

The Practicing

CPA

THE NEWSLETTER OF THE AICPA PRIVATE COMPANIES PRACTICE SECTION



pcps.aicpa.org

November 2009

Inside

4 A Conference Board report urges companies to build risk awareness into performance by integrating enterprise risk management with performance management.

5 A management consulting firm asks clients and prospective clients "Are you paying employees just to show up?"

5 Does the proliferation of social media mean "a fundamental shift in the way we communicate?"

6 COSO highlights four critical areas that contribute to effective board oversight of enterprise risk management.

6 As fraudsters continue to grab media headlines with new schemes, AICPA offers practitioners a tool to help them stay up to date on investigating business fraud.

8 A new SBA online training course helps women entrepreneurs win federal contracts.

PCPS Update

7 PCPS spotlights profitability and pricing strategies ♦ CPAs and SBA loan program business valuations ♦ More connections through PCPS

Protecting a Business and Maintaining Clients' Trust

The ability of any organization to collect personal and sensitive information (data) has grown exponentially over the past few years, and the complexity and risks of managing that data have grown at an even greater pace.

A 2007 study by a University of Washington researcher indicated that more incidents of compromised data were reported in 2005 and 2006 than in the previous 25 years combined. The study also indicated that about one-third of incidents were attributable to malicious hacks, whereas more than 60% involve combinations of mismanagement, criminal intent and, occasionally, bad luck.¹

More recently, one of the top consumer advocacy groups, the Identity Theft Resource Center, reported that data breach incidents increased by 47% from 2007 to 2008.

CPA firms and their clients that collect, manage, and store information face the risk that their data may be lost, misused, or accessed by or disclosed to unauthorized individuals. According to the AICPA, individuals expect their privacy to be respected and their personal information to be protected. With identity theft being reported almost daily, they are no longer willing to overlook a company's failure to protect their privacy.²

Businesses should understand and effectively address privacy and information security as a risk

management issue. Noncompliance or failure to properly respond to a breach of a customer's personal information may result in the following outcomes:

- Damage to the company's reputation, brand, or business relationships
- Legal liability and industry or regulatory sanctions
- Charges of deceptive business practices
- Customer or employee distrust

General regulations and requirements

If a company collects, uses, shares, or retains individual customer information, it should be aware of the specific laws and regulations that apply to it. Several federal and state laws require that the organization implement "reasonable" privacy and information security practices. Depending on the scope of a company's services, the following laws and regulations may apply.

The Federal Trade Commission (FTC) Act

The FTC Act prohibits deceptive or unfair trade practices. Under the FTC Act businesses must handle information in a way that is consistent with their promises to their customers, as in their privacy statements, and avoid data security practices that create an unreasonable risk of harm to a customer's personal information.

By Eric Nelson, CIPP

1. K. Erickson and P. Howard, "A case of mistaken identity? News accounts of hacker, consumer, and organizational responsibility for compromised digital records," *Journal of Computer-Mediated Communication* 12, no. 4 (2007), <http://jcmc.indiana.edu/vol12/issue4/erickson.html>.
2. See AICPA Information Technology Center Web site, "Generally Accepted Privacy Principles," <http://infotech.aicpa.org/Resources/Privacy/>.

continued on next page

continued from page 1

The FTC is the primary agency charged with consumer protection in the United States and enforces company-made privacy promises as well as obligations imposed on companies by privacy and security laws. The FTC also brings actions against companies for failure to comply with federal privacy laws, including the following.

The Gramm-Leach-Bliley Act (GLBA)

Although accounting firms are no longer subject to the notice requirements of GLBA, they must still comply with the Privacy Rule and the Safeguards Rule. Specific requirements for CPA firms may apply to the following:

- Employee information
- Client tax information
- Transmission of client data (encrypted over e-mail)
- Computer and network security
- Accountability
- Retention

The GLBA authorizes eight federal agencies and the states to administer and enforce the [Financial Privacy Rule](#) and the [Safeguards Rule](#).

