2002

E-business industry developments - 2002/03; Audit risk alerts

American Institute of Certified Public Accountants

AUDIT RISK ALERTS

E-Business Industry Developments—2002/03

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA

Notice to Readers

This Audit Risk Alert is intended to provide auditors with an overview of recent economic, technical, and professional developments that may affect the audits they perform.

This publication is an *Other Auditing Publication* as defined in Statement on Auditing Standards (SAS) No. 95, *Generally Accepted Auditing Standards* (AICPA, *Professional Standards*, vol. 1, AU sec. 150). Other Auditing Publications have no authoritative status; however, they may help the auditor understand and apply SASs.

If an auditor applies the auditing guidance in an Other Auditing Publication, he or she should be satisfied that, in his or her judgment, it is both appropriate and relevant to the circumstances of his or her audit. The auditing guidance in this document has been reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA and is presumed to be appropriate. This document has not been approved, disapproved, or otherwise acted on by a senior technical committee of the AICPA.

Written by J. Russell Madray, CPA
Edited by Leslye Givarz
Technical Manager
Accounting and Auditing Publications

The AICPA acknowledges and appreciates the fine contribution of J. Russell Madray, CPA, who developed this Audit Risk Alert. In addition, we thank Walt Rivenbark and Joel Lanz for their reviews of this Alert.

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

TABLE OF CONTENTS

E-BUSINESS INDUSTRY DEVELOPMENTS—2002/03 5

How This Alert Helps You 5

E-Business Background 5

Internet and E-Business Development 6

E-Business Models 7

E-Business Economic Environment 14

The U.S. Business Environment 14

The Sarbanes-Oxley Act 15

General E-Business Trends 15

Recent Regulatory Developments 18

E-Fraud 23

Extensible Business Reporting Language 25

General Audit Issues and E-Business 27

The Scope of E-Business Client Activities 27

Audit Timing and Planning 28

Adequate Technical Training 29

Using the Work of a Specialist 30

Internal Control as It Affects Audit Evidential Matter 31

Reports From Service Organizations 36

IT Vendor Management 36

Current Audit Issues and Developments 37

Assessing Audit Risks in the Current Environment 37

Long-Lived Assets, Including Goodwill and Intangibles 39

Debt 40

Going Concern 40

Consideration of Fraud 42

General Accounting Issues Affecting E-Business 44

Stock Options 45

Business Combinations 46
SEC Internet-Related Concerns 48
Other E-Business Accounting Issues Important to Investors 51

Recent Auditing and Attestation Pronouncements and Other Guidance 59
SAS No. 99, *Consideration of Fraud in a Financial Statement Audit* 61
Audit Guide *Service Organizations: Applying SAS No. 70, as Amended* 63

Accounting Pronouncements and Guidance Update 63

On the Horizon 64
FASB Issues EDs Related to Stock-Based Compensation 64

AICPA Resource Central 65
Audit and Accounting Manual 65
AICPA reSOURCE: Online Accounting and Auditing Literature 65
Educational Courses 66
Member Satisfaction Center 67
Technical and Ethics Hotlines 67
Conference: The Business of E-Business 67
Web Sites 68

APPENDIX A: IDENTIFYING AND MANAGING E-BUSINESS RISKS 69

APPENDIX B: TRUST ASSURANCE SERVICES 76

APPENDIX C: THE INTERNET—AN AUDITOR'S RESEARCH TOOL 83

E-Business Industry Developments—2002/03

How This Alert Helps You

This Audit Risk Alert helps you plan and perform your e-business audits. The knowledge delivered by this Alert assists you in achieving a more robust understanding of the business environment in which your clients operate—an understanding that is more clearly linked to the assessment of the risk of material misstatement of the financial statements. Also, this Alert delivers information about emerging practice issues and information about current accounting, auditing, and regulatory developments.

If you understand what is happening in the world of e-business activities, and if you can interpret and add value to that information, you will be able to offer valuable service and advice to your clients. This Alert assists you in making considerable strides in gaining knowledge of e-business issues and understanding them.

This Alert is intended to be used in conjunction with the AICPA general *Audit Risk Alert—2002/03* (product no. 022333kk).

E-Business Background

A critical component of a successful e-business audit is a comprehensive knowledge of the environment in which e-business operates. The e-business environment is almost borderless—and, because of the relative infancy of this environment, established standard guidelines and metrics for performance may not be as robust as in other areas. For these reasons, among others, you should carefully consider the unique audit implications of dealing with or being in such a new and vaguely defined industry. For example, the e-business environment contains unique business risks resulting from the reliance on technology. These risks can include lack of paper audit trails, extensive use of information technology, risks/exposure of loss of data, and system interdependencies, among others.

The primary purpose of this Alert is to address the most important current auditing, accounting, and regulatory issues related to e-business to help you as you plan your engagements. See the later sections of this Alert that relate directly to these topics.

Internet and E-Business Development

The Internet occupies a large presence today in our everyday lives and business lives. Among the many things that Internet technologies allow is providing the opportunity for using e-business to:

- Increase brand awareness and expand sales opportunities (by opening additional sales channels, for example)
- Improve communications and customer service (by providing product descriptions, facilitating order placement and tracking order status, for example)
- Enhance purchasing and selling functions (by linking systems to sales and inventory databases to allow for production of automatic purchase orders, for example)
- Create more efficient, convenient, and customized customer transactions (for example, allowing larger items for selection at the tip of the customer's typing fingers)

These business functions, and the use of the Internet to conduct business, improve and expand the horizon for conducting business in a convenient, efficient, and timely manner. However, these somewhat rosy descriptors about conducting e-business are somewhat offset by the tradeoff of risk necessary to obtain them. Consider, for example, the daily reminders of the risk associated with various security vulnerabilities, "denial of service" attacks, and other threats to revenues and assets. In addition, special e-business risks can stem from an enterprise's information technology (IT) infrastructure, either through inherent vulnerabilities or through internal or external attacks. Further, vulnerabilities in IT infrastructure can create exposure to other e-business risks, such as those associated with compromised privacy, falsified authenticity, destructive programs, and issues surrounding the availability and integrity of data. System interdependencies can sometimes

make an e-business enterprise vulnerable through the system of a business partner, even if the enterprise itself effectively manages the risk within its own boundaries. You can find a more detailed discussion of e-business risk later in this Alert in Appendix A, "Identifying and Managing E-Business Risks."

E-Business Models

The variety of e-business models is limited only by entrepreneurial vision. Companies are constantly innovating to compete in the marketplace. Many e-business models encompass business-to-consumer (B2C) transactions, business-to-business (B2B) transactions, and variations on these themes, as noted in the following chart. Several new models have emerged, as well. (Note the acronyms in the following chart as they relate to government, business, consumer, and employee.)

	Government (G)	*Business (B)*	*Consumer (C)*	*Employee (E)*
Government	G2G	G2B	G2C	G2E
Business	B2G	B2B	B2C	B2E
Consumer	C2G	C2B	C2C	—

The key models can be described as follows:

- B2C—Typically a retailer selling directly to the consumer; until recently, this is the sector that has shown the fastest growth. Lately, however, B2B has shown the most growth potential, and the B2C growth rate now appears to be decelerating. (See the following section for additional information on B2Cs.)
- B2B—Typically a business selling up, down, or across the supply chain, involving business partners or business consortia. (See the subsequent section of this alert for additional information on B2Bs.)
- B2E—Typically a system enabling intercompany (intragroup) e-mails over the Internet to be directed to the correct department.

- B2G—A system that allows for electronic submission of business information to governmental entities, for example, the filing of corporate tax returns.
- C2G—A system that allows for electronic submission of individual information to governmental entities, for example, the filing of income tax returns.

The Differences Between B2C and B2B E-Commerce

The participants of B2C and B2B e-commerce differ. B2B users are other companies, whereas B2C users are individuals. Overall, B2B transactions are more complex and have higher security needs. And, in general, B2B involves processing large transaction volumes and potentially large dollar amounts.

Beyond that, there are other major distinctions:

- *Negotiation* is selling to another business and involves haggling over prices, delivery, and product specifications. This is not the case with most consumer sales because, for example, it is easier for retailers to place a catalog online and also explains why the first B2B applications were for buying finished goods or commodities that are simple to describe and price.
- *Integration* involves a situation in which retailers conducting B2C transactions don't have to integrate with their customers' systems. Companies selling to other businesses, however, need to make sure they can communicate without human intervention.

Business-to-Consumer Models

Although the term *e-commerce* generally refers to the value of goods and services sold online, B2C applies to any business or organization that sells its products or services over the Internet to consumers for their own use. A good example of B2C e-commerce is Amazon.com, the online bookseller that launched its site in 1995 and quickly took on the nation's major retailers. However, in addition to online retailers, B2C has grown to include the online

sale/provision of services such as online banking, travel services, online auctions, health information, and real estate sites.

Some of the Major Challenges of B2C E-Commerce. When it comes to determining what B2C presents as challenges, you can think about:

- *Getting consumers to buy things*—An e-commerce site cannot live on traffic alone. Getting visitors to the site is only half the battle. Whether they buy something is what determines if the business wins. The so-called conversion rate (converting visitors into purchasers) for B2C e-commerce sites is still fairly low. Some ways to boost conversion rate include improving navigation, simplifying checkout process (such as one-step checkout and easily replaced passwords), and sending out e-mails with special offers.
- *Building customer loyalty*—With so many sites out there, how can companies build a strong relationship with customers? Here are a couple of suggestions:
  - Focus on personalization. A wide array of software packages is available to help e-commerce sites create unique boutiques that target specific customers. For example, American Airlines has personalized its Web site so business fliers view it as a business airline and leisure travelers see it as a vacation site. Amazon, which built its own personalization and customer relationship management (CRM) systems, is well known for its ability to recognize customers' individual preferences.
  - Create "stickiness." Stickiness of a Web site refers to the site's ability to keep visitors engaged for long periods and to keep them coming back. Examples of sticky Web sites include www.Yahoo.com, www.AOL.com, and www.eBay.com. One solution to the challenge of creating stickiness is to keep content fresh and frequently update offerings.
  - Create an easy-to-use customer service application. Providing just an e-mail address can be frustrating to customers

with questions. Live chat or, at the very least, a phone number contact to help resolve questions can help.

- *Providing order fulfillment*—E-commerce has increased the focus on customer satisfaction and delivery fulfillment. One cautionary tale is the Toys "R" Us holiday debacle in 1999, when fulfillment problems caused some Christmas orders to be delivered late. Since then, companies have spent billions of dollars trying to improve their logistical systems, to guarantee on-time delivery. Providing instant gratification for customers still isn't easy, but successful B2C e-commerce operations are finding that fulfillment headaches can be eased with increased focus and investment in supply chain and logistical technologies.

Importance of Channel Conflict to E-Business. Channel conflict, or disintermediation, occurs when a manufacturer or service provider bypasses a reseller or salesperson and starts selling directly to the customer. Some sectors, including the PC and automobile industries, are particularly vulnerable to entities that engage in disintermediation, as are service industries such as insurance and travel. Levi's, for example, pulled its Web site after its resellers protested. Now, some entities that struggled with channel conflict are now finding ways to approach e-commerce without upsetting their salespeople. For example, big car companies and manufacturers, such as Maytag, are setting up Web sites that allow customers to decide what they want before being redirected to a local dealer.

Major B2C Models. As noted in last year's Alert, the short lifetime of the digital economy has witnessed evolution of the following four major categories of B2C models:

- Online stores, marketplaces, and services (Dell, amazon.com, eBay, and Charles Schwab)
- Content providers (the *Wall Street Journal* and *Consumer Reports*)
- Content aggregators and portals (Yahoo)
- Infrastructure providers (Sprint, Cisco Systems, Lucent, and BroadVision)

Within each of these categories, there are many different business models that include an enormous amount of hybridization and innovation. There is also cross-pollination between B2C and B2B variations of these models because what works for B2C also can apply to B2B.

Business-to-Business Models

The term *B2B* is used generically, to describe all online marketplaces where buyers and sellers congregate to exchange goods and services for money. It is important to note that B2B can be organized either horizontally or vertically.

- *Horizontal markets* cut across many industries, typically providing a common service, such as financial services; benefits management; and maintenance, repair, and operating (MRO) equipment procurement process management. Popular examples are Ariba Network and Commerce One's MarketSite.net.
- *Vertical markets* concentrate on one specific industry, such as agriculture and chemicals, and seek to provide all the services needed by that industry. Popular examples are VerticalNet, Chemconnect, and Covisint.

There are three common models currently in use:

- *Buy-centric markets* are the exact opposite of sell-centric markets. In these markets, a few big buyers join forces to build a marketplace where small fragmented sellers can sell their goods. This is great for buyers because it permits quick and easy price comparison-shopping. Popular examples are K-Mart's Retail Link, FreeMarkets.com, and Covisint.
- *Sell-centric markets* are markets in which one or a few big sellers work together to build a marketplace for many small fragmented buyers. Typically revenues are derived from ads, commissions on sales, or fees for delivering qualified leads to suppliers. Popular examples are Grainger.com, GE Global Exchange, DoveBid, GoFish.com, GlobalFoodExchange.com, E2Open.com, andTradeOut.com.

- *Neutral exchanges* appear where both the sellers and buyers are fragmented. In this environment, a third party creates a neutral exchange and performs the transactions through a bid/ask system. The middleman, or "net market maker," here cause "disintermediation," for which they receive a cut or transaction fee for each deal. The most important success factor for these exchanges is to reach "liquidity" or critical mass of both number and size of the transactions running through the exchange. Popular examples are NASDAQ, Altra, Paper Exchange, and Arbinet.

Some more specific examples of several B2B models are presented below.

- *Public exchanges (also called marketplaces).* A public vertical B2B electronic marketplace is a Web site run by a third party centered around a commodity or service that is open to many buyers and sellers. At a vertical B2B Web site, an e-business purchasing function may provide a link to its own purchasing Web site or post the specifications for its purchasing requirements. Not only does this type of arrangement provide the opportunity for great cost savings and efficiency in the electronic marketplace, but the public exchange also allows purchasers and sellers to obtain the best price quotes in minutes instead of days.

  Auditors of e-businesses that participate in a vertical B2B electronic marketplace should remember that some of the source records for purchasing transactions may exist on computer systems outside of the control of the audit client. If so, it is necessary to be familiar with Statement on Auditing Standards (SAS) No. 70, *Service Organizations* (AICPA, *Professional Standards*, vol. 1, AU sec. 324.24–.56), and with the AICPA Audit Guide *Service Organizations: Applying SAS No. 70, as Amended.* See the "Reports From Service Organizations" section later in this Alert for further discussion of SAS No. 70 issues.

