2001

WebTrust program : availability principle and criteria, Version 3.0, January 1, 2001

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

AICPA
The CPA. Never Underestimate The Value.SM

Chartered
Accountants
of Canada

Comptables
agréés
du Canada

AICPA/CICA

WebTrust SM/TM
Program

Availability Principle and Criteria

January 1, 2001

Version 3.0

The Principles and Criteria contained in this document supersede the WebTrust – ISP Principles and Criteria for Internet Service Providers insofar as they relate to availability and are effective for examination periods beginning after February 28, 2001. Earlier adoption is encouraged.

This document is available on AICPA Online at http://www.aicpa.org and on CICA Online at http://www.cica.ca.

COMMITTEE AND TASK FORCE MEMBERS

AICPA
Assurance Services Executive Committee

Susan C. Rucker, *Chair*

Gari Fails

Ted Horne

Everett C. Johnson, Jr.

John Lainhart

J. W. Mike Starr

Wendy E. Visconty

Thomas E. Wallace

Neal West

<u>Staff Contacts:</u>

Alan Anderson,
Senior Vice President, Technical Services

Anthony J. Pugliese,
Director of Assurance Services

CICA
Assurance Services Development Board

Doug McPhie, *Chair*

Diana Chant

Douglas C. Isaac

Marilyn Kuntz

Jeff Orchard

Frederick J. Phillips

David W. Stephen

Doug Timmins

Keith S. Vance

<u>Staff Contacts:</u>

Cairine M. Wilson,
Vice President, Innovation

Gregory P. Shields,
Director
Assurance Services Development

AICPA / CICA Electronic Commerce
Assurance Services Task Force

Everett C. Johnson, Jr., *Chair*

Bruce R. Barrick

Jerry R. DeVault

Joseph G. Griffin

Christopher J. Leach , *Vice Chair*

Patrick J. Moriarty

William Powers

Kerry L. Shackelford

Donald E. Sheehy

Christian R. Stormer

Alfred F. Van Ranst

<u>Staff Contacts:</u>

Bryan Walker, CICA
Principal, Assurance Services Development

Sheryl Martin, AICPA
WebTrust Team Leader

CONTENTS

WEBTRUST AVAILABILITY PRINCIPLE AND CRITERIA

Introduction

For entities to transact business through Web sites in either a business-to-consumer or a business-to-business electronic commerce (e-commerce) relationship, it is imperative that customer access be available to entities' sites as advertised or promised in a service-level agreement

Service providers facilitate their customers' communication and business over the Internet through a number of services. These are provided in various capacities, ranging from providing customers a pipeline to the Internet, to providing online processing and other applications for use by their customer, to acting as a data center processing operation for customers' businesses. Because a customer's e-commerce business can be totally reliant on a service provider having its service available, it is critical that a customer's access to the data center, network, and Internet backbone is available as advertised or promised by the service provider in its service-level agreement. If the service is unavailable for a significant period, each of the customers may likewise suffer temporary loss of revenue, impaired cash flow, or diminished public image.

The WebTrust Availability Principle sets out an overall objective for availability. In the course of a WebTrust audit, the practitioner uses the WebTrust Criteria as the basis for assessing whether the Principle has been achieved. It should be noted that this Principle does not, in itself, set an acceptable minimum availability percentage performance level for Web sites or service provider access. The minimum availability percentage is established by mutual agreement (contract) between the customer and the service provider.

The WebTrust criteria are supported by illustrative controls. These controls address matters related to (1) the availability of a business-to-consumer or a business-to-business Web site and other operations of a service provider data center, (2) security and related controls that are needed to ensure availability, and (3) the continuous performance monitoring and management of availability and anticipation of potential problems that could reduce availability. The availability criteria contemplate that business continuity and disaster recovery plans are in place and periodically tested to ensure the integrity and continuity of systems and minimize the impact on the customer in the event of disaster or temporary outage. These and other related matters are important to promote confidence in e-commerce.

The WebTrust Availability Principle

The entity discloses its availability practices, complies with such availability practices, and maintains effective controls to provide reasonable assurance that electronic commerce systems and data are available in conformity with its disclosed availability practices.

The WebTrust Criteria[1]

The WebTrust Criteria are organized into four broad areas – disclosures, policies, procedures, and monitoring.