The Fair and Accurate Credit Transactions Act of 2003 Red Flags Rules

On June 1, 2010, FTC rules go into effect requiring businesses to recognize the “red flags” that tell them someone may be committing fraud. The Red Flags Rules comprise an antifraud regulation that requires creditors and financial institutions with covered accounts to implement programs to identify, detect, and respond to the red flags that could indicate identity theft. According to the FTC,³ the rules “apply to financial institutions and creditors.” The rules define a financial institution as (1) a state or national bank, (2) a state or federal savings and loan association, (3) a mutual savings bank, (4) a state or federal credit union, or (5) any other entity that directly or indirectly holds a “transaction account belonging to a consumer.”

Under the rules the definition of creditor is broad and includes businesses or organizations that regularly provide goods or services first and allow customers to

pay later. Examples of groups that may fall within this definition are health care providers, utilities, telecommunications companies, lawyers, accountants, and other professionals.

State Regulations

In 2003 California was the first state to pass a data breach law, and since that time, more than 45 states have implemented various privacy and information protection laws. These laws generally require a business to protect clients’ personal information and to take specific measures if a breach of that information occurs.⁴

State regulations are enforced by state attorneys general and may include civil and criminal penalties. Failure to properly protect personal information can also fall under both federal and state jurisdictions.

Protecting personal information and mitigating risk

CPA firm clients most likely will need assistance in protecting personal information and mitigating risk. The FTC has developed general guidelines to help businesses understand how to protect sensitive personal information and mitigate the risks of a data breach. These guidelines include the following:⁵

1. *Take Stock.* Know what personal information is in files and on computers.

Understand what personal or sensitive information your organization collects, manages, and stores, as well as information shared with third parties. In addition to knowing where information is, know also who has, or could have, access to that information. If you allow employees or contractors to take information off-site, be sure that the information is encrypted.

2. *Scale Down.* Collect and keep only what you need for business.

Keep sensitive information in the company’s system only as long as you have a business reason to do so. Once that business need is over, properly dispose of the information. If you must keep information for business reasons or to comply with the law, develop a written records retention policy to identify what

3 Federal Trade Commission, “Fighting Fraud with the Red Flag Rules: A How-To Guide for Business,” <http://ftc.gov/bcp/edu/microsites/redflagrule/index.shtml>.

4 See AICPA Information Technology Center Web site, State Security Breach Laws, <http://infotech.aicpa.org/Resources/Privacy/Federal+State+and+Other+Professional+Regulations/State+Privacy+Regulations/State+Security+Breach+Laws.htm>.

5 Federal Trade Commission, “Protecting Personal Information: A Guide for Business,” <http://www.ftc.gov/bcp/edu/pubs/business/idthefi/bus69.pdf>.

The Practicing CPA (ISSN 0885-6931) November 2009, Volume 33, Number 9. Publication and editorial office: 220 Leigh Farm Road, Durham, NC 27707. Copyright © 2009 AICPA. Opinions of the authors are their own and do not necessarily reflect policies of the AICPA.

Editor: William Moran.

Editorial Advisors: William R. Pirolli, Warwick, RI; Barry D. Beck, Woburn, MA; Peggy A. Dzierzawski, Troy, MI; Jina Etienne, Silver Spring, MD; Kevin R. Heppner, Madison, WI; Scott W. Kies, Tucson, AZ; Victoria A. Martin, Hickory, NC; Dennis K. Meservy, Las Vegas, NV; Marc Parkinson, San Jose, CA; Phillip J. Santarelli, Philadelphia, PA; Melody D. Schneider, Fairbanks, AK; Jerry A. Topp, Fargo, ND; George S. Willie, Washington, DC; Lee D. Wunschel, Toledo, OH; Michelle L. Zimmerman, Indianapolis, IN

information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when it is no longer needed.

3. *Lock It:* Protect information that you keep.

According to the FTC, the most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers.