- *Industry portals.* An industry portal is very similar to a vertical B2B electronic marketplace except that a portal may

include many more links to information and services common to any business in that industry. Such links might provide general news, sports, financial services, and other non-industry-specific services.

An e-business may conduct the purchasing function on an industry portal in the same manner as for a vertical B2B electronic marketplace. Consider, for example, the industry portal www.cpa2biz.com, which offers many things a CPA might need, from the latest authoritative publications to conference registration, CPE products, and state society news and announcements.

- *Supply-chain extranets.* An *extranet* is a Web site that an e-business sets up for its prospective and current trading partners. The site is accessible to registered users, with a user ID (identification) and password. The extranet site provides information about the products and services the company is interested in purchasing as well as specification requirements. Information about the company's current inventories is linked to its internal databases and also may be available to certain customers. Access to the site usually requires establishing a preexisting relationship between the trading partners. Ford's AutoXchange and GM's TradeXchange are extranets designed not only to link Ford and GM with suppliers, but also to link suppliers with each other.

  The audit implication for a client that operates its own extranet for purchasing is that the supplier may control elements of the electronic purchasing function, and the auditor will have to gain an understanding of the internal controls over these functions at the supplier. For further discussion of internal control issues, see the "Internal Control as It Affects Audit Evidential Matter" section later in this Alert.

- *Virtual private networks or private trading networks.* Some e-businesses may establish virtual private networks (VPNs) with trading partners. A VPN is a logical network that provides user privacy over a public network, such as a frame relay or, especially, the Internet, using tools such as

encryption in various combinations. When used in the purchasing function, VPNs are a good means to ensure the secure transmission of data.

From an audit standpoint, VPNs offer strong controls over the purchasing function. These networks offer transactions logging and authenticating trading partners, as well as the integrity of information, the identification of suppliers, and the nonrepudiation of transactions using digital signatures. See more on the issue of digital signatures later in this Alert in the "Recent Regulatory Developments" section.

E-Business Economic Environment

The U.S. Business Environment

As of late in the third quarter of 2002, anxious economists are downgrading their forecasts, and some crucial sectors of the economy are pushing the likelihood of a rebound into next year because of the abrupt slowdown in the economic recovery. For now, the overall economy is expanding, but sluggishly. Jobs are growing, but barely. And with a depressed stock market and reactions to further fears of terrorist strikes weighing on the national psyche, there is none of the exuberance that marked the recovery in the late 1990s.

The economy appears to be in a struggle between declining business confidence and strong consumer spending. Eventually, consumer demand should overcome business wariness unless cautious businesses cut so many jobs that consumers finally give up. The same dynamic was at work during the fall of 2001. After September 11 of that year, the business sector froze, but the consumer sector did not, and eventually consumer demand jumpstarted the economy.

The underlying economic fundamentals[1] in our economy remain relatively sound and point toward a moderate economic growth

1. Underlying economic fundamentals determine the long-term trend around which the business cycle weaves. The dips stem from temporary deficiencies of investment, consumption, net exports, and government spending. The task of stabilization is to minimize the swings over and under the sustainable trend of gross domestic product growth.

scenario. However, stock market weakness, coupled with recent data releases, has prompted downward forecast revisions.

The Sarbanes-Oxley Act

On July 30, 2002, President Bush signed into law the Sarbanes-Oxley Act of 2002 (the Act). The Act includes far-reaching changes in federal securities regulation that could represent the most significant overhaul since the enactment of the Securities Exchange Act of 1934. The Act creates the Public Company Accounting Oversight Board (PCAOB) to oversee the audit of public companies that are subject to the securities laws of the Securities and Exchange Commission (SEC). In addition, the Act prescribes a new set of auditor independence rules, new disclosure requirements applicable to public companies and insiders, and harsh civil and criminal penalties for persons responsible for accounting or reporting violations. The Act also imposes new restrictions on loans and stock transactions involving corporate insiders.

A more complete summary of the Act is available on the AICPA Web site at www.aicpa.org/info/sarbanes_oxley_summary.htm.

General E-Business Trends

Although numerous market research firms have tracked and reported information about e-business sales for several years, the U.S. government began officially reporting such information only in late 1999. For the year 2001 (totals reported in this section are the most recent available as of the printing of this Alert), the U.S. Department of Commerce reported total e-commerce sales of $35.9 billion.[2] For the second quarter of 2002, the Department of Commerce reported total e-commerce sales of $10.2 billion (compared to $8.2 billion for second quarter 2001), a 24.2 percent increase in sales over the prior year's quarter.

2. The Department of Commerce limits the definition of *e-commerce* to the value of goods and services sold online.

Although the Department of Commerce does not separately track B2C and B2B, it estimates that more than 90 percent of e-commerce is concentrated in the B2B area. A number of market forecasters are predicting even bigger things down the road for B2B companies. However, their estimates vary widely depending on what they measure and how they measure it. According to IDC (a Boston-based market research firm), worldwide B2B e-business will generate $2.6 trillion in revenues by 2004. On the other hand, Gartner, Inc., a Stamford, Connecticut, research firm, forecasts that the worldwide B2B market should total $1.9 trillion in 2002 and $8.5 trillion by 2005. Not to be left out, small businesses (those with fewer than 100 employees) are also jumping on the B2B bandwagon. Although only 850,000 small businesses were engaged in B2B transactions in 1999, a U.S. Small Business Administration survey projects that this figure will leap to 2.9 million by 2003.

On the B2C side, despite a disastrous couple of years recently for many dot-com merchants, online retail sales grew 21 percent, to $51.3 billion in 2001, according to a study conducted by the Boston Consulting Group. Predictions indicate further profitability and growth for 2002 due to continued growth in consumer spending online and additional cost efficiencies, with an anticipated increase of 41 percent in consumer spending online.

Online penetration by product category also grew. Out of 15 categories studied, sales in seven, including computer hardware and software, books, music and videos, toys, and consumer electronics, represented more than 5 percent of all retail sales for those respective categories, with penetration in some categories as high as 17 percent.

The Boston Consulting Group predicted that 2002 would be the beginning of a profitable era in online retailing. It was anticipated that retailers not only would continue to improve marketing effectiveness, but they also would have opportunities to realize efficiencies in the supply chain and product fulfillment.

Online holiday sales in 2002 are projected to total $38.2 billion worldwide, a 48 percent increase from the same period last year, according to Gartner, Inc. Also, according to Gartner, Inc., Europeans will spend more money online this holiday season than any other region, with revenue reaching $15.77 billion. North America will fall to second place with revenue at $15.66 billion.

Electronic commerce is a small part of total retail sales, so e-commerce growth depends less on retail ups and downs and more on the experience of Internet users and the maturity of Internet retailers, according to Gartner, Inc.

Where Are We Headed?

We have now lived through so many iterations of e-business that it's hard to keep track of its rapid development. For example, several years ago, the hottest topic of discussion was business-to-consumer e-commerce applications, which were going to radically alter the way we shopped for everything. Since then, the scales have tipped in the direction of both dollar and transaction volumes from the B2C to the B2B models.

The B2B model became the rage with such companies as Ariba and Extensity, which facilitated the ability to do business electronically. This minor subset of the entire business-to-business equation soon gave rise to the notion of electronic exchanges. These exchanges for vertical markets promised to reinvent how companies transact business by letting them essentially bid in real time for business among an established set of buyers and suppliers. With companies such as Oracle, CommerceOne, and Ariba leading the charge, these types of exchanges popped up in every major industry segment.

According to some experts, the next wave of e-business will be driven by business-to-business-to-consumer systems. Otherwise known as b-to-b-to-c, these systems will emerge because business models in the digital economy will not tolerate inefficiencies.

Recent Regulatory Developments

Internet Tax Issues

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 lost in 2002 because of the nontaxation of Internet sales puts the amount at more than $10 billion.

On November 28, 2002, President Bush signed a bill to extend the Internet Tax Freedom Act (ITFA) until November 1, 2003. This no-frills extension keeps Internet access free of sales tax in most states and puts off for two years any further action by Congress on Internet taxation. The extension was passed in spite of the objection of some in Congress, who wanted a commitment to give states the power to enforce sales tax collection, if the states simplify sales tax compliance.

The bill is the culmination of a long debate in both houses of Congress on the role of the federal government in state sales tax. At different times during the debate, those opposed to taxing e-commerce floated proposals to make the ITFA permanent, or to ban sales tax on digital products. Those supporting the states pushed for a commitment on the part of Congress to grant states the power to enforce sales tax collection, if the states simplify sales tax compliance (see the following section on state sales tax simplification).

Internet Tax Freedom Act Basics. The ITFA exempts Internet access services from state and local taxes, such as sales tax. In addition to Internet access, this ban extends to many Internet-based services. However, the ban on taxation of Internet access is not complete. The eight states that currently tax Internet access can continue to do so. The ITFA also prohibits multiple and discriminatory taxation of electronic commerce. However, the ITFA does not directly affect sales of tangible products over the Internet.

Not all Internet access is protected by the ITFA. In addition to allowing tax in states that already tax Internet access, the ITFA allows tax on Internet providers that engage in certain kinds of activities. These activities include knowingly providing access to materials

that are harmful to minors, unless access to those materials is restricted. This exception does not apply to Internet access providers, to the extent they are providing Internet access. Presumably, an Internet service provider (ISP) engaged in providing Internet access, and engaged in the business of providing unrestricted access to materials harmful to minors, would be partly taxable.

The ITFA prohibits discriminatory taxes on e-commerce. Discriminatory taxes include taxes imposed on e-commerce that are not generally imposed on transactions accomplished by other means. For example, a state could not impose a tax on access to an online newspaper, when newspaper sales from a street corner are tax free.

In addition, discriminatory taxes include taxes imposed at a different rate on e-commerce than on the same transactions accomplished by other means. For example, a state could not impose a 7 percent sales tax on sales of flowers via the Internet, when it imposes a 5 percent tax on sales from a local flower shop.

The ITFA includes provisions relating to the ability of a state to require a remote seller to collect sales and use tax. One provision relates to the effect of access to a Web site on a vendor's liability to collect sales tax. According to the ITFA, states may not require a vendor to collect a tax if "the sole ability to access a site on a remote seller's out-of-state computer server is considered a factor in determining a remote seller's tax collection obligation."

The ITFA prevents states from imposing an obligation to collect or pay tax on a different person than in the case of non-Internet transactions involving similar goods and services.

State Sales Tax Simplification. States are attempting to address the issue of sales tax simplification. The District of Columbia, 45 states, and thousands of local governments impose sales taxes. To cope with complaints about disparities among the jurisdictions, the National Governors Association created the Streamlined Sales Tax Project (SSTP). The SSTP, comprising tax administrators from 30 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, entitled 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.

The SSTP has now gathered half the states into its fold. The SSTP process consists of two parts. First, states must pass enabling legislation that allows tax administrators from the different states to work together to craft a new set of model sales tax laws. Second, states must individually amend their sales tax laws to conform to the model legislation. As of April 1, 2002, 25 states and the District of Columbia have passed enabling legislation. The legislatures of eight other states have introduced the legislation.

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 at www.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.

Online Sales to European Union Consumers

The European Union (EU) is in the process of adopting new rules that would require non-EU suppliers (including many U.S. companies) to collect and remit a value-added tax (VAT) on digital goods and services supplied to EU consumers. However, these new rules do not apply to non-EU suppliers selling to business customers in the union because existing self-assessment arrangements already cover VAT collection in these situations.

Non-EU suppliers will have to register in an EU member state of their choice, and levy VAT at the rate applicable in the member state where the customer resides.

Goods and Services Included. These new rules will apply to the online sale of digital products, such as software, music, games, databases, and broadcasts of events.

The VAT situation will lead to discrepancies in taxation between digital goods and services and their tangible equivalents. Books, magazines, and newspapers physically available in the EU member states are taxed at reduced rates, or not at all. E-books or electronic subscriptions to newspapers or magazines provided by non-EU vendors will be subject to VAT under these new rules.

Thresholds. There is no provision in these new rules for any sort of a *de minimis* amount; theoretically, a vendor with $1 of digitized-goods sales in the EU would need to register and collect the VAT. In addition, each of the EU states can enact its own threshold amount. Currently, this can range from zero to approximately 85,000 euros (about $75,000).

Documentation. Under these new rules, a non-EU company must charge VAT based on the customer's location. The vendor would be required to verify the information concerning the purchasers and their locations. The vendor would be responsible if the individual consumer provided inaccurate or fraudulent information, even if it was accepted in good faith; a purchaser's declaration would not be sufficient. In addition, the vendor would presumably be responsible if there were discrepancies between the customer's ordering location and shipping address (for example, a customer purchased goods via the Internet while on vacation but had them delivered to his or her home address).

Collection. Under these new rules, a U.S. company will have to register in one of the EU countries; however, the U.S. company will have to charge and collect VAT at the rate that applies in the country of consumption. Currently, there are 15 different rates, ranging from 15 percent (in Luxembourg) to 25 percent (in Sweden). Thus, a non-EU vendor will have to register in one country in the EU but collect VAT at the correct rate in 15 different countries.

Such a requirement contrasts sharply with those imposed on EU vendors. In general, an EU vendor will have to charge VAT only at the rate that applies in the country where it (the seller) is established.

E-Signature Act

In June 2000, the President signed into law the Electronic Signatures in Global and National Commerce Act (E-SIGN). E-SIGN contains provisions that ensure the legal validity of electronic (digital) signatures and contracts, permit the electronic delivery of legally required notices and disclosures, and allow for the satisfaction of record retention requirements through electronic means. An electronic signature can be "an electronic sound, symbol, or process, attached to or logically associated with a contract or record and executed or adopted by a person with the intent to sign the record." Digital signatures are created and verified using cryptography, the science of encoding and unencoding data. The technique allows recipients of Web-based documents to identify the sender and be assured of the validity of electronically transmitted data.

Even though such technology could vastly expand the realm of business that can be conducted electronically, adoption has been slow because of the lack of flexibility from older signature technologies. Recently, however, leading Internet security companies and top industry standards-setting bodies have settled on a more flexible way to verify electronic signatures for documents sent over the Web.

The World Wide Web Consortium (W3C), the standards-setting body founded by Web co-inventor Tim Berners-Lee, said that the agreement would help Internet users to more safely share documents, fill out forms and trade images and other media. The W3C group said the XML (Extensible Markup Language) Signature Syntax and Processing standard is now ready to be incorporated into new products and services from companies such as Microsoft, IBM, VeriSign, and scores of other security software developers.