A four-column format has been used to present and discuss the criteria. The first column presents the criteria—the attributes that the entity must meet to be able to demonstrate that it has achieved the principle. The second, third and fourth columns provide illustrative disclosures and controls for business-to-consumer transactions, business-to-business transactions, and for transactions applicable to service providers. These are examples of disclosures the entity might make and controls that the entity might have in place to conform to the criteria. Alternative and additional disclosures and controls also can be used.

For the purpose of these criteria, the term “customer” includes (1) individual consumers who have provided information and consummated transactions and (2) business partners.

[1] These criteria meet the definition of “criteria established by a recognized body” described in the third General Standard for attestation engagements in the United States (AICPA, *Professional Standards*, vol. 1, AT sec. 100.14) and in the standards for assurance engagements in Canada (CICA *Handbook*, paragraph 5025.41).

WebTrust Principle and Criteria
Availability

Principle

The entity discloses its availability practices, complies with such availability practices, and maintains effective controls to provide reasonable assurance that electronic commerce systems and data are available in conformity with its disclosed availability practices.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A	**Disclosures**			
A.1	The entity discloses the terms, conditions and practices for the availability to its data center, network, Internet backbone, or both by its customers.	To allow sufficient time for file maintenance and backup, the maximum number of hours per day that our network will be made available is twenty-two hours per day/seven days a week. In the event of a disaster or other prolonged service interruption, the entity has arranged for the use of alternative service sites to allow for full business resumption within twenty-four hours.		
A.2	The entity discloses its procedure for individuals, companies or other users to inform the entity about breaches or possible breaches to the security of its e-commerce system(s).	Should you believe that there has been a breach to the security of this site please contact us *immediately* at (800) 123-1234.		

<table>
<tr><th></th><th>Criteria</th><th>Illustrative Disclosures for Business-to-Consumer E-Commerce</th><th>Illustrative Disclosures for Business-to-Business E-Commerce</th><th>Illustrative Disclosures for Service Providers</th></tr>
<tr><td>A.3</td><td>The entity discloses its procedures for customer recourse for system availability issues that are not resolved by the entity. This resolution process should have the following attributes —
• Management's commitment to use a specified third-party dispute resolution service or other process mandated by regulatory bodies, in the event the customer is not satisfied with the entity's proposed resolution of such a complaint, together with a commitment from such third party to handle such unresolved complaints.
• Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party.</td><td colspan="3">Transactions at this site, with respect to system availability, are covered by binding arbitration and are arbitrated by the National Arbitration Forum. They can be reached at www.arb-forum.org or by calling toll-free (800) 474-2371. For the details of the terms and conditions of arbitration, click here.

Transactions at this site, with respect to system availability, are covered by binding arbitration conducted through our designated arbitrator (name of arbitrator). They can be reached at www.name.org or by calling toll-free (800) 111-2222. For the details of the terms and conditions of arbitration, click here.

Transactions at this site, with respect to system availability, are covered by the Banking (Canadian Banking) Industry Ombudsman of the Bankers Association who can be reached at www.bankom.org.xy or by calling toll-free (800) xxx-xxxx.

For transactions at this site, with respect to system availability, should you, our customer, require follow up or response to your questions or complaints, you may contact us at www.xxx.org. If your follow up or your complaint is not handled to your satisfaction, then you should contact the electronic commerce ombudsman who handles consumer complaints for e-commerce in this country. He can be reached at www.ecommercombud.org or by calling toll-free at (800) xxx-xxxx</td></tr>
</table>

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.4	The entity discloses any common applications, hardware, software or other functionality that it offers for use by other individuals, users or groups, and the extent to which its disclosures and controls address the availability of such functionality.	N/A	N/A	We provide on our Web site facilities for Web hosting and the use, by business customers, of the XYZ ERP software. The ERP software has a common configuration for application functionality and security configuration customized to meet the needs of each business customer. Our disclosures on this Web site and the related controls include the common application functionality of the XYZ ERP software but exclude the security features and controls, which are customized for each business customer.

