

University of Mississippi

eGrove

Newsletters

American Institute of Certified Public
Accountants (AICPA) Historical Collection

4-1997

Members in Medium Public Accounting Firms, April 1997

American Institute of Certified Public Accountants (AICPA)

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_news



Part of the [Accounting Commons](#)

Members in Medium Public Accounting Firms

April 1997

AICPA

How Managing Your Software Assets Can Minimize Potential Piracy

Highlights

B2

Will Your Firm Be in Compliance? The Newly Issued Statements on Quality Control Standards

B3

Proposed Solutions to Standards Overload

B3

Volunteerism at Its Best

B3

Obtaining Other Supplements

B4

Assessing Year 2000 Vulnerabilities: A Concern for CPAs in Public Practice

B4

T2: Technology Solutions for Tomorrow Today

Each year, the software industry loses an estimated \$12.8 billion due to software piracy—or the unlicensed use of software. Firms using software that is not covered by a license are guilty of engaging in piracy. Even if the piracy is committed by one staff member who is careless or ignorant of the laws, the firm can face both civil and criminal charges despite the fact that the action does not reflect management policy. A civil action may be instituted for injunction, actual damages (including infringer's profits) or statutory damages up to \$100,000 per infringement. Criminal penalties include fines up to \$250,000 and jail terms up to five years, or both. In many cases, a company agrees to a financial settlement but may also incur legal fees, negative publicity and possible business disruption from the loss of key business software.

The software industry takes this problem very seriously. It has created the Business Software Alliance (BSA) and the Software Publishers Association (SPA) to police the illegal use of software. Both organizations have toll-free numbers for whistle-blowers that are well publicized and are called frequently by disgruntled employees. Here are some recent examples of financial settlements with the BSA:

- Professional Service Industries Inc., a Chicago-area engineering consulting firm, paid a \$325,000 penalty.
- Massachusetts-based Memotec Communications Corp. paid a \$175,000 penalty.
- Enterprise Products Company, a petrochemical company in Houston paid a \$160,000 penalty.
- Electronic Measurements, Inc., an engineering firm in Neptune, New Jersey, paid a \$97,500 penalty.
- Ironstone Group, Inc., a real estate tax con-

sulting firm headquartered in San Francisco, paid a \$77,000 penalty.

Limiting Software Piracy

Firms that want to limit the possibility of piracy should focus on the management of their software assets. In many cases, businesses do not have sufficient control over these assets because of the way that computer usage has evolved. Since its introduction over 20 years ago, the PC has forever changed the way we do business. As a result of huge technology advances and a highly competitive market, technology costs have plummeted and a PC on every desktop has become a reality.

In small businesses, where no prior computer technology existed, PCs were introduced as collections of isolated workstations and now are part of integrated networks. In larger businesses, PC networks have replaced or supplemented mainframe or minicomputers. In all businesses, PCs, minicomputers and mainframes are becoming part of the mother of all networks, the Internet.

This distributed-computing model increases the benefits of technology by bringing information closer to the knowledge worker and end-user. At the same time, this decentralized approach is inherently more challenging for technology professionals to manage and often results in unknown and uncontrolled ownership costs.

One contributing factor is the lack of software standardization across an enterprise. Business PCs usually start their service life in an approved configuration but over time are modified through software upgrades and installation of non-approved user software. Eventually, no two PCs are alike.

Some of this is to be expected, but the

continued on page B2



Continued from page B1—Piracy

lack of an enforced standard creates a support challenge for information system personnel and encourages end-user practices that are not in the firm's best interest. Some of these practices include:

- Decentralized software purchases.
- Copying company software for home use.
- Installing unauthorized software of unknown origins (that may be infected with viruses).
- Installing software on multiple workstations when only one license exists.

These practices increase support costs and may lead to possible under- or overlicensing of software. A firm that is unaware of what is installed on its workstations may be surprised to learn that it has more software licenses than it needs—or that it is guilty of piracy. By keeping track of software and licenses through a comprehensive software asset management program, you will be assured that you are paying only for the software you need.

What Should You Do?

A software user's first responsibility is to purchase original programs only for individual use. In a business, every computer

must have its own set of original software and the appropriate number of manuals. It is illegal to purchase a single set of original software to load onto more than one computer or to lend, copy or distribute software for any reason without the prior written consent of the software manufacturer.

