2001

AICPA/CICA WebTrust program : business practices/transaction integrity principle and criteria, January 1, 2001, Version 3.0

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

Business Practices / Transaction Integrity Principle and Criteria

January 1, 2001

Version 3.0

The Principles and Criteria contained in this program supersede Version 2.0 of the WebTrust Principles and Criteria insofar as they relate to business practices and transaction integrity 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 BUSINESS PRACTICES / TRANSACTION INTEGRITY PRINCIPLE AND CRITERIA 5

Introduction 5

The WebTrust Business Practices / Transaction Integrity Principle 5

The WebTrust Criteria 6

APPENDIX A WEBTRUST$^{SM/TM}$ SELF-ASSESSMENT QUESTIONNAIRE FOR BUSINESS PRACTICES AND TRANSACTION INTEGRITY 28

WEBTRUST BUSINESS PRACTICES / TRANSACTION INTEGRITY PRINCIPLE AND CRITERIA

Introduction

In the course of communicating and transacting business over the Internet, consumers and businesses expect their business transactions to be processed completely, accurately and timely. Completeness generally indicates that all transactions are processed without exception, and that transactions are not processed more than once. Accuracy includes assurances that key information associated with the submitted transaction will remain accurate throughout the processing of the transaction. The timeliness of delivery of goods or services is addressed in the context of commitments made for such delivery. The risk is that the consumer or business initiating the transaction will not have the transaction completed correctly in accordance with the desired or specified request.

Business transactions that are sent electronically to another party are susceptible to loss, duplicate processing or the introduction of inaccurate information associated with the transaction. For example, if an electronic order is sent through the Internet from one company to another, without appropriate transaction integrity controls, the buyer may not receive the goods ordered, receive more of the goods than originally requested, or receive the wrong goods altogether. However, if appropriate business practices are followed and transaction integrity controls exist and are operational within the system, the buyer can be reasonably assured that the correct goods, in the correct quantity, at the correct price are received when promised.

The WebTrust Business Practices / Transaction Integrity Principle sets out an overall objective in respect to the completeness and accuracy of processing of electronic transactions sent over the Internet. In the course of a WebTrust audit, the practitioner uses the WebTrust Criteria as the basis for assessing whether the Principle has been achieved.

The WebTrust Business Practices / Transaction Integrity Principle

> *The entity discloses its business practices for electronic commerce, executes transactions in conformity with such practices, and maintains effective controls to provide reasonable assurance that electronic commerce transactions are processed completely, accurately, and in conformity with its disclosed business 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
Business Practices / Transaction Integrity