XML Signature is designed to work with existing XML software, making it easier for modern software developers to incorporate the signature verification technology into new programs they develop.

Internet Privacy

Advances in computer technology have made it possible to compile and share detailed information about people more easily and cheaply than ever. That situation can be good for society as a whole and for individual consumers as well. For example, it is easier for law enforcement to track down criminals, for banks to use electronic information to help detect and prevent fraud, and for consumers to learn about new products and services, allowing them to make better-informed purchasing decisions. At the same time, as personal information becomes more accessible, companies, associations, government agencies, and consumers must take precautions to protect against the misuse of that information. Along these lines, the privacy of information collected by operators of Web sites is a growing issue of concern.

In the current Congress, there are more than 60 House bills and more than 30 Senate bills that address Internet privacy in whole or in part. Advocates of self-regulation argue that industry efforts, such as seal programs, for example, AICPA Trust Assurance Services (see the AICPA Web site, www.aicpa.org, for a detailed discussion), demonstrate the industry's ability to police itself. However, advocates of legislation argue that, although the seal programs are useful, they do not carry the weight of law, limiting the remedies available to consumers whose privacy is violated. Auditors should monitor potential Internet privacy legislation closely and be prepared to advise their clients on compliance and other voluntary privacy efforts.

> **Help Desk**—The Electronic Privacy Information Center tracks legislation and provides information on privacy, speech, and cyberliberties. Information is available at www.epic.org.

E-Fraud

The Internet Fraud Complaint Center (IFCC), which began operation on May 8, 2000, is a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI). The IFCC's primary mission is to address fraud committed over the Internet. The mission is accomplished

by facilitating the flow of information between law enforcement agencies and the victims of fraud—information that might otherwise go unreported.

From January 1, 2001, to December 31, 2001, the IFCC Web site received 49,711 complaints. This total includes many different fraud types and nonfraudulent complaints: computer intrusions, SPAM/unsolicited e-mail, and child pornography. During this same time period, the IFCC referred 16,775 complaints of fraud, the majority of which was committed over the Internet or similar online service. The total dollar loss from all referred cases of fraud was $17.8 million, with a median dollar loss of $435 per complaint. Some significant findings of this report include:

- Internet auction fraud was by far the most reported offense, comprising 42.8 percent of referred complaints. Nondeliverable merchandise and payment account for 20.3 percent of complaints, and the Nigerian Letter Scam (individuals representing themselves as Nigerian or foreign government officials asking for help in placing large sums of money in overseas bank accounts) made up 15.5 percent of complaints. Credit and debit card fraud and confidence fraud (such as home improvement scams and multilevel marketing) round out the top five categories of complaints referred to law enforcement during the year. Among those individuals who reported a dollar loss, the highest median dollar losses were found among the Nigerian Letter Scam ($5,575), identity theft ($3,000), and investment fraud ($1,000) complainants.
- Nearly 76 percent of alleged fraud perpetrators tend to be individuals (as opposed to businesses), 81 percent are male, and half reside in one of the following states: California, Florida, Illinois, New York, and Texas. Even though most are from the United States, perpetrators have a representation in Canada, Nigeria, Romania, and the United Kingdom.
- Of the male complainants, half are between the ages of 30 and 50 (the average age is 38.6), and over one-third resides in one of the four most populated states: California, Texas,

Florida, and New York. Most are from the United States, but the IFCC has received a number of complaints from Canada, United Kingdom, Australia, and Japan.

- The amount of loss by complainants tends to be related to a number of factors. Business victims tend to lose more than individuals and males tend to lose more than females. This may be a function of both online purchasing differences by gender and the type of fraud in which individuals find themselves. Even though there isn't a strong relationship between age and loss, the proportion of individuals losing at least $5,000 is higher for those 60 years and older than it is for any other age category.

- E-mail and Web pages are the two primary mechanisms by which the fraudulent contact took place. Nearly 70 percent of complainants reported they had e-mail contact with the perpetrator.

> **Help Desk**—Further information on Internet fraud is available at the Internet Fraud Complaint Center Web site at http://www1.ifccfbi.gov/index.asp.

Extensible Business Reporting Language

Extensible Business Reporting Language (XBRL) is a royalty-free, open specification for software that uses Extensible Markup Language (XML) data tags to describe financial information for public and private companies and other organizations. XBRL benefits all members of the financial information supply chain.

XBRL:

- Is a standards-based method with which users can prepare, publish in a variety of formats, exchange, and analyze financial statements and the information they contain.

- Is a licensed royalty-free worldwide by XBRL International, a nonprofit consortium consisting of more than 140 leading companies, associations, and government agencies.

- Permits the automatic exchange and reliable extraction of financial information across all software formats and technologies, including the Internet.
- Benefits all users of the financial information supply chain: public and private companies, the accounting profession, regulators, analysts, the investment community, capital markets, and lenders, as well as key third parties, such as software developers and data aggregators.
- Does not require a company to disclose any additional information beyond that which it normally discloses under existing accounting standards. XBRL does not require a change to existing accounting standards.
- Improves access to financial information by improving the form of the information and making it more appropriate for the Internet.
- Reduces the need to enter financial information more than one time, reducing the risk of data entry error and eliminating the need to manually key information for various formats (for example, printed financial statement, an HTML document for a company's Web site, an EDGAR filing document, a raw XML file, or other specialized reporting formats, such as credit reports and loan documents), thereby lowering a company's cost to prepare and distribute its financial statements while improving investor or analyst access to information.
- Leverages efficiencies of the Internet as today's primary source of financial information. More than 80 percent of major U.S. public companies provide some type of financial disclosure on the Internet, and the majority of information that investors use to make decisions comes to them via the Internet.

In October 2002, the XBRL-US Domain Working Group and the AICPA posted for public review a public working draft of the "U.S. Financial Reporting Taxonomy Framework" and "U.S. GAAP Commercial and Industrial Taxonomy." The "U.S. Financial

Reporting Taxonomy Framework" provides a foundation that will be used in future taxonomy development; the "U.S. GAAP Commercial and Industrial Taxonomy" provides companies within that industry the ability to create XBRL financial statements.

Help Desk—Further information on XBRL is available at www.xbrl.org.

General Audit Issues and E-Business

E-business is an ever more commanding presence in the lives of investors and businesses. The powerful force of e-business, in addition to its potential effect on the way we do business, directly affects practitioners and the avenues open to them as providers of services to the companies that engage in e-business. This electronic world is a unique and challenging frontier in many regards. It is an environment that will pose new demands on the auditors of both fledgling Web-play-only e-businesses and brick-and-mortar entities that are expanding their traditional business into e-business. Transactions conducted in an e-business environment may have a significant impact on audit process.

The Scope of E-Business Client Activities

E-business activities can occur in many aspects of your clients' businesses. For this reason, you may need to search for information about your clients' e-business activities and consider their effects on your audit planning. Specific techniques to consider in the search for e-business activities include:

- Modifying engagement acceptance procedures to include questions about the client's e-business activities.
- Reviewing minutes of board meetings, paying particular attention to discussions about the entity's e-business strategy, related issues, and timing.
- Examining the entity's annual budget for information about e-business plans.

- Looking for unusual increases in other budget line items—marketing and technology budgets, for example.
- Performing transaction reviews.
- Performing inquiries as part of obtaining an understanding of the business.
- Searching the Internet and carefully reviewing the client's Web site.

Although not all-inclusive, these techniques may reveal evidence of the nature, scope, and depth of the client's e-business activities.

Audit Timing and Planning

E-business transactions may automatically initiate, authorize, record, summarize, and settle electronically without human intervention or physical documentation. As a result, key audit evidence in electronic form may exist only for a limited amount of time. Therefore, you will need to understand and be able to rely on IT general controls. Computer programs may summarize transactions on a periodic basis and then purge, update, change, modify, or write over the original detail records of the transaction. Traditionally, audit procedures are performed after a client's fiscal year end. With e-business activities, however, traditional audit timing may be inadequate. One audit implication of sometimes short-term electronic evidence in e-business audits is that waiting until after the fiscal year end to begin auditing procedures may be too late to obtain competent sufficient evidence of controls or transactions.

As noted in last year's Alert, SAS No. 22, *Planning and Supervision* (AICPA, *Professional Standards*, vol. 1, AU sec. 311.09), indicates that "the extent to which computer processing is used in significant accounting applications, as well as the complexity of that processing, may also influence the nature, timing, and extent of audit procedures."

Many e-businesses may not have hard-copy or paper evidence of transactions. Sales orders, purchase orders, invoices, delivery,

settlement, and authorization may be prepared and performed electronically, leaving no paper trail behind. The failure of e-business companies to retain the details of transactions can create troublesome issues for the auditor who is considering whether internal control is functioning as planned. According to SAS No. 31, *Evidential Matter* (AICPA, *Professional Standards*, vol. 1, AU sec. 326.18), as amended:

> Certain electronic evidence may exist at a certain point in time. However, such evidence may not be retrievable after a specified period of time if files are changed and if backup files do not exist. Therefore, the auditor should consider the time during which information exists or is available in determining the nature, timing, and extent of his or her substantive tests, and if applicable, tests of controls.

If the retention of evidential matter is questionable, the auditor may want to begin audit procedures before year end. This may also drive the need for continuous auditing.

Adequate Technical Training

The rapid evolution of technology has profound implications for all those affected by computer technology, including auditors. Existing e-business hardware and software may need to be replaced every 18 months, or more frequently, to remain competitive. This rapid rate of technological change means that, to remain current, ongoing training in the underlying Internet technologies is requisite.

Auditing through the computer and the nature of electronic evidence require that the auditor gain a more detailed understanding of the controls over transactions and records than that traditionally obtained for paper-based manual audits. Experienced auditors with traditional audit skills already have 60 percent to 80 percent of what is needed to audit e-business. You can obtain the balance of the more specific technology skills through technical training courses, seminars, IT reference materials, research, and through other methods. You need look no further than SAS No. 1, *Codification of Auditing Standards and Procedures*

(AICPA, *Professional Standards*, vol. 1, AU sec. 210.04, "Training and Proficiency of the Independent Auditor"). The ubiquitous nature of e-business places even more demands on auditors than ever before.

Using the Work of a Specialist

Due to the rapid advance of technology, you may not have all the skills necessary to audit e-business activities. Until you and your staff have the technical skills needed to audit e-business, you may need to engage IT audit specialists to perform certain procedures. Qualified IT specialists are sometimes available from another part of the firm, such as the consulting division or the internal IT support staff. If not, you may have to go outside your own organization to obtain qualified specialists.

Engaging a specialist for gaining an understanding of internal controls, tests of controls, substantive tests, and analytical procedures requires awareness of guidelines available in the authoritative literature. According to SAS No. 73, *Using the Work of a Specialist* (AICPA, *Professional Standards*, vol. 1, AU sec. 336.06), specialized assistance is advisable for auditors who:

> May encounter complex or subjective matters potentially material to the financial statements. Such matters may require special skills or knowledge and in the auditor's judgment require using the work of a specialist to obtain competent evidential matter.

The use of an outside specialist[3] in an e-business context does not absolve the auditor from a certain level of understanding about computers. Audit planning comes into play because of the lead time necessary to contract for a specialist's services and the time required for the auditor to obtain the minimum technological

3. Note that Statement on Auditing Standards (SAS) No. 73, *Using the Work of a Specialist* (AICPA, *Professional Standards*, vol. 1, AU sec. 336), does not apply to specialists who are employed by the firm and are part of the engagement team. SAS No. 73 indicates that the auditor uses the work of the specialist as evidential matter in performing substantive tests to evaluate material financial statement assertions. The specialist does not, however, perform the substantive tests or analytical procedures.

knowledge necessary to supervise the specialist. According to SAS No. 22 (AU sec. 311.10):

> If specialized skills are needed, the auditor should seek the assistance of a professional possessing such skills, that is, someone who may be either on the auditor's staff or an outside professional. If the use of such a professional is planned, the auditor should have sufficient computer-related knowledge to communicate the objectives of the other professional's work; to evaluate whether the specified procedures will meet the auditor's objectives; and to evaluate the results of the procedures applied as they relate to the nature, timing, and extent of other planned audit procedures. The auditor's responsibilities with respect to using such a professional are equivalent to those for other assistants.

Internal Control as It Affects Audit Evidential Matter

SAS No. 55, *Consideration of Internal Control in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 319), as amended, provides guidance on the independent auditor's consideration of an entity's internal control in an audit of financial statements in accordance with generally accepted auditing standards (GAAS). For traditional businesses, the auditor's consideration of internal control typically involves updating prior-year checklists, questionnaires, and procedural narratives. Using a traditional audit approach for e-business clients would be insufficient because, in the e-business environment, almost all of the evidence of transactions is electronic. Critical records may consist of e-mail, database records, electronic documents, spreadsheets, and server logs. In addition, e-business transactions are subject to intentional and unintentional alteration and manipulation at many points between transaction initiation and summarization in the financial statements. Because e-businesses generally lack much of the paper evidence found in audits of traditional businesses, your approach to understanding internal controls when planning the e-business audit and determining the nature and extent of substantive tests must take this into account.

SAS No. 55, as amended, provides guidance to auditors about the effect of IT[4] on internal control and on the auditor's understanding of internal control and assessment of control risk. The Auditing Standards Board (ASB) believed the guidance was needed because entities of all sizes increasingly are using IT in ways that affect their internal control and the auditor's consideration of internal control in a financial statement audit. Consequently, in some circumstances, auditors may need to perform tests of controls to perform an effective audit.

Remember that SAS No. 94 does not:

- Eliminate the alternative of assessing control risk at the maximum level and performing a substantive audit, if that is an effective approach.
- Change the requirement to perform substantive tests for significant account balances and transaction classes.

The Importance of Software Controls

As noted earlier, technology continues to evolve rapidly. Most e-business server software is constantly upgraded, modified, and configured with components from different vendors. Often, when software is upgraded, previous control settings are lost, with no warning to managers. If procedures are performed before year end, you have the additional responsibility to consider whether there are frequent and significant changes being made to e-business systems that might affect the remainder of the period. According to SAS No. 55 (AU sec. 319.99):

> When the auditor obtains evidential matter about the design or operation of controls during an interim period, he or she should determine what additional evidential matter should be obtained for the remaining period. . . The auditor should obtain evidential matter about the nature and extent of any

4. According to SAS No. 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 319), information technology (IT) encompasses automated means of originating, processing, storing, and communicating information, and includes devices, communication systems, computer systems (including hardware and software components and data), and other electronic devices.

significant changes in internal control, including its policies, procedures, and personnel, that occur subsequent to the interim period.

