2001

E-business industry developments - 2001/02; Audit risk alerts

American Institute of Certified Public Accountants

AUDIT RISK ALERTS

E-Business Industry Developments—2001/02

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA

Notice to Readers

This Audit Risk Alert is intended to provide auditors of financial statements of entities that engage in e-business activities with an overview of recent industry, regulatory, and professional developments that may affect the audits they perform. The document has not been approved, disapproved, or otherwise acted upon by any senior technical committee of the AICPA.

Written by J. Russell Madray, CPA
Edited by Leslye Givarz
Technical Manager

The AICPA acknowledges and appreciates the fine contribution of J. Russell Madray, CPA, who developed this Audit Risk Alert. In addition, we thank Bruce H. Nearon, CPA, for his review of this Alert.

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

AUDIT RISK ALERTS

E-Business Industry Developments—2001/02

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA

Table of Contents

E-Business Industry Developments—2001/02

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 that industry knowledge and understanding it.

> This Alert is intended to be used in conjunction with the AICPA general *Audit Risk Alert—2001/02* (Product No. 022280kk).

E-Business Background

What do auditors need to know about the background of the e-business "industry"?

A critical component of a successful e-business audit is a comprehensive knowledge of the industry environment. The *e-business industry*, however, is almost a borderless industry—depending on how you define e-business. In addition, because of the relative infancy of this industry, standard guidelines and metrics for performance have not yet emerged. For these reasons, you should carefully consider the unique audit implications of dealing with or being in such a new and vaguely defined industry.

This Alert provides you with a glimpse into the background of the e-business environment to provide you with a frame of reference for e-business activities. 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.

Internet Beginnings

Let us begin by talking about the Internet. Throughout this Alert, the term *Internet* means the interconnected system of networks that connects computers around the world via the transfer control protocol/Internet protocol (TCP/IP).[1] The Internet is a vast global interconnected network of computers—literally a network of networks—owned by no single entity and accessible to anyone with a means to connect to it.

The Internet was first developed in 1969 for military research scientists at universities and defense labs as decentralized computer networks that could survive a nuclear attack. Then, in 1972, electronic mail (e-mail) service was added to the Internet. By the mid 1970s, it was apparent that use of the Internet was a very effective method for collaboration on research projects and sharing news and messages of a personal nature. Through the 1970s, the network grew, largely as a result of use by governments and educational institutions. Businesses began investigating the commercial potential of the Internet in the 1980s. Introduction of the World Wide Web[2] (the Web) in the 1990s, with its point-and-click links, and the subsequent opening of the Internet to commercial use, catapulted the Internet into everyday living and made e-business a viable medium for consumers. Individuals and businesses scrambled to conduct business online, and that trend continues.

1. *The American Heritage Dictionary of the English Language.* Boston: Houghton Mifflin Company, 4th edition, 2000.

2. The *World Wide Web* means an information server, or service computer on the Internet composed of interconnected sites and files, accessible with a browser, which is a program that accesses and displays files available on the Web.

E-Business Defined

Before going further, e-business and the related term, e-commerce, must be described in more detail.

E-Business

In general, e-business is defined as the use of information technology (IT) and electronic communication networks to exchange business information and conduct transactions. A more precise notion of the term e-business means business to vendors, customers, employees, and suppliers via intranets, extranets, and the Internet.[3] An expansion of the definition of e-business encompasses conducting business using electronic and IT (including telephone and fax), instead of limiting the means of doing business to paper or mail.

This Alert accepts the wider definition of e-business that includes all business functions that use Internet technologies, including business-to-business (B2B) and business-to-consumer (B2C) transactions.

E-Commerce

E-commerce is only a small subset of e-business and is defined differently by different organizations. For example, in 1997, the AICPA's Assurance Services Committee defined e-commerce broadly enough to include individuals and organizations conducting business transactions electronically over public or private networks. That definition includes electronic data interchange (EDI) and bulletin board services (BBSs). In 2000, the Information Security and Control Association (ISCA) limited the definition of e-commerce to transactions conducted over the Internet. The U.S. Census Bureau defines e-commerce as the value of goods and services sold online. The general public, media, and businesspeople commonly accept an even more restrictive concept of e-commerce by limiting its definition to mean online B2C retail sales conducted over the Internet.

3. *Intranets* are privately maintained computer networks that can be accessed only by authorized persons, such as members or employees of the organization; *extranets* are Web sites that an e-business sets up for its prospective and current trading partners, accessible to registered users, with a user identification (ID) and password.

Regardless of whether e-commerce is considered to include a wide range of transactions or a more limited range, the emphasis in this Alert when referring to e-commerce is on the B2C aspect of the Internet transactions being conducted.

Use of Internet Technologies for Business Functions

Internet technologies include the following:

- The use of graphical user interface (GUI) Web browsers as the interface by end users
- The Internet's packet switching network as the communications medium
- Internet routers to route information between different networks using hypertext transfer protocol (HTTP) and TCP/IP
- Web servers, hypertext mark-up language (HTML), extensible mark-up language (XML), and extensible business reporting language (XBRL) to publish information

Many companies adopting e-business strategies make Internet technologies the heart of their information system. The use of Internet technologies extends beyond marketing, sales, and consumer services to include other business functions and services. The rapid growth in e-business clearly indicates that potential benefits greatly exceed costs. The following sections examine a few of these functions in detail.

Using E-Business to Increase Brand Awareness and Expand Sales Opportunities

The brand is one of the most valuable of an entity's assets. Entities use e-business to increase brand awareness. By designing a corporate Web page with their logo, mission, and other corporate information, companies can uniquely identify themselves. E-business also can allow an entity to open additional sales channels to new customers or add a new storefront to a traditional brick-and-mortar company. In addition, companies can use e-business

to provide product information, technical support, and order information, all of which frees sales personnel to pursue higher value activities that generate new sales. Think about a bank customer who can access account information and initiate transfers or payments via the bank's Web site, rather than working directly with a bank teller. The teller, then, is free to sell new services to other bank customers or potential new bank customers.

Using E-Business to Improve Communications and Customer Service

With Internet technologies, companies can provide product descriptions, facilitate order placement, and allow for tracking order status. In addition, direct and customized product promotion is possible. For example, ticketmaster.com e-mails customers the play list from the most recent concert they attended with an offer to sell a concert T-shirt. Companies using the Internet can also slash customer service costs dramatically by providing a frequently asked questions (FAQ) page and an e-mail customer service form or even by having chat sessions with customer service reps, who can carry on eight to ten conversations at once via the keyboard. In addition, many companies include "call back" buttons on their Web sites. When a user clicks the button and enters a phone number, software forwards the information to a call center, and a representative calls the customer directly.

Using E-Business to Enhance Purchasing and Selling Functions

When suppliers link their systems to a company's sales and inventory databases, they can automatically issue purchase orders for restocking. This capability helps eliminate out-of-stock items, decrease the amount of lost sales, and reduce inventory holding costs. Companies may be able to lower other costs as well. Procurement costs are an example. In addition, many companies use Internet technologies for supply chain and human resource management functions. Consider Home Depot, which recently automated its hiring and promotion processes by installing computer kiosks in its stores. Job seekers apply for positions at the kiosks.

The computer administers an extensive skills test and informs applicants when they are eligible for higher level positions.

Using E-Business to Create Customer-Perceived Benefits

Internet technologies allow for more efficient and convenient transactions. E-business also allows for the customization of information, products, and delivery to fit individual desires. Consider amazon.com. Once a shopper locates a book at amazon.com, the company also provides the shopper with recommendations for other similar offerings. Some companies provide other benefits, including customized and personalized product feedback. (For instance, landsend.com includes a three-dimensional model builder to let customers see how clothes would potentially look on a particular body type.) A number of companies are using the Internet to increase price competition, as is the case with priceline.com. Still others are using the Internet to offer increased product or vendor selection, as noted in the case of W.W. Granger, a provider of machine maintenance and repair supplies, which formerly offered customers a single option—a 4,000-page catalog listing 70,000 products. Now, on the grainger.com Web site, users can search electronically through even more products (220,000) in a fraction of the time, and can even determine whether a particular product is in stock.

E-Business Risks

What is the tradeoff for all of the benefits of e-business?

Although the previous section paints a somewhat rosy picture of e-business in terms of the benefits of the services and opportunities it provides, risk is the tradeoff that is sometimes necessary to obtain them. Although many of the risks faced by e-business enterprises are common to all businesses, some are unique. Examples include the daily reminders of the risk associated with various computer viruses, "denial of service" attacks, and other threats to revenues and assets.

Special e-business risks can stem from an enterprise's 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, and destructive programs. 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

How are companies using e-business? What is meant by B2C and B2B?

There are many e-business models, encompassing B2C transactions, B2B transactions, and variations on these themes. The variety of e-business models is limited only by entrepreneurial vision. Companies are constantly innovating to compete in the marketplace.

Business-to-Consumer Models

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. For example, W.W. Grainger, a B2B catalog company, uses the Web as a much more efficient delivery vehicle for its catalog business. Although we normally think of online catalogs as a B2C model, in many cases, B2B companies use online catalogs as an efficient way to deliver products and services to their business customers. The point here is that many B2C models, with some modification, also work well in the B2B space.

Business-to-Business Models

Besides the significant shift in customer profile in the B2B market, to fewer and larger B2B customers, B2B customers are also likely to be involved in trade, not just purchase. B2B companies make money not just by selling their products and services, but also by becoming more efficient in their interactions with trading partners. At the core of B2B e-business models is the competitive advantage provided by using electronic means to transfer information. Electronic information and processes flow at lower costs and increased speeds compared to traditional information and process flow. We provide examples of several B2B models 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 also the public exchange allows purchasers and sellers to obtain the best price quotes in minutes instead of days.

  One important note is that 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 SAS No. 70, *Service Organizations* (AICPA, *Professional Standards*, vol. 1, AU secs. 324.24-.56). See the

"Reports from Service Organizations" section later in this Alert for further discussion of this issue.

- *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 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 to not only 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 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 the logging of transactions, the authentication of trading partners, as well as the integrity of information, the identification of suppliers, and the nonrepudiation of transactions using with digital signatures. See more on the issue of digital signatures later in this Alert in the "Recent Regulatory Developments" section.

E-Business Economic Environment

What is the economic outlook for e-business and e-commerce?
What is the impact on e-business of recent regulatory actions?
How is e-business changing the nature of business?

The U.S. Business Environment

As of the third quarter of 2001, even before the events of September 11, the U.S. economy was weak and its outlook uncertain. Adding further agitation and uncertainty to that weak economic picture are the untold ramifications of the September 11 attacks upon America. The effects of those attacks are likely to further unhinge consumer confidence, decrease corporate earnings, increase layoffs, and further depress the stock market. To be sure, the short-term economic picture looks unclear.

Still, the financial underpinnings of the U.S. economy remain strong. Inflation is contained, interest rates have been cut, taxes have been lowered, energy prices have fallen, and the public debt has diminished. Additionally, in response to the September 11

attacks, government stimulus measures are likely to be enacted in the form of increased spending on defense, spending on recovery efforts, direct aid to certain industries, and further tax cuts. The potential seeds of economic recovery are in place. So, although the health of the economy might appear to be uncertain and might continue to worsen before it achieves stability and then improves, the economic malaise could be short-lived and mild.

Factors Related to the Current Economic and Business Environment

Plunging Capital Spending, Tumbling Profits, Eroding Stock Market, Layoffs

The initial, primary cause of the economic slowdown was a breathtaking decline in business capital spending and investment. When the dot-com bubble burst, businesses took a more pessimistic view of the economic future and drastically curtailed their spending on equipment, software, real estate, inventories, and other business investments. The high-tech sector was one of the first to suffer the effects of that reduction in capital spending when its high-tech companies experienced earnings and share prices that nosedived.

As the drastic cutbacks in corporate spending rippled through the business environment, soaring energy prices took money out of consumers' pockets and ate into corporate earnings. Earnings throughout the business world sank, borrowing dwindled, office vacancies increased, economic growth slowed, and the stock market tumbled. Trillions of dollars of investor wealth vanished. Moreover, as earnings sank, layoffs followed. The unemployment rate rose sharply (although remaining historically low), undermining the economy's reliance on hardy consumer spending.

September 11, 2001 Attacks

In addition to causing profound personal tragedy, the September 11 attacks upon the United States were a jarring shock to the business environment, most likely causing further economic decline. The shock of September 11 was particularly severe for the tourism, hotel, airline, insurance, and restaurant industries.

Partly in response to these events, U.S. companies have initiated restructurings, inventory liquidations, and large writeoffs.

Weakening Consumer Spending

Until recently, the pillars of consumer spending and a strong housing market have supported the weakening economy. Throughout these difficult economic times, housing construction and purchases have soared, spurred on by low mortgage rates and poor investment alternatives. Despite layoffs and a deteriorating business environment, consumer spending remained robust, helped by plenty of refinancing loans. Now, however, consumer confidence has eroded somewhat, and the attacks of September 11 and their aftermath could send consumers into a full-blown retreat. The psychological effects of the attacks, continuing layoffs, and falling stock prices will most likely lend significant slowdowns in consumer spending, at least in the short term.