Principle

The entity discloses its business practices for electronic commerce, executes transactions in conformity with such practices, and maintains effective controls to provide reasonable assurance that electronic commerce transactions are processed completely, accurately and in conformity with its disclosed business 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 descriptive information about the nature of the goods that will be shipped or the services that will be provided, including, but not limited to, the following:			
A.1.1	Condition of goods (meaning, whether they are new, used, or reconditioned).	You can purchase new and used books on our site; used books are clearly labeled as such.	The mortgage rate information we obtain for your brokerage transaction is gathered from twelve different lending institutions on a daily basis. A complete listing of these lending institutions can be obtained by clicking here.	The business applications we provide at this site are fully licensed by the vendors we represent. A complete listing of all of our business vendors can be obtained on our “Business Partners” page.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.1.2	Description of services (or service contract).	ABC Trading Inc. provides various trading accounts, including cash accounts, margin accounts, options accounts, and short sell accounts. All pay interest so your money earns even when it is idle. Our Internet Services are as follows: • U. S. and Canadian Equities – Buy or sell securities listed on the AMEX, NASDAQ, NYSE, TSE, ME, VSE, ASE. • Options Trading - Buy puts and calls or write (sell) covered puts and calls on any exchange in the United States or Canada. • Short Selling - Short selling involves us borrowing the stock on the investor's behalf to cover the short-sale initially. The short sale of securities involves a high degree of risk and therefore may not be suitable for every investor.	ABC's Online RFQ Brokerage is the online clearing house for requests for quotes (RFQ) on custom-made parts. Through our unique service, OEM manufacturers looking for parts will be connected to contract manufacturers looking for work. RFQs published on our online brokerage undergo an intensive review process to ensure that contract manufacturers get all the information needed to compose a quote. ABC's trained personnel will work closely with OEM manufacturers new to the out-sourcing market to ease their fears. Contract manufacturers participating in the RFQ bidding process are members of ABC's BizTrust program. New members are subjected to an assortment of checks such as credit checks and reference checks to ensure that they are qualified to bid on RFQs. The results from these checks are organized into an easy to read BizTrust Report accessible by all members of ABC.	Backup Services: ABC Networks trained systems administrators will perform complete tape backup procedures including manual rotation, cataloging and shipping of material. On- and off-site storage is also available. Switch/Router Administration: ABC Networks provides setup and day-to-day management of your network devices, such as Cisco routers and switches. We offer configuration as well as administration of network devices. Personal Administrator: ABC Networks can provide a personal administrator who will maintain and update your network. With Microsoft NT, Solaris, Linux, Free BSD, or BSDI, your personal administrator will be available to you directly and will personally see to your needs. Usage management statistics: ABC Networks supplies each client with a private Web page giving them analysis of traffic patterns and usage for better site management.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.1.3	Sources of information (meaning, where it was obtained and how it was compiled).	ABC Trading Inc. uses a computerized routing system to obtain pricing information. Orders are directed to the market based on price and liquidity.	The nationwide survey, conducted by the compensation-research firm of Dowden & Co., presents data on 2000 compensation gathered from among more than 900 employers of information systems professionals, including corporations of all sizes, in every industry group, and from every U.S. region. The survey was completed July 1999.	N/A
A.2	The entity discloses the terms and conditions by which it conducts its electronic commerce (e-commerce) transactions including, but not limited to, the following -			
A.2.1	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).	Our policy is to ship orders within one week of receipt of a customer-approved order. Our experience is that over 90 percent of our orders are shipped within forty-eight hours, the remainder is shipped within one week.	Our policy is to ship orders as agreed in the standard sales agreement, unless specific contractual arrangements are in place.	You can access the services at our site within twenty-four hours from the time you set up an account with us, including your payment options.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.2.2	Time frame and process for informing customers of exceptions to normal processing of orders or service requests.	We will notify you by e-mail within twenty-four hours if we cannot fulfill your order as specified at the time you placed it and will provide you the option of canceling the order without further obligation. You will not be billed until the order is shipped.		ABC Applications takes your existing software and lets you deliver it to your customers on a rental basis over the Internet. With ABC Applications, applications are rapidly published over the Internet as an application service provider (ASP) proof of concept. Assistance is provided to develop an ASP business plan including pricing, sales and marketing, first- and second-line support mechanisms, and service level agreements. Field trials can be carried out with prospective customers before making ASP available on your price list.
A.2.3	Normal method of delivery of goods or services, including customer options, where applicable.	You have the option of downloading the requested information now or we will send it to you on CD-ROM by UPS two-day or Federal Express overnight delivery.	In the absence of a specified customer preference, we will ship by ground transportation locally and nationally.	ABC Applications are delivered to any desktop and anywhere in the world as long as the workstation has a browser and a connection to the Internet.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.2.4	Payment terms, including customer options, if any.	Your credit card will be charged at the time of shipment or you can send us a check or money order.	Credit approval is required before shipment. All goods will be invoiced on shipment according to either our normal terms of settlement (net thirty days), or where alternative contractual arrangements are in place, those arrangements shall prevail.	Your credit card will be charged at the time the service is initiated, you can send us a check or money order, or when your anticipated monthly charge is expected to exceed $1,000 per month, you can obtain credit approval from us. Credit accounts will be billed monthly on a net thirty-day basis.
A.2.5	Electronic settlement practices and related charges to customers.	Your bank account will be charged $12.95 monthly for our service fee.	We require an electronic funds transfer of fees and costs at the end of the transactions. For new customers, a deposit may be required.	At your option, your credit card or bank account can be charged monthly for any fees for additional services.
A.2.6	How customers may cancel recurring charges, if any.	To cancel your monthly service fee, send us an e-mail at Subscriber@ABC.COM or call us at (800) 555-1212. Be sure to include your account number.		
A.2.7	Product return policies and limited liability, where applicable.	Purchases can be returned for a full refund within thirty days of receipt of shipment. Call our toll-free number or email us for a return authorization number, which should be written clearly on the outside of the return package. Transactions that occur at this site are in accordance with the laws and business practices of Alberta, Canada.		Disputes or service complaints need to be filed within seventy-two hours of service. We will evaluate your problem and respond to you within forty-eight hours of the filing of your complaint. The laws and business practices of the province and country where our company is located govern our business.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.3	The entity discloses on its Web site (or in information provided with the product, or both), where customers can obtain warranty, repair service, and support related to the goods and services purchased on its Web site.	Warranty and other service can be obtained at any one of our 249 locations worldwide that are listed on this Web site. A list of these locations also is provided with delivery of all of our products.	Warranty and other service can be obtained at any one of our locations that are listed on this Web site.	Technical support is available 24x7 by contacting (877) 111-1234. This service is free for the initial ninety days you have our service. After that you may sign up for one of our customer care programs at http://ABC.COM/CUSTCARE.html.
A.4	The entity discloses information to enable customers to file claims, ask questions and register complaints, including, but not limited to, the following: • Telephone number (a number to reach an employee on a reasonably timely basis and not only a voice mail system or message machine). • Days and hours of operation. • If there are several offices or branches, the same information for the principal office.	For service and other information, contact one of our customer service representatives at (800) 555-1212 between 7:00 A.M. and 8:00 P.M. (central standard time) or you can write to us as follows: Customer Service Department ABC Company 1234 Anystreet, Anytown, Illinois 60000 or CustServ@ABC.COM		For all inquires and complaints (other than technical support), contact customer service at (877) 111-4321 between the hours of 8:00 A.M. and 8:00 P.M. (mountain time) Monday through Friday. International callers, please consult our Web site for additional telephone numbers.

