2001

Webtrust - 2001; Assurance services alerts

American Institute of Certified Public Accountants

ASSURANCE SERVICES ALERTS

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

WebTrust℠—2001

Notice to Readers

The AICPA staff has prepared this document. This Alert has not been approved, disapproved, or otherwise acted on by any other senior technical committee of the AICPA.

Lori A. West, CPA
Technical Manager
Accounting and Auditing Publications

Special thanks to Sheryl Martin, CPA; Karyn Waller, CPA; and Ron Halse for their assistance in developing and reviewing this Alert.

1 2 3 4 5 6 7 8 9 0 AAG 0 9 8 7 6 5 4 3 2 1

Table of Contents

Introduction

This Alert is intended to provide practitioners with an overview of developments in the emerging practice area of WebTrust. It can serve as a source of information about WebTrust in addition to an update of important new developments for those who have expanded their practice to include WebTrust engagements. WebTrust services offer great potential for CPA practitioners when it comes to issues such as security and privacy, among others. There's a natural fit between practitioners, who can build on their reputation for independence, objectivity, and integrity, and WebTrust. Practitioners have experience in providing assurance. This experience, coupled with practitioners' reputation for compliance with comprehensive ethics rules and professional standards, provides a great foundation from which to launch assurance services involving controls and compliance with specified principles and criteria. Further, WebTrust practitioners have developed many "spin-off" consulting and advisory services. Firms now offer security consulting, privacy reviews, strategic planning, and other related services. Often, engagements begin with readiness assessments or gap analyses, which identify the areas of weakness of a company. The CPA's knowledge of internal control and assessment techniques are important traditional competencies that translate directly into WebTrust engagements. Indeed, many CPAs who perform attest engagements in computerized environments are likely to already possess many of the skills necessary to provide WebTrust services.

E-Commerce Industry Developments

What recent e-commerce developments are important for practitioners?

Business-to-Consumer (B2C) Developments

According to Boston Consulting Group (BCG), B2C commerce sales in the United States grew 66 percent, to $45 billion, last year and are anticipated to increase by 45 percent, to $65 billion, this year.

High-performing categories this year include toys, clothes, home and office, and travel sites. Growth in other categories such as computer products and books appear to be slowing down this year.

Notwithstanding the dot-com economic slump, BCG found that online retailers' operating losses as a percentage of revenue declined from 19 percent in 1999 to 13 percent in 2000.

According to Forrester Research, Inc., online sales increased from $3.5 billion in March 2001 to $4.3 billion in April 2001. Moreover, consumers spent an average of $273 per person in April 2001, compared to $263 in March 2001.

Business-to-Business (B2B) Developments

Thousands of companies world-wide are conducting more and more of their B2B commerce online. Sales and purchases that in the past would have been arranged by fax, face-to-face meetings, or telephone calls are now transacted over the Internet. Online B2B commerce promises more than just buying and selling over the Internet. Indeed, the Internet gives birth to true and deep collaboration between businesses as a way to manage production and supply needs.

The role and design of online industry-wide market places are being rethought throughout the economy. Many companies dislike public exchanges for a variety of reasons. Suppliers are hesitant to post their prices where the whole world can see them and buyers often dislike divulging their every requirement.

Private Exchanges Gaining in Popularity

Current market data indicates that companies are increasingly turning to "private exchanges" to link with specific groups of suppliers and partners over the Web. According to the *Wall Street Journal*, Hewlett-Packard Co., International Business Machines Corp., and Wal Mart Stores Inc. are operating substantial private exchanges. Many other companies are developing similar Internet systems. AMR Research now calls private exchanges the "cornerstone" of B2B commerce and predicts most of the $5.7 trillion in commerce transacted over the Internet by 2004 will pass through private exchanges. AMR projects that the world's largest firms will spend anywhere from $50 million to $100 million each to build private exchanges over the next five years.

There are numerous kinds of private exchanges. Some are developed between a company and its suppliers to purchase goods and track their status and location. Others are used to facilitate commerce among subsidiaries within a company and to strengthen relationships. With private exchanges, companies can automate their B2B activities and collaborate in real time with trusted suppliers and other business partners. Furthermore, companies avoid divulging sensitive information to unwanted eyes. Unlike the early B2B exchanges, not every company is allowed to participate in a private exchange—only invited companies can participate.

Private Internet-based systems can link a company's computer network with those of its key suppliers. In doing so, a company can monitor its suppliers' inventory listings and prices.

Online Marketplaces

Private and public online exchanges among companies and their suppliers are not the only way B2B commerce is being conducted. Some companies, rather than establishing their own private trading networks to link up with their suppliers, are simply establishing alliances with other companies in their industry. Big corporations have linked with others in their industries to build online purchasing networks. Target, for instance, is a founding member of the Worldwide Retail Exchange, an e-marketplace formed in March

2000 by more than fifty large retailers. Retailers participating in this e-marketplace have experienced significant cost reductions.

Helping Clients

You can guide your clients toward greater and more effective use of exchange-enabling technology by emphasizing the importance of careful and thorough planning. Since the practitioner understands the organization's business objectives and financial capabilities, he or she can help identify new technologies the client may require, the affordability of those technologies, and how such technologies will interact with existing systems.

WebTrust—What's New?

What's new with WebTrust?

There have been a number of significant developments both in the WebTrust program and in e-commerce events since our last Alert. In this section, we provide a brief summary of some of the more noteworthy events.

New WebTrust Consumer Protection Service

Online shoppers consistently cite privacy and failed delivery promises as impediments to purchases. As a result, the AICPA and Canadian Institute of Chartered Accountants (CICA) have developed a new defined service offering called WebTrust—Consumer Protection. The WebTrust Seal for Consumer Protection attests to the fact that a site offers the kind of protection and reliability that online shoppers are now demanding. To display the WebTrust Seal for Consumer Protection, the entity must meet both the WebTrust Online Privacy Principle and the WebTrust Business Practices/Transaction Integrity Principle. A site may receive a WebTrust Seal for Consumer Protection if it undergoes a WebTrust Consumer Protection examination by a WebTrust licensee, successfully meets the underlying principles and criteria, and is issued an unqualified report.