Some Positive Indications

While the short-term economic forecast might look grim, not all the news is negative. Certain economists have been optimistic about the long-term outlook for the U.S. business environment. As stated above, interest rates have been lowered and taxes have been slashed. Furthermore, inflation remains low, and the housing sector appears sound. Businesses have shed excess inventories, and the trade deficit is improving. Although the aftermath of September 11 could cause the price of energy to soar, the prices of natural gas, crude oil, gasoline, and electricity have fallen from earlier highs. Spending less on energy frees up capital for consumers to spend and businesses to invest. All of these factors form a favorable medium that can help the economy grow strongly.

Help to the business environment may also come in the form of government stimulus packages. As of the writing of this Alert, Congress and President Bush were considering additional individual tax cuts, business tax cuts, increased spending on defense and intelligence, expanded unemployment benefits, and subsidies to certain industries. These packages could total hundreds of

billions of dollars to help aid the economy's health. A number of economists nevertheless believe that the additional government spending will not have a substantial medicinal effect on the health of the economy. They fear that heightened government spending will lead to higher long-term interest rates and reduced private investment, thus damaging the economy.

Threats to Economic Recovery

A risk exists that the ramifications of the September 11 attacks could deepen any black hole into which business earnings might plummet. In this scenario, earnings could worsen, igniting more layoffs. Consumer spending could grind to a halt, and the stock market could erode further. Consequently, the nation's economic woes could linger on and grow worse. This could, in turn, drag down foreign economies and heighten the sense of unraveling, as discussed in the next section of this Alert.

For Better or Poorer, in Sickness and in Health—America and the Global Economy

The U.S. economy drives the world economy. The U.S. buys one-fourth of the world's exports. Indeed, 28 cents out of every dollar spent in the U.S. is spent on imported goods. The economies of America and foreign nations are intertwined and interdependent. As can then be expected, any deterioration in the U.S. business environment can and will strike foreign economies. Many of the layoffs announced by U.S. companies are cuts in overseas jobs since many U.S. firms have established and transferred manufacturing facilities and other operations abroad. Also, foreign companies, especially those that export technology equipment, have absorbed the harsh blow of reduced capital spending by American businesses.

As foreign economies weaken and suffer from the long reach of the anemic U.S. economy, global exports and imports have slackened. This in turn punishes many U.S. firms that rely on exporting their goods and services to foreign markets. U.S. multinational firms are deeply affected also, as their sales and

earnings deteriorate in the weakening economies of foreign nations. As the U.S. economy goes, so goes the world, and foreign economies will not improve until the U.S. business environment improves.

Uncertain

The economic word of the day is *uncertain.* Surely the outlook for the U.S. business environment remains uncertain. For the short term, the economy looks as if it will remain troubled and deteriorate even further. The long term could be brighter, however. As news of worldwide events continues to break in the wake of September 11, too many variables are in play to really be certain about what the economy will do. Will businesses finish liquidating inventories and resume capital spending? Will consumers start spending or will they retreat and extinguish businesses' incentive to invest? Will the stock market drift lower or turn up? Will energy prices remain stable or soar? What impact will the government's stimulus packages have on the business environment? Will the aftermath of September 11 cripple the economy, have little ultimate effect, or provide fuel for growth? Management, auditors, and many others will be seeking the answers to these questions as they assess the business environment in which they and their clients operate.

General Industry Trends

Numerous market research firms have tracked and reported information about e-business sales for several years, but the U.S. government only began officially reporting such information in late 1999. For the year 2000, the U.S. Department of Commerce reported total e-commerce sales of $25.8 billion.[4] For the first quarter of 2001, the Department of Commerce reported total e-commerce sales of $7.6 billion (compared to $5.3 billion for first quarter 2000)! This represented a 37.4 percent increase in sales

4. Recall that the Department of Commerce limits the definition of e-commerce to the value of goods and services sold online.

compared to same quarter in 2000. In the second quarter of 2001, the Department of Commerce reported total e-commerce sales of $7.5 billion, which is down slightly from the first quarter, but still represents a 24.7-percent increase over the first quarter of 2000.

Keeping in mind that e-commerce is only a small percentage of total Internet transactions (or e-business), this growth rate is still phenomenal. 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-commerce will generate $2.6 trillion in revenues by 2004—a rise from $280 billion in 2000. Gartner, Inc., forecasts that the worldwide B2B Internet commerce market should total $919 billion in 2001, $1.9 trillion in 2002, and $8.5 trillion in 2005. Gartner reports that, in 2000, the value of global B2B sales transactions was more than $433 billion, a 189-percent increase over 1999 figures. Not to be left out, small businesses (those with fewer than one hundred 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 year for many dot-com merchants, online retail sales grew 66 percent, to $44.5 billion in 2000, according to a study conducted by the Boston Consulting Group. But, in a sign of an emerging distinction among online retailers, the study concludes that mail-order catalog companies selling on the Internet are proving to be the only consistently profitable players in the business. The study, based on data for 550 retailers, notes that Internet-retail sales still represented a small portion of total retail sales at 1.7 percent, which are expected to jump to 2.5 percent in 2001.

According to a Harris Interactive survey, more than $3.5 billion was spent online in March 2001, an increase of about 36 percent from the dollars spent in April 2000. Two product categories accounted for more than half of this growth. Online travel spiked 58.5 percent to more than one billion dollars in March 2001,[5] while clothing and apparel jumped 122.3 percent to $368 million. According to another survey conducted by Harris Interactive, brick-and-mortar mass retailers are driving mainstream shoppers online. In June 2001, walmart.com attracted more than two million unique visitors online, an increase of 133 percent since June 2000. JCPenny followed, a close second, jumping 34 percent, to two million visitors. Target.com seized the highest percentage growth among the brick-and-mortar sites, a skyrocketing 142 percent compared to June 2000. Among these merchants, clothing and apparel was the top revenue generator, followed by home and garden, toys, health and beauty, and video. According to the survey, online spending across fourteen categories spiked 71 percent for all merchants in the past year to $5.3 billion in June 2001. Offline spending generated by online shopping rose to nearly $5.5 billion in the same period.

In spite of the amount of Internet activity and predictions regarding increasing e-business sales volumes, recent events suggest that the cautionary warnings given to dot-com companies doing e-business still apply. Along with the consequences of the recent tragic events of September 11, companies remain vulnerable to the unpredictable nature of investors and consumers, as noted in the next section of this Alert.

Significant Recent Developments Affecting E-Business

Continuing Market Downturn

Throughout 2000 and 2001, dot-com companies cut back, trimmed work forces, slashed expenses, and closed their doors. Some recent actions companies have taken as a result of challenges in this market include the following:

5. Keep in mind, however, that travel was one of the industries most affected by the September 11 terrorist attacks.

- *January 2001.* amazon.com cuts 1,300 jobs, or 15 percent of its work force.
- *February 2001.* After laying off 70 percent of its work force in January, eToys announces it will file for bankruptcy protection.
- *April 2001.* In what is being dubbed the most spectacular and expensive failure of the Internet era, online grocery delivery service Webvan shuts down and files for bankruptcy protection.
- *June 2001.* Despite the backing of major venture capitalist Kleiner Perkins Caufield & Byers, photo storage and display Web site zing.com closed its doors.
- *August 2001.* build.net, the Durham, NC-based provider of B2B solutions for the residential construction industry, along with six of its subsidiaries, files for bankruptcy protection.
- *September 2001.* stamps.com, the Santa Monica, CA-based leader of Internet-based postage, makes its third round of job cuts in less than a year, slashing an already depleted staff by an additional 25 percent.

The recent plunge in market value for Internet market leaders, and the even greater plunge for the dot-com companies in 2001, is compelling evidence that the premises of efficient market theory are still valid—investors are rational, markets are efficient, and price changes only reflect new information. The downturn of dot-coms occurred when the market took off its blinders and factored in the reality of going-concern issues for these companies, the vulnerability of high-tech companies to government intervention, and the real losses of dot-coms to share prices.

Light at the End of the Tunnel?

In spite of many challenges for e-business, there is promising news. For example, recently, priceline.com—the name-your-own-price travel retailer that used to be emblematic of the excesses of the Internet era—announced its first-ever profit. Other

e-business companies have also reached a milestone recently by reporting positive earnings, minus some noncash expenses. They include the online travel sites expedia.com and travelocity.com, the online brokerage firm Ameritrade, real estate listings site homestore.com, and ticketmaster.com, which does online ticketing.

However, not all of these firms meet the test of profitability by generally accepted accounting principles (GAAP). In several cases, the companies reported profitable results by reporting pro forma earnings. The term *pro forma* describes earnings that exclude some costs such as goodwill amortization, which can greatly affect earnings and profitability.[6]

What Have We Learned?

Everywhere, the once limitless potential of the Internet appears to be fading. The dot-com powerhouses that were supposed to topple industry giants have mostly vanished. And the dot-coms that are still around continue to struggle to produce a profit.

However, looking beyond the current economic and market plight, a different picture emerges. As with any new technology, the early years of the Internet have been a learning experience. We have all heard the phrase, "The Internet is going to change everything." But as we all know now, that is just not the case so far. To be sure, the Internet has changed certain industries and parts of the economy, but has not and will not change everything.

Where Are We Headed?

As discussed in the previous section on "General Industry Trends," most analysts are forecasting significant growth in the B2B sector. However, B2C continues to grow, and several paths to profit are emerging. *BusinessWeek* magazine has pinpointed these four B2C models that not only work, but work well:

6. Because of the increasing practice of reporting pro forma earnings, the FASB is considering a project to examine the practice. If the FASB decides to regulate the practice of reporting pro forma information, it would apply only to information reported in financial statements. The FASB has no authority to regulate what companies report in press releases.

- *Niche marketing.* E-businesses that focus on a niche will fare better. Profitable pet supplier Waggin' Tails specializes in high-margin products, unlike the defunct pets.com, which tried to do it all.
- *Information brokers.* The number one thing consumers look for online is information. Those that make it pay will win. The job-listing site monster.com, which charges employers to post positions, works.
- *Fence-straddlers.* Businesses in both the physical and virtual worlds win. Combining traditional brick-and-mortar retailing with online sales has allowed companies like Staples (an office supply retailer) to prevail over Internet-play-only retailers.
- *A la carte models.* Business models that boast multiple ways of making money have good odds. Real estate listing service homestore.com, which sells technology and ads, will be successful this year with projected revenues of $440 million.

It is no secret that most experts believe the real future of e-business lies in the trillions of dollars spent annually in B2B trade, but the past year has seen its share of B2B failures as well. By some estimates, more than one hundred of the public marketplaces, also called exchanges, have shut down. Analysts at Forrester Research Inc. estimate that only about two hundred of the thousand or so exchanges that existed at the peak last year will be around in two years. However, despite these failures, the following B2B models, among others, are emerging as profitable initiatives:

- *Online catalogs.* Although traditionally seen as a B2C model, online catalogs are proving to be an efficient way to deliver products and services to other businesses. For example, about 80 percent of Cisco System's orders are taken online, saving the company $760 million in annual operating costs.

- *Public marketplaces.* Transactions in public marketplaces are expected to reach $2.8 trillion in 2004, according to AMR Research. Defense contractor United Technologies bought $450 million worth of metals, motors, and other products from a public marketplace in 2000 and saved approximately 15 percent of the amount it usually pays.
- *Supply-chain management.* Businesses are predicted to buy $2.8 trillion in supplies over the Internet in 2004, excluding public marketplace purchases, says AMR Research. Eastman Chemical is buying 19 percent of its supplies online now, up from almost nothing two years ago. That has helped boost productivity 9 percent per year.
- *Knowledge management.* Companies will spend $10.2 billion to store and share their employees' knowledge over the Internet by 2004, according to IDC Research. Electronics manufacturer Siemans has spent $7.8 million to create a Web site for employees to share expertise to help win contracts. This resulted in new sales of $122 million.
- *Customer relationships.* Corporations will invest $12.2 billion by 2004 on linking customers, sales, and marketing over the Web, says META Group.

Auditors can help their e-business clients as they change their e-business models or move to new models. For example, you can help your client decide whether membership in an exchange is worth the price of admission. Or, you can help your clients understand the internal changes necessary to integrate new e-business models by identifying gaps between e-business plans and actual practice. Whether your client is implementing basic or advanced e-business models, it can benefit from your expertise as it aligns its technology plans and resources with its business needs and goals.

How the "E" Is Changing Business

E-business companies continue to experience numerous changes in the way they behave as organizations, the way they view themselves, and, importantly, what they define as valuable. In some

cases, the long-term implications of these changes are not yet clear. However, it is important to consider the following ideas as you review and develop engagement plans for the e-business industry in which your clients participate.

- *Management.* Whether in new companies or old, the ability of management to inspire and implement a plan is crucial, especially in times of rapid change like that in the e-world. But a number of theorists have suggested that the ubiquity of information that the Internet provides changes the balance of power in organizations. Knowledge becomes difficult to control and may change the managerial dynamic in some companies.