- *Physical security.* Ensure that paper documents and electronic storage files are secured properly and access is limited to those with a specific need. Employees should log off their computers, lock their file cabinets, and ensure office doors are locked at the end of the day.
- *Electronic security.* Identify all computers or servers that store sensitive personal information as well as all connections to computers and computer systems. This includes internal connections, for example wired or wireless network connections, and external connections to the Internet, third parties, etc. Encrypt files transmitted to third parties or over a public network.

Electronic and administrative security includes controlling sensitive information by implementing access controls. The controls can include password management, for example, strong requirements, frequent password changes, policies against sharing passwords, and technology solutions that prevent unauthorized access and log unsuccessful access attempts. According to the *Desktop Computer Encyclopedia*, a *strong password* is one that is hard to detect by both humans and the computer. Two things make a password stronger: (1) a larger number of characters, and (2) mixing numeric digits, upper and lower case letters and special characters (for example, \$, #).

- *Employee training.* A well-trained workforce is necessary to ensure personal information is protected. It is also a requirement of a number of state and federal regulations. Employee training is not a one-time event. All employees must be reminded regularly of the company's policy—and any legal requirement—to keep customer information secure and confidential.
- *Security practices of contractors and service providers.* Sharing of personal information with third parties, including client and employee information, is one of the greatest risks associated with a data breach.

Before outsourcing any business functions—payroll, web hosting, customer call center operations, data processing and the like—investigate the company's data security practices and compare their standards with yours.

Address security issues related to the type of data service providers handle in your contract with them

Small Businesses Targeted by Cyber Criminals

Small and medium-sized businesses are increasingly becoming targets of cyber criminals. Testifying before the Senate Committee on Homeland Security and Governmental Affairs, Michael Merritt, assistant director of the U.S. Secret Services' Office of Investigations, said that organized cyber groups based abroad are stealing not only credit card numbers, but also personal information, including Social Security numbers of the card holders.

Merritt attributes the shift to targeting small and medium-sized businesses to their lack of high level security. Consequently they are more vulnerable than larger companies with more sophisticated computer network protections.

Red Flags Rules Enforcement Postponed Again

Bowing to pressure from Congress, the Federal Trade Commission (FTC) has once again delayed enforcement of the Red Flags Rules. The controversial regulation (which seeks to prevent identity theft) was set to take effect November 1, 2009 but will now be postponed to June 1, 2010. Many professional organizations (including AICPA) object to application of the Red Flags Rules to professionals who bill customers only *after* providing services.

and insist that they notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of your data.

4. *Pitch It.* Properly dispose of what you no longer need.

Improperly disposing of personal information, such as leaving personally identifying information in a dumpster, can facilitate fraud and expose individuals to the risk of identity theft.

The FTC requires businesses to implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to—or use of—personally identifying information.

5. *Plan Ahead.* Create a plan for responding to security incidents.

Protecting personal data is the first step in preventing a data breach; however, breaches can still happen. Preparing and responding to a breach includes designating a senior staff member to coordinate and implement a response plan. The response may include notifying individuals, law enforcement, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, many

continued on next page

continued from page 3

states and federal regulatory agencies have laws or guidelines addressing data breach and notification requirements.

Risk management

Every CPA firm and its client companies should recognize privacy and information security as risk management issues. Practitioners and their clients should tailor their programs to the sensitivity of their customer information and design programs that are appropriate to the size and complexity of their individual businesses.

Protecting the personal information of clients and employees is not only the law, it is also good business.

Eric Nelson is a practice leader with Lyndon Group, which serves clients that have needs associated with privacy and information security. He is a Certified Information Privacy Professional (CIPP) and specializes in federal, state, and international privacy and information security compliance and breach mitigation.

Eric has participated on legislative and regulatory committees and has served as an advisor to local and state governments. He has contributed to federal identity theft legislation and developed the privacy and information security student curriculum currently used by the University of Illinois. Eric is an active member of The Privacy Consortium, a collaborative group of leading international privacy experts, and a frequent speaker on the subject of privacy and information security. For more information visit www.lyndon-group.com.