Exposure Draft Released on WebTrust Confidentiality Principle and Criteria

The WebTrust Confidentiality Principle and Criteria have been released for exposure under Version 3.0 of the WebTrust Program. WebTrust Confidentiality focuses on confidential information obtained as a result of e-commerce from existing or potential business partners. The WebTrust Confidentiality Principle sets out an overall objective for the confidentiality of data exchanged over electronic networks such as the Internet or a virtual private network. Information on this Principle and related early implementation guidance can be found at www.aicpa.org/assurance/webtrust/princip.htm. Comments are due by July 31, 2001 to Karyn Waller at AICPA, 1211 Avenue of the Americas, New York, NY 10036-8775 or via e-mail at kwaller@aicpa.org.

Establishing an International Presence

WebTrust's international expansion continued after the AICPA signed agreements with the accounting bodies in Hong Kong, Denmark, the Netherlands, Spain, Austria, Argentina, and Italy to offer WebTrust in those countries. The program with the only comprehensive, global set of best practices, WebTrust is now available in Australia, Germany, England, Wales, Scotland, Ireland, and France, as well as the United States and Canada.

Chief Privacy Officer

One of the hottest trends sweeping corporate America is the job of chief privacy officer (CPO). There are now at least one hundred CPOs in the United States. A CPO is responsible for privacy at e-commerce ventures. According to a *Mercury News* article, the CPO position is responsible for a number of tasks, including giving greater visibility to privacy efforts, streamlining the process for privacy questions, negotiating with advertisers, and troubleshooting. Although the title is not yet a common one, observers believe it is one way for savvy companies to enhance their Internet efforts.

E.U.-U.S. Internet Safe Harbor Agreement

In July, the Department of Commerce negotiated a safe harbor e-commerce privacy arrangement with the European Commission that allows U.S. business to comply with the European Union's Directive on Data Protection so the United States may continue to conduct e-business in Europe. The Safe Harbor Privacy Principles, which were published in the *Federal Register* on July 21, 2000, can be found online at www.ita.doc.gov/td/ecom/menu.html.

WebTrust Program for Certification Authorities, Version 1.0

What is the WebTrust Program for Certification Authorities, Version 1.0?

The WebTrust program for Certification Authorities, Version 1.0, provides standards for performing and reporting on the results of an audit of a certification authority. Certification authorities are third-party organizations that help enable parties to conduct secure e-commerce transactions. These authorities sign the digital certificate and then manage its life cycle. The digital certificate is an electronic document vouching for the link between the individual party conducting an e-commerce transaction and that party's identification means. In other words, it provides proof that the parties are who they say they are.

This new AICPA program provides a framework for licensed WebTrust practitioners to assess the adequacy and effectiveness of the controls employed by certification authorities. Given the technical nature of the activities involved in securing e-commerce transactions, the program also provides a brief overview of public key infrastructure (PKI) using cryptography, trusted third-party concepts, and their increasing use in e-commerce.

Public Key Infrastructure Technology

Confidentiality, authentication, integrity, and nonrepudiation are the four key elements required for trust in e-commerce transactions. The emerging response to these requirements is the implementation of PKI technology. PKI uses digital certificates and asymmetric cryptography to address these requirements.

PKI provides a means for relying parties (recipients of certificates who act in reliance on those certificates or digital signatures verified using those certificates) to know that another individual's or entity's public key actually belongs to that individual or entity. Certification authority organizations or certification authorities acting as trusted third parties have been established to address this need. PKI uses public-private key pairs—two mathematically related keys. One of these keys remains private, while the other typically is made public, by posting it in a publicly accessible read-only repository, for example. Public key cryptography works in such a way that a message encrypted with the public key can be decrypted only with the private key, and conversely, a message signed with a private key can be verified only with the public key. This technology can be used in different ways to provide confidentiality, authentication, integrity, and nonrepudiation.

Cryptography

Cryptography is critical to establishing secure e-commerce. However, it has to be coupled with other secure protocols to provide a comprehensive security solution. Several cryptographic protocols require an independent trusted third party (the certification authority) to authenticate the transaction. Certification authorities have assumed an increasingly important role in secure e-commerce. Although there is a large body of existing national, international, and proprietary standards and guidelines for the use of cryptography, the management of digital certificates, and the policies and practices of certification authorities, these standards have not been applied uniformly.

New Service Establishes Principles and Criteria for Certification Authorities

To increase consumer confidence in the Internet as a vehicle for conducting e-commerce and in the application of PKI technology, the AICPA Electronic Commerce Task Force has developed and is promoting a set of principles and criteria for certification authorities. If you or your firm are specifically licensed by the AICPA or the CICA, you can provide assurance services to evaluate and test

whether the services provided by a particular certification authority meet these principles and criteria. The posting of the AICPA/CICA WebTrust Seal for the certification authority model of assurance is a symbolic representation of a practitioner's unqualified report.

Public accounting firms and practitioners are well positioned to offer this service because they are licensed specifically by the AICPA or CICA to provide assurance services to evaluate and test whether the services provided by a particular certification authority meet these specific principles and criteria.

The AICPA/CICA WebTrust Program for Certification Authorities is consistent with the standards being developed by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF).[1]

> **Help Desk**—*The WebTrust Program for Certification Authorities, Version 1.0*, is available to download as a Microsoft Word document at the AICPA's Web site atwww.aicpa.org/assurance/webtrust/princip.htm.

WebTrust Programs, Version 3.0

What do the new WebTrust programs offer practitioners?