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
B	**Policies**			
B.1	The entity's policies related to availability cover the e-commerce system and data and include, but are not limited to, the following items: • Who is allowed access, what is the nature of that access, and who authorizes such access • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access • Who is accountable for security, system upgrades, backups, and maintenance • Disaster recovery and business continuity planning • Controls over physical access to the system(s). • How complaints about availability can be addressed • Procedures to handle security incidents • Process to monitor disclosed system availability • The entity's commitment to use third-party dispute resolution that conforms to the Principles of Arbitration for WebTrust	The company's policy provides detailed guidelines for user profile creation, modification and deletion along with the assignment of corresponding permissions for the user. Management has also assigned accountability for security of the system (both physical and logical) to the information technology (IT) department. Such security includes policies covering system-wide backup, upgrades, and maintenance. These procedures are reviewed annually. The IT department, with input from the entity executive committee has the responsibility for the development and maintenance of the disaster recovery plan. This plan is reviewed annually or when changes have been made to the entity system infrastructure. A mock disaster drill is performed annually to test the functionality of the plan. Management has in place a consumer hot line to allow customers to telephone in any comments, complaints or concerns regarding the security of the site and availability of the system. On a monthly basis, the IT department provides to management a report of system availability for the prior month. This report is evaluated to ascertain whether disclosed availability levels are met, to provide a basis for capacity and upgrade planning, and to evaluate other potential system weaknesses.		
B.2	The employees responsible for availability are aware of and follow the entity's policies related to availability and relevant security matters.	The company's policies related to availability and security are reviewed with new employees as part of their orientation and the key elements of the policies and their impact on the employee are discussed. New employees must then sign a statement signifying that they have read, understand and will follow these policies. Each year employees reconfirm their understanding of and compliance with these policies.		

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
B.3	Accountability for the entity's policies related to availability and relevant security matters has been assigned.	Management has assigned responsibilities for the implementation of the company availability policy to the chief information officer (CIO). Others on the executive committee assist in the review and update of the policy as outlined in the executive committee handbook.		
B.4	The entity has allocated training and other resources to support its policies related to availability and relevant security matters.	Capacity and performance management processes exist to monitor, manage and report on network performance and processing thresholds. Procedures exist for monthly measurement, formal reporting of actual performance, and measuring capacity results against disclosed service levels. Capacity requirements are compared with capacity estimates. The company has established procedures to estimate future capacity requirements and has defined specific trigger events that will result in obtaining additional capacity with sufficient lead-time for acquisition, development, testing and implementation of additional systems.		
B.5	The entity's policies related to availability and relevant security matters are consistent with disclosed availability requirements, security practices, and applicable laws and regulations.	Management reviews its disclosed availability policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. The executive committee makes any changes or needed modifications to the policy or disclosure within five business days from management's evaluation. Laws and regulations that affect the disclosed site security policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update.		

	Criteria	**Illustrative Controls for Business-to-Consumer E-Commerce**	**Illustrative Controls for Business-to-Business E-Commerce**	**Illustrative Controls for Service Providers**
C	**Procedures**			
	Security Criteria That Relate to Availability			
C.1	The entity has security procedures to establish new users.	New users are given a secure session in which to provide new user information and select an appropriate user identification (ID) and password.	New users are given a secure session in which to provide new user information and select an appropriate user ID and password. Passwords must contain at least six characters, one of which is non-alphanumeric.	New users provide information in a Secure Socket Layer (SSL) session. User IDs and passwords are provided to the user and contain non-alphanumeric characters.
C.2	The entity has security procedures to identify and authenticate authorized users.	All users are required to provide a unique user ID and password to place an order or access their specific customer information.	To enter the site all customers are required to provide a unique user ID and password. These passwords are case sensitive and need to be updated every ninety days. Users are required to use a digital ID provided by the company to access, place or update orders. File and directory level user and group permissions are used to further restrict access based on information contained within the digital certificate.	System level access to all production systems (for example, UNIX and Windows NT) is provided via a strong identification and authentication mechanism (digital ID, one-time password, SecureID or other system). Strong, static passwords are used for systems that do not require a strong identification and authentication mechanism. Controlled access by a software authentication product with a strong identification and authentication mechanism is required for access to any routers.