- *Corporate culture.* The challenge of management in the e-business era is to maintain a corporate culture that is strong enough to inspire innovation and loyalty, but flexible enough to withstand great changes.

- *Get bigger? Get smaller?* The Internet creates an interesting conflict between the need for scale and the need to be narrow. Because overhead does not rise in the e-business model when volume rises, companies may wish to pursue megamergers to create a richer product line to sell to an existing customer base. However, as information about businesses becomes cheaper to gather and easier to read and measure, companies should be able to clearly discern which businesses are most profitable and which are least profitable. It may also be easier to determine who outside the company is the most efficient producer, which may lead to more outsourcing of functions and in fact produce a wave of divestitures.

- *Value of brands and proprietary processes.* The value of brands and proprietary processes becomes more complex in the e-world. For instance, priceline.com received a patent for its process of bringing together buyers and sellers of unused airline tickets and hotel space. But the Internet is an open system with mostly open protocols, so any process of using the Internet might not be able to stay

proprietary for long. The value of well-established brands would appear to be even more valuable in the clutter of the e-business model. But apart from amazon.com and a few others, companies apparently find it hard to establish a new brand identity on the Internet.

- *Constantly changing prices.* Whether price or service or both drive transactions in e-commerce, pricing, or at least how a company determines pricing, seems bound to change in the Internet environment. Pricing has traditionally been based on costs. But costs are changing—transaction costs drop in e-business; inventory costs should drop; fixed costs should drop. A number of analysts predict that pricing will ultimately be based on demand, resulting in prices that change fast. Consider, for example, priceline.com and the empty airline seat.

- *Changes in sales and distribution functions.* Most companies have significantly invested in their sales force and distribution systems. For many hard-goods companies in the Internet realm, sales forces will get smaller and might be redirected to other functions. For information-based companies, sales forces could become even more important. Traditional sales channels may also conflict in the e-world.

- *Changing assets and liabilities.* Balance sheets may look very different for e-businesses in the future. Instant payments will affect receivables and payables. Inventory levels, and the capital to finance them, will decline; in fact, the Department of Commerce reports that inventory to sales ratios are already less than 1.4:1, down from 1.5:1 ten years ago.

- *Social costs.* Companies cannot ignore the social ramifications of e-business engendered by the de-layering of functions like sales and fixed asset maintenance. What about pension costs for larger numbers of workers made obsolete by new technologies? Companies will have to consider these and other costs as companies depend more and more on e-business in the future.

Because of these issues and others, the "E" is not only changing business, but it is also changing how we audit the business—how we plan the audit, how we perform the audit, and how we report on the audited financial statements. The next section highlights some specific areas that require close attention in auditing e-businesses.

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 that will be lost in 2001 because of the nontaxation of Internet sales puts the amount at $2 billion.

Last year, the Advisory Commission on Electronic Commerce (ACEC) submitted its report to Congress. That report recommended that, among other actions, Congress:

- Extend the existing ban on new taxes on Internet access and on multiple or discriminatory taxes on e-commerce. (The ban's original expiration date was October 2001; see subsequent discussion in this paragraph.)
- Take steps to simplify state and local sales and use taxes. Internet businesses claim that disparities in sales tax systems among the various jurisdictions are too burdensome to administer.

Despite the introduction of numerous bills regarding taxation-related matters on the Internet, Congress was unable to pass Internet taxation legislation this year. However, the attempts continue.

In July 2001, Congressmen Istook (R-OK) and Delahunt (D-MA) introduced legislation on H.R. 1410, The Internet Tax Moratorium and Equity Act. The bill supports the actual simplification of state and local governments' complex sales tax structures to establish a uniform streamlined sales tax system. In turn, brick-and-mortar retailers and Internet retailers would treat all retail sales of tangible property in the same manner. The current

moratorium, the Internet Tax Freedom Act of 1998 (IFTA), on access taxes and on new discriminatory taxes on the Internet would be extended until December 31, 2005.

However, Congress failed to pass new legislation and the moratorium on Internet taxes expired on October 21, 2001. Analysts and lawmakers say it is unlikely that state and local governments will rush to impose e-commerce sales taxes, but, given enough time and an increasing need to raise revenue, that could change. There is concern that tax officials around the country could begin interpreting a variety of their current tax laws as applying to the Internet. Observers say such a move would drag down a crucial engine of the U.S. economy, adding to the nation's economic woes.

States are attempting to address the issue of sales tax simplification. The District of Columbia, forty-five 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 thirty states, developed model legislation to unify and simplify sales and use tax administration among the states that adopt the legislation. The SSTP hopes that, by unifying and simplifying sales tax systems, Internet businesses will voluntarily collect sales taxes. The model legislation, 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.

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. In addition, the Web site www.e-commercetaxation.com serves as a free resource center focused on the taxation of e-commerce and contains articles on e-commerce taxation as well as government tax policies and regulations.

E-Signature Act

As we discussed in last year's e-business alert, 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 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."[7]

The Act ensures that online consumers using e-signatures will have legal protections equivalent to those in the offline world. However, controversy surrounds the issue of electronic signatures and their legal validity in court. Currently, there is the suggestion that, to stand up in court, documents signed electronically will need a rigorous set of mechanisms to validate the identity of a person doing the signing. Companies that can help address concerns about signature authenticity include but are not limited to PKI (public key infrastructure) companies, for example. PKI companies make a public "key" available via a digital certificate, which is a specialized electronic document. The PKI company investigates the identity of the client company and maintains a protected record of its public key. The party receiving a document with a digital signature receives the public key from the digital

7. "New Electronic Signature Law," Mondaq Business Briefing, Mondaq Ltd., August 11, 2000.

certificate. If the document can be decrypted using the certified public key, then the receiver can be confident that the document is from the assumed party and that the "signature" is valid.

Given the confusion and potential security issues surrounding e-signatures, one-third of companies seeking to implement digital signatures have decided to seek outsourcing help, according to the San Antonio-based research firm Frost and Sullivan. Moreover, Frost and Sullivan predicts that the number of companies seeking help with implementing digital signatures will increase to two-thirds by the year 2006.

New Domain Names

The Internet Corporation for Assigned Names and Numbers (ICANN) is an international, not-for-profit organization charged with expanding the current system of domain names that had been in place since 1969. The new domain names will join the familiar *.com*, along with *.org* for not-for-profit organizations, *.edu* for educational institutions, *.gov* for governmental bodies, *.mil* for military, and *.net* for computer networks.

The early days of domain name registration operated on a first-come, first-served basis which led to a flurry of lawsuits alleging "cybersquatting"—people registering names such as coke.com or ford.com with hopes of reselling the rights to the companies with those names later. To prevent this practice from recurring, ICANN now requires the firms it hires to sell registrations under the new domain names to charge a small fee (around $2), to keep people from registering thousands of names at a time. ICANN also demands that its firms determine whether individuals and companies registering for a particular name have a rightful claim to that address (usually by providing proof of trademark of a particular name).

Web sites using *.info* suffixes for Web sites that do not fall under any existing categories will appear in the Fall of 2001, as will *.biz*[8] names for business-related Web sites. Other names, such as *.coop*,

8. Recent news indicates that the scramble for new business Web addresses is delayed by a need to allow more time to test the registration system and by a lawsuit about how *.biz* addresses are being awarded when contested by more than one applicant.

for non-profit cooperatives such as credit unions; *.aero*, for the air transport industry; *.museum*, for museums; *.pro*, for professionals such as accountants, lawyers, and physicians; and *.name*, for individuals, will come online over the next year.

Internet Privacy

The privacy of information collected by operators of Web sites is a growing issue of concern. Many in Congress prefer to rely on industry self-regulation to protect consumer privacy, but frustration at the industry's slow pace led to the 1998 passage of the Children's Online Privacy Protection Act. In 1999 and 2000, Congress devoted considerable attention to the issue of Internet privacy, but the only legislation passed was amendments to two appropriations bills concerning the collection of data by certain federal agencies about visitors to Web sites.

In the current Congress, there are more than sixty House bills and more than thirty 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, WebTrust™ (see Appendix B, "Trust Assurance Services," 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 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 http://www.epic.org.

Audit Issues and E-Business

What general audit issues could affect e-business clients?

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

affect 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 or 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

As you plan your audits, you may need to search for information about and consider the effects of clients' e-business activities. For example, you might need to modify engagement acceptance procedures to include questions about the client's e-business—its current and future status as well as planned scope. Auditors reviewing the minutes of board of directors meetings will want to be on the lookout for discussions about the entity's e-business strategy, related issues, and timing. An examination of the entity's annual budget may indicate the client's e-business plans and might include separate estimates of projected e-business revenue, expenses, and investments. If this is not the case, you might inquire about e-business matters with senior management, especially if there is evidence of e-business plans in the board minutes. Also, even if the minutes are silent and there are no separate budgets for e-business, unusual increases in other budget lines—marketing and technology budgets, for example—could indicate planned e-business activity. Finally, an Internet search and a detailed review of the client's Web site may reveal evidence of the nature, scope, and depth of the company's e-business activity.

Audit Timing and Planning

The timing of audit procedures is a critical part of auditing e-business transactions. Traditionally, auditors begin performing audit procedures after the client's fiscal year end. In the e-business world, however, traditional audit timing may be inadequate as a result of the design and implementation of new e-business software

applications and because of the electronic evidence. E-business transactions may automatically initiate, authorize, record, summarize, and settle electronically without human intervention or physical documentation. As a result, sometimes key audit evidence in electronic form may exist only for a limited amount of time. 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. 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.

Statement on Auditing Standards (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 physical evidence of transactions. Sales orders, purchase orders, invoices, delivery, settlement, and authorization may be prepared and performed electronically, leaving no physical 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*, as amended by SAS No. 80, *Amendment to Statement on Auditing Standards No. 31*, Evidential Matter (AICPA, *Professional Standards*, vol. 1, AU sec. 326.18):

> 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.

Clients Affected by the September 11 Terrorist Attacks

As you prepare to conduct quarterly reviews and annual audits of e-businesses affected by the events of September 11, some of your clients might find themselves working in a new business environment. If this is the case, you must first gain an understanding of this new environment in order to adequately plan and perform the audit. Some industries have been affected directly; for example, the airline, financial services, and insurance industries. Other industries will experience more indirect effects; for example, the tourism, hospitality, and real estate industries. Many clients will experience effects related to shifts in demand for their products or services, the collectibility of accounts receivable, or the valuation of their investments.

You may wish to begin the planning process early for the audit of clients affected by these events. Materials traditionally used to help you gain an understanding of the business and plan the audit may have been destroyed or rendered unavailable; for example, correspondence files, prior year's working papers, permanent files, financial statements, and auditor's reports. Evidential matter and information systems may have been destroyed, requiring the re-creation of systems and data. Conditions may require the extension or modification of audit tests.

During the planning process, you should discuss the timing and extent of the recovery process with your client. You should also understand the client's processes for ensuring that the recovery of the accounting records is complete. In a number of companies, the internal audit function may have tested the recovery process and may be able to provide information regarding the nature of the process and any perceived weaknesses in it.

You may want to talk to the client about the status of its facilities. Depending on the timing of the fieldwork, it may be necessary to arrange for alternative working space to accommodate the client and the audit staff. You may be helpful to the client by establishing immediate working space. When planning the audit, determine how any alternative working space might affect the use of

technology and its application in the audit. Access to facilities and records also may affect the timing of audit procedures.

Consider the availability of needed documents and how to apply nontraditional auditing procedures to verify account balances, if necessary. By beginning the planning process early, you may be able to identify some of these issues early enough to allow your client time to re-create the information necessary for the audit.

Early planning also allows you more time to determine, based on the extent of damage to the accounting records and your client's ability to recover, the most effective way to conduct the audit.

Adequate Technical Training

Technology has evolved according to Moore's law for the past fifty years. In 1965, Gordon Moore, one of the founders of Intel Corporation, predicted that computer processing power would double every year. Ten years later his prediction proved true, and he predicted that processing power would continue to double every two years for the foreseeable future. Moore's predictions have approximated the actual rate of increase, but the rate has been even greater—doubling every eighteen months.

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

Do traditional financial statement auditors have the technical skills necessary to audit e-business activities? 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. However, with increased understanding of underlying systems and controls, the auditor may be able to perform substantive tests of 100 percent of the records

summarized in certain financial statement balances.[9] To do this, auditors will need additional training in Internet and network technologies, computer audit software, statistical methods, and analytical procedures for their e-business engagements. You need look no further than the discussion entitled "Training and Proficiency of the Independent Auditor," in SAS No. 1, *Codification of Auditing Standards and Procedures* (AICPA, *Professional Standards*, vol. 1, AU sec. 210). AU Section 210.04 indicates, "The training of a professional man includes a continual awareness of developments taking place in business and his profession." The ubiquitous nature of e-business places even more demands on auditors than ever before.

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.