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.5	The entity discloses its procedures for customer recourse for issues that are not resolved by the entity regarding transaction integrity. These complaints may relate to any part of a customer's electronic commerce transaction, including complaints related to the quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints. 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.	Transactions at this site are covered by binding arbitration and arbitrated by the National Arbitration Forum. They can be reached at www.arb-forum.org or by calling toll-free (800) 474-2371. Our process for consumer dispute resolution requires that you contact our customer hot-line, toll-free at (800) 555-1234 or contact us via e-mail at custhelp@ourcompany.com. If your problem has not been resolved to your satisfaction you may contact the Cyber Complaint Dispute Resolution Association. They can be reached at (877) 123-4321 during normal business hours (8:00 A.M. – 5:00 P.M. central time) or via their Web site at www.ccomplaint.com. For the details of the terms and conditions of arbitration, click here. For transactions at this site, should you, our customer, require follow up or response to your questions or complaints, you may contact us at www.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		

	Criteria	Illustrative Disclosures for Business-to-Consumer E-Commerce	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A.6	The entity discloses its procedure for individuals, companies or other users to inform the entity about breaches or possible breaches to the integrity (including security) of its e-commerce system(s).	Should you believe that there has been a breach to the integrity or security of this site please contact us *immediately* at (800) 123-1234.		
A.7	The entity discloses the nature of common application services provided to business customers and the extent to which the entity's disclosed business practices and transaction integrity controls apply to such services.	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 customized security configurations to meet the needs of each business customer. Our disclosures on this Web site and the related transaction integrity controls include the common application functionality of the XYZ ERP software, but exclude the security features and controls that 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 transaction integrity 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 • Security procedures to protect transaction integrity • Procedures to document and allow for follow-up on transactions • How complaints and requests about transactions can be addressed • Procedures to handle security incidents • 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. Proper accountability to the transactions has been assigned to the information technology (IT) and accounting departments. The IT department is responsible for the systems that retain transaction history, including proper backup and storage of the information. The accounting department is responsible for the controls, checks and balances of the transactions. 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 the details of the customer's transaction. Proper historic audit trails of e-commerce transactions are maintained for any needed follow-up. These records are maintained for the time mandated by the cognizant regulatory agency or legal entity, after which time they are deleted. The record retention and deletion policy is reviewed on a periodic basis by company management. Management has procedures in place to allow employees and customers to report a breech or suspected breech to the security of the Website. Employees are required to report such incidents within two hours of the breech (or suspected breech). Customers are encouraged to call the toll-free number posted at the company Web site.		
B.2	The employees responsible for transaction integrity are aware of and follow the entity's policies related to transaction integrity and relevant security matters.	Company policies that relate to transaction integrity and related security are reviewed with new employees as part of their orientation and the key elements of these 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 such policies. Each year employees reconfirm their understanding of and compliance with such policies.		
B.3	Accountability for the entity's policies related to transaction integrity and relevant security matters has been assigned.	Management has assigned responsibilities for the enforcement of the company transaction integrity policy to the chief financial officer (CFO). Others on the executive committee assist in the review and update of the policy as outlined in the executive committee handbook.		