WebTrust Program for Online Privacy, Version 3.0

The Internet provides consumers with a new means for obtaining useful information and for purchasing goods, information, and services. Its growth has been inhibited by consumer fears and

1. The ANSI X9F5 Digital Signature and Certificate Policy working group is developing the X9.79 PKI *Practices and Policy Framework* (X9.79) standard for the financial services community. This standard includes detailed certification authority control objectives against which certification authorities may be evaluated. An International Organization for Standardization (ISO) working group has been formed to standardize X9.79 based on international requirements in a new international standard. In addition, the American Bar Association's Information Security Committee (ABA-ISC) is developing the *PKI Assessment Guidelines* (PAG), which address the legal and technical requirements for certification authorities. The PAG refers to the certification authority control objectives that are detailed in the draft X9.79 standard and reflected in the *WebTrust Program for Certification Authorities*. The certification authority control objectives referred to in each of these documents were developed based on the existing body of ANSI, ISO, IETF, and other existing standards.

concerns about the risks, both real and perceived, of doing business electronically. The WebTrust Program for Online Privacy was developed by the public accounting profession to address these consumer fears and concerns and to increase consumer confidence in this new electronic marketplace.

The new WebTrust Program for Online Privacy allows WebTrust practitioners to independently verify that a Web site informs customers about privacy policies and that the site actually follows those policies. It allows WebTrust practitioners to provide standalone assurance for online privacy.

This version of the WebTrust Program for Online Privacy supercedes the recently released exposure draft. Its Principles and Criteria supercede Version 2.0 of the WebTrust Principles and Criteria insofar as they relate to privacy and information protection, and are effective for examination periods beginning after December 31, 2000.

> **Help Desk**—Practitioners can download the final version of WebTrust Program for Online Privacy, Version 3.0, at www.aicpa.org/assurance/webtrust/princip.htm.

WebTrust Program for Business Practices/Transaction Integrity, Version 3.0

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. The risk is that the consumer or business 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. 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, will be received when promised.

The WebTrust Business Practices/Transaction Integrity Principle sets out an overall objective with respect to the completeness and accuracy of processing of electronic transactions sent over the Inter-

net. In the course of the 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 is defined as the following:

> The entity discloses it 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 Principles and Criteria contained in the WebTrust Program Business Practices/Transaction Integrity Principle and Criteria supercede 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.

> **Help Desk**—Practitioners can download the final version of WebTrust Program for Business Practices/Transaction Integrity Principle and Criteria, Version 3.0, at www.aicpa.org/assurance/webtrust/princip.htm

WebTrust Program for Availability, Version 3.0

For entities to transact business through Web sites in either a B2C or a B2B e-commerce relationship, it is imperative that customer access be available to an entity's sites as advertised or promised in a service-level agreement. 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. 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 percent-

age 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—

- The availability of B2C or a B2B Web site and other operations of a service provider data center.
- Security and related controls that are needed to ensure availability.
- The continuous performance monitoring and management of availability and anticipation of potential problems that could reduce availability.

The WebTrust Availability Principle is defined as follows:

> 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 Principles and Criteria contained in WebTrust Program Availability Principle and Criteria supercede the WebTrust—ISP Principles and Criteria for Internet Service Providers (ISPs) insofar as they relate to availability and are effective for examination periods beginning after February 28, 2001.

> **Help Desk**— Practitioners can download the final version of WebTrust Program for Availability Principle and Criteria, Version 3.0, at www.aicpa.org/assurance/webtrust/princip.htm.

WebTrust Program for Security, Version 3.0

In the course of communicating and transacting business over the Internet, consumers and businesses must send and receive information about the other party. In most instances, parties that are interested in engaging in e-commerce will be anxious to ensure that the information they provide is available only to those individuals who need access to complete the transaction or follow up on any questions that arise.

Information provided to other parties is susceptible to unauthorized access during transmission over the Internet as well as when it is stored on the other party's computer systems.

The WebTrust Security Principle and Criteria set out an overall objective for the security of the data transmitted over the Internet and stored on an e-commerce system. 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 Security Principle is defined as the following:

> The entity discloses its key security practices, complies with such security practices, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorized individuals in conformity with its disclosed security practices.

The Principles and Criteria contained in the WebTrust Program Security Principle and Criteria supercede Version 2.0 of the WebTrust Principles and Criteria insofar as they relate to security and are effective for examination periods beginning after February 28, 2001.

> **Help Desk**—Practitioners can download the final version of WebTrust Program for Security Principle and Criteria, Version 3.0, at www.aicpa.org/assurance/webtrust/princip.htm.

WebTrust Program Practitioner Guidance on Scoping and Reporting Issues

The *WebTrust Program Practitioner Guidance on Scoping and Reporting Issues* assists practitioners in dealing with many issues related to engagement scoping and reporting under the WebTrust Program, Version 3.0, and provides reporting examples for situations that the practitioner could likely encounter, including—

- Issuing engagement letters and opinions on multiple WebTrust principles.
- Point-in-time reporting.
- Cumulative reporting.

- Responsibility for communicating lack of compliance with a principle.

The guidance includes many illustrative practitioner reports to be used in a variety of situations (reporting on multiple principles, point-in-time reporting, or reporting on management assertions, and so on).

> **Help Desk**—This new document, *WebTrust Program Practitioner Guidance on Scoping and Reporting Issues*, is available to download at www.aicpa.org/assurance/webtrust/princip.htm.

WebTrust Version 3.0 and Its Effect on ISPs

What impact does WebTrust Version 3.0 have on Internet service providers?

The Principles and Criteria issued under Version 3.0 supercede Version 2.0 of the WebTrust Principles and Criteria and, as a result, replace those previously issued in the WebTrust for the Internet Service Providers program. Version 3.0 has modified the WebTrust principles to apply to other service providers in addition to ISPs.

The AICPA Electronic Commerce Task Force decided that a definitive package of Version 3.0 principles for ISPs and service providers in general would be difficult to establish at this time, as it would depend on specific service providers' needs based on their particular businesses and markets. As a result, the special WebTrust Principles and Criteria for ISPs program was discontinued on March 1, 2001. As the combination of principles may differ among service provider examinations, practitioners working with ISPs would issue a generic WebTrust Seal, along with the independent auditor reports reflecting which principles the practitioners audited. Therefore, if a practitioner performs an examination on a service provider using Version 3.0 of the WebTrust Principles and Criteria, that provider would be eligible to receive a generic WebTrust Seal that would link to the practitioner's report, identifying the particular WebTrust principles that the service provider has met.