Using the Work of a Specialist

Even though you have most of the skills you need to audit e-business, you may not have *all* of the skills necessary. 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:

9. Note, however, that the goal of an audit is not 100 percent substantive testing. A more detailed understanding of systems and controls may also allow you to reduce the extent of substantive testing.

> ...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[10] 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 knowledge necessary to supervise the specialist. According to SAS No. 22, AU Section 311.10:

> If specialized skills are needed, the auditor should seek the assistance of a professional possessing such skills, 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), 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). (See the important related discussion about SAS No. 94 , *The Effect of Information Technology on Auditor's Consideration of Internal Control in a Financial Statement Audit* (AICPA, *Professional*

10. Note that SAS No. 73 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.

Standards, vol. 1, AU sec. 319), which amends SAS No. 55, in the "Auditing Considerations of Information Technology on Internal Control" section of this Alert.) SAS No. 94 provides guidance to auditors about the effect of information technology on internal control and on the auditor's understanding of internal control and assessment of control risk.

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 physical 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.

The Importance of Software Controls

One important factor to consider regarding controls in the e-business environment relates to software. 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 Section 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 significant changes in internal control, including its policies, procedures, and personnel, that occur subsequent to the interim period.

You should also consider the type of software you use in the audit.[11] Specifically designed audit software is available and can provide a way to increase the value of the audit by ferreting out control weaknesses as well as increasing the number of records that can be audited. In some e-business systems, it may be impossible to efficiently discover control weaknesses without special network monitoring software.

The use of special audit software also requires mention of these important considerations. Operating system and e-business application software is often installed at the default settings, which generally leave accounting records wide open to unauthorized access and alteration. For example, popular operating systems include built-in accounts with default passwords or no passwords at all. Default passwords to operating systems are well known to hackers and widely published on the Internet at hacker Web sites. Default passwords are the easiest way to gain unauthorized access to the system and obtaining such passwords is usually the first attempt by those desiring unauthorized access.

In order to test controls over e-business, 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 in order to gain a sufficient understanding of controls and to perform substantive tests. Sometimes this will require the CFO's involvement to obtain this access.

11. Note, however, that the audit literature does not require the use of audit software.

As we discussed previously in this Alert, e-business transactions may be initiated by a trading partner's software. Customer and supplier companies may be directly linked to your client's computers with Internet technologies. Customer software may detect its own increased sales volumes, low inventory levels, or your client's price changes and automatically issue purchase orders based on preset rules. Or, your client's software may be able to read the customer's computer databases and issue sales orders based on customer sales volumes or inventory levels. Your client may have similar electronic relationships with suppliers. 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—a 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. 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 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. When network administrators disable logging functions because they believe it impedes performance (which logging may do if improperly implemented), businesses

may not know that their records have been altered. Those administrators who do enable logging rarely retain the logs or protect the logs themselves from alteration, reducing their credibility as audit evidence. 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.

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.* The duties of security administration, security monitoring, system administration, application maintenance, software development, and daily accounting operations should be performed by different employees.
- *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 only be granted network access 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.

- *Software development life cycle standards.* E-businesses should adopt authoritative standards for the development and implementation of new e-business systems.
- *Sequentially numbered records.* Financial transaction journals such as sales orders, sales invoices, purchase orders, cash receipts, and adjustments should be sequentially numbered to control for completeness.
- *Methods of error correction.* E-business software should have controlled rollback procedures so that records are not purged or lost when servers crash and programs abort. Controls preventing changes to historical records should be in place so that 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 accounting department 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 accounting department.
- *Disaster recovery.* The nature of e-business often requires that systems be capable of operating twenty-four 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 accounting department should periodically test the plan. The events of September 11 vividly illustrate this need.

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. See the important related discussion about SAS No. 94, which amends SAS No. 55, in the "Auditing Considerations of Information Technology on Internal Control" section of this Alert.

How Does E-Business Change the Nature of Evidential Matter?

E-business controls have been described in sufficient detail to illustrate the idea that good controls and reliable audit evidence are inextricably linked. According to the AICPA Auditing Practice Release, *The Information Technology Age: Evidential Matter in the Electronic Environment* (Product No. 021068kk):

> The intended purpose of electronic evidence does not differ from traditional forms of evidence, but it is distinguished by the need for controls to ensure validity.

The competence of the electronic evidence usually depends on the effectiveness of internal controls over its validity and completeness. A major consideration for auditors is the credibility of the evidence obtained. For e-business audits, there may be few or no physical documents to examine. Without testing the internal controls surrounding the electronic evidence (for example, controls over generation, storage, manipulation, and transmission), the auditor may not recognize a lack of credibility.

A detailed understanding of internal control over e-business transactions and control testing requires that you keep the following in mind: According to SAS No. 1, AU Section 150.02, "Generally Accepted Auditing Standards:"

> Sufficient competent evidential matter is to be obtained through inspection, observation, inquiries, and confirmations to afford a reasonable basis for an opinion regarding the financial statements under audit.

Other Internal Control Considerations

SAS No. 78, *Consideration of Internal Control In a Financial Statement Audit: An Amendment to Statement on Auditing Standards No. 55* (AICPA, *Professional Standards*, vol. 1, AU sec. 319) amends SAS No. 55 to include many terms and concepts from the report of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. Although the framework of internal control was developed before the concept and practical implementation of e-business, SAS No. 78 identifies the following special circumstances that you might want to consider according to SAS No. 47, *Audit Risk and Materiality in Conducting an Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 312), when assessing the risk of e-business:

- *Changed economic operating environment.* E-business has dramatically changed the operating environment in many industries. Many dot-coms are built upon alliances with other traditional companies or other dot-coms. Managers of traditional companies may be at a technical disadvantage relative to managers of new dot-coms, who might have grown up in an open network environment or have prior experience with successful technology leaders.
- *New personnel.* The scarcity of qualified high-tech personnel has spiked the demand for these personnel, and, consequently, they have strong financial incentives to move around and often do not stay at one company very long. Moreover, new managers of e-business subsidiaries or divisions of larger companies may have goals that conflict with the corporate mission and may be unwilling to conform to corporate cultures or norms. This characteristic may also contribute to the high turnover.
- *New or revamped information system.* When an established business decides to adopt Internet technologies, it often finds it is not feasible for business and technology reasons to just terminate the old systems. Therefore, adding new e-business operations usually requires integration between the legacy, or old, systems and new Internet technologies.

Such integration introduces instability, errors, and new control weaknesses in previously reliable systems.

- *Rapid growth.* When companies open their e-business doors, they expand their potential market from their own geographic area and existing customer base to the world and its global market. When an e-business has not accurately predicted sales and provided for systems flexibility and scalability, existing controls may fail.
- *New technology.* Two key new technologies that will affect companies that conduct e-business are broadband and wireless technologies. Broadband technology is a means to quickly deliver huge amounts of data, including music, video, software, and financial data in an "always on" environment. Wireless technology allows users to remotely access information and conduct e-commerce and e-business transactions. Both of these technologies pose similar problems for e-businesses, including integration with existing systems and scalability.
- *New lines, products, and activities.* When companies add new lines, products, and activities, the managers of old systems may not understand the controls in the new system. Conversely, new managers of new activities may not understand existing corporate control policies. The end result can be that new systems are beyond the control of either old or new managers.
- *Corporate restructuring.* All corporate restructuring (mergers, acquisitions, discontinued operations, layoffs, and downsizing, for example) creates control issues for auditors of e-businesses. Companies may underestimate the complexity, extent, and cost of the change and the expertise needed to modify their business strategies.

Reports From Service Organizations

Many clients use an ISP to host their web site, including the databases used to initially record sales and credit card receivables. In a

number of cases, ISP servers provide fulfillment by allowing users to immediately download their purchase after credit approval for software, digitized music, videos, books, and other electronic documents.

ISPs are computer service bureaus and similar entities providing computer services to businesses that have been operating for decades. For clients that use traditional service bureaus, auditors can sometimes obtain a report on controls from the service organization. According to SAS No. 70, AU secs. 324.24-.56, 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. Unfortunately, as a result of the relative infancy of e-business, you may not be able to obtain a SAS No. 70 report from an ISP that hosts your client's web site. If you cannot obtain a SAS No. 70 report or be granted access to the ISP to gain an understanding and test internal control, you may have to consider a scope limitation.

Going-Concern Issues

Why is going concern an important issue for e-business? What is the auditor's responsibility in addressing it?

E-business activities' sensitivity to negative changes in economic conditions is a relatively recent phenomenon since the e-business industry is relatively new. However, e-business activities and companies embrace many of the factors that can give rise to going-concern issues. Think about general economic factors giving rise to such concerns, for example, reductions in personal income, layoffs, higher unemployment levels, and decreases in consumer confidence. 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.[12] Or, more specifically, think of the client's short-term cash requirements and

12. See the discussion of the auditor's responsibility related to going concern in the next section.

cash-generating ability. These two issues alone are critical enough for survival to prompt auditors to consider whether clients that require additional cash in the next twelve months to maintain operations can continue as going concerns.

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 disaster occurrences like the attacks of September 11, 2001, pending legal proceedings, or the loss of a principal supplier, or (5) the inability to retain key technical or managerial talent. Also consider the case of an entity's excessive and unusual reliance on external financing, rather than money generated from the company's own operations as a going-concern issue. We know that the external financing reliance is one major factor leading to the recent failures of many dot-com companies, including, pet.com, Quepasa.com, Mothernature.com, and ValueAmerica.com.

Implications of the September 11 Terrorist Attacks for Going-Concern Issues

Continuation of an entity as a going concern is assumed in financial reporting in the absence of significant information to the contrary. When auditing a client that has been affected by the September 11 attacks, you should carefully consider a company's ability to continue as a going concern. The client's business may be interrupted for an indeterminate amount of time. The sustainability of the business may depend on receiving insurance proceeds from an insurance company that is itself struggling to remain viable as it faces similar business issues, compounded by the difficulty of paying out unprecedented numbers of insurance claims.

When evaluating management's plans to continue as a going concern, adopting an appropriate level of professional skepticism is important. For example, scrutinize the company's assumptions to continue as a going concern in order to assess whether the assumptions are based on overly optimistic or "once-in-a-lifetime"

occurrences. Consider the viability of the insurance companies from which payments are expected. The review of insurance policies and other documents may be helpful in trying to gain an understanding of any insurance proceeds the client expects.

Auditor's Responsibilities Related to a Going-Concern Issue

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. 341.01 and .03b). 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 reasonable period of time.

As noted previously in this Alert, continuation of an entity as a going concern is generally assumed in the absence of significant information to the contrary. 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. 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 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 prior to fresh-start accounting under SOP 90-7.

The Risk of Financial Fraud

According to SAS No. 82, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 316.06), 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. 82, AU Section 316.17, 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. 82, AU Section 316.17, 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. See AU Section 316.21. 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, according to SAS No. 82, AU Sections 316.21-.22.

If you believe that there is a high level of risk of material misstatement attributable to fraud during an audit of an e-business, you may need to modify the nature, timing, and extent of audit procedures. 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, according to SAS No. 82, AU Sections 316.29-.30. According to SAS No. 82, AU Section 316.35, if you determine that a misstatement is, or may be, the result of fraud, you should:

- Consider the implications for the other aspects of the audit.
- Discuss the matter with the appropriate level of management.
- Attempt to obtain additional evidence to determine whether material fraud has occurred.
- If appropriate, suggest that the client consult with legal counsel.

For some clients, 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(s) 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 Securities and Exchange Commission (SEC). If fraud is present, other reports also may be required under section 10A(b)1 of the Securities and Exchange Act of 1934. See SAS No. 82, AU Section 316.40.

The events of September 11 may raise several fraud risk factors. For example, management may be under significant pressure to obtain the additional capital necessary to rebuild, or the entity may depend on debt with debt covenants that are difficult to maintain under the circumstances. The entity may be facing the threat of imminent bankruptcy. Also, the recordkeeping and physical safeguards over assets that are susceptible to misappropriation may be compromised. You may wish to consider fraud risk factors separately for the period following the attack.

Revenue Recognition

Revenue recognition continues to pose significant audit risk to auditors and has contributed to a perceived erosion in the integrity of the financial reporting process. Staff Accounting Bulletin (SAB) No. 101, *Revenue Recognition in Financial Statements*, summarizes the SEC staff's views in applying GAAP to selected revenue recognition issues for your public clients. SAB No. 101 presents various fact patterns, questions, and interpretive responses concerning whether the following criteria of revenue recognition are met:

- Persuasive evidence of an arrangement exists.
- Delivery has occurred or services have been rendered.
- The seller's price to the buyer is fixed or determinable.
- Collectibility is reasonably assured.

SAB No. 101 addresses recurring questions from preparers, auditors, and analysts about how to apply the guidance in SAB No. 101 to particular transactions.

SAB No. 101 reflects the basic principles of revenue recognition in GAAP and does not supersede any existing authoritative literature. Accordingly, although it is directed specifically to transactions of public companies, management and auditors of nonpublic companies may find the guidance helpful in analyzing revenue recognition matters.