Access is another issue to consider when testing controls over e-business activities. To test controls, auditors need access to networks, servers, and databases on which companies store their accounting records. Information technology managers may be reluctant to grant auditors the level of access they need, preferring, instead, to provide lengthy printouts, files on diskettes, or files as e-mail attachments. Access to copies of records in these forms is insufficient. E-business auditors must have full read-access rights to all system and database security settings and tables as well as the underlying electronic accounting records to gain a sufficient understanding of controls and to perform substantive tests. Sometimes this will require the CFO's involvement to obtain this access.

We already know that e-business transactions may be initiated by a trading partner's software. If transactions are automatically initiated between customer and supplier computers, the trading parties should require an independent auditor's report on controls at the other party. (The report—an SAS No. 70 report—is described in the subsequent section of this Alert, "Reports From Service Organizations.")

E-business software should include controls to prevent the repudiation or alteration of records that initiate transactions. Such controls might include digital signatures or server certificates that authenticate the parties to the transaction, as well as traditional edit and validation controls. Electronic (digital) signatures reduce the likelihood of the parties claiming that they never initiated the transaction or that the record of the terms of the transaction has been altered. Without server certificates, an initiator of a transaction has no assurance that it is dealing with the intended party's computer. Without digital signatures and server certificates, it may be difficult to determine that transactions are neither fictitious nor fraudulent. See the discussion of digital signatures in the "E-Signature Act" section in the "Recent Regulatory Developments" section of this Alert.

The Importance of Monitoring

A key control in a system of internal control is monitoring. Routers, firewalls, Web servers, e-mail servers, databases, and operating systems all have the ability to log traffic and specific security events. Properly implemented and controlled logs can provide some evidence that a transaction occurred and that the transaction record has not been altered. Independent audits of the controls carried out at third parties, along with the use of digital certificates, encryption, access controls, and logging, help provide evidence for the auditor regarding the integrity of recorded transactions.

Key Controls in an Electronic Environment

As noted in last year's Alert, to reduce the chance of an auditor relying on evidence that lacks credibility, he or she must understand the key controls over validity, completeness, and integrity. In the electronic environment, these typically include the following:

- *Segregation of duties.* Different employees should perform the duties of security administration, security monitoring, system administration, application maintenance, software development, and daily accounting operations.
- *Authorization.* User access to networks, systems, servers, services, programs, data, and records should be authorized based on the company's security policy and documented.
- *Authentication.* The identity of authorized users should be established by the use of logon IDs, hard-to-guess and hard-to-crack passwords, and, where appropriate, smart cards.
- *Access limitations.* Authorized users should be granted access to networks and application systems only after they authenticate themselves, and their access rights should be commensurate with their job responsibilities.
- *Activity logging.* Logging should be enabled on all routers, firewalls, servers, databases, and operating systems. The logs should be protected from tampering and alteration and should be retained.

- *Independent monitoring.* Employees independent of the IT department should monitor the activity logs on a frequent enough basis to detect suspicious, unusual, and unauthorized activity. Due to integration of e-business as discussed above, it should be independent of operations including IT.
- *Software development life cycle standards.* E-businesses should adopt and comply with authoritative standards for the development and implementation of new e-business systems.
- *Methods of error correction.* E-business software should have controlled rollback procedures so records are not purged or lost when servers crash and programs abort. Controls preventing changes to historical records should be in place so errors are corrected by entries made by the accounting department. Programmers and other IT personnel should not make changes to actual accounting records.
- *Backup procedures.* Grandfather, father, and son daily backup procedures should be performed, as well as weekly, monthly, quarterly, and annual backups. All files that include the details of transactions should be included in the backup. With the advice of legal counsel, the key user or owner of the data should establish retention schedules to satisfy legal and regulatory requirements. The backup media should have clear exterior identification, and there should be an offline log and inventory of what was backed up, when, by whom, and where stored. Backups should be stored in a safe location off-site and tested periodically by the key user of the data.
- *Disaster recovery.* The nature of e-business often requires that systems be capable of operating 24 hours a day, seven days a week. Even short periods of outage may mean significant financial loss to some e-businesses. There should be a written plan on how systems will roll over to alternative systems should the data center be destroyed or rendered inoperable. The plan should periodically be tested.

The strength of controls in an electronic environment is like a chain, where strength is determined by the weakest link. You should consider whether any weak links are present and, if so, consider the need to adjust your risk assessment and substantive tests accordingly.

Reports From Service Organizations

Many clients use an ISP or application service provider (ASP) to host their Web site, including the databases used to initially record sales and credit card receivables. In a number of cases, ISP/ASP servers provide fulfillment by allowing users to immediately download their purchase after credit approval for software, digitized music, videos, books, and other electronic documents. For clients that use outsourced services, auditors can sometimes obtain a report on controls from the service organization. According to SAS No. 70, *Service Organizations* (AU sec. 324.24), the report would be either (1) reports on controls placed in operation, or (2) reports on controls placed in operation and tests of operating effectiveness.

See the discussion about the recently published AICPA Audit Guide related to service organizations in the subsequent section of this Alert, "Audit Guide *Service Organizations: Applying SAS No. 70, as Amended.*"

IT Vendor Management

IT vendor management provides clients with expert IT services that allow them to control direct labor costs and leverage their high volume to obtain more competitive rates. The scenario involves the management of IT vendors through effective controls and service level agreements.

In the United States, many IT contractors are employed in vendor-management arranged deals. This trend is increasing because companies are operating on a global basis now and want to make use of their global buying power, so they outsource contractor employment to large vendor management companies.

From an audit perspective, you should understand and review not only the performance of the IT vendor manager, but also the impact of vendor management controls over e-business operations. This has been a major issue during the past year in the financial services industry.

Current Audit Issues and Developments

Assessing Audit Risks in the Current Environment

The proper planning and execution of an audit have always required you to have a thorough understanding of e-business and the nature of your client's business. For most audit firms, this in-depth understanding means that the most experienced partners and managers must become involved early and often in the audit process. In today's economic environment, your judgment, knowledge, and experience are even more important than they were in the past.

During the past several months, the U.S. economy has suffered significant declines and uncertainties: Consumer confidence has dropped, plant closings and layoffs have increased dramatically, profit margins for many companies have slipped, and many companies have failed. Periods of economic uncertainty like this lead to challenging conditions for companies due to potential deterioration of operating results, increased external scrutiny, and reduced access to capital. During such times, professional skepticism should be heightened, and the status quo should be challenged.

Evaluating Audit Risks

Your evaluation of audit risk should start with a good understanding of your client's business. To develop this understanding, you should be knowledgeable about the entity's strategies for dealing with business conditions—both current conditions and those most likely to exist in the near future.

Professional Skepticism

The third general audit standard stipulates that due professional care be exercised in planning and conducting an audit engagement. Due professional care requires that you exercise professional skepticism in gathering and evaluating audit evidence. Although you assume neither management dishonesty nor unquestioned honesty, you should consider the increased risk associated with the potential increases in external pressure on management during the current economic climate. For a more detailed discussion of these risks, see the "Consideration of Fraud" section of this Alert.

Earnings Management Challenges. As a result of perceived external pressures, companies may be tempted to manage earnings by using nonrecurring transactions or changing the method of calculating key estimates, such as reserves, fair values, or impairments. Companies may also adopt inappropriate accounting practices resulting in improper recognition or omission of financial transactions. For material nonrecurring transactions that may require special disclosure to facilitate the readers' understanding of the reported financial results, apply the guidance in Accounting Principles Board (APB) Opinion No. 20, *Accounting Changes*, in reporting the effects of changes in estimates. Inappropriate transactions or accounting practices that may result in errors requiring adjustments of financial statements include, for example, premature recognition of revenue, failure to appropriately accrue for contingent liabilities that are probable and estimable, and failure to record unpaid purchase invoices. As mentioned earlier in this Alert, the use of outsourcing deals may affect current financial performance. Additionally, you should be particularly skeptical of fourth-quarter events that result in significant revenue recognition, loss accrual, or noncash earnings.

The appropriate level of professional skepticism is needed when corroborating management's representations. Management's explanations should make business sense. Additionally, you may need to consider corroborating management's explanations with members of the board of directors or the audit committee.

Indicators of Reporting Risk. Other indicators of potential increased accounting and reporting risk calling for increased professional skepticism include:

1. Liquidity matters
    - The company is undercapitalized, relying heavily on bank loans and other credit, and is in danger of violating loan covenants.
    - The company appears to be dependent on an initial public offering for future funding.
    - The company is having difficulty obtaining or maintaining financing.
    - The company is showing liquidity problems.
2. Quality of earnings
    - The company is changing significant accounting policies and assumptions to less conservative ones.
    - The company is generating profits, but not cash flow.
3. Management characteristics
    - Management's compensation is largely tied to earnings or appreciation of stock options.
    - The company appears vulnerable to the weakening economic conditions and management is not proactive in addressing changing conditions.
    - The company's management is selling their investment in company securities more than in the past.
    - There is a significant change in members of senior management or the board of directors.

Long-Lived Assets, Including Goodwill and Intangibles

Industry downturns and cash flow erosion may indicate an impairment of fixed assets, goodwill, or other intangibles. Financial Accounting Standards Board (FASB) Statement of Financial Accounting Standards No. 144, *Accounting for the Impairment or Disposal of Long-Lived Assets*, provides guidance in this area. In

that regard, significant idle equipment or assets no longer used in operations may need to be written off. (See the "Asset Impairment" subsection later in this Alert for related information.)

FASB Statement No. 142, *Goodwill and Other Intangible Assets*, was issued in June 2001. This Statement requires that goodwill be tested for impairment at least annually using a two-step process that begins with an estimation of the fair value of a reporting unit. The first step is a screen for potential impairment, and the second step measures the amount of impairment, if any.

In addition, FASB Statement No. 142 provides specific guidance on testing intangible assets that are not being amortized for impairment and thus removes those intangible assets from the scope of other impairment guidance. Intangible assets that are not amortized are tested for impairment at least annually by comparing the fair values of those assets with their recorded amounts.

Debt

You should carefully review loan agreements and test for compliance with loan covenants. In this regard, consider any "cross default" provisions, that is, a violation of one loan covenant that affects other loan covenants. Keep in mind that any debt with covenant violations that are not waived by the lender for a period of more than one year from the balance sheet date may need to be classified in the balance sheet as a current liability.

As always, review the debt payment schedules and consider whether the company has the ability to pay current debt installments or to refinance the debt if necessary. When making an evaluation, it is important to remember that it is quite possible that the company will not generate as much cash flow as it did in previous years.

Going Concern

As you plan and perform audits of e-business activities, you should consider general economic factors that give rise to going-concern issues. For example, reductions in personal income, layoffs, higher unemployment levels, changing or outdated

technology, and decreases in consumer confidence all give rise to such concerns. These factors have combined recently to result in high rates of business failure. Accordingly, auditors should be alert to general economic and other conditions and events which, when considered in the aggregate, indicate that there could be substantial doubt about the entity's ability to continue as a going concern.

In general, conditions and events that might indicate caution about going-concern issues could include (1) negative trends, such as recurring operating losses (2) financial difficulties, such as loan defaults or denial of trade credit from suppliers (3) internal challenges, such as substantial dependence on the success of a particular product line or service (4) external matters, such as pending legal proceedings or the loss of a principal supplier or (5) the inability to retain key technical or managerial talent. Also consider the possibility of the entity's excessive and unusual reliance on external financing, rather than money generated from the company's own operations as a going-concern issue. External financing reliance is one major factor that led to the many of the failures of dot-com companies.

Auditors should be aware of their responsibilities pursuant to SAS No. 59, *The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern* (AICPA, *Professional Standards*, vol. 1, AU sec. 341.02–.04). That Statement provides guidance about conducting an audit of financial statements in accordance with GAAS to evaluate whether there is substantial doubt about a client's ability to continue as a going concern for a reasonable period of time.

Information that significantly contradicts the going-concern assumption, or the ability to remain a going concern, relates to the entity's inability to continue to meet its obligations as they become due without substantial disposition of assets outside the ordinary course of business, restructuring of debt, externally forced revisions of its operations, or similar actions. SAS No. 59 does not require you to design audit procedures solely to identify conditions and events that, when considered in the aggregate, indicate there could be substantial doubt about the entity's ability to continue as a going concern. The results of auditing procedures designed and performed to achieve other audit objectives should be sufficient for that purpose.

If there is substantial doubt about the entity's ability to continue as a going concern, consider the likelihood that management plans can mitigate existing conditions and events and whether those plans can be effectively implemented. If you obtain sufficient competent evidential matter to alleviate doubts about going-concern issues, then consider the need for disclosures of the conditions and events that initially caused you to believe there was substantial doubt.[5] If, however, after considering identified conditions and events, along with management's plans, you conclude that substantial doubt remains about the entity's ability to continue as a going concern, consider the possible effects on the financial statements and the adequacy of the related disclosure. Additionally, the audit report should include an explanatory paragraph to reflect your conclusion. In these circumstances, refer to the specific guidance set forth under SAS No. 59.

E-Businesses in Bankruptcy Reorganization

For those e-business entities or operations that are under bankruptcy reorganization pursuant to Chapter 11 of the Bankruptcy Code, or emerging from it, consider whether the company is following the accounting guidance of Statement of Position (SOP) 90-7, *Financial Reporting by Entities in Reorganization Under the Bankruptcy Code*. E-business entities that filed for bankruptcy may have impairments that need to be recorded before fresh-start accounting under SOP 90-7.

Consideration of Fraud

Recently, the ASB issued SAS No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316), which supersedes SAS No. 82, *Consideration of Fraud in a Financial Statement Audit*; amends SAS No. 1, *Codification of Auditing Standards and Procedures* (AICPA, *Professional Standards*, vol. 1, AU sec. 230, "Due Professional Care in the

5. Note that SAS No. 96, *Audit Documentation* (AICPA, *Professional Standards*, vol. 1, AU sec. 339), amended SAS No. 59, *The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern* (AICPA, *Professional Standards*, vol. 1, AU sec. 341), to require that this evidence be documented.

Performance of Work"); and amends SAS No. 85, *Management Representations* (AICPA, *Professional Standards*, vol. 1, AU sec. 333).