WebTrust Client Exam Requirements Revised

How often does WebTrust mandate client update examinations and refreshed practitioner reports?

WebTrust examination updates and refreshed practitioner reports were mandatory at least every three months in the previous versions of WebTrust. Under Version 3.0, the timing requirement has been changed. The time between updates now should not exceed six months, although this interval often may be considerably shorter depending on the circumstances, including—

- The nature and complexity of the entity's operation.
- The frequency of significant changes to its disclosures, policies, and related controls.
- The relative effectiveness of the entity's monitoring and change management controls for ensuring continued conformity with the applicable WebTrust Criteria as changes are made.
- The practitioner's professional judgment.

Once an engagement letter has been signed reflecting the company's move to WebTrust Version 3.0, the practitioner may wait up to six months to perform the next update examination and issue a new audit report (assuming there are no other substantive changes to the site). If this engagement letter is issued before the company has actually had an engagement performed under the WebTrust 3.0 Principles and Criteria, the engagement letter should also reflect the client's commitment to comply with the current Principles and Criteria until the report is updated.

For example, if a WebTrust report is issued as of October 31, 2000, and the client is currently following Version 2.0, the report and Seal normally would be refreshed on January 31, 2001. The practitioner may wait up to six months to update and refresh the report if—

- A new engagement letter is signed before that January date, noting the shift to Version 3.0 at the next engagement.

- The company agrees to stay in compliance (in the engagement letter) with the Version 2.0 principles until it receives a report under WebTrust Version 3.0 Principles and Criteria.

If the client has not signed an updated engagement letter, three-month updates are still required.

Outstanding Exposure Draft

What exposure draft have the AICPA and CICA issued that is important to WebTrust practitioners and licensees?

The Electronic Commerce Task Force has issued an exposure draft. We summarize here for you the major issues included in the exposure draft. You can download copies of the exposure draft at the AICPA's Web site at www.aicpa.org/assurance/webtrust/princip.htm.

WebTrust Program for Confidentiality

In the course of communicating and transacting business over the Internet (or a more focused business extranet), business partners must send and receive information about the other party that needs to be maintained on a confidential basis. In most instances, parties who are interested in engaging in e-commerce will be anxious to ensure that the information they provide is available only to those individuals who need access to complete the transaction or follow up on any questions that arise.

To enhance business partner confidence in e-commerce, it is important that the business partner is informed about the entity's confidentiality practices for e-commerce transactions. The entity needs to disclose its practices relating to the manner in which it provides for authorized access to, uses, and shares information designated as confidential.

Unlike personally identifiable information (that is, private information), which is being defined by regulation in a number of countries worldwide, there is no widely recognized definition of confidential information. Also, unlike personal private information, there are no defined rights of access to confidential information to

ensure its accuracy and completeness. As a result, interpretations of what is deemed to be confidential information can vary significantly from business to business and in most cases is driven by contractual arrangements. As a result, it is important for those engaged, or expecting to be engaged, in business relationships to understand and to accept what information is to be maintained on a confidential basis and what, if any, rights of access or other expectations that an entity might have to update that information to ensure its accuracy and completeness.

Information that is provided to another party is susceptible to unauthorized access during transmission over the Internet and while it is stored on the other party's computer systems. For example, business partner profile information and transaction and settlement instructions may be intercepted by an unauthorized party while they are being transmitted over the Internet. However, if the information is encrypted, it is difficult for the unauthorized party to decipher it. Also, if the computer system where the data is stored is not protected by a firewall and a rigorous system of access controls, unauthorized persons may access the information.

WebTrust Confidentiality focuses on confidential information obtained as a result of e-commerce from existing or potential business partners. The WebTrust Confidentiality Principle sets out an overall objective for the confidentiality of data exchanged over electronic networks such as the Internet or a virtual private network. The privacy of personally identifiable information is covered in WebTrust Program for Online Privacy. In the course of a WebTrust examination, the practitioner uses the WebTrust Criteria as the basis for assessing whether the Principle has been achieved.

WebTrust Confidentiality focuses on information designated as confidential and obtained online from business partners as a prelude to or as a result of e-commerce. Where such information is commingled with information obtained by other means, however, the practitioner will need to consider the entity's confidentiality practices and related controls covering all such information.

Examples of information subject to confidentiality include the following:

- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists

Examples of personally identifiable information subject to privacy include the following:

- Name, address, and home phone number
- Banking information about individuals
- Health information
- Employee earnings
- Individual credit history

The WebTrust Confidentiality Principle is defined as the following:

> The entity discloses its confidentiality practices, complies with such confidentiality practices, and maintains effective controls to provide reasonable assurance that access to information obtained as a result of electronic commerce and designated as confidential is restricted to authorized individuals, groups of individuals, or entities in conformity with its disclosed confidentiality practices.

To enhance business partner confidence in e-commerce, it is important that the business partner is informed about the entity's confidentiality practices for e-commerce transactions. The entity needs to disclose its practices relating to the manner in which it provides for authorized access to, uses, and shares information designated as confidential.

The Confidentiality Principle and Criteria have been issued for exposure for comment by July 31, 2001. During this comment period and until final approval and issuance by the AICPA and CICA, the task force believes that this Principle and Criteria are

suitable for engagements that could result in the issuance of a WebTrust Seal.

> **Help Desk**—The exposure draft WebTrust Program for Confidentiality is available to download as a Microsoft Word document on the AICPA's Web site at www.aicpa.org/assurance/webtrust/princip.htm.

Internet Privacy Issues

First There Were Cookies, Now There Are WebBugs

How can WebBugs affect consumer privacy?

Relatively new to the Internet scene is a marketing and tracking tool known as a "WebBug." A WebBug is a graphic embedded in a Web page or e-mail message designed to monitor who is reading a specific page or message along with the corresponding date and time it was read.