The SEC continues to see instances of questionable and inappropriate revenue recognition practices. Significant issues encountered recently include the following:

- Complex arrangements that provide for separate, multiple deliverables (for example, multiple products and/or services), at different points in time, during the contract term
- Nonmonetary (for example, barter) transactions in which fair values are not readily determinable with a sufficient degree of reliability)

The SEC has requested that the Financial Accounting Standards Board (FASB) Emerging Issues Task Force (EITF) address certain of these issues to clarify the application of GAAP in these transactions. However, the SEC staff generally believes that the existing accounting literature provides analogous guidance for a number of these issues, including: Statement of Position (SOP) 97-2, *Software Revenue Recognition*; Accounting Principles Board (APB) Opinion No. 29, *Accounting for Nonmonetary Transactions*; SOP 81-1, *Accounting for Performance of Construction-Type and Production-Type Contracts*; FASB Statement of Accounting Concepts No. 5, *Recognition and Measurement in Financial Statements of Business Enterprises*; and FASB Concepts Statement No. 6, *Elements of Financial Statements.*

AICPA's New Audit Guide on Revenue Recognition

The AICPA recently issued a new Audit Guide, *Auditing Revenue in Certain Industries.*[13] This Guide:

- Discusses the responsibilities of management, boards of directors, and audit committees for reliable financial reporting.

13. One purpose of this Guide is to assist auditors in auditing assertions about revenue in selected industries not covered by existing AICPA Audit and Accounting Guides. You can look to this Guide for descriptions and explanations of auditing standards, procedures, and practices as they relate to auditing assertions about revenue in both the computer software and high tech manufacturing industries. You may order *Auditing Revenue in Certain Industries* (Product No. 012510) from the AICPA at (888) 777-7077.

- Summarizes key accounting guidance regarding whether and when revenue should be recognized in accordance with GAAP.
- Identifies circumstances and transactions that may signal improper revenue recognition.
- Summarizes key aspects of the auditor's responsibility to plan and perform an audit under GAAS.
- Describes procedures that the auditor may find effective in limiting audit risk arising from improper revenue recognition.

Independence

No discussion of auditing e-business would be complete without a discussion of auditor independence. Independence, as you know, is a unique and important quality that sets CPAs apart from other professionals providing auditing and other services to clients.

The issue of independence currently is basking in a prime spotlight as the AICPA and the SEC, among other regulatory groups, address independence issues. During the past year, new AICPA and SEC independence standards were issued. In addition, the SEC issued a statement regarding independence as it relates to the events of September 11.

AICPA Independence Rule Modernization—Spotlight on the Engagement Team and Those Who Influence the Engagement Team

In an effort to modernize the profession's rules on independence, the Professional Ethics Executive Committee (PEEC) of the AICPA approved new independence rules in the Summer of 2001. The rules become effective May 31, 2002. These significant revisions to Section 101 of the Code of Professional Conduct seek to modernize and harmonize independence rules with other governing bodies, most notably with the SEC (see section on the SEC that follows), while simplifying the rules at the same time.

The rules are based on an approach to independence whereby the highest level of restrictions is generally limited to persons on the attest engagement team and to those who are presumed to be able to influence the engagement. The engagement-team-focused-approach centers on the idea that the actions and judgments of those closest to the performance of the attest engagement pose the greatest potential risk to independence. You may obtain additional information about the new rules at: http://www.aicpa.org/members/div/ethics/independence.htm.

SEC Issues Revised Independence Rules

Rule 2-01 of Regulation S-X addresses the independence requirements for auditors of companies filing financial statements with the Commission. In November 2000, the SEC adopted its final rule, *Revision of the Commission's Auditor Independence Requirements*. Among other matters, the rule addresses:

- Investments by auditors or their family members in audit clients (stocks, bonds, and stock options and other ownership interests)
- Other financial relationships between auditors or their family members and audit client (for example, broker-dealer, savings or checking accounts, and loans)
- Employment and business relationships between auditors or their family members and audit clients (joint business investments, membership on a client's board of directors, and others)
- The scope of services provided by audit firms to their audit clients (nonaudit services, including areas of services relating to financial information systems design and implementation, bookkeeping, valuation, and appraisal, among other services). The rule also requires public companies to disclose in their statements the amount of nonaudit services provided by the auditor during the most recent year.

The effective date of the SEC rule was February 5, 2001, with different transition dates for firms providing certain nonaudit services, for example, valuation services. You can download a copy of the SEC's final rule, which includes all of its detailed provisions at their Web site at www.sec.gov/rules/final/33-7918.htm.

Provision of IT Services

Both the AICPA and SEC have issued rules related to IT services that you can provide clients. According to the AICPA, your firm may assist in the design or installation of a client's information system provided the client makes all the relevant management decisions about the service. Your firm also may provide initial training to the client's employees on the new system. However, your firm may not supervise the client's employees in their day-to-day use of the system. Similar to AICPA rules, the SEC rule states that your firm may not operate or supervise the operation of a client's IT systems.

Independence Issues Related to the September 11 Terrorist Attacks

You may provide bookkeeping services to and help recover records for your *public* attest clients with offices in and around the World Trade Center in New York City, without violating auditor independence rules under the following conditions:

- Rule 2-01(c)(4)(i)(A) states that, among other things, maintaining or preparing an audit client's accounting records or preparing or originating source data underlying the client's financial statements will impair an auditor's independence. Rule 2-01(c)(4)(i)(B)(1), however, permits such bookkeeping services "in emergency or other unusual situations, provided the accountant does not undertake any managerial actions or make any managerial decisions."
- The SEC believes that the events of September 11, 2001, clearly meet the definition of an unusual situation for those companies that have been directly affected by the destruction of the World Trade Center and damage to surrounding buildings. See www.sec.gov/rules/interp/33-8004.htm for more information.

- Services under this exception may continue until the client's lost or destroyed records are reconstructed and its financial systems are fully operational, and the client can effect an orderly and efficient transition to management or other service providers. Contact the SEC at (202) 942-4400 for further information.

You may encounter situations in which your attest clients (public, private, or governmental) request assistance performing bookkeeping, information technology, controllership, human resource, or similar services. See Interpretation 101-3, *Performance of Other Services* (AICPA, *Professional Standards*, vol. 2, ET Sec. 101.05), and www.aicpa.org/about/code/et101.htm#r3 for more information. As in the case of the SEC rule, you may not perform functions that place you in the position of management. For example, you may not make decisions for the client, sign checks, or authorize transactions.

Attest clients may also request internal audit assistance during the recovery period. Independence rules related to such services are addressed in the following:

- Interpretation 101-13, *Extended Audit Services* (AICPA, *Professional Standards*, vol. 2, ET sec. 101.15) (For more information, see www.aicpa.org/about/code/et101.htm#r13.)
- Ethics Rulings No. 103, "Member Providing Attest Report on Internal Controls;" 104, "Member Providing Operational Auditing Services;" and 105, "Frequency of Performance of Extended Audit Procedures" (AICPA, *Professional Standards*, vol. 2, ET sec. 191.206-.211. (See www.aicpa.org/about/code/et191b.htm#r103 for more information.)

If you are asked to lease your firm employees to attest clients for a period of time, you should also be aware that the aforementioned AICPA rules still apply.

If you will be providing services to attest clients on a contingent fee basis you should refer to Rule 302 of the AICPA Code of Professional Conduct, as several prohibitions exist. See www.aicpa.org/about/code/et302.htm for more information. In addition, state boards of accountancy may have more restrictive rules.

Help Desk—Contact the AICPA staff at (888) 777-7077 or by e-mail (ethics@aicpa.org) for assistance with the AICPA Code of Professional Conduct. Members providing attest services to public companies or those subject to other regulatory oversight should consider rules of both the AICPA and other regulator(s). Where two or more rules apply, members should comply with the more restrictive standard.

Selected Audit Issues Related to the September 11 Terrorist Attacks

There are additional audit issues resulting from the September 11 attacks, previously mentioned, that will affect both those businesses and auditors directly affected by the attacks and those businesses and auditors who were not directly affected, but whose clients, vendors, suppliers, and others were directly affected.

Obtaining Audit Evidence

You must obtain sufficient competent evidential matter to provide a reasonable basis for an audit opinion. Some of the entities affected by the events may keep their records at a site that remains unaffected by the attack. Others may have sophisticated backups of their systems and data. In the cases in which there are backups, consider whether the backed up systems are processing data as intended and whether the backed-up data are valid in the new business environment.

Will it be necessary to perform extended walk-throughs and tests of controls to determine that they continue to function effectively? When testing controls, be aware of the possible effect of key unfilled positions on internal control. You also may consider obtaining additional evidence to corroborate backed-up data. Of particular concern to the auditor is the client's completeness assertion because it may be difficult to obtain reasonable assurance that all material transactions have been recorded.

In cases in which systems and data have not been adequately backed up, you might determine whether sufficient evidence can be obtained using other audit techniques. For example, confirmation procedures might be used to verify certain activity.

Roll-forward procedures also may be effective. These techniques may also be useful to corroborate backed-up data.

In some cases, you may not be able to obtain sufficient evidence to support the audit opinion because sufficient competent audit evidence may not be recoverable. Your understanding of internal control may raise doubts about the auditability of an entity's financial statements, and performing only substantive tests may be ineffective or impossible. In those cases, you may be required to express a qualified opinion or a disclaimer of opinion because of a scope limitation.

Auditing Estimates

Because of the uniqueness of the events of September 11, estimates may be difficult for management to make and for auditors to audit. Pay close attention to the underlying assumptions used by management when auditing accounting estimates. Management is responsible for making the estimates included in the financial statements, and those estimates may be based in whole or in part on subjective factors such as judgment based on experience about past as well as current events and about conditions it expects will exist. Be alert to the possibility of management's over-reliance on economic information based on favorable conditions to predict future outcomes.

When auditing estimates, turn to SAS No. 57, *Auditing Accounting Estimates* (AICPA, *Professional Standards*, vol. 1, AU sec. 342); the AICPA Practice Aid, *Auditing Estimates and Other Soft Information*; and SOP 94-6, *Disclosure of Certain Significant Risks and Uncertainties.*

General Accounting Issues Affecting E-Business

What general accounting issues could affect e-business clients?

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 EITF is addressing. See the section in this Alert entitled "SEC Internet-Related Concerns" for a discussion of these issues.

Stock Options

Stock options are still an important accounting-related area for your e-business clients. As described in last year's Alert, 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.

There are two permissible methods of accounting for employee stock options: APB Opinion No. 25, *Accounting for Stock Issued to Employees*, which uses the intrinsic value method, and FASB Statement of Financial Accounting Standards No. 123, *Accounting for Stock-Based Compensation*, which uses the fair-value method. Most e-businesses choose APB Opinion No. 25, which is easier to apply.

Stock options granted to consultants, contractors, and nonemployees for services rendered or goods purchased must be accounted for in accordance with FASB Statement No. 123. Accordingly, companies must use the fair value method, not the intrinsic value

method. EITF Issue No. 96-18, *Accounting for Equity Instruments That Are Issued to Other than Employees for Acquiring, or in Conjunction with, Selling Goods and Services*, offers guidance in applying FASB Statement No. 123 to these transactions.

With the downturn in share prices of many e-businesses continuing throughout 2001, the stock options previously granted to many essential employees may now have lost much of their value. In order to retain these employees, many companies may reprice the options. FASB Interpretation No. 44, *Accounting for Certain Transactions Involving Stock Compensation*, is an interpretation of APB Opinion No. 25, and provides that "if the exercise price of a fixed stock option award is reduced, the award shall be accounted for as variable from the date of the modification to the date the award is exercised, is forfeited, or expires unexercised." The EITF also addressed the repricing issue in EITF Topic No. D-91, *Application of APB Opinion No. 25*, Accounting for Stock Issued to Employees, and FASB Interpretation No. 44, *Accounting for Certain Transactions Involving Stock Compensation, to an Indirect Repricing of a Stock Option.*

FASB Interpretation No. 44 indicates that any modification or sequence of actions by a grantor to directly or indirectly reduce the exercise price of an option award causes variable accounting for the repriced or replacement award for the remainder of the award's life. The change from a fixed to a variable plan triggers the requirement to record income statement charges (or credits) at each reporting date. So, although the intrinsic value of the option may be zero at the repricing (or modification) date, from that date until the final exercise (or expiration or forfeiture), the company must report an expense or reversal of that expense even though the options are not vested. This expense is the difference between the fair value of the shares at each balance-sheet date and the exercise price.

The change in accounting triggered by repricing requiring compensation to be recorded has no effect on cash flow. However, it may reduce net income and earnings per share. Management should be made aware of the consequences of making any modification to

their option plans and outstanding options and the financial statement impact of giving equity instruments to nonemployees.

Business Combinations—A New FASB Standard

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 purchased method. Use of the pooling method was required whenever twelve criteria were met; otherwise, the purchase method was used. Because those twelve 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.