To ensure that they are in compliance with the laws, firms should establish the following procedures:

- *Analyze the organization annually to determine what software is needed.* The basic questions to answer include: Is the firm using the most efficient and effective software to meet its needs? Is the staff satisfied with current software packages? Would other packages enable the staff to operate more efficiently? Identify the appropriate software profile for each computer user by assessing whether departments or individual staff members need alternative or extra software packages. Network operators should consider purchasing a network metering package to restrict the number of users according to the number of licenses.
- *Prepare an inventory of your current software with licenses and conduct periodic*

physical checks to determine compliance. Any illegal software discovered during the inspection should be deleted right away.

- *Purchase licenses for enough copies of each program to meet current needs.* Budget for future software to keep up with staff requirements.
- *Demonstrate the firm's commitment to software management and use of legal software by adopting appropriate procedures.* For example, appoint a software manager to ensure that all the software analysis and management functions are conducted efficiently; create and circulate an antipiracy policy to all employees; and ensure that all staff understand management's commitment to software management.

For further information contact:

- Business Software Alliance, 1150 18th St. N.W., Suite 700, Washington, D.C. 20036; telephone: 202/872-5500; Web site: www.bsa.org.
- Software Publishers Association, 1730 M St. N.W., Suite 700, Washington, D.C. 20036-4510; telephone: 202/452-1600; Fax On Demand Service: 800/637-6823; Web site: www.spa.org.

Will Your Firm Be in Compliance? The Newly Issued Statements on Quality Control Standards

At the beginning of this year, two important new standards became effective. Issued in May 1996 by the AICPA Auditing Standards Board, Statement on Quality Control Standards (SQCS) No. 2, *System of Quality Control for a CPA Firm's Accounting and Auditing Practice* (No. 067018CLB4), and SQCS No. 3, *Monitoring a CPA Firm's Accounting and Auditing Practice* (No. 067019CLB4), provide CPA firms with improved guidance for establishing and maintaining a quality control system for their accounting and auditing practices. SQCS No. 2 supersedes SQCS No. 1, *System of Quality Control for a CPA Firm*. The new standards apply to all CPA firms that have an accounting and auditing practice and are enrolled in an Institute-approved practice-monitoring program. Both apply to a CPA firm's system of quality control for its accounting and auditing practice as of Jan. 1, 1997.

SQCS No. 2, known as the general standard, replaces the nine specific elements of quality control presented in SQCS No. 1 with five broad elements. Although many aspects of the previous nine elements have been retained, there have been some changes. It also redefines a firm's accounting and auditing practice to include all

audit, attest and accounting and review services for which professional standards have been established by the ASB or the Accounting and Review Services Committee under rules 201 and 202 of the AICPA Code of Professional Conduct. A firm's accounting and auditing practice includes engagements performed under Statements on Standards for Attestation Engagements (these standards had not been issued when SQCS No. 1 was promulgated) and any other future professional standards that may be issued.

The five broad elements of quality control are:

- *Independence, integrity and objectivity.*
- *Personnel management.*
- *Acceptance and continuance of clients.*
- *Engagement performance.*
- *Monitoring.*

To help firms implement the new standards, a booklet titled *Guide for Establishing and Maintaining a System of Quality Control for a CPA Firm's Accounting and Auditing Practice* (No. 067020CLB4) is available. This guide includes examples of four hypothetical firms and the suggested policies and procedures for design and maintenance of a quality control system that is appropriate for each one's accounting and auditing practice.

Published for AICPA members in medium firms. Opinions expressed in this supplement do not necessarily reflect policy of the AICPA.

Anita Dennis, supplement editor

201/763-2608; fax 201/763-7036; e-mail: adennis20@aol.com

Ellen J. Goldstein, CPA Letter editor

212/596-6112; egoldstein@aicpa.org

Proposed Solutions to Standards Overload

How can CPAs committed to maintaining the highest level of professionalism keep up with the ever-expanding volume of new pronouncements? This issue is referred to as "standards overload," and it is one of the most vexing problems facing many CPA firms. "It affects practices of all sizes," observes Judy O'Dell, chair of the AICPA Private Companies Practice Section Special Task Force on Standards Overload.