The word *bug* refers here to a small eavesdropping device—because eavesdropping is exactly what a WebBug does. The following is a partial listing of the information that a WebBug can capture:

- The IP address of the computer that fetched the WebBug
- The URL of the page that the WebBug is located on
- The URL of the WebBug image
- The time the WebBug was viewed
- The type of browser that fetched the WebBug image
- A previously set cookie value

WebBugs are valuable because they can—

- Add information to a personal profile of which sites someone visits.
- Provide an independent accounting of how many people have visited a particular Web site.

- Gather statistics about browser usage at different places on the Internet.

On the e-mail side, WebBugs have other uses, including—

- Finding out if and when someone has read a particular e-mail message.
- Providing the IP address of the recipient if the recipient is attempting to remain anonymous.
- Within an organization, tracking how often a message is being forwarded and read

The size and makeup of WebBugs renders them difficult to identify and filter out. WebBugs are GIF files (that is, image files with the extension .gif) and can be as small as one pixel by one pixel, a size that can't be seen by the human eye without aid. A WebBug cannot be easily distinguished from other GIF files. If the user were to filter out all GIF files, Web pages would lose much of their functionality and appeal.

The only surefire method of identifying WebBugs is to analyze the HTML programming, which is confusing and complex to most users.

The informed user can evaluate the benefits and risks of a particular site and the potential of providing personal information. Businesses also need to weigh the benefits of the information the tracking tools provide against the risk of losing potential customers. A well-defined and audited privacy policy seemingly could provide the best of both worlds.

As WebTrust practitioners know, the WebTrust Privacy program is the only program of its kind in the global community that provides best practices and independent verification of a Web site's privacy practices.

Privacy Concerns Rise

While companies want data that can help them refine marketing approaches, their attempts to collect personal data "have created an

intense consumer backlash from an increasingly tech-savvy public. Consumers are stepping up demands for control of their private data and accountability from the companies who have it," according to an article in *Red Herring* magazine. A Forrester research survey found that 41 percent of online shoppers check a Web site's privacy policy when visiting for the first time, according to a VAR *Business* article. Consumers' concerns over privacy have placed pressure on politicians to act.

The Consumer Privacy Act, which is in U.S. Senate committee review, would make it illegal for an Internet company or organization "to collect personal or identifiable data from a user without consent, and makes violations punishable under the FTC standards," according to VAR *Business*. Under another proposal, the Federal Trade Commisson (FTC) could fine companies $22,000 per violation of privacy standards.

Opposing widespread governmental regulation are groups such as the Online Privacy Alliance, an industry group that advocates continued self-regulation. VAR *Business* notes that laws that completely eliminate the use of cookies, which identify and track Internet users, would stamp out personalized e-commerce services.

Some in Congress agree that there is a need for privacy protection. "There is a market demand for privacy protection, and a lot of firms are meeting and doing it in very effective ways," Representative Jim Moran (D-Va.) told VAR *Business*. "If the federal government comes up with a cookie-cutter solution, we're liable to arrest that innovation."

A major privacy issue is a choice of the opt-in or opt-out requirement. Users opt-in when they actively agree to something, for instance, "To receive newsletters, click on the box shown." While opt-out can be active, the deployment of these more common approaches is that the user has to knowingly tell the Web site operator that he or she does not want to be included. "Indeed," stated a recent article in the *Red Herring* magazine, "the consent debate may be the most contentious question of this entire issue. Some companies think opt-in makes it too burdensome for consumers to gain access to a site: opt-in supporters say opt-out gives compa-

nies too much leeway to create wordy, confusing privacy polices that make it difficult for consumers to know what's really being done with their personal data."

While some companies are fighting privacy policy demands, the article noted that many believe smart businesses will use this issue to their advantage. "In other words, a privacy-friendly stance could win over more potential customers than the hard line would," as stated in the article.

According to Michael Erbschole, vice president of research at Computer Economics, "During 2001 another 12.6 percent of organizations will formalize their privacy policies and plans, and by the end of 2002 over 50 percent of all organizations will have formalized a privacy policy."

Microsoft's P3P

Does Microsoft have the solution that will solve consumer privacy concerns?

Microsoft Corp. says it has a high-tech solution to the problem of Internet privacy. The software giant has developed a system that would allow consumers to choose how much protection they want. The approach will realistically let PC users adjust the dial as a kind of privacy thermostat built into their Web browsers. There are many more technological approaches being touted. Ultimately, the site must be tested and the tests cover policies, procedures, systems, practices, and people. Security and privacy can not be ensured by just plugging in any piece of software; auditors—not machinery—provide assurance. The Platform for Privacy Preferences (P3P) symbolizes the biggest weapon yet in the combat against new regulations and in providing much better control over personal information for consumers, if it works. Microsoft is building the technology into Version 6 of its Internet Explorer browser to be officially released in October 2001.

The most heated debate is over the so-called default settings. The default settings will go from maximum privacy, which will make Web surfing unreasonably difficult, to the other end, which will allow maximum exposure. Microsoft's default will be preset some-

where in the middle. The technology is a set of standards developed by a group called the World Wide Web Consortium. P3P is a complicated set of rules about how to depict privacy rules in a format computers can comprehend.

Widespread support will be a key factor to the success of P3P and in heading off new privacy laws in Washington. P3P is evidence to lawmakers that Internet companies can regulate themselves and additional regulations are not required.

Web Privacy Laws

Will privacy legislation cost consumers?

Four industry studies affirm that privacy legislation would cost consumers billions of dollars annually.

The Online Privacy Alliance, in an effort to cease the progression of dozens of privacy bills in Congress and in state legislation, is leading a campaign against legislative proposals on three fronts, according to a *Wall Street Journal* article. They include the following:

1. Identifying expensive regulatory burdens
2. Raising questions about how any U.S. Internet law would apply to non-Internet industries
3. Assuring lawmakers that privacy is best guarded by new technology, not new laws

The industry studies concluded that proposals to limit companies from sharing or selling customer information without permission would cost ninety of the largest financial institutions $17 billion a year of added expenses, and would result in a $1 billion "information tax" on consumers through costs tacked onto products from catalogs and Internet retailers. The study also states that tougher privacy rules would promote the risk of fraud by not allowing the Internet retailer to verify the consumer address information, therefore making fraud harder to police.