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
B.4	The entity’s policies related to transaction integrity and relevant security matters are consistent with disclosed business practices and applicable laws and regulations.	Management reviews its disclosed transaction integrity and security 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. Laws and regulations that affect the disclosed transaction integrity practices 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 Transaction Integrity

Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
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 the 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.	All system-level access to all production systems (for example, UNIX and Windows NT) is provided via a strong identification and authentication mechanism (for example, 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 process changes to a user profile only 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 (for example, firewalls, routers and password controls) is 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.		

	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 transaction information.	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.
		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 will disconnect from the user and report the security breach for follow-up.		
C.6	The entity has procedures to limit access 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 30 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.		
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 company 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. The company does not use encryption for authentication purposes, but uses one-time passwords or tokens to authenticate users.		

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C.8	The entity has procedures to maintain system configurations that minimize transaction integrity and related security exposures.	Company management routinely evaluates the level of performance it receives from the ISP which hosts the company Web site. This evaluation is done by evaluating the security controls the ISP has in place by an independent 3rd 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 on by an ISP representative
C.9	The entity has procedures in place to monitor and act on security breaches that affect transaction integrity.	System logs are monitored and evaluated on a daily basis. Monitoring software is in place that will notify the IT manager via e-mail 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 back 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
Requesting Goods and Services			
C.10 The entity checks each request or transaction for accuracy and completeness.	Web scripts contain error checking for invalid inputs. The company's computer system automatically checks each order for accuracy and completeness of information before processing. All customer-provided information for the order is displayed to the customer. Customer accepts an order, by clicking yes, before the order is processed.	Web scripts contain error checking for invalid inputs. The company's computer system automatically checks each transaction for accuracy and completeness of information before processing. All transactions are displayed to the customer to accept, by clicking yes, before the transaction is processed.	After the user creates an initial order for services, the system takes the user to a confirmation screen, where positive confirmation is required from the user before the order is processed.
C.11 Positive acknowledgment is received from the customer before the transaction is processed.	Before a transaction is processed by the company, 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 then processed.		
Processing Requests for Goods and Services			
C.12 The correct goods are shipped in the correct quantities in the time frame agreed, or services and information are provided to the customer as requested.	Packing slips are created from the customer sales order and checked again as the order is packed. Commercial delivery methods are used that reliably meet expected delivery schedules. Service delivery targets are maintained and actual services provided are monitored against such targets. The company uses a feedback questionnaire to confirm customer satisfaction with completion of service or delivery of information to the customer.		N/A

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C.13	Transaction exceptions are promptly communicated to the customer.	Computerized backorder records are maintained and are designed to notify customers of backorders within twenty-four hours. Customers are given the option to cancel a backorder or have an alternate item delivered.		In case of loss of transmission, computerized records are maintained to allow for verification of services provided.
C.14	Incoming messages are processed and delivered accurately and completely to the correct IP address.	N/A	N/A	Appropriate monitoring software (for example, What's Up Gold, NOCOL, SiteScope and Keynote Systems) is used to perform network monitoring. Monitoring of latency, packet loss, hops, and network hardware is a continuous process. 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. The Web site and hardware owners are notified of unfavorable network performance, as part of the escalation procedures, on a weekly basis to assist in the escalation process.