The Conference Board: Integrating Risk Assessment and Strategic Planning

Integrating risk assessment data into performance management adds significantly to strategic and operations planning, according to a Conference Board report released September 15, 2009. However, few companies have integrated their enterprise risk management (ERM) and performance management processes.

Ellen S. Hexter, author of the report, along with Daniel Sandy Bayer, president of Bayer Consulting, said, "This integration provides decision makers with a dynamic analytical framework for evaluating operational strategies, acquisitions and divestitures, and capital investments across business units, asset types, and risk profiles. The combination of ERM and performance management is very valuable for strategic and operating plans that have long-term business consequences. A risk-adjusted performance framework offers organizations the ability to explicitly link personal and performance objectives."

ERM and performance management are two complementary processes essential for managing an organization. Both disciplines support organizations' efforts in making decisions and meeting their goals: ERM by identifying and managing the risks that could affect business objectives, and performance management by identifying and measuring the drivers needed to achieve results.

Risk-adjusted performance metrics offer managers tools that strike the appropriate balance between meeting performance goals and achieving appropriate returns for the risks being taken. Applying risk-based performance management also may lead to incentives that are more aligned with an organization's long-term success.

Despite these benefits, integration of these processes in companies has not been universal. In a recent survey by The Conference Board of 97 senior executives, 57% of the responding organizations had both a formal ERM program and a performance management program. Of this group

only 43% said that integrating the programs would be extremely or very valuable. When asked if their companies would increase their use of risk assessment data in planning during the next 12 months, just slightly more than half of respondents from companies with both programs (53%) said that such an increase was extremely or very likely.

The report concludes that organizations are reluctant to include risk assessment data in their planning processes for the following reasons:

- *The ERM program is not considered effective.* Only 52% of the executives with both an ERM and a performance management program considered their ERM programs to be extremely or very effective at the corporate level, and just 30% rated their programs that highly at the business unit level.
- *A lack of commitment from the top.* Executives cited a lack of management focus as one of the greatest challenges to the integration of ERM and performance management.
- *A need for more sophisticated performance metrics.* Only 34% said that their companies use risk-adjusted return on capital at the corporate level, and even fewer (21%) do so at the business unit level. Seventy-three percent said that their risk measures were not compatible with their planning metrics.

Hexter feels recent and continuing economic conditions may spur further use of risk assessment data. "Given the dramatic losses suffered by some major companies in recent years, including during the recent financial crisis, boards of directors and senior management will become increasingly interested in ensuring that planning processes throughout their organizations incorporate an explicit assessment of risk," he says.

Source: *Building Risk Awareness into Performance: Integrating ERM and Performance Management* Report # 1448-09-RR, The Conference Board.

Are You Paying Employees Just to Show Up?

Data suggest a correlation between compensation approach and profitability

Beware small businesses—you get exactly what you pay for. Such is the advice of management consulting firm George S. May International Company, Park Ridge, IL, in a press release issued August 26, 2009. The advice is based on the consulting firm's recent survey of 1,000 small businesses in the United States. Survey results indicated that 41% of owners pay employees just to show up, and that model is killing profitability.

"Too many small businesses still reward employees for just showing up, for being a warm body every day, when they should be paying them based on performance related to specific, measurable goals," said Paul Rauseo, managing director of George S. May International. "You're setting the stage to destroy profits when employees expect compensation for participation in collaborative activities, regardless of results."

According to the survey 45% of small businesses claim to be unprofitable. Rauseo feels the relationship

between the compensation and profitability data may not be a coincidence. "The similarity of those numbers shows how closely your compensation style and profitability are linked. Small businesses can no longer turn a blind eye to that connection. They need to shake off their complacency and commit to making real change in operational efficiencies," he said.

The "pay-for-performance" concept was limited initially to a small group of companies. However, the concept has expanded rapidly over the past year as businesses look for ways to improve operations. About 60% of small businesses claim to use the model, although not all (only 55%) institute the specific, measurable employee goals needed to make the system work.