SAS No. 99 addresses the following issues:

- Description and characteristics of fraud
- The importance of exercising professional skepticism
- Discussion among engagement personnel regarding the risks of material misstatement due to fraud
- Obtaining the information needed to identify risks of material misstatement due to fraud
- Identifying risks that may result in a material misstatement due to fraud
- Assessing the identified risks after taking into account an evaluation of the entity's programs and controls
- Responding to the results of the assessment
- Evaluating audit evidence
- Communicating about fraud to management, the audit committee, and others
- Documenting the auditor's consideration of fraud

According to SAS No. 99, fraud frequently involves a pressure or incentive to commit fraud. The lack of industry self-regulation of e-business and, in some cases, the lack of established accounting practices relative to the industry could provide management with the opportunity to manipulate income.

SAS No. 99 specifically recognizes certain conditions as risk factors that motivate management to engage in fraudulent financial reporting. For example, factors include situations in which a significant portion of management compensation is represented by bonuses, stock options, or other incentives; and ones in which there is an excessive interest by management in maintaining or increasing an entity's stock price. SAS No. 99 also identifies other risk factors related to misstatements arising from fraudulent financial reporting, such as a high degree of competition or market

saturation, and rapidly changing technology or rapid product obsolescence. All of these factors are present in the e-business environment, implying potential audit concerns.

As a result of the opportunity for fraud that is present in audits of e-businesses, you should consider whether specific controls exist that mitigate the risks. Mitigating controls at larger companies may include an effective board of directors, audit committee, and an internal audit function. Smaller companies may have an environment that fosters integrity and ethical behavior, as well as management by example.

You may need to modify the nature, timing, and extent of audit procedures if you believe that there are risks of material misstatement attributable to fraud during an audit of an e-business. For example, you may choose to perform detailed substantive analytical procedures or conduct interviews in areas where fraud may be present, or both. For potential fraud related to revenue recognition issues, you may decide to confirm certain relevant terms of customer contracts. SAS No. 99 contains specific guidance on revenue recognition as a potential fraud risk.

In certain situations, you may have a duty to disclose the circumstances of the fraud to outside parties. For public companies, if the fraud or related risk factor results in termination of the engagement, is considered a reportable event, or is the source of a disagreement, you may be required to report this situation to the SEC. If fraud is present, other reports also may be required under section 10A(b)1 of the Securities and Exchange Act of 1934.

For more information on SAS No. 99, see the discussion in the "Recent Auditing and Attestation Pronouncements and Other Guidance" section later in this Alert.

General Accounting Issues Affecting E-Business

Accounting for e-business involves the application of many complex accounting principles and transactions for which there may be diversity in practice or no authoritative guidance. The diversity in accounting treatment for e-business transactions

leads to incomparable financial statements and potential earnings-management issues and may cause investors to rely on unaudited sources of information for stock valuation and investment decisions.

Accounting regulators and standard-setters are aware of the issues raised by the diversity in accounting by e-businesses. In addition, the SEC staff has identified several accounting issues for Internet companies that the Emerging Issues Task Force (EITF) is addressing. See the section in this Alert titled "SEC Internet-Related Concerns" for a discussion of these issues.

Stock Options

As noted in last year's Alert, stock options are an important accounting-related area for your e-business clients. Knowledgeable workers are the prime assets of e-businesses and are the key to wealth creation. Accounting for their compensation sometimes raises difficult accounting issues if e-businesses include stock options in employee compensation packages. E-businesses grant stock options to essential employees to attract, motivate, and retain them, in addition to granting stock options, awards of stock, or warrants to consultants, contractors, vendors, lawyers, finders, lessors, and others. Issuing equity instruments makes a lot of sense, partly because of the favorable accounting treatment and partly because the use of equity conserves cash and generates capital.

The accounting for employee stock options has received renewed attention in recent months. There have been two important developments. First, several major U.S. companies have announced their intentions to change their method of accounting for employee stock options to an approach that recognizes an expense for the fair value of the options granted in arriving at reported earnings. Recognizing compensation expense relating to the fair value of employee stock options granted is the preferable approach under FASB Statement No. 123, *Accounting for Stock-Based Compensation.* It also is the treatment advocated by an increasing number of investors and other users of financial statements.

When the FASB developed FASB Statement No. 123 in the mid-1990s, the FASB proposed requiring that treatment because it believed it was the best way to report the effect of employee stock options in a company's financial statements. The FASB modified that proposal in the face of strong opposition by many in the business community and in Congress who directly threatened the existence of the FASB as an independent standard setter. Thus, while FASB Statement No. 123 provides that expense recognition for the fair value of employee stock options granted is the preferable approach, it permitted the continued use of existing methods with disclosure in the footnotes to the financial statements of the pro forma effect on net income and earnings per share as if the preferable, expense recognition method had been applied. Until now, only a handful of companies elected to follow the preferable method. (See related information in the subsequent section of this Alert, "FASB Issues ED on Stock-Based Compensation.")

Second, the International Accounting Standards Board (IASB) has concluded its deliberations on the accounting for share-based payments, including employee stock options, and announced plans to issue a proposal for public comment in the fourth quarter of 2002. That proposal would require companies using IASB standards to recognize, starting in 2004, the fair value of employee stock options granted as an expense in arriving at reported earnings. Although there are some important differences between the methodologies in the IASB proposal and those contained in FASB Statement No. 123, the basic approach is the same—fair value measurement of employee stock options granted with expense recognition over the vesting period of the options. See information related to FASB exposure drafts about stock options (stock-based compensation) in the "On the Horizon" section of this Alert.

Business Combinations

In June 2001, the FASB issued FASB Statement No. 141, *Business Combinations*, to address financial accounting and reporting issues for business combinations. This Statement supersedes APB Opinion No. 16, *Business Combinations*, and FASB Statement No. 38, *Accounting for Preacquisition Contingencies of Purchased Enterprises.*

Under FASB Statement No. 141, all business combinations will be accounted for using one method—the purchase method. Given the economic environment of e-business, mergers and acquisitions have been prevalent, so this change to a single method of accounting for business combinations may have major implications for e-businesses.

Under APB Opinion No. 16, business combinations were accounted for using one of two methods, namely, the pooling-of-interests method (pooling method) or the purchase method. Use of the pooling method was required whenever 12 criteria were met; otherwise, the purchase method was used. Because those 12 criteria did not distinguish economically dissimilar transactions, similar business combinations were accounted for using different methods, producing dramatically different results.

The provisions of FASB Statement No. 141 reflect a fundamentally different approach to accounting for business combinations. The single-method approach reflects the conclusion that virtually all business combinations are acquisitions and, thus, all business combinations should be accounted for in the same way that other asset acquisitions are accounted for—based on the values exchanged. Specifically, FASB Statement No. 141 changes the accounting for business combinations in APB Opinion No. 16 in the following respects:

- FASB Statement No. 141 requires that all business combinations be accounted for by a single method—the purchase method.
- In contrast to APB Opinion No. 16, which required the separate recognition of intangible assets that can be identified and named, FASB Statement No. 141 requires that intangible assets be recognized as assets apart from goodwill if they meet one of two criteria—either the contractual-legal criterion or the separability criterion.
- In addition to the disclosure requirements in APB Opinion No. 16, FASB Statement No. 141 requires the disclosure of the primary reasons for both the business combination and the allocation of purchase price paid to the assets acquired and liabilities assumed by major balance-sheet caption.

The provisions of FASB Statement No. 141 apply to all business combinations initiated after June 30, 2001. The Statement also applies to all business combinations accounted for using the purchase method for which the date of acquisition is July 1, 2001, or later.

SEC Internet-Related Concerns

The SEC staff expressed concern about issues that they believed warranted consideration by the EITF or another standard-setting body. Since 1999, the SEC and the EITF have worked to resolve these issues, which we discuss here.

Rebates and Free Products or Services

ISPs and computer retailers commonly offer a rebate to purchasers of new computers who contract for three years of Internet service. In most cases, the rebate cost is borne by the ISP while a portion is borne by the retailer. In addition, the retailer provides advertising and marketing for the arrangement, and the rebate must be returned by the consumer if the consumer breaks the contract with the ISP. Some ISPs and retailers believe their portion of the cost of the rebate should be a marketing expense, as opposed to a reduction of revenues. However, according to SEC's Staff Accounting Bulletin (SAB) No. 101, *Revenue Recognition in Financial Statements—Frequently Asked Questions and Answers*, the SEC staff generally believes that such rebates should be considered a reduction of revenue.

On a related matter, some e-businesses offer free or heavily discounted products or services in introductory offers (for example, a free month of service or six CDs for a penny). Some businesses conclude that these introductory offers should be accounted for at full sales price, with the recognition of marketing expense for the discount. The section titled "One-Cent Sales" in AICPA Technical Practice Aid *Revenue Recognition* (AICPA, *Technical Practice Aids*, vol. 1, sec. 5100.07) addresses this issue, concluding, "The practice of crediting sales and charging advertising expense for the difference between the normal sales price and the 'bargain day' sales price of merchandise is not acceptable for financial reporting."

The FASB's EITF addressed these issues in EITF Issue No. 00-14, concluding that sales incentives, such as rebates and free products, should be treated as a reduction of revenue.

Auction Site Fees

Internet auction sites usually charge both up-front (listing) fees and back-end (transaction-based) fees. In many cases, the listing fees are being recognized as revenue when the item is originally listed, despite the requirement for the auction site to maintain the listing for the duration of the auction. In addition, some auction sites recognize the back-end fees as revenue at the end of the auction despite the fact that the seller is entitled to a refund of the fee if the transaction between the seller and the buyer does not close. According to the SEC's SAB No. 101, the SEC staff generally believes that the up-front (listing) fees should be recognized over the listing period, which is the period of performance. Because the facts and circumstances of the agreements among the auction site, the buyers, and the sellers may vary significantly concerning the back-end fees, each situation will have to be evaluated to determine the appropriate method of revenue recognition.

Application Service Providers

Some purchasers of software do not actually receive the software. Rather, the software application resides on the vendor's or a third party's server, and the customer accesses the software on an as-needed basis over the Internet. Essentially, the customer is paying for two elements—the right to use the software and the storage of the software on someone else's hardware. The latter service is referred to as *hosting*. If the vendor also provides the hosting, several revenue recognition issues may arise. First, there may be transactions structured in the form of a service agreement providing Internet access to the specified site, without a corresponding software license. In such instances, it may not be clear how to apply SOP 97-2, *Software Revenue Recognition*. Second, if the transaction is viewed as a software license with a service element, it is not clear how to evaluate the delivery requirement of SOP 97-2.

The EITF addressed this topic in EITF Issue No. 00-3, *Application of AICPA Statement of Position 97-2*, Software Revenue Recognition, *to Arrangements That Include a Right to Use Software Stored on Another Entity's Hardware.* The consensus of the EITF was that SOP 97-2 does not apply to all of these arrangements, but if it does, revenue should be allocated to the software element based on vendor-specific evidence of fair value. Revenue should be recognized on the software element when the delivery has occurred and on the hosting element when the services are performed.

Web Site Access and Maintenance

Some e-businesses provide customers with services that include access to a Web site, maintenance of a Web site, or the publication of certain information on a Web site for a period of time.[6] Some companies have argued that, because the incremental costs of maintaining the Web site and/or providing access to it are minimal, this ongoing requirement should not preclude upfront revenue recognition. According to the SEC's SAB No. 101, the SEC staff believes, however, that fees like this should be recognized over the performance period, which would be the period over which the company has agreed to maintain the Web site or listing.

Accounting for Customer or Membership Base Costs

E-businesses often make large investments in building a customer or membership base. Consider the following examples:

- Sites that give users rewards, such as points, products, discounts, and services, in exchange for setting up an account with the site
- Sites that make payments to business partners for referring new customers or members
- Businesses that give users a computer and Internet service for free if they are willing to spend a certain amount of

6. EITF Issue No. 00-2, *Accounting for Web Site Development Costs*, describes the accounting treatment for costs associated with developing a Web site.

time on the Internet each month and are willing to have advertisements reside permanently on their computers

In each of these examples, a question may arise about whether the costs represent customer acquisition costs or the costs of building a membership base that qualifies for capitalization, for example, by analogy to FASB Statement No. 91, *Accounting for Nonrefundable Fees and Costs Associated with Originating or Acquiring Loans and Initial Direct Costs of Leases*, as amended.

The EITF has not reached a consensus on Issue No. 00-22, *Accounting for "Points" and Certain Other Time-Based or Volume-Based Incentive Offers, and Offers for Free Products or Services to Be Delivered in the Future*, although it still plans further discussion. Specific industries would be excluded from the scope of EITF Issue No. 00-22 to the extent that they are addressed by higher level GAAP; however, not much guidance currently exists.

Other E-Business Accounting Issues Important to Investors

E-business analysts have identified several essential e-business accounting issues of interest to auditors. These issues are presented from the point of view of investors evaluating Internet companies.

Recognition of Costs

Customer solicitation and software development costs are key costs for e-businesses that present cost recognition issues. Currently, there is diversity in accounting for these costs by Internet companies—they could either capitalize or expense the costs—which makes it difficult to compare their financial statements.[7] If they capitalize the costs, amortization periods for essentially the same transactions could differ between companies. Compounding the problem is the practice by some established companies of masking these costs by spreading them across existing operations.

7. If the costs incurred relate to internal-use software, Statement of Position (SOP) 98-1, *Accounting for the Costs of Computer Software Developed or Obtained for Internal Use* requires that these costs be capitalized and amortized over the useful life of the software.

If alternative accounting treatments give management the ability to choose between capitalizing or expensing a cost, management may use the alternatives to manage earnings. If investors cannot compare audited financial statements reliably, they may turn to potentially unreliable sources of information as a basis for their investment decisions. The use of unreliable information can cause volatility in the stock prices, misvaluation, and losses for investors.

In the two major categories of customer solicitation and software development costs, auditors should be aware of current GAAP, as follows:

- SOP 93-7, *Reporting on Advertising Costs*
- EITF Issue No. 00-22, *Accounting for "Points" and Certain Other Time-Based or Volume-Based Incentive Offers, and Offers for Free Products or Services to Be Delivered in the Future*
- SOP 98-1, *Accounting for the Costs of Computer Software Developed or Obtained for Internal Use*
- EITF Issue No. 00-2, *Accounting for Web Site Development Costs*

Research and Development Costs

The e-business industry is still in its infancy. Often, the competitive advantage of an e-business rests on an idea that is still in the conceptual stage, with no existing commercial software process to implement the strategy. Therefore, many e-businesses undertake the research and development (R&D) activities themselves.

Ongoing innovation is the heart of competition in e-business and is required for survival. Consequently, most e-businesses devote a substantial portion of their resources to R&D activity. According to paragraphs 8(a) and 8(b) of FASB Statement No. 2, *Accounting for Research and Development Costs*:

> Research is planned search or critical investigation aimed at discovery of new knowledge with the hope that such knowledge will be useful in developing a new product or service.