Goodwill and Other Intangible Assets—A New FASB Standard

The FASB issued FASB Statement No. 142, *Goodwill and Other Intangible Assets*, in June 2001. This Statement supersedes APB Opinion No. 17, *Intangible Assets*, and addresses how to account for intangible assets that are acquired individually or with a group of other assets upon their acquisition. This Statement also addresses how to account for goodwill and other intangible assets after they have been initially recognized in the financial statements.

FASB Statement No. 142 changes the unit of account for goodwill and takes a very different approach to how goodwill and other intangible assets are accounted for subsequent to their initial recognition. Because goodwill and some intangible assets will no longer be amortized, the reported amounts of goodwill and intangible assets will not decrease at the same time and in the same manner as under previous standards. Specifically, FASB Statement No. 142 changes the subsequent accounting for goodwill and other intangible assets in the following respects:

- FASB Statement No. 142 adopts a more aggregate view of goodwill and bases the accounting for goodwill on the units of the combined entity into which an acquired entity is integrated. Those units are referred to as reporting units.
- APB Opinion No. 17 presumed that goodwill and all other intangible assets were wasting assets (that is, finite lived). FASB Statement No. 142 does not presume that those assets are wasting assets. Instead, goodwill and other intangible assets are presumed to have indefinite useful lives and will not be amortized but, rather, will be tested at least annually for impairment.
- FASB Statement No. 142 provides specific guidance for testing goodwill for impairment. The annual test for goodwill impairment uses a two-step process that begins with an estimation of the fair value of a reporting unit. However, if certain criteria are met, the requirement to test goodwill for impairment annually can be satisfied without a remeasurement of the fair value of the reporting unit.

The provisions of FASB Statement No. 142 are required to be applied starting with fiscal years beginning after December 15, 2001. This Statement is required to be applied to all goodwill and other intangible assets recognized in the financial statements at that date. Goodwill and intangible assets acquired after June 30, 2001, will be subject immediately to the nonamortization provisions of FASB Statement No. 142.

The fact that there have been numerous combinations of e-business companies in recent years and because goodwill may represent a significant asset on the balance sheets of these combined companies should lead you to carefully consider the impact of these changes on your e-business clients. Specifically, the change regarding goodwill will necessitate the need to identify the reporting units of the organization and test for the impairment of goodwill at the reporting unit level. This process will require extensive valuation judgments and calculations.

Help Desk—A good tool to use when valuing intangibles is the new AICPA 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*. Contact the AICPA Order Desk at (888) 777-7077 for further information on how to obtain this publication.

Income Statement Classification

The appropriate classification of amounts within the income statement or balance sheet can be as important as the appropriate measurement or recognition of such amounts. Several EITF consensus provisions provide guidance on the proper classification of certain revenue and expense items. For example, consider EITF Issues No. 99-17, *Accounting for Advertising Barter Transactions*; 99-19, *Reporting Revenue Gross as a Principal versus Net as an Agent*; 00-10, *Accounting for Shipping and Handling Fees and Costs*; 00-14, *Accounting for Certain Sales Incentives*; all of which were to be applied no later than in the December 31, 2000, financial statements for calendar year-end companies. SEC registrants should apply the guidance provided in SEC Regulation S-X regarding classification of amounts in financial statements.

SEC Internet-Related Concerns

In October 1999, the chief accountant of the SEC sent a list of Internet accounting issues to the EITF that the SEC staff believed warranted consideration by the EITF or another standard-setting body. During the past year, the SEC and the EITF have worked to resolve the remainder of these issues, which we discuss here. Exhibit 1, "Resolution of SEC Internet Accounting Issues," presents a summary of the issues raised by the SEC in its October 1999 letter to the EITF. As noted in Exhibit 1, we presented several of these issues in the 2000/01 edition of this Alert.

EXHIBIT 1

Resolution of SEC Internet Accounting Issues[14]

Note: Exhibit items are set up in the following order—

SEC Issue to Address
Priority (By SEC)
Where Found
EITF Status

Advertising barter transactions*
Level 1
EITF Issue No. 99-17
Consensus†

Gross versus net revenue and display cost*
Level 1
EITF Issue No. 99-19
Consensus†

Accounting for the costs of developing a Web site*
Level 1
EITF Issues No. 00-2 and 00-20
Consensus* on EITF Issues No. 00-2 and 00-20 (content) to be discussed further

Accounting for shipping and handling revenues and costs*
Level 2
EITF Issue No. 00-10
Consensus†

Accounting for the costs of computer files that are essentially films, music, or other content
Level 2
To be discussed
May ultimately be addressed in EITF Issue No. 00-20 (below)

Application of SOP 97-2 to arrangements that include the right to use software stored on another entity's hardware
Level 2
EITF Issue No. 00-3
Consensus†

Accounting for "point" and other loyalty programs
Level 2
EITF Issue No. 00-22
Discussed, but no consensus. Further discussion expected

Accounting by the holder of an instrument (not defined as derivative instrument) with conversion or terms that are variable based on exercisability upon future events
Level 2
EITF Issue No. 00-8
Consensus†

(continued)

EXHIBIT 1—*(continued)*

Resolution of SEC Internet Accounting Issues

Accounting for coupons, rebates, and discounts
Level 2
EITF Issue No. 00-14
Consensus†

Accounting for service outages
Level 2
Classification addressed indirectly in EITF Issue No. 00-14
Consensus†

Accounting for advertising or other arrangements where the service provider guarantees a specified amount of activity
Level 3
To be discussed
Appears to be addressed in SAB No. 101, related Q&A, and EITF Issue No. 00-22

Accounting for front-end and back-end fees
FE—potential SEC staff announcement BE—Level 3
To be discussed
Appears to be addressed in SAB No. 101, related Q&A, and EITF Issue No. 00-21

Income statement classification of rebates and other discounts
Potential SEC staff announcement
EITF Issue No. 00-14
Consensus†

Accounting for free or heavily discounted products
Potential SEC staff announcement
EITF Issue No. 00-14
Consensus†

Accounting for access, maintenance, and publication fees
Potential SEC staff announcement
To be discussed
Appears to be addressed in SAB No. 101, related Q&A, and EITF Issue No. 00-21

FASB Statement No. 131 disclosures about Internet portion of a company's business
No level assigned
Removed from agenda
N/A

* Discussed in Audit Risk Alert, *E-Business Industry Developments—2001/02.*

† When consensus is reached, it becomes a GAAP requirement.

14. "The Right Way to Recognize Revenue," *Journal of Accountancy*, June 2001.

Rebates and Free Products or Services

Internet service providers (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 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 entitled "One-Cent Sales," in AICPA Technical Practice Aid *Revenue Recognition* (AICPA, *Professional Standards*, vol. 2, TPA 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.[15] 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 up-front 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 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 as to 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.

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

The EITF added 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*, to its agenda and, although it has not reached a consensus on this issue, 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.[16] 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.

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.

16. If the costs incurred relate to internal-use software, SOP 98-1, *Accounting for the Costs of Internal-Use Software*, requires that these costs be capitalized and amortized over the useful life of the software.

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 8a and 8b 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**—A newly issued AICPA Practice Aid entitled, *Assets Acquired in a Business Combination to Be Used in Research and Development Activities: A Focus on Software, Electronic Devices, and Pharmaceutical Industries*, may be helpful in valuing these intangible assets. It is available from the AICPA Order Department at (888) 777-7077.

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:

> If no accrual is made for a loss contingency because one or both of the conditions in paragraph 8 [*see extract above*] 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 will devote 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 since 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 SX, 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 the following occur:

- 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, 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. See the "General Accounting Issues Affecting E-Business" section of this Alert for a discussion of FASB Statement No. 142.

Asset Impairment: A New FASB Standard

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.

Some Accounting and Regulatory Issues Related to the September 11 Terrorist Attacks

Remain alert to any accounting or regulatory guidance that may affect your clients. Some regulatory bodies may provide guidance as a result of the attack, including extending some filing dates. Consider notifying your clients of Web sites to monitor that contain accounting and regulatory guidance.

The EITF addressed the September 11 events in EITF Issue No. 01-10, *Accounting for the Impact of the September 11, 2001 Terrorist Acts*. Initially, the EITF concluded that some of the losses attributable to the events should be shown as extraordinary and undertook an effort to clarify how to separate such losses from other financial results. However, the EITF ultimately decided that the economic effects of the events were so extensive and pervasive that it would be impossible to capture them in any one financial statement line item and decided against extraordinary treatment for any of the costs attributable to the terrorist attacks. For more information, see www.fasb.org.

Carefully consider accounting issues associated with the impairment of assets, including long-lived assets, inventories, and investments in securities; the collectibility of receivables; contingent liabilities; and related disclosures that are required.

Auditing Considerations of Information Technology on Internal Control

What new auditing standard might prove to be important to your e-business clients?

Later in this Alert in the section, "Recent Auditing and Attestation Pronouncements," a list of recently issued Auditing Pronouncements is presented that you might want to consider as you plan your engagements. Here, we provide more detail on SAS No. 94, which might affect some of your e-business clients.

SAS No. 94 Issued Describing the Effect of Information Technology on Internal Control

SAS No. 94 was issued in May 2001. This statement is an amendment of SAS No. 55. This Standard provides guidance to auditors about the effect of IT[17] on internal control, and on the auditor's understanding of internal control and assessment of control risk. The Auditing Standards Board believes the guidance is 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.

SAS No. 94:

- Incorporates and expands the concept from SAS No. 80, *Amendment to Statement on Auditing Standards No. 31*, Evidential Matter (AICPA *Professional Standards*, AU sec. 326.14), that in circumstances in which a significant amount of information supporting one or more financial statement assertions is electronically initiated, recorded, processed, and reported, the auditor may determine that it is not practical or possible to restrict detection risk to an

17. According to SAS No. 94, 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.

acceptable level by performing only substantive tests for one or more financial statement assertions. In such circumstances, the auditor should obtain evidential matter about the effectiveness of both the design and operation of controls to reduce the assessed level of control risk.

- Describes how IT may affect internal control, evidential matter, and the auditor's understanding of internal control and assessment of control risk.
- Describes both the benefits and risks of IT to internal control, and how IT affects the components of internal control, particularly the control activities and information and communication components.
- Provides guidance to help auditors determine whether specialized skills are needed to consider the effect of computer processing on the audit, to understand the controls, or to design and perform audit procedures.
- Clarifies that in obtaining an understanding of the entity's financial reporting process, the auditor should understand the automated and manual procedures an entity uses to prepare financial statements and related disclosures, and how misstatements may occur.
- Updates terminology and references to IT systems and controls.

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 effective date of the amendments is for audits of financial statements for periods beginning on or after June 1, 2001. Earlier application is permissible.

Recent Accounting Pronouncements and Guidance Update

Here is a list of recently issued accounting pronouncements and other guidance issued since the publication of last year's Alert. See the AICPA general *Audit Risk Alert—2001/02* (Product No. 022280kk) 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 *Journal of Accountancy.*

FASB Statement No. 141	*Business Combinations* (See "Business Combinations—a New FASB Standard" section of this Alert for more detailed discussion.)
FASB Statement No. 142	*Goodwill and Other Intangible Assets* (See "Goodwill and Other Intangible Assets—A New FASB Standard" section of this Alert for more detailed discussion.)
FASB Statement No. 143	*Accounting for Asset Retirement Obligations*
FASB Statement No. 144	*Accounting for the Impairment or Disposal of Long-Lived Assets* (See "Asset Impairment—A New FASB Standard" in the "General Accounting Issues Affecting E-Business" section of this Alert for more detailed discussion.)
FASB Technical Bulletin No. 01-1	*Effective Date for Certain Financial Institutions of Certain Provisions of Statement 140 Related to the Isolation of Transferred Financial Assets*
SOP 01-1	*Amendment to Scope of Statement of Position 95-2,* Financial Reporting by Nonpublic Investment Partnerships, to Include Commodity Pools
SOP 01-2	*Accounting and Reporting by Health and Welfare Benefit Plans*
AICPA Audit and Accounting Guide	*Audits of Investment Companies*
Questions and Answers	*FASB Statement No. 140*

We have discussed some of the pronouncements and other guidance listed above as they relate to e-business activities in previous sections of this Alert, as noted in the preceding table.

Recent Auditing and Attestation Pronouncements

Presented below is a list of recently issued auditing pronouncements, statements of position, guides, and practice alerts issued since the publication of last year's Alert. See the AICPA general *Audit Risk Alert—2001/02* for a summary explanation of these pronouncements. 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* and *Journal of Accountancy.*

To obtain copies of AICPA standards and guides, contact the AICPA Order Desk at (888) 777-7077 or go online at www.cpa2biz.com.

SAS No. 94	*The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit* (See the previous section of this Alert, "Auditing Considerations of Information Technology on Internal Control" for more detailed information.)
SOP 00-3	*Accounting by Insurance Enterprises for Demutualizations and Formations of Mutual Insurance Holding Companies and for Certain Long-Duration Participating Contracts*
SOP 01-3	*Performing Agreed-Upon Procedures Engagements That Address Internal Control Over Derivative Transactions as Required by the New York State Insurance Law*
SSAE No. 10	*Attestation Standards: Revision and Recodification*
Audit Guide	*Auditing Derivative Instruments, Hedging Activities, and Investments in Securities*
Audit Guide	*Auditing Revenue in Certain Industries*
Audit Guide	*Audit Sampling*
Audit Guide	*Analytical Procedures*
Practice Alert 01-1	*Common Peer Review Recommendations* (See the section below for more detailed information.)

