For its non-e-commerce system, the entity has provided a system description to authorized users. <i>(For an example of a system description for a non-e-commerce based system, refer to appendix B [paragraph.46].)</i></p>
2.2 The security obligations of users and the entity's security commitments to users are communicated to authorized users.	<p>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.</p> <p>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.</p> <p>New employees must sign a statement signifying that they have read, understand, and will follow these policies.</p> <p>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.</p> <p>A security awareness program has been implemented to communicate the entity's IT security policies to employees.</p> <p>The entity publishes its IT security policies on its corporate intranet.</p>
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.	<p>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.</p> <p>Written job descriptions have been defined and are communicated to the security administration team.</p> <p>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.</p>
2.4 The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.	<p>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.</p> <p>The entity's security awareness program includes information concerning the identification of possible security breaches and the process for informing the security administration team.</p> <p>Documented procedures exist for the identification and escalation of security breaches and other incidents.</p>
2.5 Changes that may affect system security are communicated to management and users who will be affected.	<p>Planned changes to system components and the scheduling of those changes are reviewed as part of the monthly IT steering committee meetings.</p> <p>Changes to system components, including those that may affect system security, require the approval of the security administrator before implementation.</p>

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.
- Security configuration parameters force passwords to be changed every 90 days.
- Login sessions are terminated after 3 unsuccessful login attempts.

Criteria

*Illustrative Controls*¹

-
- | | |
|--|--|
| <p>c. Registration and authorization of new users.</p> | <ul style="list-style-type: none">• 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. |
| <p>d. The process to make changes and updates to user profiles.</p> | <ul style="list-style-type: none">• 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. |
| <p>e. Distribution of output restricted to authorized users.</p> | <ul style="list-style-type: none">• 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. |
| <p>f. Restriction of access to offline storage, backup data, systems, and media.</p> | <ul style="list-style-type: none">• 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).	<ul style="list-style-type: none"> • 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.	<p>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.</p> <p>Physical access cards are managed by building security staff. Access card usage is logged. Logs are maintained and reviewed by building security staff.</p> <p>Requests for physical access privileges to the entity's computer facilities require the approval of the manager of computer operations.</p> <p>Documented procedures exist for the identification and escalation of potential physical security breaches.</p> <p>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.</p>
3.4 Procedures exist to protect against unauthorized access to system resources.	<p>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.</p> <p>Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and reviewed daily by the security administrator.</p> <p>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.</p> <p>Intrusion detection systems are used to provide continuous monitoring of the entity's network and early identification of potential security breaches.</p>

Criteria	Illustrative Controls ¹
3.5 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.	<p>The entity contracts with third parties to conduct periodic security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management.</p> <p>In connection with other security monitoring, the security administration team participates in user groups and subscribes to services relating to computer viruses.</p> <p>Antivirus software is in place, including virus scans of incoming e-mail messages. Virus signatures are updated promptly.</p> <p>Any viruses discovered are reported to the security team, and an alert is created for all users notifying them of a potential virus threat.</p> <p>The ability to install, modify, and replace operating system and other system programs is restricted to authorized personnel.</p> <p>Access to superuser functionality and sensitive system functions is restricted to authorized personnel.</p>
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.	<p>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.</p> <p>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.</p>
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.	<p>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.</p> <p>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.</p> <p>Incident logs are monitored and evaluated by the information security team daily.</p> <p>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.</p> <p>Procedures include a defined incident escalation process and notification mechanisms.</p> <p>All incidents are tracked by management until resolved.</p> <p>Closed incidents are reviewed by management for appropriate resolution.</p> <p>Resolution of incidents not related to security includes consideration</p>

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	<p>Data owners periodically review data access rules and request modifications based on defined security requirements and risk assessments.</p> <p>Whenever new data are captured or created, the data are classified based on security policies,</p> <p>Propriety of data classification is considered as part of the change management process.</p>
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.	<p>All incidents are tracked by management until resolved.</p> <p>Closed incidents are reviewed by management for appropriate resolution.</p> <p>The internal audit process includes the development of management actions plans for findings and the tracking of action plans until closed.</p>
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.	<p>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.</p> <p>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.</p> <p>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.</p> <p>Changes to system components that may affect security require the approval of the security administration team.</p>
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.	<p>The entity has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions.</p> <p>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.</p> <p>Candidates, including internal transfers, are approved by the line-of-business manager before the employment position is offered.</p> <p>Periodic performance appraisals are performed by employee supervisors and include the assessment and review of professional development activities.</p> <p>Personnel receive training and development in system security concepts and issues.</p>

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 authorized timely.