> Development is the translation of research findings or other knowledge into a plan or design for a new product or process . . . whether intended for sale or use.

E-business management may reduce net loss or increase earnings by capitalizing R&D costs, which are significant for many companies involved in e-business. However, FASB Statement No. 2, as interpreted by FASB Interpretation No. 4, *Applicability of FASB Statement No. 2 to Business Combinations Accounted for by the Purchase Method*, prohibits capitalization and requires R&D to be expensed when incurred, except for acquired R&D with alternative future uses purchased from others. In addition to the requirement to expense internal R&D, FASB Statement No. 2 requires disclosure in the financial statements regarding the total amount of R&D costs charged to expense.

Some e-businesses acquire their assets through mergers and acquisitions. One purpose of these business combinations is to acquire in-process e-business R&D. You may need to hire a technology specialist to determine which acquired technology objects have alternative future uses. For clients with technology with alternative future uses, you should verify that they are properly valued and capitalized.

> **Help Desk**—The AICPA Practice Aid titled *Assets Acquired in a Business Combination to Be Used in Research and Development Activities: A Focus on Software, Electronic Devices, and Pharmaceutical Industries* (product no. 006609kk) may be helpful in valuing these intangible assets. It is available from the AICPA Order Department at (888) 777-7077 or online at www.cpa2biz.com.

Contingency Losses

E-businesses that conduct retail transactions over the Internet with consumers might experience contingent losses for sales returns, allowances, and credit card chargebacks. Auditors of e-businesses should ensure that clients conducting online retail sales accrue an adequate loss contingency for sales returns, allowances, and credit card chargebacks, or that they make adequate disclosure that they cannot reasonably estimate the amount of loss.

Usually, estimates of anticipated losses are based on the normal experience of the business and its transaction history. For many e-businesses, however, there is not enough transaction history to reasonably estimate these amounts. In that case, according to paragraph 10 of FASB Statement No. 5, *Accounting for Contingencies*:

> If no accrual is made for a loss contingency because one or both of the conditions in paragraph 8 [see previous extract] are not met . . . disclosure of the contingency shall be made where there is at least a reasonable possibility that a loss . . . may have been incurred. The disclosure shall indicate the nature of the contingency and shall give an estimate of the possible loss or range of loss or state that such an estimate cannot be made.

Start-Up Activity Costs

As a result of the recent pace of e-business investment, you should take the time to understand how to apply the provisions of SOP 98-5, *Reporting on the Costs of Start-Up Activities*, for your clients. In addition, you may want to review the provisions of FASB Statement No. 7, *Accounting and Reporting by Development Stage Enterprises*. Paragraph 5 of SOP 98-5 defines start-up activities as:

> Those one-time activities related to opening a new facility, introducing a new product or service, conducting business with a new class of customer or beneficiary, initiating a new process in an existing facility, or commencing some new operation. Start-up activities include activities related to organizing a new entity (commonly referred to as organization costs).

Certain costs that ongoing enterprises would be able to capitalize under GAAP, such as acquiring or constructing long-lived assets and getting them ready for their intended uses, acquiring or producing inventory, and acquiring intangible assets, are not subject to SOP 98-5. Costs of start-up activities, including organization costs, should be expensed as incurred.

FASB Statement No. 7 defines a development stage enterprise as one that is devoting substantially all of its efforts to establishing a new business, whose principal operations have not commenced, or for which there is no significant revenue. In addition, a development stage enterprise typically devotes most of its activities to acquiring or

developing operating assets, recruiting and training personnel, and developing markets, as well as other activities. Clearly, FASB Statement No. 7 applies to most new e-businesses because they are typically involved in the activities described by the Statement. According to paragraph 10 of FASB Statement No. 7:

> Financial statements issued by a development stage enterprise shall present financial position and results of operations in conformity with the generally accepted accounting principles that apply to established operating enterprises.

Furthermore, FASB Statement No. 7 requires additional balance-sheet disclosures. These disclosures include cumulative net losses, with special descriptive captions, income statement disclosure of cumulative revenue and expenses, and a statement of stockholder equity showing each issuance of equity securities, including dollar amounts, dollar amounts assigned for noncash consideration, the nature of noncash consideration, and the basis for assigning amounts.

The applicability of FASB Statement No. 7 is especially important for new e-businesses that might be tempted to play by their own rules, and to pick and choose between what to report and disclose. Public development stage companies are subject to article 5A of SEC Regulation S-X, which requires separate statements of assets and unrecovered promotional and development costs. Rule 12-06a of Regulation S-X allows the offset of certain proceeds and other income against promotional and development costs.

Footnote Disclosures

Under current GAAP, there are no special reporting or disclosure requirements specifically related to e-business. On the other hand, SEC reporting companies with multiple operating segments are required to report and disclose financial and descriptive information about reportable operating segments. According to paragraphs 3 and 4 of FASB Statement No. 131, *Disclosures About Segments of an Enterprise and Related Information*:

> The objective of requiring disclosures about segments of an enterprise and related information is to provide information about different types of business activities in which an enterprise engages and the different economic environments in which it operates to help users of financial statements better understand the enterprise's performance, better assess its prospects for future net cash flows, and make more informed judgments about the enterprise as a whole.
>
> The method the Board chose for determining what information to report is referred to as the management approach . . . [*which is*] based on the way that management organizes the segments within the enterprise for making operating decisions and assessing performance.

Information about the e-business activities of public companies is important and valuable information to investors. Reliable financial information about the nature of a company's e-business activities is crucial to assessing that company's future prospects. E-business activities may meet the guidelines for an operating segment, according to paragraph 10 of FASB Statement No. 131, if one of the following occurs:

- The segment engages in activities from which it may earn revenues and incur expenses.
- The enterprise's chief operation decision-maker regularly reviews its operating results.
- There is discrete financial information available.

Further, these e-business activities that meet the definition of operating segments may meet the guidelines for a reportable segment (segments for which specific disclosures are required), according to paragraph 18 of FASB Statement No. 131, if the following occur:

- The segment's reported revenue to both external customers and intersegment sales is 10 percent or more of the combined revenue of all operating segments;
- The absolute amount of reported profit or loss is 10 percent or more of the combined operating profit or loss; or

- Its assets are 10 percent or more of the combined assets of all operating segments.

FASB Statement No. 131 is not intended to discourage the disclosure of additional information about e-business activities. Audited information disclosed in the notes to the financial statements that investors may use to value e-business companies, such as Web site traffic, growth in customer base, customer retention ratios, and employee turnover, could help dampen stock market volatility by improving the quality of information available to investors.

On a related matter, as noted in the "Long-Lived Assets, Including Goodwill and Intangibles" section of this Alert, FASB Statement No. 142, *Goodwill and Other Intangible Assets*, requires public and nonpublic companies to test goodwill for impairment at least annually at the "reporting unit" level. A reporting unit is defined as "an operating segment or one level below an operating segment." FASB Statement No. 142 further requires specific disclosures about goodwill and other intangible assets at the reporting unit or operating segment level.

Asset Impairment

Moving sales and distribution networks to the Internet can displace existing traditional distribution channels, deconstruct industries and companies, and cause assets to lose significant value. For example, e-business can threaten existing branch office operations, travel agencies, bookstores, stockbrokers, insurance agents, music distributors, automobile dealerships, and newspaper classified advertising departments. Where does the auditor come into play in all of this? Auditors of businesses subject to deconstruction by the Internet need to consider whether management has appropriately accounted for asset values that have been impaired. FASB Statement No. 144, *Accounting for the Impairment or Disposal of Long-Lived Assets*, provides you with some relevant guidance.

FASB Statement No. 144 supersedes FASB Statement No. 121 and the accounting and reporting provisions of APB Opinion No. 30, *Reporting the Results of Operations—Reporting the Effects of Disposal of a Segment of a Business, and Extraordinary, Unusual,*

and Infrequently Occurring Events and Transactions, for the disposal of a segment of a business (as previously defined in the Opinion). This Statement also amends ARB51, *Consolidated Financial Statements*, to eliminate the exception to consolidation for a subsidiary for which control is likely to be temporary.

FASB Statement No. 144 retains the requirements of FASB Statement No. 121 to (1) recognize an impairment loss only if the carrying amount of a long-lived asset is not recoverable from its undiscounted cash flows and (2) measure an impairment loss as the difference between the carrying amount and the fair value of the asset. To resolve implementation issues, the Statement:

- Removes goodwill from its scope and, therefore, eliminates the requirement of FASB Statement No. 121 to allocate goodwill to long-lived assets to be tested for impairment.
- Describes a probability-weighted cash-flow estimation approach to address situations in which alternative courses of action to recover the carrying amount of a long-lived asset are under consideration or a range is estimated for the amount of possible future cash flows.
- Establishes a "primary asset" approach to determine the cash-flow estimation period for a group of assets and liabilities that represents the unit of accounting for a long-lived asset to be held and used.

The accounting model for long-lived assets to be disposed of by sale is used for all long-lived assets, whether previously held and used or newly acquired. That accounting model retains the requirement of FASB Statement No. 121 to measure a long-lived asset classified as held for sale at the lower of its carrying amount or fair value less cost to sell and to cease depreciation. Therefore, discontinued operations are no longer measured on a net realizable value basis, and future operating losses are no longer recognized before they occur.

According to paragraph 8 of FASB Statement No. 144:

> A long-lived asset (asset group) shall be tested for recoverability whenever events or changes in circumstances indicate that its carrying amount may not be recoverable.

A significant adverse change in the business climate is one example that paragraph 8 of FASB Statement No. 144 provides to determine whether it is necessary to assess the recoverability of an asset. Some assets, particularly legacy software and hardware systems, or even relatively recently installed enterprise resource planning, network operating, and software systems, have been rendered obsolete by changing technology and may have fair values that are significantly less than book value. In addition to single assets, FASB Statement No. 144 also applies to groups of assets.

The provisions of FASB Statement No. 144 are effective for financial statements issued for fiscal years beginning after December 15, 2001, and interim periods within those fiscal years, with early implementation encouraged. The provisions of the Statement generally are to be applied prospectively.

Recent Auditing and Attestation Pronouncements and Other Guidance

Presented below is a list of auditing and attestation pronouncements, guides, and other guidance issued since the publication of last year's Alert. For information on auditing and attestation standards issued subsequent to the writing of this Alert, please refer to the AICPA Web site at www.aicpa.org/members/div/auditstd/technic.htm. You may also look for announcements of newly issued standards in the *CPA Letter*, *Journal of Accountancy*, and the quarterly electronic newsletter, *In Our Opinion*, issued by the AICPA Auditing Standards team and available at www.aicpa.org.

SAS No. 95	*Generally Accepted Auditing Standards*
SAS No. 96	*Audit Documentation*
SAS No. 97	*Amendment to Statement on Auditing Standards No. 50,* Reports on the Application of Accounting Principles
SAS No. 98	*Omnibus Statement on Auditing Standards—2002*
SAS No. 99	*Consideration of Fraud in a Financial Statement Audit*

(continued)

SAS No. 100	*Interim Financial Information*
SOP 02-1	*Performing Agreed-Upon Procedures Engagements That Address Annual Claims Prompt Payment Reports as Required by the New Jersey Administrative Code*
SSAE No. 11	*Attest Documentation*
SSAE No. 12	*Amendment to Statement on Standards for Attestation Engagements No. 10*, Attestation Standards: Revision and Recodification
SQCS No. 6	*Amendment to Statement on Quality Control Standards No. 2*, System of Quality Control for a CPA Firm's Accounting and Auditing Practice
Audit Guide	*Service Organizations: Applying SAS No. 70, as Amended*
Audit and Accounting Guide	*Audits of State and Local Governments (GASB 34 Edition)*
Audit Interpretation No. 4 of SAS No. 70	"Responsibilities of Service Organizations and Service Auditors With Respect to Forward-Looking Information in a Service Organization's Description of Controls"
Audit Interpretation No. 5 of SAS No. 70	"Statements About the Risk of Projecting Evaluations of the Effectiveness of Controls to Future Periods"
Audit Interpretation No. 12 of SAS No. 1	"The Effect on the Auditor's Report of an Entity's Adoption of a New Accounting Standard That Does Not Require the Entity to Disclose the Effect of the Changes in the Year of Adoption"
Audit Interpretation No. 14 of SAS No. 58	"Reporting on Audits Conducted in Accordance With Auditing Standards Generally Accepted in the United States of America and in Accordance With International Standards on Auditing"
Auditing Interpretation No. 15 of SAS No. 58	"Reporting as Successor Auditor When Prior-Period Audited Financial Statements Were Audited by a Predecessor Auditor Who Has Ceased Operations"
Related-Party Toolkit	*Accounting and Auditing for Related Parties and Related Party Transactions: A Toolkit for Accountants and Auditors*
Practice Alert No. 02-1	*Communications With the Securities and Exchange Commission*
Practice Alert No. 02-2	*Use of Specialists*
Practice Alert No. 02-3	*Reauditing Financial Statements*

Practice Aid	*Fraud Detection in a GAAS Audit: SAS No. 99 Implementation Guide*
Practice Aid	*New Standards, New Services: Implementing the Attestation Standards*
Practice Aid	*Assessing the Effect on a Firm's System of Quality Control Due to a Significant Increase in New Clients and/or Experienced Personnel*
Booklet	*Understanding Audits and the Auditor's Report: A Guide for Financial Statement Users*

The following summaries of available guidance might have particular significance in the e-business environment. The summaries are for informational purposes only and should not be relied on as a substitute for a complete reading of the applicable standards. To obtain copies of AICPA standards and guides, contact the Member Satisfaction Center at (888) 777-7077 or go online at www.cpa2biz.com.