"We tell clients to stop paying employees just to show up," Rauseo said. "Pay-for-performance doesn't guarantee profitability, but it has advantages in a down economy. Now is the time to climb out of the cellar of economic despair and plan for profit. There are things you can do to turn your business around—taking a long, hard look at your compensation practices is one of them."

The Stability of Social Media

"Are social media a fad or the biggest shift since the Industrial Revolution?" asks Erik Qualman in a *Search Engine Watch* article, "Social Media: Fad or Revolution?" published August 10, 2009. Qualman quickly answers his question with the subheadline, "Welcome to the Social Media Revolution."

To support his confidence that social media are not fads, Qualman presents 37 statements as evidence that social media are "a fundamental shift in the way we communicate."

Employee recruitment and retention

The following statements in Qualman's long list may be of interest to CPA firms and their clients in that they might remind firm recruiters to be aware of probable differences in the culture and expectations of younger prospective employees:

- By 2010 Gen Y will outnumber baby boomers—96% of Gen Y have joined a social network.
- Eighty percent of companies use LinkedIn as their primary tool to find employees.
- A 2009 U.S. Department of Education study revealed that, on average, online students outperformed those receiving face-to-face instruction.
- One in six higher education students is enrolled in online curriculum.

- Generations Y and Z consider e-mail passé. Boston College stopped distributing e-mail addresses to incoming freshmen in 2009.

Client recruitment and retention

Many firms and their clients use social media for marketing. Qualman points out that not only is the venue different, but also the approach by providers should be different. Here are a few of his statements:

- In the near future, we won't search for products and services; they will find us via social media.
- Successful companies in social media act more like Dale Carnegie and less like David Ogilvy—listening first, selling second.
- Successful companies in social media act more like party planners, aggregators, and content providers than traditional advertisers.
- There are more than 200,000,000 blogs.

Qualman closes by saying to readers, "Please feel free to share [his statistics and observations] with any non-believers!"

The article can be found online at <http://searchenginewatch.com/3634651>.

Qualman is the author of recently published *Socialnomics* (Wiley Publishing).

COSO Supports Improved Board Risk Oversight

COSO highlights four critical areas that contribute to effective board oversight of enterprise risk management.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) organization provides thought leadership and guidance on internal controls, enterprise risk management, and fraud deterrence. On September 1, 2009, COSO released a new thought paper, *Effective Enterprise Risk Oversight: The Role of the Board of Directors*. Its purpose is to help boards of directors strengthen their oversight of enterprise risks.

“The role of the board of directors in enterprise-wide risk oversight has become increasingly challenging, especially in light of the current economic crisis,” said COSO Chairman David Landsittel. “The challenge facing boards is how to effectively oversee an organization’s enterprise risk management (ERM) in a way that provides improved oversight while adding value to the organization.”

The four-page paper, which is available for free download on COSO’s Web site, www.coso.org, calls attention to COSO’s *Enterprise Risk Management—Integrated Framework* (2004) and its definition of ERM.

In emphasizing the critical role boards of directors play in overseeing ERM, the paper points to four specific areas discussed in COSO’s 2004 ERM framework that contribute to board risk oversight.

“Although ERM is not a panacea for all the turmoil in the markets today, robust engagement by the board in enterprise risk oversight strengthens an organization’s resilience to significant risk exposures,” added Landsittel.

COSO is developing an additional thought paper that will provide more in-depth discussion on how senior management can strengthen risk management processes to improve the board’s risk oversight processes. That thought paper is expected to be released in the fall of 2009.

COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. COSO is a voluntary, private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. COSO comprises the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Management Accountants, and the Institute of Internal Auditors.

A Tool for Fighting Company Fraud

Fraud continues to fill headlines, whether the schemes are old or new. Here’s a tool to help practitioners stay up to date on investigating business fraud.

Although media coverage of the Madoff Ponzi scheme has abated, similar schemes earn headlines even when they are less spectacular in the volume of victims and their losses. Other frauds continue to gain notoriety, for example, hedge fund fraud, mortgage fraud, identity theft, and data and intellectual property theft.