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C.3	The entity has procedures to allow users to change, update, or delete their own user profile.	To update, change, or delete user information, the user’s current ID and password are required. After providing this information in a secure session, the user can proceed to the user profile section for any changes.	The user can only process changes to a user profile after a processing code is obtained from the entity. This code is obtained after verification with the user’s company about the need for the update or change.	All changes to user profiles are done after providing user ID and password. The only changes allowed are updates to the user ID and password. Changes to personal information or deletions must be processed in writing.
C.4	The entity has procedures to limit remote access to the internal network to only authorized personnel.	Remote access is provided to key employees; the system accepts remote calls, verifies the user, and then hangs up and calls the user back at the authorized number. Logical access control procedures (for example, firewalls, routers and password controls) are maintained by the IT department. These controls are tested on a periodic basis by performing penetration testing from both within the internal network and from the Internet. Identification and authentication is accomplished through the combination of a user ID and one-time password. The remote access to and use of the computing resources are restricted by the implementation of an authentication mechanism of identified users and resources associated with access rules. User IDs and passwords are stored in an encrypted database with the associated encryption key stored off-line.		
C.4.1	The entity has procedures to protect internal systems from viruses and malicious code	The company maintains anti-virus software on its systems, updates its virus signatures at least monthly, and takes reasonable precautions to protect both its systems and the customer's computer from viruses during the e-commerce session.	In connection with other security monitoring, management participates in user groups and subscribes to services relating to computer viruses. Daily the server downloads the most current virus definitions and any updates are then automatically “pushed” to users as they log on. Any viruses discovered are reported to the security team and an alert is created for all users notifying them of a potential virus threat.	Management subscribes to several services relating to viruses and other malicious codes. The service provider’s systems run two separate virus scanning programs at all times that are updated daily. Internal users are required to run a full scan on their local machines once a month.

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C.5	The entity has procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information in a manner that could affect availability.	Customers are required to enter a user ID and password to access private customer information and orders. A challenge word or phrase (for example, favorite sport or music – not a word that is easily identifiable such as mother's maiden name) is stored on the system in the event a user forgets or misplaces a password.	All access to customer accounts is restricted to the customer through the use of a unique digital certificate associated with each customer. Customer sessions between the browser and e-commerce systems are protected to avoid other users from hijacking a customer's session (for example, use of unique digital certificates or cookies checking for random unique identifiers before the start of each session).	One-time passwords, smart cards, or both restrict all system access from outside the entity, other than for customary e-commerce transactions through the Web page. Customer Web sites hosted by the Internet service provider (ISP) are prevented from intercepting messages not addressed to them. Packet filters are implemented on the ISP Internet gateway routers using access control lists (ACLs) according to the ISP firewall policy. Anti-spoof filters are used on the routers to prevent spoofing of trusted sources. Additional ACLs are used to control customer access to only their network segments. The various local area networks (LAN) segments are firewalled from the rest of the networks.
		The authentication process allows the user to access only information relevant to that particular user. Other methods are in place to detect users attempting to guess another password or if a brute force attack is under way. If such an attack is detected, the system disconnects from the user and reports the security breach for follow up.		
C.6	The entity has procedures to limit access (in a manner that could affect availability) to systems and data to only authorized employees based upon their assigned roles and responsibilities.	Employee access to customer data is limited to individuals based upon their assigned responsibilities. Idle workstations are timed-out after thirty minutes. Access to the corporate information technology facilities is limited to authorized employees by use of a card/key system supported by video surveillance monitoring.		

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C.7	The entity uses encryption or other equivalent security procedures to protect transmissions of user authentication and verification information passed over the Internet.	The entity uses 128-bit encryption for all transmission of private or confidential information, including user ID and password. Users are also encouraged to upgrade their browser to the most current version to avoid any possible security problems. [Add one-time password example] The company does not use encryption for authentication purposes, but uses one-time passwords or tokens to authenticate users.		
C.8	The entity has procedures to maintain system configurations that minimize availability and related security exposures.	Company management routinely evaluates the level of performance it receives from the ISP that hosts the company Web site. This evaluation is done by evaluating the security controls the ISP has in place by an independent third party as well as by following up with the ISP management on any open items or causes for concern.		The service provider meets with its technology vendors on a regular basis (for example, SUN, Cisco and Microsoft). Identified vendor security issues are documented and conveyed to the vendor to the appropriate level of management, depending on the severity of the exposure and risks associated with its planned or current deployment in the network. All vendor security issues are associated with agreed upon time frames and followed up by an ISP representative.
C.9	The entity has procedures in place to monitor and act on security breaches that affect availability.	System logs are monitored and evaluated on a daily basis. Monitoring software is in place that notifies the IT manager via email and pager should any incident be in progress. If an incident occurs, a report is filed within twenty-four hours for follow-up and analysis. Customers are directed to an area of the Web site to post a message about security breaches or possible breaches as soon as they become concerned. These customer comments are followed up within twenty-four hours for evaluation, and a report is issued to the customer and CIO, or the customer may contact the incident response hot-line by telephoning (888) 911-0911 24x7.		