In Dec., the Institute Board of Directors endorsed seven recommended action steps proposed by the task force. O'Dell says the task force considered the need for a separate set of accounting standards specifically for private companies but ultimately rejected this idea. "Instead of generally accepted accounting principles, you would have two sets of rules, creating more overload," she says. AICPA President & CEO Barry Melancon has assigned follow-up responsibilities for the action steps to appropriate Institute staff—who are to report back to him with their accomplishments by July 1. Here are the seven recommendations:

- *Increase small firm input into the standard-setting process.* The task force has made recommendations to enhance the effectiveness of the Institute's PCPS Technical Issues Committee, which monitors technical developments that affect private companies, and has called on its current and former committee chairs to help. For example, "Instead of looking at all proposed standards, the committee could focus on the ones that most affect private companies," O'Dell says. In addition, the task force would like to see increased awareness at the Financial Accounting Standards Board of the different issues faced by non-public companies.
- *Facilitate access to the professional literature and improve the*

understandability of that literature. The Institute has taken action on this proposal by creating a CD-ROM containing professional standards and practice aids. Another possible step would be to encourage standard setters to use language that is easy to understand and to apply terms consistently in different standards. In an especially timely initiative, the Institute is offering assistance to members in implementing SAS No. 82, *Consideration of Fraud in a Financial Statement Audit*, including a practice aid, a CPE self-study course, nationwide presentations in late April and early May, a speech outline and more. See SAS No. 82 for further details.

- *Sensitize peer reviewers and reviewed firms to standards overload concerns.* O'Dell observes that in some cases, reviewers impose requirements that are higher than what is actually called for in the standards.
- *Provide guidance on disclosure in other comprehensive bases of accounting presentations.* In many cases, O'Dell says, there is insufficient explanation of how new standards apply to tax- and cash-basis financial statements.
- *Provide guidance concerning materiality and financial statement disclosures.* The task force perceived a need for greater understanding among CPAs in these areas.
- *Provide practical practice guidance concerning compilation engagements.* "There is still confusion about the most effective way to perform a compilation," says O'Dell.
- *Continue to evaluate the effectiveness and relevance of disclosures.* A follow-up step here could be to support the FASB's project on disclosure effectiveness.

"The business environment is complex, so our standards have to reflect the state of the world," says O'Dell, a managing shareholder of Beucler, Kelly & Irwin, Ltd., in Wayne, Pa. The task force believes, however, that despite the necessary complexity, the AICPA can make it easier for CPAs to master and apply new pronouncements.

professional
issues

Obtaining Other Supplements

To obtain any of the seven other *CPA Letter* supplements, or to get copies of Mar. supplements, members can either look for them on the AICPA Web site after Apr. 17 or use the AICPA faxback system.



www.aicpa.org/pubs/cpaltr/index.htm



201/938-3787; key in these numbers at the prompt (documents remain on faxback for two months after publication):

Mar. issue

Large Firms: 1550
Small Firms: 1552
Business & Industry: 1553
Finance & Accounting: 1554
Internal Audit: 1555
Government: 1556
Education: 1557

Apr. issue

Large Firms: 1558
Small Firms: 1560
Business & Industry: 1561
Finance & Accounting: 1562
Internal Audit: 1563
Government: 1564
Education: 1565

Volunteerism at Its Best

Every year, the AICPA provides the CPA volunteers that *USA Today* needs to operate its annual tax hotline. This year, one CPA made a gesture that was above and beyond the call of duty. Claude D. Renshaw, an educator from Saint Mary's College, Notre Dame, Indiana, called to volunteer his time and expenses after he saw the notice in the Jan./Feb. *CPA Letter*.

Renshaw joined a roster of 15 Washington, D.C.-area CPAs at one of several three-hour shifts that began at 9 a.m. and ended on 9 p.m. Eastern Standard Time on Mar. 6. The CPAs who work on the hotline can answer a total of more than 1,800 calls from across the country. Because of their efforts, not only do callers get needed advice, but also the profession's expertise and public spirit receive well-deserved recognition in a *USA Today* article about the hotline that runs the next day.