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C.15	Outgoing messages are processed and delivered accurately and completely to the service provider's (SP’s) Internet access point.	N/A	N/A	Appropriate monitoring software (for example, What’s Up Gold, NOCOL, SiteScope and Keynote Systems) is used to perform network monitoring. Monitoring of latency, packet loss, hops and network hardware is a continuous process.
C.16	Messages remain intact while in transit within the confines of the SP’s network.	N/A	N/A	Appropriate monitoring software (for example, What’s Up Gold, NOCOL, SiteScope and Keynote Systems) is used to perform network monitoring. Monitoring of latency, packet loss, hops and network hardware is a continuous process. Any network outage is immediately escalated to determine the root physical cause. Escalation procedures result in the initiation of corrective actions to improve unfavorable network performance. The Web site and hardware owners are notified of unfavorable network performance, as part of the escalation procedures, in a timely manner to assist in the escalation process.

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
	Processing, Billing and Payment			
C.17	The entity displays sales prices and all other costs and fees to the customer before processing the transaction.	Customers have the option of printing, before an order is processed, an "order confirmation" on-line for future verification with payment records (such as credit card statement) detailing all information of the order (such as item(s) ordered, sales prices, costs, sales taxes, and shipping charges). All costs, including taxes, shipping and duty costs, and the currency used, are displayed to the customer. Customer accepts an order, by clicking yes, before the order is processed. All foreign exchange rates are displayed to the customer before performing a transaction involving foreign currency.		
C.18	Transactions are billed and electronically settled as agreed.	Total costs and the expected shipping and billing dates are displayed to the customer before the customer accepts the order.		
C.19	Billing or settlement errors are promptly corrected.	Billing or settlement errors are followed up and corrected within twenty-four hours of reporting by the customer.		

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C.20	Transaction histories are retained in a secure location, may not be altered without appropriate authorization, and are retrievable for review and investigation.	The company maintains a transaction history for each order. Appropriate physical security and access control measures have been established for information technology assets, including those maintained at an off-site location in conformity with the general security policy. Access to facilities and physical data storage is controlled (for example, doors and cabinets are locked at all times). Backup media library management responsibilities and controls exist to protect and ensure the accuracy of data and information stored in backup libraries. Each order has a unique identifier that can be used to access order information. This information can also be accessed by customer name, and dates of ordering, shipping or billing. The company maintains this identifier and detailed order records that enable customers to contact the entity about details of orders for at least ninety days from order fulfillment. Procedures are in place to ensure that data files are inventoried systematically. An off-site inventory list provides details of all data stored off-site. Order history information is maintained for six months from the date of shipment and is available for immediate access by customer service representatives. After six months, this information is maintained in a form that can be accessed by customer service representatives within three days. The company performs an annual audit of tapes stored at the off-site storage facility. As part of the audit, tapes at the off-site location are matched to the appropriate tape management system. System backups are stored off-site in a fireproof safe. Backups are stored for twelve months. The storage site is periodically reviewed regarding physical access security and security of data files and other items.		
C.21	Transactions are processed accurately and in conformity with the entity's disclosed business practices.	Management has implemented a process to regularly review customer complaints, backorder logs and other transactional analysis. This information is compared to the company's disclosed practices to ascertain the company's compliance.		

	Criteria	Illustrative Controls for Business to Consumer E-commerce	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
C.22	The entity logs transactions for subsequent follow-up.	The company maintains a transaction history for each order. Each order has a unique identifier that can be used to access order information. Such information also can be accessed by customer name and dates of ordering, shipping or billing. The company maintains this identifier and detailed order records that enable customers to contact the entity about details of orders for at least ninety days from order fulfillment. Order history information is maintained for six months from the date of shipment and is available for immediate access by customer service representatives. After six months, this information is maintained in a form that can be accessed by customer service representatives within three days.		

	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 transaction integrity of its e-commerce systems and to identify any need for changes to its transaction integrity and related security controls.	The Customer Service group monitors transactions 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-tie 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 output from these programs is 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 to provide that transaction history and related information is monitored and 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. Monitoring tools and response processes adequately identify and address network and system problems in a timely manner to ensure integrity of the network and related systems.		