Despite the notoriety of fraudulent acts and their repercussions for perpetrators, the fraudsters carry on, some apparently sure of being untouchable. Consider, for example, United States Attorney Tim Johnson’s announcement in early September, 2009 that a former accounts supervisor for a Houston area chemicals company was charged with embezzling more than \$3.6 million from her employer.

The suspected embezzler pleaded not guilty to wire fraud arising from a scheme she allegedly devised to steal more than \$3.6 million from her employer, Kaneka Texas, a subsidiary of Kaneka Japan, a chemicals company. The indictment alleges that as an accounts supervisor with Kaneka, she was responsible for processing invoices submitted by Kaneka’s vendors for payment and supposedly used that process to implement a scheme to have \$3,621,220 from Kaneka’s bank account wired to her own account at a Houston area bank from June 2006 through February 2008. Allegedly she used the embezzled money to buy a luxury home, luxury vehicles, and jewelry and to finance several gambling trips to Louisiana and Las Vegas.

The investigation leading to charges was conducted by the FBI and initiated in 2008 prompted by Kaneka’s discovery of the embezzlement.

Since the FBI’s announcement of the Kaneka theft, the print media have published several similar tales of employee embezzlement. Although these thefts took

continued on page 8



New PCPS Resource Spotlights Profitability and Pricing Strategies

The AICPA PCPS team works continuously to create new and improved resources for PCPS members. The latest example is a useful section addition to the PCPS Web site. The new section focuses on firm profitability and pricing, which are critical concerns for all CPA firm owners. To help members understand and address the issues involved, the new PCPS Web site section, **Profitability and Pricing Strategies**, has a wealth of practical tools created by the Rainmaker Consulting Group that CPAs can put to use immediately. The tools include:

- A learning guide that explains the keys to profitability, billing rates, and price differentiation, among other topics.
- An action plan that sets out the necessary steps to improvement and provides links to useful resources for each step.
- A firm comparison tool that enables PCPS members to measure their own results against the benchmarks in

the 2008 PCPS/TSCPA National MAP Survey.

- A sales presentation preparation tool that lists possible client negotiating strategies and enables practitioners to develop compelling responses.

These are just a few of the resources and articles available on the site created to help practitioners maintain Five-Star Client Service while enhancing their bottom lines. Visit the site today to see all it has to offer.

CPAs and SBA Loan Program Business Valuations

Practitioners who comply with AICPA business valuation services standards can continue to provide business valuations when lenders and development companies participate in Small Business Administration (SBA) loan programs. In its revised SOP 50-10 5 (B), which became effective October 1, the SBA reaffirmed that licensed CPAs who perform the business valuations in accordance with the AICPA's **Statement on Standards for Valuation Services (SSVS1)** are considered to be a "qualified source," as are AICPA ABV credential holders. Added by this SOP revision is a requirement that the valuation professional's qualifications must be presented in the report, and the report must be specifically requested by and prepared for the lender. The SBA first added "CPAs who follow SSVS1" to its list of those considered to be a "qualified

source" in the wake of AICPA advocacy efforts earlier this year.

Making Even More Connections Through PCPS

Are you aware that you can use the professional networking site LinkedIn to follow PCPS activities and network with other PCPS members? If you are registered with LinkedIn, look for the **Private Companies Practice Section Group** to find news and contacts. You can join group discussions, access special resources, and learn the latest developments affecting smaller firms. It's a great way to extend the networking and informational benefits of PCPS membership. If you haven't already joined the site, go to the **LinkedIn** home page to learn how to sign up for free membership.

This publication has not been approved, disapproved or otherwise acted upon by any senior technical committees of, and does not represent an official position of, the American Institute of Certified Public Accountants. It is distributed with the understanding that the contributing authors and editors, and the publisher, are not rendering legal, accounting, or other professional services in this publication. The views expressed are those of the authors and not the publisher. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

In Case You Missed It . . .