Cybercrime and Security

As cybercrime escalates, will companies worry more about security breaches?

IDC Research issued a report stating that the main driving force behind companies implementing security technology is when they endure a security breach in their organization. Other reasons companies are taking on security technology are the increased use of the Internet, the execution of virtual private networks, and e-business projects. Remember, that technology is only part of the picture. Policies, procedures, people and systems are also integral parts of good security.

Anti-virus software is the most common security technology, while intrusion-detection solutions and hardware-based firewall systems are also popular. The most proactive industries to adopt security are financial services, communications, healthcare services, banking, government, and utilities. In contrast, security is seldom well thought-out in the retail industry.

A 2001 survey performed by the FBI and the Computer Security Institute (CSI) revealed that 85 percent of the 538 respondents had detected security breaches within the last twelve months, with almost two-thirds suffering financial losses as a result. Of the respondents, only 186 were willing to disclaim the amount of money they lost due to computer crime. The amount of financial losses the respondents reported approximated $378 million.

The theft of proprietary information and financial fraud contributed to the highest losses, with the Internet being the most frequent point of attack.

Companies should have a security policy that explains and identifies security requirements. Such issues as identification and authentication, password guidelines, standard host-server software settings, and malicious software should be addressed. Companies should—

- Look at the existing architecture, since common architectural problems can lead to sizable security breaches.
- Evaluate the configuration of the existing systems, since many systems are infiltrated because available security mechanisms were turned off or misconfigured.
- Set controls, such as minimum password lengths or required passwords.
- Consider having an audit performed that would evaluate the findings compared to the stated policy.

According to the chief executive officer (CEO) of Sanctum Inc., an e-commerce security firm, Web application developers are stuck creating susceptible sites that are easy targets for hackers. The reason is that management wants them to produce sites that are downloaded faster, keep visitors at the site longer, and are more eye-catching than the competitors'. So function is compromised for form. There is also a disturbing lack of education in application security, which makes numerous sites vulnerable to hackers. According to the Sanctum CEO, there are 640,000 B2B and B2C registered sites worldwide and only 2,000 qualified developers.

In the seventy audits performed by Sanctum in its three years of operation, the CEO stated her team was able to compromise the integrity of 97 percent of sites identified in one of four ways, including stealing proprietary corporate information, gathering customer information such as credit card numbers, changing the price on e-commerce sites, or defacing the site itself.

In spite of who is at fault for security lapses, two recent studies highlight one fact: Companies had better get their security policies and procedures in place if they want to benefit from the growing number of online shoppers.

Taxation of Internet Sales: The Debate Continues

Will there be taxation of Internet sales?

For the past few years, we have been following the continuing debate over the taxation of Internet sales. State and local governments

are concerned about losing sales and use tax revenue because of untaxed Internet sales. A recent estimate of the amount of sales tax revenue that will be lost in 2001 because of the nontaxation of Internet sales puts the amount at $2 billion.

When we left the saga of the taxation of Internet sales last year, the Advisory Commission on Electronic Commerce (ACEC) had just submitted its report to Congress. That report recommended that among other actions, Congress (1) extend the existing ban (which is slated to expire in October 2001) on new taxes on Internet access and on multiple or discriminatory taxes on e-commerce and (2) take steps to simplify state and local sales and use taxes. (Internet businesses claim that disparities in sales tax systems among the various jurisdictions are too burdensome to administer.) Despite the introduction of numerous bills, Congress was unable to pass Internet taxation legislation this year. However, the attempts continue.

The states are attempting to deal with the issue of sales tax simplification. The District of Columbia, forty-five states, and thousands of local governments impose sales taxes. To deal with complaints about disparities among the jurisdictions, the National Governors Association created the Streamlined Sales Tax Project (SSTP). The SSTP, comprising tax administrators from thirty states, developed model legislation to unify and simplify sales and use tax administration among the states that adopt the legislation. The SSTP hopes that, by unifying and simplifying sales tax systems, Internet businesses will voluntarily collect sales taxes. The model legislation, titled the Uniform Sales and Use Tax Administration Act (the Act), would authorize a state taxing authority to enter into an interstate contract, the Streamlined Sales and Use Tax Agreement (the Agreement). The Act and related Agreement would, among other matters, establish more uniform administrative standards, and develop and adopt uniform definitions of sales and use tax terms.

Recently, the Act ran into a snag when a task force of the National Conference of State Legislatures (NCSL) took significant exception to some of its measures. The NCSL drafted and distributed its own version of model legislation to simplify sales tax. State legislatures are now considering whether to adopt legislation and, if so, which version.

Help Desk—The Act is available on SSTP's Web site at www.streamlinedsalestax.org. The NCSL's version of the model legislation is available on the NCSL Web site atwww.ncsl.org/programs/fiscal/tctelcom.htm. The NCSL site also includes a document that lists the amendments that the NCSL made to the SSTP Act.

SSAE No. 10, *Attestation Standards: Revision and Recodification*

What are the requirements of SSAE No. 10 and how does it affect the WebTrust practitioner?

WebTrust practitioners should be aware of changes made by Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification*, issued by the Auditing Standards Board in January 2001. SSAE No. 10—

- Renumbers AT section 100 to AT section 101 and renames it "Attest Engagements."
- Changes the definition of an attest engagement into a statement of applicability of the standard, as follows:

  > This Statement applies to engagements in which a certified public accountant in the practice of public accounting is engaged to issue or does issue an examination, a review, or an agreed-upon procedures report on subject matter, or an assertion about the subject matter, that is the responsibility of another party.

- Revises the third general standard to focus on the essential elements of criteria: The criteria must be suitable and must be available to users. The subject matter also must be capable of reasonably consistent evaluation against the criteria.
- Enables true direct reporting on subject matter by eliminating the requirement to make reference to the assertion in the practitioner's report.
- Provides expanded guidance on the circumstances in which the use of attest reports should be restricted to specified parties.