APPENDIX A

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

FOR BUSINESS PRACTICES / TRANSACTION INTEGRITY

This questionnaire is for use by electronic commerce (e-commerce) service providers to document their business practices / transaction integrity disclosures, policies, procedures and monitoring for e-commerce 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 business practices for electronic commerce,
- Executed transactions in conformity with such practices, and
- Maintained effective controls to provide reasonable assurance that electronic commerce transactions are processed completely, accurately and in conformity with its disclosed business practices

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 Business Practices / Transaction Integrity

A Disclosures

1. Does the entity disclose information about the nature of the goods that will be shipped or the services that will be provided, including, but not limited to, the following:

   a) The condition of goods (meaning are they new, used or reconditioned).

   b) Description of services (or service contract).

   c) Sources of information (meaning, where the information was obtained and how it was compiled).

2. Does the entity disclose the terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following:

   a) The time frame established and disclosed for completion of transactions (transaction means fulfillment of orders where goods are being sold and delivery of service where a service is being provided).

   b) The time frame and the process for informing customers of exceptions to normal processing of orders or service requests.

   c) The normal method of delivery of goods or services, including customer options, where applicable.

   d) The payment terms, including customer options, if any.

   e) The electronic settlement practices and related charges to customers.

   f) How customers may cancel recurring charges, if any.

   g) The product return policies and limited liability, where applicable.

3. Does the entity disclose on its Web site (or in information provided with the product, or both) where customers can obtain warranty, repair service, and support related to the goods and services purchased on its Web site?

4. Does the entity disclose information to enable customers to file claims, ask questions and register complaints, including, but not limited to, the following:

   a) Telephone number (a number to reach an employee on a reasonably timely basis and not only a voice mail system or message machine).

   b) Days and hours of operation.

c) If there are several offices or branches, the same information for the principal office.

5. Does the entity disclose the procedures for consumer recourse for issues that are not resolved by the entity regarding transaction integrity? These complaints 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. This resolution process should have the following attributes:

   a) Management's commitment to use a specified third-party dispute resolution service in the event the customer is not satisfied with the entity's proposed resolution of such a complaint.

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

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

7. Does the entity disclose the nature of common application services provided to business customers and the extent to which the entity's disclosed business practices and transaction integrity controls apply to such services?

B Policies

1. Does the entity's policies related to transaction integrity include at least the following items:

   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) Security procedures to protect transaction integrity.

   d) Procedures to document and allow for follow-up on transactions.

   e) How complaints and requests about transactions can be addressed.

   f) Procedures to handle security incidents.

   g) 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 transaction integrity made aware of and required to follow the entity's published policies that cover transaction integrity and relevant security matters?

3. Identify the individual assigned responsibility for the entity's policies related to transaction integrity and relevant security matters?

4. Are the entity's policies related to transaction integrity and relevant security matters consistent with disclosed business practices and applicable laws and regulations?

C Procedures

Security Criteria That Relate to Transaction Integrity

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

2. Does the entity have 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?

5. Does the entity have procedures to prevent customers, groups of individuals, or other entities from accessing information other than their own transaction information?

6. Does the entity have procedures to limit access 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 integrity and related security exposures?

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

Requesting Goods and Services

10. Does the entity check each request or transaction for accuracy and completeness?

11. Does the entity receive positive acknowledgment from the customer before the transaction is processed?

Processing Requests for Goods and Services

12. Are the correct goods shipped in the correct quantities in the time frame agreed, or services and information are provided to the customer as requested?

13. Are transaction exceptions communicated promptly to the customer?

14. Are incoming messages processed and delivered accurately and completely to the correct IP address?

15. Are outgoing messages processed and delivered accurately and completely to the service provider's (SP's) Internet access point?

16. Do messages remain intact while in transit within the confines of the SP's network?

Processing, Billing and Payment

17. Are sales prices and all other costs and fees displayed to the customer before processing the transaction?

18. Are transactions billed and electronically settled as agreed?

19. Are billing or settlement errors promptly corrected?

20. Are transaction histories retained in a secure location, may not be altered without appropriate authorization, and are retrievable for review and investigation?

21. Are transactions processed accurately and in conformity with its disclosed business practices?

22. Does the entity log transactions for subsequent follow-up?

D Monitoring

1. Does the entity have procedures to monitor the transaction integrity of its e-commerce systems and to identify any need for changes to its transaction integrity and related security controls?

2. Does the entity have procedures to provide that transaction history and related information is monitored and corrective action is taken on a regular and timely basis?