SAS No. 99, *Consideration of Fraud in a Financial Statement Audit*

As noted previously in the "Consideration of Fraud" section of this Alert, SAS No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316), supersedes SAS No. 82, *Consideration of Fraud in a Financial Statement Audit*; amends SAS No. 1 (AU sec. 230, "Due Professional Care in the Performance of Work"); and amends SAS No. 85, *Management Representations*. The Statement does not change the auditor's responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud as stated in SAS No. 1 (AU sec. 110.02, "Responsibilities and Functions of the Independent Auditor").[8] However, SAS No. 99 establishes standards and provides guidance to auditors

8. The auditor's consideration of illegal acts and responsibility for detecting misstatements resulting from illegal acts is defined in SAS No. 54, *Illegal Acts by Clients* (AICPA, *Professional Standards*, vol. 1, AU sec. 317). For those illegal acts that are defined in that Statement as having a direct and material effect on the determination of financial statement amounts, the auditor's responsibility to detect misstatements resulting from such illegal acts is the same as that for errors (see SAS No. 47, *Audit Risk and Materiality in Conducting an Audit* [AICPA, *Professional Standards*, vol. 1, AU sec. 312]), or fraud.

in fulfilling that responsibility, as it relates to fraud, in an audit of financial statements conducted in accordance with GAAS.[9]

Among other things, SAS No. 99 also includes Exhibit 1, "Management Antifraud Programs and Controls: Guidance to Help Prevent, Detect, and Deter Fraud." This document was developed by the AICPA and other sponsoring organizations to assist management, audit committees, and board of directors to better understand the types of programs and controls that would be effective in preventing and deterring fraud. The document has been included with the SAS to assist auditors in obtaining an understanding of programs and controls that management and those with corporate governance responsibility may use to mitigate specific risks of fraud, or that otherwise help to prevent, deter, and detect fraud. SAS No. 99 also revises the guidance for management representations about fraud currently found in SAS No. 85, *Management Representations.*

SAS No. 99 is effective for audits of financial statements for periods beginning on or after December 15, 2002. Early application is permissible. (See related discussion in the previous section of this Alert, "Consideration of Fraud.")

The AICPA is completing a fraud Practice Aid titled *Fraud Detection in a GAAS Audit—SAS No. 99 Implementation Guide* that will be published by the end of 2002. The Practice Aid addresses such topics as how the new SAS changes audit practice, characteristics of fraud, understanding the new SAS, best practices, and practice aids, including specialized industry fraud risk factors, common frauds, and extended audit procedures. Auditors should be on the lookout for this new publication.

9. Auditors are sometimes requested to perform other services related to fraud detection and prevention, for example, special investigations to determine the extent of a suspected or detected fraud. These other services usually include procedures that extend beyond or are different from the procedures ordinarily performed in an audit of financial statement in accordance with generally accepted auditing standards (GAAS). Chapter 1, "Attest Engagements," of Statements on Standards for Attestation Engagements No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol.1, AT sec. 101), and Statements on Standards for Consulting Services (AICPA, *Professional Standards*, vol. 2, CS sec. 100) provide guidance to accountants relating to the performance of such services.

Audit Guide *Service Organizations: Applying SAS No. 70, as Amended*

The objective of this Guide recently issued by the AICPA is to help auditors implement SAS No. 70, as amended. Guidance included is for service auditors engaged to issue reports on a service organization's controls that may be part of a user organization's information system in the context of an audit of financial statements. In addition, the guidance is for user auditors engaged to audit financial statements of entities that use service organizations.

Some of the new elements included in the revised Guide are illustrative control objectives for various types of service organizations as well as three recently issued audit interpretations that address the responsibilities of service organizations and service auditors with respect to forward-looking information and the risk of projecting evaluations of controls to future periods. The Guide also clarifies that the use of a service auditor's report should be restricted to existing customers and is not meant for potential customers.

> **Help Desk**—You can obtain the Guide by contacting the AICPA at (888) 777-7077 and requesting product number 012772kk or by going online at www.cpa2biz.com.

Accounting Pronouncements and Guidance Update

Presented below is a list of recently issued accounting pronouncements and other guidance issued since the publication of last year's Alert. See the general AICPA *Audit Risk Alert—2002/03* (product no. 022333kk) for a summary explanation of these issuances. For information on accounting standards issued subsequent to the writing of this Alert, please refer to the AICPA Web site at www.aicpa.org, and the FASB Web site at www.fasb.org. You may also look for announcements of newly issued standards in the *CPA Letter* and the *Journal of Accountancy.*

FASB Statement No. 145	*Rescission of FASB Statements No. 4, 44, and 64, Amendment of FASB Statement No. 13 and Technical Corrections*
FASB Statement No. 146	*Accounting for Costs Associated with Exit or Disposal Activities*
FASB Statement No. 147	*Acquisitions of Certain Financial Institutions*
SOP 01-5	*Amendments to Specific AICPA Pronouncements for Changes Related to the NAIC Codification*
SOP 01-6	*Accounting by Certain Entities (Including Entities With Trade Receivables) That Lend to or Finance the Activities of Others*

On the Horizon

You should keep abreast of auditing and accounting developments and anticipated guidance that may affect your engagements. In considering exposure drafts toward this end, remember that they are nonauthoritative and cannot be used as a basis for changing GAAP or GAAS.

FASB Issues EDs Related to Stock-Based Compensation

In October 2002, the FASB issued an exposure draft, *Accounting for Stock-Based Compensation: Transition and Disclosure—an Amendment of FASB Statement No. 123.* The proposed standard would amend the transition and disclosure provisions of FASB No. 123 but would not amend its recognition and measurement provisions. In addition, in November 2002, the FASB issued an exposure draft, *Accounting for Stock-Based Compensation: A Comparison of FASB Statement No. 123, Accounting for Stock-Based Compensation, and Its Related Interpretations, and IASB Proposed IFRS, Share-based Payment.* For more information about these proposed standards, go to the FASB Web site at www.fasb.org. (See discussion of Stock Options in the previous "Stock Options" section of this Alert.)

AICPA Resource Central

The following publications deliver valuable guidance and practical assistance as potent tools to be used on your e-business engagements (product numbers appear in parentheses).

- AICPA general *Audit Risk Alert* (022333kk)
- Audit Guide *Auditing Revenue in Certain Industries* (012510kk)
- Audit Guide *Audit Sampling* (012530kk)
- Audit Guide *Analytical Procedures* (012551kk)
- Practice Aid *Auditing Estimates and Other Soft Accounting Information* (010010kk)
- *Accounting Trends and Techniques—2002* (009894kk)
- Practice Aid *Preparing and Reporting on Cash- and Tax-Basis Financial Statements* (006701kk)
- Practice Aid, *Assets Acquired in a Business Combination to Be Used in Research and Development Activities: A Focus on Software, Electronic Devices, and Pharmaceutical Industries* (006609kk)

Audit and Accounting Manual

The *Audit and Accounting Manual* (product no. 005132kk) is a valuable nonauthoritative practice tool designed to provide assistance for audit, review, and compilation engagements. The Manual contains numerous practice aids, samples, and illustrations, including audit programs; auditors' reports, checklists, and engagement letters; management representation letters; and confirmation letters.

AICPA reSOURCE: Online Accounting and Auditing Literature

Get access—anytime, anywhere—to the AICPA's latest *Professional Standards, Technical Practice Aids*, Audit and Accounting Guides (more than 20), Audit Risk Alerts (more than 15) and *Accounting*

Trends and Techniques. To subscribe to this essential online service for accounting professionals, go to www.cpa2biz.com.

Educational Courses

The AICPA has developed a number of continuing professional education (CPE) courses that are valuable to CPAs working in the e-business environment. Those courses include (product numbers are in parentheses):

- *AICPA's Annual Accounting and Auditing Workshop* (2002–2003 edition) (737082kk, text; 187082kk, video). Whether you are in industry or public practice, this course keeps you current and informed, and shows you how to apply the most recent standards.
- *The AICPA's Guide to Consolidations and Business Combinations* (735125kk). Learn how FASB Statements No. 141 and No. 142 have changed the rules for business combinations and goodwill accounting.
- *E-Commerce: Controls and Audit* (731551kk). Do you want to have a basic, yet comprehensive overview of the world of e-commerce? If so, this is the self-study course for you.
- *Guide to XBRL* (731111kk). XBRL (eXtensible Business Reporting Language) has sweeping implications for CPAs in industry and in public practice. The course begins with a big-picture introduction, then covers the enabling technologies, XBRL itself, and the strategic issues.
- *Auditing in a Paperless Society* (730121kk). Now that paper is slowly diminishing, where do you go? This course will teach you how to develop strategies for auditing around, through, and with a computer.

Online CPE

The AICPA offers an online learning tool titled *AICPA InfoBytes.* An annual fee ($119 for members and $319 for nonmembers) offers unlimited access to hundreds of hours of CPE content in

one- and two-credit courses. Register today at www.cpa2biz.com/infobytes.

CPE CD-ROM

The Practitioner's Update (product no. 738110kk) CD-ROM helps you keep on top of the latest standards. Issued twice a year, this cutting-edge course focuses primarily on new pronouncements that will become effective during the upcoming audit cycle.

Member Satisfaction Center

To order AICPA products, receive information about AICPA activities, and find help on your membership questions, call the AICPA Member Satisfaction Center at (888) 777-7077.

Technical and Ethics Hotlines

Do you have a complex technical question about GAAP, OCBOA, accounting, auditing, compilation engagements, review engagements, or other technical matters? If so, use the AICPA's Accounting and Auditing Technical Hotline. AICPA staff will research your question and call you back with their answer. You can reach the Technical Hotline at (888) 777-7077.

In addition to the Technical Hotline, the AICPA also offers an Ethics Hotline. Members of the AICPA's Professional Ethics Team answer inquiries concerning independence and other behavioral issues related to the application of the AICPA Code of Professional Conduct. You can reach the Ethics Hotline at (888) 777-7077.

Conference: The Business of E-Business

Among the many conferences the AICPA offers, there is one that might interest you or your e-business clients: the AICPA/ISACA/MIS Training Institute—The Business of E-Business: Audit, Control, and Accounting in a Dot.Com World, which addresses the latest trends, strategies, and best practices of innovative companies involved in e-business.

For additional information, contact CPA2biz at its Web site, www.cpa2biz.com.

Web Sites[10]

AICPA Online and CPA2Biz

AICPA Online, at www.aicpa.org, informs you of developments in the accounting and auditing world as well as developments in congressional and political affairs affecting CPAs. In addition, CPA2Biz, at www.cpa2biz.com, offers you all the latest AICPA products, including more than 15 Audit Risk Alerts, more than 20 Audit and Accounting Guides, the professional standards, and CPE courses.

.....

This Audit Risk Alert replaces the *E-Business Industry Developments—2001/02 Audit Risk Alert.* The *E-Business Alert* is published annually. As you encounter audit or industry issues that you believe warrant discussion in next year's Alert, please feel free to share them with us. Any other comments that you have about the Alert would also be appreciated. You may e-mail these comments to Leslye Givarz at lgivarz@aicpa.org, or write to:

Leslye Givarz
AICPA
Harborside Financial Center
201 Plaza Three
Jersey City, NJ 07311-3881

10. Additional helpful Web sites are presented in Appendix C.

APPENDIX A

Identifying and Managing E-Business Risks

Risks in E-Business

Business risk is a term used to describe the risk inherent in a firm's operations. If a firm engages in e-business, its business risk typically changes in nature and increases. This is a result of the risks associated with e-business, such as increased reliance on technology and the fact that this technology changes rapidly. Deloitte and Touche, LLP, has identified common risk-increasing characteristics of firms engaged in e-business.[1] Some of these characteristics include the following:

- Rapid growth
- Mergers and acquisitions
- Formations of new partnerships
- Obtaining financing through debt and equity offerings and/or initial public offerings
- Upgrading and installing new technology
- Taking new products to market
- Complex information systems
- Changes in management
- Regulatory compliance difficulties
- Increasingly complex business models and processes

Any firm's risk management program should be comprehensive enough to encompass the risks stemming from these characteristics. However, effectively managing these risks is an increasingly high priority for e-business firms because they are currently more likely than other firms to exhibit these characteristics.

1. *Enterprise Risk Services*, Deloitte and Touche LLP, 1998.

Remember, e-business is not only the buying and selling of goods and services over the Internet. Any electronic transfer of information that facilitates a company's operations can be termed e-business. Consequently, the risks of e-business are as broad as the term itself. However, the general categories of e-business risk can be summarized as follows:[2]

- IT infrastructure vulnerabilities
- Falsified identity
- Compromised privacy
- Destructive or malicious code
- System interdependencies

Information Technology Infrastructure Vulnerabilities

One of the primary sources of risk facing e-business firms stems from vulnerability in the organization's IT infrastructure—the hardware, software, and processes that allow day-to-day operations to be carried out. Other risks associated with infrastructure vulnerabilities include the following:

- Denial-of-service attacks, such as the one experienced by Yahoo and others
- Physical outages, such as those caused by hardware failures
- Design failures, such as in February 2000, when the NASDAQ suffered an outage because a problem in a communications feed to one of its mainframe computers froze the NASDAQ Composite Index for two-and-a-half hours
- Operations failures, such as errors or malicious acts by operations personnel
- Environmental outages, such as those caused by natural disasters

2. Steven M. Glover, Stephen W. Little, and Douglas F. Prawitt. *E-Business Principles and Strategies for Accountants.* Englewood Cliffs, N.J.: Prentice Hall, 2001.

- Reconfiguration outages, such as those caused by software upgrades, database maintenance, or hardware changes

Controlling Risks Associated With Infrastructure Vulnerabilities

Companies stand to lose millions of dollars in equipment, software, and sensitive information when a disaster strikes. Enterprises should prepare to minimize the effects of disasters by having a good disaster recovery plan. In addition to a good disaster recovery plan, e-businesses may use software-based security packages as an integral part of controlling the risks associated with infrastructure vulnerabilities. There are several different types of software security packages, including the following:

- *Firewalls.* Software applications designed to block unauthorized access to files, directories, and networks.
- *Intrusion detection software.* Applications that constantly monitor a system and its components and notify users of unauthorized entrance into a system.
- *Scanners or security probes.* Applications that test the strength of security measures by actively probing a network for vulnerabilities. (The SATAN and COPS probes, available for free on the Internet, are examples of general security probes.)

Other ways to protect an organization from the risk associated with infrastructure vulnerabilities include the encryption of information, physical controls, and use of passwords (with periodic password change requirements).

Falsified Identities

Falsified identity is a major source of exposure and risk in conducting e-business. For an electronic transaction to take place, each party to the transaction needs to be confident that the claimed identity of the other party is authentic. These threats are less of a concern in traditional electronic data interchange environments because they involve relatively limited access points, dedicated

lines, and established network providers as intermediaries. But authenticity is a significant concern for transactions conducted in an Internet-based environment. The following are examples of risks associated with identification and authenticity:

- *E-mail spoofing.* Hackers can hide their identity simply by changing the information in an e-mail header. In addition, e-mail spoofing can be associated with virus transfers and "spam" mail.
- *IP spoofing.* Some security measures, such as firewalls, may be configured to disallow access to incoming requests with certain IP addresses. By changing the IP address to one that the security system will not block, an unauthorized person can sometimes gain access to the system.
- *Customer impersonation.* Like traditional businesses that accept checks or credit cards, e-businesses face the burden of verifying customer identity. If a consumer has falsified his or her identity, businesses can lose money on fraudulent requests for products or services.
- *False Web sites.* Also called false storefronts, false Web sites are set up to grab confidential information, leading to further misdeeds.