- Supersedes SSAE Nos. 1 through 9.

The new SSAE also eliminates the requirement in AT section 201, "Agreed-Upon Procedures Engagements," for the practitioner to obtain a written assertion in an agreed-upon procedures attest engagement. It also incorporates changes needed as a result of the withdrawal of Statement on Auditing Standards (SAS) No. 75, *Engagements to Apply Agreed-Upon Procedures to Specified Elements, Accounts, or Items of a Financial Statement* (AICPA, *Professional Standards*, vol. 1, AU sec. 622). That withdrawal is reflected in SAS No. 93, *Omnibus Statement on Auditing Standards—2000.*

SSAE No. 10 is effective when the subject matter or assertion is as of or for a period ending on or after June 1, 2001. Early application is permitted.

WebTrust Training Courses

Where can CPAs obtain training for WebTrust?

AICPA/CICA Conference on Assurance Services

Don't miss this year's Conference and Expo, "*The Business of eBusiness—Audit, Control, and Accounting Strategies for Today's Economy,*" to be held at the Pointe Hilton Resort in Phoenix, Arizona. Mark your calendars for December 3-5, 2001. Join us December 2, 5, and 6 for pre- or post-conference Optional Workshops, including "Network Security" and other offerings. Then attend the conference, which, among other things, will offer the following preliminary tracks:

- Financial—financial and accounting issues in the e-business world
- Business—the operational issues for the e-business model
- Audit—business audit issues
- Infrastructure—briefings to enhance e-business-related technical skills of information technology (IT) audit professionals

- Information Technology Audit—highly technical e-business issues

For more information about this or future conferences, visit the Web site at www.ebizconf.com.

Any comments that you have about this Alert are appreciated. You may e-mail your comments to lwest@aicpa.org or send them to:

Lori A. West, CPA
AICPA
Harborside Financial Center
201 Plaza Three
Jersey City, NJ 07311-3881

APPENDIX A

Electronic Commerce Task Force

The AICPA/CICA Electronic Commerce Task Force and the AICPA staff contacts listed here welcome your comments and questions about the WebTrust program.

Name	*Address*	*Phone/Fax/E-Mail*
Anthony J. Pugliese Vice President Member Innovation	American Institute of CPAs 1211 Avenue of the Americas New York, NY 10036-8775	Phone: (212) 596-6083 Fax: (212) 596-6233 E-mail: apugliese@aicpa.org
Louis Matherne Director	American Institute of CPAs 1211 Avenue of the Americas New York, NY 10036-8775	Phone: (212) 596-6027 Fax: (212) 596-6233 E-mail: lmatherne@aicpa.org
Karyn Waller Senior Manager Trust Family Services	American Institute of CPAs 201 Plaza Three Harborside Financial Center Jersey City, NJ 07311-3881	Phone: (212) 596-6054 Fax:(212) 596-6233 E-mail: kwaller@aicpa.org
AICPA/CICA Electronic Commerce Task Force		
Everett C. Johnson, Jr. Chair	Deloitte & Touche LLP P.O. Box 820 10 Westport Road Wilton, CT 06897-0820	Phone: (203) 761-3022 Fax: (203) 761-3418 E-mail: ejohnson@dttus.com E_C_Johnson@compuserve.com
Bruce R. Barrick	Deloitte & Touche 181 Bay St. Bay Wellington Tower BCE Place, Suite 1400 Toronto, ON M5J 2V1 Canada	Phone: (416) 601-5656 Fax: (416) 601-6151 E-mail: bbarrick@sympatico.ca Bbarrak@deloitte.ca
Gary S. Baker	Arthur Andersen LLP 1900-79 Wellington Street West P.O. Box 29, TD Centre Toronto, ON M5K 1B9 Canada	Phone: (416) 814-7250 Fax: (416) 947-7878 E-mail: gary.s.baker@ca.arthur andersen.com
Jerry R. DeVault	Ernst & Young, LLP 1300 Huntington Bldg. 925 Euclid Avenue Cleveland, OH 44115-1405	Phone: (216) 861-2214 Fax: (216) 861-8346 E-mail: jerry.devault@ey.com
Joseph G. Griffin	PricewaterhouseCoopers 1100 Campanioe Bldg. 1155 Peachtree Street Atlanta, GA 30309	Phone: (404) 870-1480 Fax: (404) 870-1262 (no legal size paper) E-mail: joseph.g.griffin@us.pwc global.com

(continued)

Name	*Address*	*Phone/Fax/E-Mail*
Christopher Leach	Grant Thornton One Prudential Plaza 130 E. Randolph Drive Chicago, IL 60601-6203	Phone: (312) 602-9003 Fax: (312) 565-5868 E-mail: CLeach@GT.com
Kerry L. Shackelford	Arthur Anderson LLP Suite 3100 1225 17th Street Denver, CO 80202-5531	Phone: (303) 291-8793 Fax: (303) 291-9200 E-mail: kerry.l.shackelford@us.arthurandersen.com
Donald E. Sheehy	Grant Thornton Royal Bank Plaza 10th Floor, North Tower 200 Bay Street, Box 55 Toronto, ON M5J 2P9 Canada	Phone: (416) 360-4964 Fax: (416) 360-4944 E-mail: dsheehy@grantthornton.ca
Gregory P. Shields	The Canadian Institute of Chartered Accountants 277 Wellington Street West Toronto, ON M5V 3H2 Canada	Phone: (416) 204-3235 Fax: (416) 204-3408 E-mail: greg.shields@cica.ca
Christian R. Stormer	Bauknight Pietras & Stormer, PA PO Box 1330 (29202) 1517 Gervais Street Columbia, SC 29201	Phone: (803) 771-8943 Fax: (803) 771-8958 E-mail: cstorm@ix.netcom.com
Al Van Ranst	KPMG LLP 99 High Street Boston, MA 02110	Phone: (617) 988-1054 Fax: (617) 988-0807 E-mail: avanranst@kpmg.com
Bryan Walker	The Canadian Institute of Chartered Accountants 277 Wellington Street West Toronto, ON M5V 3H2 Canada	Phone: (416) 204-3278 Fax: (416) 977-8585 E-mail: bryan.walker@cica.ca
Cairine Wilson	CICA 277 Wellington Street. West Toronto, ON M5V 3H2 Canada	Phone: (416) 204-3349 Fax: (416) 977-8585 E-mail: cairine.wilson@cica.ca
Others:		
Louise DeSina Senior Manager Advertising and Communications	American Institute of CPAs 1211 Avenue of the Americas New York, NY 10036-8775	Phone: (212) 596-6107 Fax: (212) 596-6121 E-mail: ldesina@aicpa.org
Linda Dunbar Director Public Relations	American Institute of CPAs 1211 Avenue of the Americas New York, NY 10036-8775	Phone: (212) 596-6236 Fax: (212) 596-6121 E-mail: ldunbar@aicpa.org
Ron Halse Marketing Manager Assurance Services	American Institute of CPAs 201 Plaza Three Harborside Financial Center Jersey City, NJ 07311	Phone: (201) 938-3788 Fax: (201) 938-3780 E-mail: rhalse@aicpa.org