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
	Availability Specific Criteria			
C.10	The entity considers environmental issues related to availability, and protects the system against potential threats that might disrupt system operation and impair availability.	Management maintains measures to protect against environmental factors (for example, fire, dust, power, and excessive heat and humidity). 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 company site is protected against a disruption in power supply to the processing environment by using both uninterruptible power supplies (UPS) and emergency power supplies (EPS). This equipment is tested on a regular basis.		
C.11	The entity has procedures to monitor availability and capacity compared to its disclosed commitments and provide for expected future requirements	Monitoring tools and response processes identify and address network and system capacity and availability problems in a timely manner to ensure continued availability of the network and related systems.		
C.12	The entity documents, authorizes, tests and approves proposed system changes before implementation to protect the availability of its e-commerce system(s).	The company employs change control procedures with required approvals. These controls include beta testing before posting changes and updates to the live site as well as authorization procedures and documentation of the testing process. All requests for changes and system maintenance are standardized and subject to formal change management procedures. Changes are categorized and ranked according to priority, and specific procedures exist to handle urgent matters. Retail customers may be required to upgrade software due to required compatibility with the entity's software, or to install bug fixes and security patches. Customers will be notified of such upgrades. The change management system provides for an adequate audit trail facility that allows tracing from incident to underlying cause. The company maintains an inventory system of all hardware, software, software licenses, patch levels, and site configurations.		
C.13	Changes made during emergencies are documented and authorized (including after-the-fact approval).	Standard procedures for emergency changes are documented. All changes made in an emergency environment use these procedures., Such changes are reviewed weekly. A process is in place to record all changes made in response to emergencies and is used to create a review and approval report for management. Management reviews and approves the emergency response change report weekly.		

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
C.14	The entity provides for backup, offsite storage, restoration, and disaster recovery processes sufficient to achieve its disclosed availability commitments.	Management has implemented a comprehensive strategy for backup and restoration based on a review of business requirements. Backup procedures for the company 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. The disaster recovery framework defines the roles and responsibilities, the approach to be adopted, and the structure of the plan. Procedures are in place that require company management approval of the disaster recovery plan after all major changes. All critical personnel hold current versions of the disaster recovery plan, both on-site and off-site. An electronic version is stored off-site. Disaster recovery capability is tested at least annually. The disaster recovery plan identifies the critical information technology application programs, operating systems, personnel, data files, and time frames needed to assure high availability and system reliability.		
C.15	The entity's protects the integrity of replicated data and information that is maintained to support its availability commitments as disclosed on its Web site.	The company protects the integrity of data and information stored in backup libraries by "hashing" the data, comparing this with expected results annually, and testing the usability of these backups. Backups are performed in accordance with the company's defined backup strategy, and usability of backups is verified at least annually. Data files are inventoried systematically. An off-site inventory list provides details of all data stored off-site with individuals who are allowed access to such backup information. The company performs an annual verification of media stored at the off-site storage facility. As part of the verification, media at the off-site location are matched to the appropriate media management system. System backups are stored off-site in a fireproof safe. Backups are stored for twelve months. The storage site is reviewed bi-annually for physical access security and security of data files and other items. Replicated data designated for systems recovery purposes in the event of a disruption are subjected to security and data integrity procedures consistent with the procedures applied to the primary systems data.		