Controlling the Risks Associated With Falsified Identity

The evolution of e-business has caused a shift in the area of identity issues. With the emergence of the Internet as the primary vehicle for e-business, the potential exists for a virtually unlimited number of parties to attempt to initiate transactions. Some of the controls available for authentication and identification in the e-business environment include the following:

- *Digital signatures and certificates.* Just as a signature on a paper document serves as the authentication or certification of a procedure or important information, a digital signature provides beneficiaries assurance that the transaction is valid.

- *Biometrics.* One of the most promising areas of technology and systems security is biometrics, the use of unique features of the human body to create secure access controls. Because each person possesses unique biological characteristics (for example, iris and retina patterns, fingerprints, voice tones, and writing styles), scientists have been able to develop specialized security devices that are highly accurate in authenticating an individual's identity.

Compromised Privacy

Consumers remain concerned that their privacy may be violated if they engage in e-business transactions. Several surveys have found that consumers' biggest concerns are privacy and security. Privacy risks are of concern to e-businesses because (1) consumers who are not confident that their personal information will be kept secure and confident are less likely to transact business with an e-business company and (2) e-businesses that either purposefully or inadvertently share customers' personal information with third parties may be exposed to legal liability and litigation.

Controlling the Risks Associated With Compromised Privacy

E-businesses interested in protecting the privacy of their customers should develop and implement effective privacy policies. Given the fact that many e-businesses are guilty of violating their own privacy policy, e-businesses that are serious about enhancing customers' confidence that their privacy will be preserved sometimes purchase independent third-party assurance services.

Destructive or Malicious Code

Regardless of their origins, harmful codes and programs have the potential to shut down entire networks and cause huge costs in the form of lost sales and productivity. The following table provides an overview of some harmful codes and programs.

Common Destructive Codes and Programs

Type	*Characteristics*	*Example*
Virus	This software was designed to replicate itself and spread from location to location without user knowledge. A virus usually attaches itself to a system in such a way that it is activated when a part of the system is activated.	The "Love Bug" virus was designed to attack users of the Microsoft Outlook® mail program.
Worm	Worms are similar to viruses except that worms do not replicate themselves. Worms are created to destroy or change data within a system.	The "Code Red" worm was designed to attack computers using Microsoft's Internet Information Server®.
Trojan horse	This malicious program appears to be a legitimate program or file. When the "legitimate" file is activated, the program is activated, detaches itself, and damages the system that activated it.	
Hoax	A file or message is sent out claiming to be a virus but it is really not a virus.	A Valentine's Day hoax read as follows: "Read this immediately...on February 14, 2000, you may receive an e-mail that says 'Be My Valentine.' Do not open it...it contains a deadly virus...it will erase all of your Windows files."
Logic bomb	This code is inserted into an operating system or application that causes a destructive or security-compromising activity whenever certain conditions are met.	The famous Michelangelo virus was embedded in a logic bomb. The virus was triggered on the artist's birthday, March 6.
Trap door	This illegitimate access is created by programmers enabling easy navigation through software programs and data without going through normal security procedures.	Trap doors are sometimes very useful in systems development, but programmers sometimes fail to close trap doors on completion of a project.

Cross-site scripting	Malicious code is embedded on Web pages with tiny "scripting" programs that make sites more interactive. An unsuspecting Web site visitor then activates the hacker's program by using the corrupted scripting program.	In August, a hacker used cross-site scripting to wipe out desktop icons of Web users visiting Price Lotto, a Japanese auction site.

System Interdependencies

System interdependencies expose e-businesses to risks that come from outside traditional organizational boundaries. E-business often involves highly interdependent relationships with customers, suppliers, and various service providers. These partnerships are vital, but the interdependent nature of these partnerships means that the risks an enterprise faces are at least partly determined by how well partners identify and mitigate the risks to their systems.

Because the quality of a partnership depends heavily on the quality of each partner's information systems, as well as on the communication system between partners, organizations must ensure that their information systems are well managed and controlled. In addition, an e-business must also ensure that the information systems of its critical partners allow for the safe acquisition, processing, storage, and communication of important information. Thus, in an e-business environment, organizations must realize their responsibility to ensure that their trading partners are using effective risk identification and management processes to protect the strength and integrity of the entire network of interdependent enterprises.

APPENDIX B

Trust Assurance Services

During the past five years, the AICPA and Canadian Institute of Chartered Accountants (CICA) introduced Principles and Criteria to address concerns in the marketplace for assurance around systems reliability and e-commerce activities. These were specifically applicable to two AICPA/CICA assurance services: SysTrust and WebTrust. Although these two initial Principles and Criteria frameworks were very similar, there were a number of differences relating to structure and style. As well, in some cases, the two sets of Principles and Criteria targeted the same basic business concerns (for example, both services provided assurance around security and availability).

After assessing the objectives of SysTrust and WebTrust, the AICPA and CICA decided that the next step in the evolution was to harmonize the underlying Principles and Criteria where commonalities existed and to conform the presentation and wording of the material. To facilitate this change, the separate SysTrust and WebTrust Task Forces were merged to form the Trust Services Task Force. Its first objective was to harmonize the Principles and Criteria and to conform the wording and structure. It was not the goal or intent to change the SysTrust or WebTrust services, or to introduce additional branded services as part of this first task.

The AICPA's Assurance Services Executive Committee and the CICA's Assurance Service Development Board have developed a framework for the development of new services. This framework recognizes that there is a need and an opportunity to build a broad range of professional services in diverse areas. Consequently, the task force issued an exposure draft to accomplish this harmonization.

Due to its unique nature and specific requirements, the Principles and Criteria for WebTrust for Certification Authorities continues as a stand-alone program and is not included as part of this harmonization.

What Are the Significant Changes?

The WebTrust and SysTrust products/services remain unchanged as examination level (audit) assurance services. WebTrust continues to enable assurance on electronic commerce systems. SysTrust continues to enable assurance on any system. As noted above, agreed-upon procedure engagements can be performed using the Trust Services Principles and Criteria that would not result in the issuance of a WebTrust/Systrust seal/logo.

The task force believes that there has been no substantive change in the scope of work necessary to perform WebTrust or SysTrust engagements. There has been a significant change, however, in the structure, order and wording of the prior Principles and Criteria to achieve the harmonization required.

The following highlights the key changes made as a result of the harmonization of the Principles and Criteria that underscored SysTrust and WebTrust.

Common Set of Principles and Criteria

The SysTrust and WebTrust Principles and Criteria have been harmonized to create a common set of Principles and Criteria, now labeled as the Trust Services Principles and Criteria. No principles have been added. In fact, the criteria for the Principle of Maintainability that existed in the SysTrust Principles have been subsumed under the other principles in the appropriate sections. Therefore, the proposed harmonized set of Principles consists of Security, Availability, Processing Integrity, Online Privacy, and Confidentiality.

Separation of the Measurement Criteria from the Specific Services

The Principles and Criteria have been separated from the specific products and services (that is, SysTrust and WebTrust). Previously they were embedded in the respective service. This separation

creates the opportunity to develop additional branded products and services based on the measurement criteria. The Trust Services Principles and Criteria are considered suitable criteria as defined by professional literature.

Minimum Initial Reporting Period

Previously, under the SysTrust program, there was no defined initial reporting period. In WebTrust 3.0, a minimum reporting period of two months was recommended. This two-month minimum requirement is now applicable to Systrust engagements.

Controls Reporting Illustrated

Under the WebTrust 3.0 model, the practitioner's report covered management's assertion that an entity disclosed its practices for electronic commerce transactions, complied with such practices, and maintained effective controls. Under SysTrust 2.0, the practitioner's report covered management's assertion that they maintained effective controls. While the examples provided in the exposure draft illustrate the use of reporting on controls only, the Task Force continues to consider the appropriateness of both models. The final release is expected to embrace the original reporting models described for WebTrust 3.0 and SysTrust 2.0.

No Cumulative Reporting

Under WebTrust 3.0, cumulative reporting was an option. Under the new reporting guidelines, it is no longer available. Additional conforming changes have been made to reflect that the services offered are based on a common set of Principles and Criteria.

Consistent Seal Process for Trust Services

WebTrust 3.0 was designed to incorporate a seal management process whereby the WebTrust seal could be used as an electronic

representation of the practitioner's unqualified WebTrust report. In contrast, SysTrust did not incorporate the concept of a seal. The SysTrust logo was primarily meant to be used as a symbol for marketing purposes. Under the revised services, the WebTrust service continues to include a seal management process. Now, however, the SysTrust logo may also be used as an equivalent to a seal when the report is presented electronically, provided the issuance of the SysTrust logo as a seal follows the same procedures required to issue a WebTrust seal. Seal management procedures will be provided in the Trust Services publication to be released after the exposure period.

Periodic Examinations

The existing WebTrust service requires updates at least every six months—more frequently if needed based on changes to the e-commerce system. The existing SysTrust service does not have an update requirement. Under the new Trust Services framework, if a report is represented by a seal/logo, updates will be required at least every 12 months—more frequently if circumstances warrant it, regardless of the service. This change reflects the maturity and stability in e-commerce systems and establishes a common standard for the seal or logo.

Licensing

There were separate licensing agreements for SysTrust and WebTrust required with significantly varying requirements. The licensing of the WebTrust Services and SysTrust Services is currently being revised.

Why Change?

The Assurance Services Executive Committee and Assurance Service Development Board concluded, based on recommendations from a working group from the SysTrust and WebTrust Task Forces, that:

- There is no conceptual difference in the respective SysTrust and WebTrust Principles and Criteria taken as a whole.
- While WebTrust was the first service developed, it is, in effect, a specific application of the SysTrust framework.
- There is marketplace confusion among key stakeholders about the differences between the two services.
- There is a need to build a framework of principles and criteria that would be more flexible in meeting the needs of stakeholders in the area of e-commerce and information systems.

For these reasons, the separate SysTrust and WebTrust Task Forces were combined into the Trust Services Task Force. Its first objective was to develop the harmonized Trust Services Principles and Criteria.

Trust Services Principles and Criteria

The following principles have been developed by the AICPA and CICA for use by practitioners in the delivery of Trust Services engagements such as WebTrust and SysTrust. In the course of completing a Trust Services engagement, the practitioner uses the identified Criteria as the basis for assessing whether the particular Principle has been achieved. These principle and criteria definitions have been updated based on the expected release of the Trust Services Principles and Criteria.

Principles

- **Security.** The system[1] is protected against unauthorized access (both physical and logical).

1. A "system" consists of five key components organized to achieve a specified objective. The components are categorized as follows: infrastructure (facilities, equipment, and networks), software (systems, applications, and utilities), people (developers, operators, users, and managers), procedures (automated and manual), and data (transaction streams, files, databases, and tables).

- **Availability.** The system is available for operation and use as committed or agreed.
- **Processing Integrity.** System processing is complete, accurate, timely, and authorized.
- **Online Privacy.** Private information[2] obtained as a result of electronic commerce is collected, used, disclosed and retained as committed or agreed.
- **Confidentiality.** Information designated as confidential is protected as committed or agreed.

Criteria[3]

The Criteria associated with each of the Trust Services Principles are organized using a framework covering the following four broad categories:

- **Policies.** The entity has defined and documented its policies[4] relevant to the particular principle.
- **Communications.** The entity has communicated its defined policies to authorized users.
- **Procedures.** The entity uses procedures to achieve its objectives in accordance with its defined policies.
- **Monitoring.** The entity monitors the system and takes action to maintain compliance with its defined policies.

2. The term *private information* includes personally identifiable information and other sensitive information for which the entity has legal or other privacy obligations and commitments.
3. 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).
4. The term *policies* refers to written statements that communicate management's intent, objectives, requirements, responsibilities and/or standards for a particular subject. Some policies may be explicitly described as such, being contained in policy manuals or similarly labeled documents. However, some policies may be contained in documents without such explicit labeling, including for example, notices or reports to employees or outside parties.

The Criteria have been specifically designed to facilitate engagements related to a single Principle, or combinations of Principles to meet the client's particular needs. Where an engagement involves more than one Principle, there may be significant areas of overlap in the Criteria. In such circumstances the practitioner must be satisfied that the criteria have been achieved for each Principle, but may not need to duplicate the effort required to accomplish this.

Help Desk—For more detailed information on Trust Assurance services, go to the AICPA Assurance Services Web site at www.aicpa.org/assurance/index.htm.

APPENDIX C

The Internet—An Auditor's Research Tool

The following table gives Web sites that you may find useful to your practice.

Name of Site	*Content*	*Internet Address*
American Institute of CPAs	Summaries of recent auditing and other professional standards as well as other AICPA activities	www.aicpa.org
Financial Accounting Standards Board	Summaries of recent accounting pronouncements and other FASB activities	www.fasb.org
Governmental Accounting Standards Board	Summaries of recent accounting pronouncements and other GASB activities	www.gasb.org
Securities and Exchange Commission	SEC Digest and Statements, EDGAR database, current SEC rulemaking	www.sec.gov
FASAB	Federal Accounting Standards Board	www.fasab.gov
U.S. Federal Government Agencies Directory	A list of all federal agencies on the Internet	www.lib.lsu.edu/gov/fedgov.html
The Electronic Accountant	World Wide Web magazine that features up-to-the-minute news for accountants	www.electronicaccountant.com
CPAnet	Online community and resource center	www.cpalinks.com/
Accountant's Home Page	Resources for accountants and financial and business professionals	www.computercpa.com/
U.S. Tax Code Online	A complete text of the U.S. Tax Code	www.fourmilab.ch/ustax/ustax.html
Federal Reserve Bank of New York	Key interest rates	www.ny.frb.org/pihome/statistics/dlyrates

(continued)

Name of Site	*Content*	*Internet Address*
FirstGov	Portal through which all government agencies can be accessed.	www.firstgov.gov
Economy.com	Source for analysis, data, forecasts, and information on the United States and world economies	www.economy.com
International Federation of Accountants	Information on standards-setting activities in the international arena	www.ifac.org
Hoovers Online	Online information on various companies and industries	www.hoovers.com
Ask Jeeves	Search engine that utilizes a user-friendly question format and provides simultaneous search results from other search engines as well (for example, Excite, Yahoo, and AltaVista)	www.askjeeves.com