Assessing Year 2000 Vulnerabilities: A Concern for CPAs in Public Practice

—by Robert R. Moeller, CPA

Robert R. Moeller, CPA, is President of Compliance & Control Systems Associates, Inc., an Evanston, IL-based consulting and seminar delivery organization. He was previously Audit Director for Sears, Roebuck & Co. He can be reached at robtm1@concentric.net.

We are on the eve of a new millennium, the Year 2000. The current warnings about the consequences to our computer systems and to our business and government organizations because of the Year 2000 sound almost as perilous as those of the prophets 1,000 years ago who predicted the imminent end of the world.

The Year 2000 may cause major problems in many organizations because of the way dates were established in computer programs written over the years. To allow for the easy calculation of interest and other time-sensitive matters, dates were often set up as a numeric YYMMDD value. Only two YY characters were used for the year rather than YYYY to save computer memory. The reasoning was that the Year 2000 was too far into the future. This date description may cause problems whenever a computer program calculates items such as future employee benefits. Today, a computer program might compute a future benefit by adding years to a current date, such as 970415. Come the Year 2000, this date would become 000415 and calculations based on subtracting days could produce unpredictable results.

The CPA in public practice should have a good understanding of these Year 2000 vulnerabilities, whether in specific computer systems supporting the financial statements or for overall client organization operations. Any computer system that uses YY format years and adds to a current date, pushing the result past the Year 2000, could cause a problem. The challenge for the CPA is to understand how

Year 2000 questions can affect various clients and to make some effective recommendations. Many clients, particularly smaller organizations, may have computer systems with software purchased years ago. Because those systems have always been reliable, management may not be aware that they have a problem. The CPA can provide a real service to these clients by asking the appropriate questions and helping a client to understand Year 2000 vulnerabilities.

The CPA in public practice might suggest that clients launch a formal Year 2000 vulnerability assessment. This review can be performed in three phases:

- Assess what actions the organization has already taken to address Year 2000 problems.
- Determine the extent of the problem.
- Working with the management, develop a plan to correct any Year 2000 threats. This assessment must go beyond the organization's basic business data processing systems and include all computer systems.

The next step in assessing Year 2000 vulnerabilities is to investigate all potential problem areas. Too often, concerns are limited to just the six-character YYMMDD format dates. Other manual and automated systems may encounter problems. Solutions can be elusive because YYMMDD dates were often coded into computer programs many years ago, and both the programmers who wrote them and the supporting documentation may no longer be available. Specialized software is available, and some organizations have resorted to a line-by-line reading of program source code to find problems.

Working with members of information systems and others in management, the CPA should suggest that an inventory be prepared of which systems depend upon these YYMMDD dates as well as their effect on external sources such as suppliers. The CPA should then discuss the results of the Year 2000 vulnerability assessment with the client and offer help for making any needed corrections. In many instances, the CPA can marshal the company's resources to do a detailed analysis of older but still functioning computer programs.

The Year 2000 is an immovable deadline that cannot be missed. CPAs in public practice can provide some very effective support to their clients—and their own firms—by assessing the corrective actions necessary to meet this deadline.

T2: Technology Solutions for Tomorrow Today

What kinds of technology needs will you and your firm have in the future? How can firms position themselves to serve clients' needs? Technology allows CPAs to deliver services they were never able to offer in the past—and the technology of tomorrow will allow firms to provide higher-valued services than ever before. To leverage these emerging opportunities, it's important to understand the strategic implications of technology by developing and implementing a technology plan.

To help you begin, the AICPA is offering *T2: Technology Planning for Tomorrow Today*—a series of one-day conferences that will be launched in 1997. T2 is a multi-tiered program designed to help small and midsize CPA firms successfully integrate technology into their practices to increase productivity and gain a competitive advantage by creating a technology blueprint.

T2 conference participants will learn how to:

- Assess their firms' technology needs.
- Develop a workable technology blueprint for their firms.
- Effectively implement the blueprint.
- Position their firms to take advantage of changes in technology.

How to obtain information. To make sure you receive a T2 program brochure as soon as possible, please provide the following information to Helen O'Shea at the AICPA via fax or e-mail: Your name and position at the firm; the firm name, address, phone and fax numbers and e-mail address; the number of professionals in your firm; the nearest major city; and whether the firm has a technology partner.



212/596-6060



hoshea@aicpa.org

technology