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.

	<p>Change requestors are kept informed about the status of their requests.</p> <p>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.</p>
4.0 Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies.	
<p>4.1 The entity's system security is periodically reviewed and compared with the defined system security policies.</p>	<p>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.</p> <p>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.</p>
<p>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.</p>	<p>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.</p> <p>Monthly IT staff meetings are held to address system security concerns and trends; findings are discussed at quarterly management meetings.</p>
<p>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.</p>	<p>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.</p> <p>The entity's IT security group monitors the security impact of emerging technologies.</p> <p>Users are proactively invited to contribute to initiatives to improve system security through the use of new technologies.</p>

Availability Principle and Criteria

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.

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

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:	<i>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.</i>
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 components 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

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*

	<p><i>e-commerce system, refer to appendix A [paragraph .45].)</i></p>
	<p>For its non-e-commerce system, the entity has provided a system description to authorized users. <i>(For an example of a system description for a non-e-commerce based system, refer to appendix B [paragraph .46].)</i></p>
<p>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.</p>	<p>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.</p> <p>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.</p> <p>A security awareness program has been implemented to communicate the entity's IT security policies to employees.</p> <p>The entity publishes its IT security policies on its corporate intranet.</p>
<p>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.</p>	<p>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.</p> <p>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.</p> <p>Written job descriptions have been defined and are communicated to the network operations team and the security administration team.</p> <p>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.</p>
<p>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.</p>	<p>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.</p> <p>The entity's user training program includes modules dealing with the identification and reporting of system availability issues, security breaches, and other incidents.</p> <p>The entity's security awareness program includes information concerning the identification of possible security breaches and the process for informing the security administration team.</p> <p>Documented procedures exist for the identification and escalation of system availability issues, security breaches, and other incidents.</p>

- 2.5 Changes that may affect system availability and system security are communicated to management and users who will be affected.
- Changes that may affect system availability, customers and users and their security obligations, or the entity's security commitments are highlighted on the entity's Web site.
- Changes that may affect system availability and related system security are 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
- 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

with the entity's defined system availability and related security policies.

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
 - 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.

- deemed to be public.
 - 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 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.

 - 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 au-

thorized 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 securi-

ty 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 completed 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 is 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 <ul style="list-style-type: none">• 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 re-

quests.

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 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).

3.17 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 improvement are reported to management.

4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.

Network performance and system processing are monitored using system monitoring tools by onsite operations staff 24 hours a day, 7 days a week. Network performance, system availability, and security incident statistics and comparisons to approved targets are accumulated and reported to the IT steering committee monthly.

Future system performance, availability, and capacity requirements are projected and analyzed as part of the annual IT planning and budgeting process.

Logs are analyzed 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

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.

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.

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

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

<i>Criteria</i>	<i>Illustrative Controls</i>
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.	<p>Written policies addressing processing integrity have been approved by the executive committee and are implemented throughout the company.</p> <p>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.</p> <p>User requirements are documented in service-level agreements or</p>

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:

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.

- 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 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 system processing integrity and related system security policies; changes, updates, and exceptions to those policies are assigned.

Management has assigned responsibilities for the implementation of the entity's processing integrity and related security policies to individual 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.

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].)*

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:

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].)*

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
 - 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 integrity policies. If the system is an e-commerce system, the entity's procedures include, but may not be limited to, the following matters: <i>a.</i> The entity checks each request or transaction for accuracy and completeness. <i>b.</i> Positive acknowledgment is received from the customer before the transaction is processed.	The entity has established data preparation procedures to be followed by user departments. Data entry screens contain field edits and range checks, and input forms are designed to reduce errors and omissions. Source documents are reviewed for appropriate authorizations before input. Error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected. Original source documents are retained on image management systems for a minimum of seven years, to facilitate the retrieval or reconstruction of data as well as to satisfy legal requirements. Logical access controls restrict data entry capability to authorized personnel. (See 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 <ul style="list-style-type: none">• 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 completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies.