Name	*Address*	*Phone/Fax/E-Mail*
Tom Higginbotham Vice President Congressional and Political Affairs	American Institute of CPAs 1455 Pennsylvania Avenue Washington, DC 20004-1081	Phone: (202) 434-9205 Fax: (202) 638-4512 E-mail: thigginbotham@aicpa.org
Richard Miller General Counsel and Secretary	American Institute of CPAs 1211 Avenue of the Americas New York, NY 10036-8775	Phone: (212) 596-6245 Fax: (212) 596-6104 E-mail: rmiller@aicpa.org
Marianne So	Canadian Institute of Chartered Accountants 277 Wellington Street, West Toronto, ON M5V 3H2 Canada	Phone: (416) 204-3306 Fax: (416) 977-8585 E-mail: marianne.so@cica.ca
Thomas E. Wallace	KPMG, LLP 3 Chestnut Ridge Road Montvale, NJ 07645 For all mailings: 15 Manor Road North Greenlawn, NY 11740	Phone: (201) 505-2145 Fax: (201) 505-6211 E-mail: tewallace@kpmg.com Phone: (516) 754-8116

APPENDIX B

The Internet: A Practitioner's Research Tool

The following list includes Web sites that may provide valuable information to CPAs who are considering providing WebTrust services, as well as those who have already expanded their practice.

Name of Site	*Content*	*Internet Address*
American Institute of CPAs	Extensive discussion of assurance services and the recent activity of related committees and task forces.	http://www.aicpa.org
CPA WebTrust	Basics about the WebTrust program for both consumers and developers.	http://www.cpawebtrust.org
The University of Texas—Electronic Commerce FAQs	Electronic commerce facts.	http://cism.bus.utexas.edu/resources/ecfaq.html
Federal Trade Commission	Information on the activities of the FTC.	http://www.ftc.gov
Forrester Research	Internet reports, studies and other research.	http://www.forrester.com
Boston Consulting Group	Internet reports, studies and other research.	http://www.bcg.com
NUA Internet Survey	Surveys about numerous Internet issues.	http://www.nua.ie/surveys
Internet News	Daily reports providing Internet research information.	http://www.internetnews.com
Computer World	Provides useful and current statistics on online commerce and the Web in general.	http://www.computerworld.com
The Electronic Accountant	World Wide Web magazine that features up-to-the-minute news for accountants.	http://www.electronicaccountant.com
CPAnet	Links to other Web sites of interest to CPAs.	http://www.cpalinks.com
Accountant's Home Page	Resources for accountants and financial and business professionals.	http://www.computercpa.com
Internet Bulletin for CPAs	CPA tool for Internet sites, discussion groups, and other resources for CPAs.	http://www.kentis.com/ib.html

APPENDIX C
Other AICPA Assurance Products

Assurance Services

- CPE—*Overview of Assurance Services* (product no. 182021kk)
- CPE—Video course: *Assurance Services Update (2000 edition)* (product no. 180580kk)

WebTrust

- The *CPA WebTrust Letter*
- CPE—*Assurance Services Electronic Commerce* (product no. 732026kk)
- Practice Aid—*CPA WebTrust Practitioner's Guide* (product no. 006604kk)
- Additional WebTrust information may be downloaded from the AICPA Web site at www.aicpa.org.
- AICPA/CICA, *Guide to Auditors and Users of a Third Party Service Provider Audit Report in a WebTrust Engagement*, March 1999 Approved Guide

CPA Sys Trust

- Assurance Service Alert—*CPA SysTrust—2001*
- AICPA/CICA *SysTrust Principles and Criteria for Systems Reliability*, Version 1.0 (product no. 060465kk; CD ROM, product no. 060466kk)
- CPE—*How to Perform a SysTrust Engagement* (product no. 730026kk)
- *SysTrust Service: An Overview to the New Assurance Services on Systems Reliability* (product no. 730027kk)

CPA ElderCare Services

- Assurance Services Alert—*CPA ElderCare Alert—2001*
- Practice Aid—*CPA ElderCare: A Practitioner's Resource Guide* (product no. 022504kk)
- CPE—*Assurance Services: ElderCare* (product no. 732032kk)

CPA Performance Views

- *CPA Performance Views—Practitioner's Guide* (product no. 006606kk)

Online CPE Offer!

The AICPA offers an online learning library, AICPA InfoBytes. An annual fee ($95 for members and $295 for nonmembers) offers unlimited access to over 1,000 hours of online CPE in one- and two-hour segments. Register today as our guest at www.cpa2biz.com.

Contact the AICPA

To order copies of AICPA publications or to obtain information about additional CPE courses for assurance services and other topics, call AICPA's toll-free information hotline at (888) 777-7077, fax a request to the twenty-four-hour fax hotline at (201) 938-3787, or visit the AICPA's Web site at http://www.aicpa.org to obtain product information and place online orders. You may also write to the American Institute of CPAs, Order Department, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881.