A new white paper, *Understanding Internal Control and Internal Control Services*, explains the concepts of internal control (specifically internal control over financial reporting) and the types of services related to internal control that may be performed by practitioners in public

practice. It is intended to address confusion among practitioners on the topic. Download the white paper at <http://www.journalofaccountancy.com/Issues/2009/Sep/White+Paper+Understanding+Internal+Control+and+Internal+Control+Services.htm>.

continued from page 6

place in professional firms rather than a larger company like Kaneka, the embezzlers were employees who handled invoices. Apparently, appropriate controls were lacking.

Employee embezzlement might be more prevalent than is evident to the public. The reason is victim companies often want to avoid the negative publicity that comes with pursuing fraud perpetrators for punishment or restitution.

Updating skills

Some CPA firms and many of their clients are not ready yet to uncover or investigate new fraud schemes and challenges. Nevertheless the burden is on them to know the latest tools and techniques for addressing these new frauds.

The *Guide to Investigating Business Fraud* can bring practitioners up to date on these tools and techniques and provide them a clearly defined framework for approaching a fraud investigation from start to finish. This resource was developed by the seasoned fraud investigation team at Ernst & Young and represents a body of veteran knowledge. Each chapter is written by subject matter experts in the issue under discussion. The chapters are designed so that they may be read individually as self-contained reference guides for specific topics of interest or together as a holistic overview of a fraud investigation.

In book format, the guide is available to AICPA members at \$79 and to nonmembers for \$98.75. For more information or to order go online to www.cpa2biz or call (888) 777-7077.

Winning Federal Contracts: A Guide for Women Entrepreneurs

SBA launches a new online training course.

As was reported in the October 2009 *The Practicing CPA*, on September 1, 2009, the U.S. Small Business Administration (SBA) launched an online training course to strengthen access to contracting opportunities for small businesses, including those owned by women, minorities, disadvantaged individuals, and veterans. The training course, "Recovery Act Opportunities: How to Win Federal Contracts," is part of a federal government initiative.

On October 14, 2009, the SBA launched another training course to help women who own small businesses. The new training course, "Winning Federal Contracts: A Guide for Women Entrepreneurs," is part of an ongoing government-wide initiative to promote opportunities in government contracting for women-owned businesses.

Contract quota: at least 5%

This free online tutorial is a practical and easy to use guide that walks a woman-owned small business through the contracting process. SBA is committed to ensuring that women-owned businesses receive at least 5% of federal contracts and believes better training opportunities are central to meeting this goal.

Administrator Karen Mills said, "Federal contracts can provide unique opportunities for women entrepreneurs and small business owners to grow their businesses and create jobs, particularly during these tough economic times. It's also a win for federal agencies, by contracting with women-owned small businesses, they are working with some of the most innovative and dynamic companies in the country."

A network of women's business centers

The SBA's Office of Women's Business Ownership oversees a national network of more than 100 Women's Business Centers (WBCs) that provide education and training to help women start and grow small businesses. In addition, the SBA has 68 district offices and other resource partners throughout the country available to train and counsel women-owned small businesses and entrepreneurs seeking government contracts.

"This online training course makes critical information and training available to an even wider array of women entrepreneurs and small business owners," said Ana Harvey, assistant administrator for SBA's Office of Women's Business Ownership. "SBA wants to help ensure they have the tools and resources they need to compete for and win federal contracts."

The Winning Federal Contracts course is designed to help women entrepreneurs learn about the federal procurement process and to prepare them to compete for contracting opportunities. The self-paced guide uses audio and script to provide information about contract rules, how to sell to the government, and where to find contracts.

The Winning Federal Contracts course is available on SBA's Web site at <http://www.sba.gov> or directly at www.sba.gov/fedcontractingtraining. It is indexed by subject matter and includes direct links to additional contracting resources.

Letters to the Editor

The Practicing CPA encourages its readers to write letters on practice management issues and on published articles. Please remember to include your name and telephone and fax numbers. Send your letters by e-mail to pcca@aicpa.org.