If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters:

- 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.
- b. Transaction exceptions are promptly communicated to the customer.
- c. Incoming messages are processed and delivered accurately and completely to the correct IP address.
- d. Outgoing messages are processed and delivered accurately and completely to the service provider's (SP's) Internet access point.
- e. Messages remain intact while in transit within the confines of the

Responsibilities for order processing, application of credits and cash receipts, custody of inventory, user account management, and database management have been segregated.

The entity's documented systems development life cycle (SDLC) methodology is used in the development of new applications and the maintenance of existing applications. The methodology contains required procedures for user involvement, testing, conversion, and management approvals of system processing integrity features.

Computer operations and job scheduling procedures exist, are documented, and contain procedures and instructions for operations personnel regarding system processing integrity objectives, policies, and standards. Exceptions require the approval of the manager of computer operations.

The entity's application systems contain edit and validation routines to check for incomplete or inaccurate data. Errors are logged, investigated, corrected, and resubmitted for input. Management reviews error logs daily to ensure that errors are corrected on a timely basis.

End-of-day reconciliation procedures include the reconciliation of the number of records accepted to the number of records processed to the number of records output.

The following additional controls are included in the entity's e-commerce system:

- Packing slips are created from the customer sales order and checked by warehouse staff as the order is packed.
- Commercial delivery methods are used that reliably meet expected delivery schedules. Vendor performance is monitored

	SP's network.	and assessed periodically.
		<ul style="list-style-type: none"> • 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.	<p>Written procedures exist for the distribution of output reports that conform to the system processing integrity objectives, policies, and standards.</p> <p>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.</p> <p>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.</p> <p>The following additional controls are included in the entity's e-commerce system:</p>
	<p>If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters:</p>	
	<ul style="list-style-type: none"> • The entity displays sales prices and all other costs and fees to the customer before processing the transaction. • Transactions are billed and electronically settled as agreed. • Billing or settlement errors are promptly corrected. 	<ul style="list-style-type: none"> • All costs, including taxes, shipping, and duty costs, and the currency used, are displayed to the customer. Customer accepts the order, by clicking on the "yes" button, before the order is processed. • Customers have the option of printing, before an online order is processed, an "order confirmation" for future verification with payment records (such as credit card statement) detailing information about the order (such as item(s) ordered, sales prices, costs, sales taxes, and shipping charges). • All foreign exchange rates are displayed to the customer before performing a transaction involving foreign currency. • Billing or settlement errors are followed up and corrected within 24 hours of reporting by the customer.
3.5	There are procedures to enable tracing	Input transactions are date and time stamped by the system and iden-

of information inputs from their source to their final disposition and vice versa.

tified 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 matters:

- | | |
|---|---|
| <p><i>a.</i> Logical access security measures to access information not deemed to be public</p> | <ul style="list-style-type: none">• 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. |
| <p><i>b.</i> Identification and authentication of authorized users</p> | <ul style="list-style-type: none">• 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. |
| <p><i>c.</i> Registration and authorization of new users</p> | <ul style="list-style-type: none">• 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 pro- |

vide 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. 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 accor-

dance 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

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

processing integrity.

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 annual-

ly.

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

The entity's data center facilities include climate and environmental monitoring devices. Deviations from optimal performance ranges

impact on system processing integrity and security is assessed on a timely basis, and policies are updated for that assessment.

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

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.

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.

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.

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

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

<i>Criteria</i>	<i>Illustrative Controls</i>
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.	<p>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.</p> <p>As part of the periodic corporate risk assessment process, the security officer identifies changes to the IT risk assessment based on</p> <ul style="list-style-type: none"> • 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. <p>The security officer then updates the confidentiality and security policies based on the IT risk assessment.</p> <p>Changes to the IT security policy are approved by the IT standards committee prior to implementation.</p> <p>User confidentiality requirements are documented in service-level agreements, nondisclosure agreements, or other documents.</p>
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:	<p><i>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.</i></p>
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 security 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 policies, 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:
- 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. Signed nondisclosure agreements are required before sharing information designated as confidential with third parties.

Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity.

- f. 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 incorpo-

rated 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 by-passes 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
- Corporate customers are assigned a unique company identifier that is required as part of the login process. Access soft-

- from accessing confidential information other than their own.
- ware 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 Internet or other public networks.
- 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 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 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.
- 3.16 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 ap-

plied.

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 corrective 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

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

policies.

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

See [generally accepted privacy principles](#) for related criteria.

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 Federling
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