	Criteria	Illustrative Controls for Business-to-Consumer E-Commerce	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
D	**Monitoring**			
D.1	The entity has procedures to monitor the availability of its e-commerce systems and to identify any need for changes to its availability and related security controls.	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 up at the monthly IT management meetings. The Information Security group uses the following monitoring tools: • COPS – This software provides a snap shot of the system which is analyzed on a monthly basis. • Tripwire – This is a real time monitor which is used to detect intruders. • SATAN -- This software is run monthly and provides a security analysis of the system. In addition, the group maintains and analyzes the server logs.		Commercial and other monitoring software (for example, COPS, SATAN and ISS) is run on a routine basis. The report outputs from these programs are analyzed for potential weaknesses and threats to the systems. Changes are made due to the information contained in these reports and with the consultation and approval of management.
D.2	The entity has procedures in place to monitor its availability and security incident procedures and to update these as needed due to technology changes, changes in the structure of the e-commerce system(s), or other information.	Weekly IT staff meetings are held to address current security concerns and their findings are discussed at quarterly management meetings.	Senior management reviews the security policy on a biannual basis and considers developments in technology and the impact of any laws or regulations.	
D.3	The entity has procedures to monitor environmental and technological changes and related risks and their impact on its disaster recovery plan. e-commerce	A risk assessment has been prepared and is reviewed on a regular basis or when a significant change occurs in either the internal or external environment. Changes in system components are assessed for their impact on documented system security objectives, policies and standards.		
D.4	The entity has procedures to provide that reports of noncompliance with availability disclosures and controls are addressed and that corrective measures are taken on a regular and timely basis.	Processing problems are recorded and accumulated in a problem report. Corrective action is noted and monitored by management. As a part of the monthly monitoring of the site, availability and site usage reports are compared to the disclosed availability levels. This analysis is used to forecast future capacity, reveal any performance issues and provide a means of fine-tuning the system.		

APPENDIX A

WEBTRUST$^{SM/TM}$ SELF-ASSESSMENT QUESTIONNAIRE

FOR AVAILABILITY

This questionnaire is for use by electronic commerce (e-commerce) service providers to document their availability disclosures, policies, procedures and monitoring as a basis for their assertion or representation that "on its Web site at www.___.____ during the period ___________, 200_ through ___________, 200_ the entity—

- Disclosed its availability practices for electronic commerce,
- Complied with such availability practices, and
- Maintained effective controls to provide reasonable assurance that electronic commerce systems and data are available as disclosed

based on the AICPA/CICA WebTrust $^{SM/TM}$ Criteria."

General Information

E-commerce Activities to Be Covered

1. Describe as applicable:

   a) The goods and services being sold or provided?

   b) The typical customer?

   c) The typical form of payment?

2. What is the Web site URL?

3. Identify the individual who has primary responsibility for controlling the online disclosure of the entity's policies and its adherence to these policies and what is this individual's reporting relationship to the entity's management?

4. How long has the entity been selling such goods and services through this form of e-commerce?

5. Has the entity made substantive changes to its disclosed policies and practices or the related disclosures in the last ninety days? If so, describe the nature of such changes and when each change occurred.

Information Systems Used to Support E-commerce Activities

6. List the Web Site or other customer interface systems and provide the following information about each:

    a) Provide a description.

    b) Indicate who, in this entity, is responsible.

    c) Describe any portion of these systems that is outsourced to third parties.

    d) Describe the frequency and nature of changes to Web site and customer interface systems.

7. List the telecommunications and network systems, including the following information.

    a) Give a description.

    b) Indicate, who, in this entity, is responsible.

    c) Describe any portion of these systems that is outsourced to third parties.

    d) Describe the frequency and nature of changes to telecommunications and network systems.

8. List the other supporting systems and technology, including the following information.

    a) Provide a description.

    b) Indicate who, in this entity, is responsible.

    c) Describe any portion of these systems that is outsourced to third parties.

    d) Describe the frequency and nature of changes to such systems and technology.

Web Site Server Technology

9. Describe the e-commerce server platform(s) in use (description and version).

10. How many e-commerce servers are in use at the primary site? How many are at an alternate or backup site?

11. Is SSL used for some, or all, Internet transactions? If so, describe the kinds of transactions for which SSL is used and the kind of digital server certificate being used.

12. Identify the technical staff (and/or whether the site is hosted by an ISP and the technical staff of the ISP) who are capable of performing the following technical tasks:

a) Generate a Certificate Signing Request (CSR) using the Web server software?

b) Install a Digital Certificate (also known as a Digital ID) on the Web server software?

c) Configure certain pages on your web server to be secure using (SSL)?

d) Install a Java Applet on the appropriate Web page?

13. Identify:

a) The WebServer package used.

b) Identify the version of Netscape that your customer base is most likely to be using.