Of the pronouncements, guides, and other guidance listed above, we feature a more in-depth explanation in a previous section of this Alert for SAS No. 94. Also note the information in the following section which might be relevant to some of your e-business clients.

Practice Alert No. 01-1, *Common Peer Review Recommendations*

Peer Review recommendations are worth mentioning here because they span many industries and, in doing so, can potentially affect many of your e-business clients.[18] Practice Alert 01, *Common Peer Review Recommendations*, provides a summary of common peer review findings that will be helpful as you consider critical and significant issues in planning and performing audits.

The Practice Alert presents common peer review recommendations grouped into five categories: (1) implementation of new professional standards or pronouncements, (2) application of GAAP pertaining to equity transactions, (3) application of GAAP pertaining to revenue recognition considerations, (4) documenting audit procedures or audit findings, and (5) miscellaneous findings.

On the Horizon

Auditors should keep abreast of auditing and accounting developments and recent guidance that may affect their engagements. Presented below is information about some ongoing projects that are especially relevant to the e-business industry. Remember that exposure drafts are nonauthoritative and cannot be used as a basis for changing GAAP or GAAS. The AICPA general *Audit Risk Alert—2001/02* summarizes some of the more significant exposure drafts outstanding.

The following table lists the various standard-setting bodies' Web sites on which you may obtain information on outstanding exposure drafts, including downloading a copy of the exposure draft.

18. The AICPA Securities and Exchange Commission Practice Section (SECPS) Executive Committee established a Professional Issues Task Force (PITF) which formulates guidance based on issues arising in peer reviews, firm inspections, and litigation to facilitate the resolution of emerging audit practice issues. This guidance takes the form of Practice Alerts. The information contained in these Practice Alerts is nonauthoritative. It represents the views of the members of the PITF and does not represent official positions of the AICPA.

Standard Setting Body	*Web Site*
AICPA Auditing Standards Board	www.aicpa.org/members/div/auditstd/drafts.htm
AICPA Accounting Standards Executive Committee	www.aicpa.org/members/div/acctstd/edo/index.htm
FASB	www.rutgers.edu/Accounting/raw/fasb/draft/draftpg.html
Professional Ethics Executive Committee	www.aicpa.org/members/div/ethics/index.htm

Help Desk—The AICPA's standard-setting committees are now publishing exposure drafts of proposed professional standards exclusively on the AICPA Web site. The AICPA will notify interested parties by e-mail about new exposure drafts. To have your e-mail address put on the notification list for all AICPA exposure drafts, send your e-mail address to memsat@aicpa.org. Indicate "exposure draft e-mail list" in the subject header field to help process the submissions more efficiently. Include your full name, mailing address and, if known, your membership and subscriber number.

New Framework for the Audit Process

The Auditing Standards Board (ASB) is reviewing the auditor's consideration of the risk assessment process in the auditing standards, including the necessary understanding of the client's business and the relationships among inherent, control, fraud, and other risks. The ASB has begun issuing a series of exposure drafts in 2001, and issuance is expected to continue into 2002. Some participants in the process expect the final standards to have an effect on the conduct of audits that has not been seen since the "Expectation Gap" standards were issued in 1988.

Some of the more important changes to the standards that are expected to be proposed are:

- A requirement for a more robust understanding of the entity's business and the environment of the business that is more clearly linked to the assessment of the risk of material misstatement of the financial statements. Among other

things, this will improve the auditor's assessment of inherent risk and eliminate the "default" to assess inherent risk at the maximum.

- An increased emphasis on the importance of entity controls with clearer guidance on what constitutes a sufficient knowledge of controls to plan the audit.
- A clarification of how the auditor may obtain evidence about the effectiveness of controls in obtaining an understanding of controls.
- A clarification of how the auditor plans and performs auditing procedures differently for higher and lower assessed risks of material misstatement at the assertion level while retaining a "safety net" of procedures.

These changes collectively are intended to improve the guidance on how the auditor places the audit risk model in operation.

You can keep abreast of the status of these projects and projected exposure drafts, inasmuch as they will substantially affect the audit process, by accessing the AICPA's Web site at www.aicpa.org.

AICPA Resource Central

What publications, educational courses, Web sites, and other resources are available to CPAs?

Audit and Accounting Guides and Other Publications

Audit and accounting guides summarize the practices applicable to specific industries and describe relevant matters, conditions, and procedures unique to these industries. The accounting guidance they include is in the GAAP hierarchy as authoritative GAAP.

Among the many industry and other guides that the AICPA offers, the following general guides and other publications can deliver valuable guidance and practical assistance as potent tools on your e-business engagements.

- AICPA general *Audit Risk Alert—2001/02* (Product No. 022280kk)
- *Audit Sampling Audit Guide* (Product No. 012530kk)
- *Analytical Procedures Audit Guide* (Product No. 012551kk)
- *Auditing Estimates and Other Soft Accounting Information Practice Aid* (Product No. 010010kk)
- *Accounting Trends & Techniques—2001*
- AICPA Practice Aid (New!), *Assets Acquired in a Business Combination to Be Used in Research and Development Activities: A Focus on Software, Electronic Devices, and Pharmaceutical Industries*
- *Considering Fraud in a Financial Statement Audit: Practical Guidance for Applying SAS No. 82* (Product No. 008883kk)

Audit and Accounting Manual

The *Audit and Accounting Manual* (Product No. 005131kk) is a valuable nonauthoritative practice tool designed to provide assistance for audit, review, and compilation engagements. It contains numerous practice aids, samples, and illustrations, including audit programs; auditors' reports; checklists; engagement letters, management representation letters, and confirmation letters.

CD-ROM: reSource

The AICPA is currently offering a CD-ROM product entitled *reSource: AICPA's Accounting and Auditing Literature.* This CD-ROM enables subscription access to the following AICPA Professional Literature products in a Windows format: *Professional Standards, Technical Practice Aids,* and *Audit and Accounting Guides* (available for purchase as a set that includes all Guides and the related Audit Risk Alerts, or as individual publications). This dynamic product allows you to purchase the specific titles you need and includes hypertext links to references within and between all products.

Educational Courses

The AICPA offers a wide range of continuing professional education courses that might interest you. Included among them are the following:

- *AICPA's Annual Accounting and Auditing Workshop* (2000-2001 Edition) (Product No. 737061kk (Text) 187078kk (Video)). Whether you are in industry or public practice, this course keeps you current, informed, and shows you how to apply the most recent standards.
- *SFAS 133: Derivative and Hedge Accounting* (Product No. 735180kk). This course helps you understand GAAP for derivatives and hedging activities. Also, you will learn how to identify effective and ineffective hedges.
- *Independence* (Product No. 739035kk). This interactive CD-ROM explains the AICPA rules (including SECPS independence quality control requirements) and SEC regulations on independence, including side-by-side comparisons of the AICPA and SEC rules.
- *SEC Reporting* (Product No. 736745kk). This course will help the practicing CPA and corporate financial officer learn to apply SEC reporting requirements. It clarifies the more important and difficult disclosure requirements.
- *Internal Control Implications in a Computer Environment* (Product No. 730617kk). This practical course analyzes the effects of electronic technology on internal controls and provides a comprehensive examination of selected computer environments, from traditional mainframes to popular personal computer setups.

Courses that might provide more specific appeal to CPAs working in the environment of e-business activities include the following:

- *Auditing in a Paperless Society* (Product No. 730120kk). How can you develop strategies for auditing around, through, and with a computer? Learn how a wide spectrum of technologies is redefining the role of auditor and auditee in this self-study course.

- *E-Commerce: Controls and Audit* (Product No. 731550kk) 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.
- *Internet Investment and Global Positioning* (Product No. 730700kk). In your role as investment adviser and for your investment clients, you might enjoy this financial planning, cutting-edge, self-study course that explains how investing and your role as investment advisor can change with the Internet.

Online CPE

The AICPA offers an online learning tool, *AICPA InfoBytes*. An annual fee ($95 for members and $295 for nonmembers) offers unlimited access to over 1,000 hours of online CPE in one- and two-hour segments. Register today at infobytes.aicpaservices.org.

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, other comprehensive bases of accounting, accounting, auditing, compilation engagements, review engagements, or other technical matters? If so, you may 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 or contact the AICPA at ethics@aicpa.org.

Conference: The Business of E-Business

Among the many interesting conferences the AICPA offers, there is one that might interest you or your e-business clients. It is 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.

Call the Member Satisfaction Center at (888) 777-7077 for additional details.

Web Sites

Additional helpful Web sites are listed in Appendix D, "The Internet: An Auditor's Research Tool."

AICPA Online: www.aicpa.org

AICPA Online offers CPAs the unique opportunity to stay abreast of matters relevant to the CPA profession. AICPA Online informs you of developments in the accounting and auditing world as well as developments in congressional and political affairs affecting CPAs. In addition, AICPA Online offers information about AICPA products and services, career resources, and online publications. See additional Web sites of interest in Appendix A of this Alert.

CPA2Biz.Com

This new Web entity is the product of an independently incorporated joint venture between the AICPA and state societies. CPA2Biz currently offers a broad array of traditional and new

products, services, communities, and capabilities so CPAs can better serve their clients and employers. Because the site functions as a gateway to various professional and commercial online resources, cpa2biz.com is considered a Web "portal."

Some features cpa2biz provides or will provide include the following:

- Online access to AICPA products like audit and accounting guides, and audit risk alerts
- News feeds each user can customize
- CPA "communities"
- Online CPE
- Web-site development and hosting
- Electronic procurement tools to buy goods and services online
- Electronic recruitment tools to attract potential employees online
- Links to a wider variety of professional literature
- Advanced professional research tools

.....

This Audit Risk Alert replaces the *E-Business Industry Developments—2000/01 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 those with us. Any other comments that you have about the Alert would also be appreciated. You may email 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

APPENDIX A

Identifying and Managing E-Business Risks

Risks in E-Business

Recently, one of the most frequently visited sites on the Internet was hit by an onslaught of illegitimate requests for information from its Web server. The company's search engine was soon disabled and could not handle the task of meeting the pressure created by the attack. The following day, other major e-businesses were brought down in a similar fashion.

The fact that these were only virtual attacks—buildings and equipment were not actually harmed—might lead you to discount the seriousness of such assaults. But for e-businesses, the attacks bring enormous financial consequences. Losses suffered in attack situations are every bit as real as the destruction of physical assets. The Federal Bureau of Investigation (FBI) estimates that computer losses in the U.S. total $10 billion a year. The Bureau also estimates that only about 10 percent of all computer crimes are reported to law enforcement because victims want to avoid the negative publicity that results from reporting these crimes. In addition, a recent survey of sixteen hundred information technology (IT) and security professionals in fifty countries performed by *Information Week* magazine revealed that organizations engaging in e-business are three times more likely than other firms to experience information loss and the theft of trade secrets.

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. Some of these characteristics include the following:[19]

- 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.

Recall that e-business is not only the buying and selling of goods and services over the Internet. Rather, 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:[20]

- IT infrastructure vulnerabilities
- Falsified identity
- Compromised privacy

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

20. Steven M. Glover, Stephen W. Liddle, and Douglas F. Prawitt. *E-Business Principles and Strategies for Accountants*. Englewood Cliffs, NJ: Prentice Hall, 2001.

- 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
- Reconfiguration outages, such as those caused by software upgrades, database work, 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 a recent security survey conducted by KPMG, eighty-four percent of responding companies reported that they have a disaster recovery plan. However, eleven percent of those companies had never actually tested the plan. And only half had tested their plans in the last six months.

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 EDI (electronic data interchange) environments because traditional EDI involves 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

Many consumers are concerned that their privacy may by violated if they engage in e-business transactions. Several surveys have found that consumers' biggest concerns are privacy and security. The Federal Trade Commission (FTC) reports that only 41 percent of the most popular Web sites adequately inform customers of their privacy policies, and only 20 percent of Web sites live up to all of the "fair information practices" that the FTC is pushing the online community to adopt. 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. See the discussion of assurance services related to security in the previous WebTrust and SysTrust sections of this appendix.

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. McAfee.com, a company specializing in computer virus protection, estimates that there were at least 50,000 different computer viruses in existence as of February 2000. And several new viruses are introduced every day. These and other malicious code that can harm systems are listed in Table 1, "Common Destructive Codes and Programs."

Table 1 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 that 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.

(continued)

Type	*Characteristics*	*Example*
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 on Web users visiting Price Lotto, a Japanese auction site.