Control Environment

14. Describe the factors in the entity's organization that contribute to a control environment that is generally conducive to reliable disclosures on its Web site and effective controls over monitoring the entities compliance with its disclosed privacy policies. Such factors might include, but are not limited to the following:

a) Management's "tone at the top"

b) Hiring, development, and retention of competent personnel

c) Emphasizing the importance and responsibilities for sound practices and effective control

d) Supervising its e-commerce related activities and control procedures

e) Employing a suitable internal auditing function that periodically audits matters related to the entity's e-commerce policies

f) Other factors

Specific to Availability

A Disclosures

1. Does the entity disclose the terms, conditions and practices for the availability to its data center, network, Internet backbone, or both by its customers?

2. Does the entity disclose the procedure for individuals, companies or other users to inform the entity about breaches or possible breaches to the security of its e-commerce system(s)?

3. Does the entity disclose the procedures for consumer recourse for issues regarding system availability for issues that are not resolved by the entity? This resolution process should

have the following attributes:

a) Management's commitment to use a specified third-party dispute resolution service or other process mandated by regulatory bodies, in the event the customer is not satisfied with the entity's proposed resolution of such a complaint, together with a commitment from such third party to handle such unresolved complaints.

b) Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party.

4. Does the entity disclose common applications, hardware, software or other functionality it offers for use by other individuals, users or groups, if any, and the extent to which its disclosures and controls address the availability of such functionality?

B Policies

1. Do the entity's policies related to availability covering the e-commerce system and data include at least the following:

   a) Who is allowed access, what is the nature of that access, and who authorizes such access.

   b) Procedures to add new users, modify the access levels of existing users, and remove users who no longer need access.

   c) Identify the individual responsible for security, system upgrades, backups, and maintenance.

   d) Disaster recovery and business continuity planning.

   e) The controls over physical access to the system(s).

   f) How complaints about availability can be addressed.

   g) Procedures to handle security incidents.

   h) The process to monitor disclosed system availability.

   i) The entity's commitment to use third-party dispute resolution that conforms to the Principles of Arbitration for WebTrust.

2. How are employees responsible for availability made aware of and required to follow the entity's policies related to availability and related security matters?

3. Identify the individual responsible for the entity's availability policy and related security matters.

4. Has the entity allocated training and other resources sufficient to support the entity's

availability policy and relevant security matters?

5. Are the entity's policies related to availability and related security matters consistent with disclosed availability requirements, security practices, and applicable laws and regulations?

C Procedures

Security Elements that Relate to Availability

1. Does the entity have security procedures to establish new users?

2. Does the entity have security procedures security procedures to identify and authenticate authorized users?

3. Does the entity have procedures to allow users to change, update or delete their own user profile?

4. Does the entity have procedures to limit remote access to the internal network to only authorized personnel?

   a) Does the entity have procedures to protect internal systems from viruses and malicious code?

5. Does the entity have procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information in a manner that could affect availability?

6. Does the entity have procedures to limit access (in a manner that could affect availability) to systems and data to only authorized employees based upon their assigned roles and responsibilities?

7. Does the entity use encryption or other equivalent security procedures to protect transmissions of user authentication and verification information passed over the Internet?

8. Does the entity have procedures to maintain system configurations that minimize availability and related security exposures?

9. Does the entity have procedures in place to monitor and act on security breaches that affect availability?

Availability Specific Criteria

10. Does the entity consider environmental issues that relate to availability and protect the system against potential threats that might disrupt system operation and impair availability?

11. Does the entity have procedures to monitor availability and capacity compared to its disclosed commitments and to provide for expected future requirements?

12. Does the entity document, authorize, test and approve proposed system changes before implementation to protect the availability of its e-commerce system(s)?

13. Does the entity document and authorize changes made during emergencies (including after-the-fact approval)?

14. Does the entity provide for backup, offsite storage, restoration, and disaster recovery processes sufficient to achieve its disclosed availability commitments?

15. Does the entity protect the integrity of replicated data and information that is maintained to support systems availability commitments as disclosed on its web site?

D Monitoring

1. Does the entity have procedures in place to monitor its availability and security incident procedures and to update these as needed due to technology changes, changes in the structure of the e-commerce system(s), or other information?

2. Does the entity have procedures to test its security incident policy and update it as needed due to technology changes, changes in the structure of the e-commerce system(s), or other information?

3. Does the entity have procedures to monitor environmental and technological changes and related risks and their impact on its disaster recovery plan?

4. Does the entity have procedures to provide that reports of noncompliance with availability disclosures and controls are addressed and that corrective measures are taken on a regular and timely basis?