System Interdependencies

The presence of system interdependencies exposes 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

WebTrust℠ and SysTrust℠ services are available for e-businesses wishing to address concerns about security and privacy issues, among others. For example, the AICPA, in conjunction with the Canadian Institute of Chartered Accountants (CICA), has developed WebTrust and SysTrust which offer the opportunity for e-businesses to take action and stem the tide of compromised Web site activities and operations. There are various principles and criteria represented under WebTrust and SysTrust programs. Some of these principles are identical in name, and the criteria that support these principles are similar in impetus as well.

WebTrust

We read again and again about everything from Internet businesses selling or sharing private customer information to consumer fraud. Internet users and the businesses that serve them are justifiably concerned about the integrity of the businesses and parties they are dealing with on the Internet.

WebTrust programs offer several types of assurances for business activities by B2B, B2C, and service provider clients. Some of these assurances include the following:

- WebTrust for Security gives assurance that an ecommerce system provides security for the data it transmits and stores.
- WebTrust for Availability lends assurance that a Web site provides access to an entity's sites as advertised or promised in a service-level agreement.
- WebTrust for Online Privacy assures that the Web site's disclosed privacy practices and related controls have been evaluated and independently verified.

- WebTrust for Business Practices/Transaction Integrity provides assurance with respect to the completeness and accuracy of processing of electronic transactions sent over the Internet.
- WebTrust for Confidentiality provides assurance on the confidentiality of data exchanged over electronic networks such as the Internet or a Virtual Private Network.
- The WebTrust Certification Authorities Program assures that certification authorities (third-party organizations that help enable parties to conduct secure e-business transactions) have certain controls in place that are consistent with WebTrust principles and criteria to provide secure Internet transactions.

There are various WebTrust seals available so that companies can visually display their compliance with WebTrust principles and criteria.

> **Help Desk**—For more detailed information on WebTrust and its certification programs, go to the AICPA WebTrust Web sites at www.aicpa.org/assurance/webtrust/index.htm and www.webtrust.org.

SysTrust

Information systems have become increasingly complex, fast, and integrated, and the number and materiality of the transactions processed by such systems continue to increase year by year. To respond to the needs of management and customers for assurance on the reliability of such systems that they often depend on for their business-related transactions, the AICPA and the CICA have joined forces in developing an attestation service called SysTrust.

SysTrust is crafted under the attestation standards in which the CPA performs procedures to determine whether the controls over a system are operating with sufficient effectiveness to enable the system to function reliably. SysTrust uses the following four principles to determine whether a system is reliable:

- *Availability* refers to whether the system operates and provides information in accordance with the specified requirements of that system, and whether the system is accessible for routine processing and maintenance.
- *Security* refers to whether the system is protected against unauthorized physical and electronic access. Restricting access to a system prevents potential abuses of system components, theft of system resources, misuse of system software, and improper access to private and confidential information. Security also refers to restrictions on the type of information that can be stored and the use of the information captured by the system.
- *Integrity* refers to whether the system processes the information it receives completely, accurately, promptly, and in accordance with the required authorizations.
- *Maintainability* refers to the entity's ability to make changes in the system in a manner that supports current and future reliability. The system should be able to be updated so that it continues to provide system availability, security, and integrity.

Systems reliability is necessary to assure system users that controls are in place relating to their transactions. Ultimately, reliable systems can produce a constant and predictable revenue stream, with minimum related costs to benefit e-business users and other stakeholders.

Help Desk—For more information on SysTrust, visit the Web site for SysTrust at www.aicpa.org/assurance/systrust/index.htm

APPENDIX C
Cyber-Terrorism

Terrorism, as defined by the Federal Bureau of Investigation (FBI), is the unlawful use of force or violence against persons or property to intimidate or coerce a government or any related segment of a government, or the civilian population, to further political or social objectives. By broadening this definition to include information technology, we can expand the scope and impact of a terrorist's attack to include infrastructure, or the services critical for continued operations at a national or corporate level.

Corporations and government agencies have long viewed the security of computer networks as an optional cost. But no more. In the era of cyber-terrorism, it is critical. The focus on "homeland security," or strengthening U.S. security against terrorists, has led federal agencies and businesses to flood network-security firms with business inquiries.

No known terrorist cyber-attacks have been launched since September 11, according to security and law enforcement officials. But on September 11, the FBI issued a 30-day alert that warned of the greater risk of cyber-attacks. Despite the dangers, however, most organizations still have gaping holes in their computer security, making it easy for hackers to attack their systems. A recent report by the U.S. General Accounting Office warned that cyber-terrorists could severely damage national security and telecommunications networks. In response to the threat, the new U.S. Homeland Security Czar, Tom Ridge, named Richard Clarke, already on the National Security Council, as a special adviser for cyber security. He will take over a new post in charge of combating cyber-terrorism and protecting essential information networks. Clarke will head up efforts to safeguard information systems, which includes transportation, communications, power utilities, industries, water and health systems, banking and finance, and emergency services organizations.

Using information technology as a strategic weapon has never been a more accurate metaphor, when attempting to critically define the concept of cyber-terrorism. Cyber-terrorism is a threat of "information warfare" in which a rogue nation, terrorist group, or criminal cartel could perform a "systematic national intrusion" into computer systems, with effects comparable to the terrorist attacks against the World Trade Center and the Pentagon on September 11.

There is the potential for devastating financial repercussions within an organization, both financially and legally. Like it or not, organizations face the legal, ethical, and more often, the social responsibility of securing data, which resides within their computer systems. Failure to establish adequate internal controls exposes the organization to financial loss and legal liabilities, as well as the loss of consumer confidence.

We must realize that cyber-terrorism in its broadest reaches is not solely restricted to national infrastructure targets, and is not solely carried out by rogue nation states, activist groups, or camouflaged, munitions-touting individuals. Cyber-terrorism can be directed at an individual organization by a competitor, for example, in an effort to eliminate the targeted organization's ability to compete in the marketplace. Cyber-terrorism is the twenty-first century version of the ever-present corporate espionage threat.

The distributed denial of service (DDoS) attacks in February 2000 thrust the subject and capability of cyber-terrorism into the mainstream conscience of the global community. While officially dubbed DDoS attacks, the goal is to cripple a device or network so those external users no longer have access to network resources. Without hacking password files or stealing sensitive data, a hacker simply fires up a program that will generate enough traffic to your site so that it denies service to the site's legitimate users. As a result, the global village witnessed its first coordinated, cyber-terrorist attack. Most of the online community was caught, obviously, unprepared.

In addition, over the past several years, various groups and individuals have carried out the following attacks on critical national and international infrastructure:

- A hacker known as "Infomaster" penetrated the Bureau of Land Management network in Portland, then skipped on to Sacramento where he or she obtained root access to the computers that controlled every dam in northern California.
- A Massachusetts teenager broke into the Bell Atlantic system and disabled communication at the Worcester airport, cutting off services to the airport's control tower and preventing incoming planes from turning on the runway lights.
- A Tamil guerrilla group known as the Internet Black Tigers launched a DDoS attack on the Sri Lankan embassy computers throughout Europe, North America, and Asia for two weeks, paralyzing the network.
- Ten thousand Internet activists calling themselves the Electronic Disturbance Theater began a DDoS attack on the Pentagon, Frankfurt Stock Exchange, and Mexico presidential Web servers in support of Zapatista rebels in Chiapas, Mexico.

Potential targets for cyber-terrorists include the following:

- Banks, international financial transactions and stock exchanges, attacks that cause people to lose confidence in the economic system
- Air-traffic control systems, resulting in collisions of civilian aircraft
- Medication formulas at pharmaceutical manufacturers
- Natural gas lines, possibly causing widespread valve failures and explosions by increasing pressure
- the electrical grid, causing blackouts

Protection of Critical National Infrastructure

Infrastructure protection, which requires a systemic approach and accounts for a wide range of vulnerabilities, could fall under both "information/cyber" and physical attacks. For instance, there is no need to destroy an electric power system if you can block the delivery of coal to the power plant. Today, this may be the best example of infrastructure vulnerability.

Critical infrastructure consists of information and telecommunications, gas and oil production, transportation, continuity of government, emergency services, electrical power systems, banking and finance, and water supply systems.

To evaluate the security of internal systems, the U.S. Government conducted a series of exercises called "Eligible Receiver" that revealed serious vulnerabilities in the government's information systems to the extent that 62 to 65 percent of all U.S. federal computer systems have known security holes that can be exploited.

Monitored user access to a specific but unnamed Department of Defense system detected 4,300 intrusion attempts during a three-month period. More than 120 countries or foreign organizations have or are developing formal programs that can be used to attack and disrupt critical Information Systems Technology (IST) used by the United States.

Because of the ambiguous nature of information attacks, it can be extremely difficult to know, even in the midst of an attack, what is really happening. Are computer outages the result of equipment failure or deliberate attack?

Internet Security

Given the uncontrolled (and in reality, the uncontrollable) nature of the Internet, it is easy to see and understand why there are so many security issues and problems. Specifically, consider the following:

1. Companies are not assigning sufficient resources to improve and maintain overall security.
2. Personnel are not given senior management support or authority to implement strategic security measures.
3. Vendors ship systems with poor default security configurations, and customers still buy these systems even with the known defaults.
4. Companies fail to install vendor patches for known security weaknesses.
5. Companies fail to monitor or restrict network access to their internal hosts.
6. Companies do not implement stringent authentication or authorization systems for remote access.
7. Companies do not enforce security policies or standards when installing new equipment on their networks.
8. Organizations continue to place too much emphasis on "security through obscurity." Many organizations still hold to the idea that their systems are not important enough to interest a hacker or terrorist, and therefore they see no need to spend time, effort, and money (especially) to secure them beyond the rudimentary controls.

Infosecurity personnel (internal and external auditors, data and network security officers, and others), should be aware of the strategic security weaknesses presented by these known exposures. An assumption that a firewall will solve all your problems, that security is sufficient, and that no further security checks or controls are needed, could be a fatal mistake.

Cyber-terrorists are very highly trained, use state-of-the-art equipment, and are highly motivated. The professional group comprises criminals, thieves, corporate spies, and general guns-for-hire. Although cyber-terrorists overlap with these professionals, are well-funded, and mix political rhetoric with criminal activity, they pose a serious threat to national governments.

Neutralizing the Terrorist Threat

Although the threat of a cyber-terrorist attack can never really be totally eliminated, the potential of an attack and its devastating aftermath can be mitigated through the implementation of logical, physical, and technical controls. Stopping the elusive cyber-terrorist will require a heightened combination of both logical and physical controls. In addition, organizations will have to establish stringent policies and procedures designed to train information technology (IT) users in better safeguard measures and methods.

What's Ahead?

Cyber-terrorism can be as obvious as the DDoS attacks played out against several prime dot-com companies in 2000, or as transparent as a seemingly loyal employee, who is actually an industrial spy for one of your competitors. Cyber-terrorism can and will assume many forms. Organizations must be vigilant and ready for all of the potential forms of such aggressive acts.

Cyber-terrorism is a reality; it cannot be wished away. Corporations, governments, and private citizens are all at risk, and all are equally responsible for preventing such attacks. There is no equivalent "neutron bomb" that affects only infrastructure and spares individuals. A cyber-terrorist's strike, coordinated against infrastructure, will certainly result in loss of life. Society has yet to truly experience and witness the breadth and devastation of a cyber-terrorist's attack capability. The recent outbreaks of malicious code, DDoS attacks, and system failures may simply have been the beta testing of the individual pieces of a more organized, coordinated, and comprehensive cyber-terrorist strategy.

Corporations, governments, and private citizens responsible for securing infrastructure must invest the time, energy, and resources to continually monitor critical systems and to be ever vigilant to the growing threats to those systems. Even though completely insulating your system or a national infrastructure from the ravages of a cyber-terrorist attack may be impossible, there are several steps which can be taken to help reduce and prevent the potential of such attacks.

Implementing good internal control procedures and structures, aggressive IT audit programs; subjecting systems to third-party, controlled penetration tests; and proactively attacking, defending, and prosecuting malicious intrusions are appropriate steps. If aggressively pursued, these precautions can help to minimize the exposure from random as well as coordinated cyber attacks. Organizations should continue the monitoring of high-speed Internet connections, so that these connections can not be used as part of a DDoS attack.

To avoid becoming victims, it is necessary to know where to find the latest security patches and updates of cyber-terrorist activities. Know how to access resources from sites such as the CERT Coordination Center at Carnegie Mellon University (www.cert.org) and ensure that all systems are adequately protected with multiple firewalls and hard-to-guess passwords. Verify that backup and recovery plans exist, are implemented, and that they work.

At the end of the day, each of us is responsible for ensuring that we remain watchful of the shifting risks that engulf our expanding virtual markets and our virtual society, and realize that each and every one of us is vulnerable.

APPENDIX D

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.financenet.gov/fasab.htm
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/
Guide to WWW for Research and Auditing	Basic instructions on how to use the Web as an auditing research tool	www.tetranet.net/users/gaostl/guide.htm
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

(continued)

Name of Site	*Content*	*Internet Address*
Federal Reserve Bank of New York	Key interest rates	www.ny.frb.org/pihome/statistics/dlyrates
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