street wise

BY STEPHEN BARLAS, JOAN DUBINSKY, MIKE OSHEROFF, CURT VERSCHOOR, KATHY WILLIAMS

[NEWS]

PCAOB Wants Advisory Group Nominations | Kathy Williams, Editor

THE PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB) IS soliciting nominations for members of a standing advisory group that will help it carry out its standards-setting responsibilities for auditing. The 25-member group will have expertise in fields such as accounting, auditing, corporate finance, corporate governance, and investing in public companies.

You may nominate yourself or someone else. Nomination forms are available under Standards on the PCAOB website, www.pcaobus.org. Deadline for submitting names is Monday, December 22, 2003.

PCAOB Proposes Auditing Standards

The PCAOB is proposing two auditing standards and an amendment to an interim auditing standard for public comment. The first proposed standard, "Audit Documentation," would establish general requirements for documentation the auditor should prepare and retain in connection with any public company audit, the Board said. This pertains to Section 103 (a)(2)(A)(i) of the Sarbanes-Oxley Act. The Board is also proposing related amendments to the interim auditing standards. Both would apply to engagements completed on or after June 15, 2004. The Board voted on this issue on November 12 and will take comments for 60 days.

The other proposed auditing standard would require registered public accounting firms to expressly state in each public company audit report that the audit was conducted in accordance with PCAOB standards. It would apply to auditors' reports dated on or after the later of January 1, 2004, or the 10th day after final approval of the standard.

To read the proposals, visit the Board's website at www.pcaobus.org, and look under Rulemaking.

Robert Denham Elected FAF Chair

Robert E. Denham, partner with Munger, Tolles & Olson LLP, has been elected chairman and president of the Financial Accounting Foundation (FAF) effective January 1, 2004. He succeeds Manuel H. Johnson, co-chairman of Johnson Smick International, who has been FAF chairman and president since 1997 and a member of the Board of Trustees since 1996.

Also, Edward V. (Ned) Regan, president of Baruch College, has been appointed to the FAF Board of Trustees. His term begins January 1, 2004.

continued on page 5

EMPLOYMENT OFFERS

When asked which benefits they were least likely to offer executive-level job candidates, CFOs in a Robert Half Management Resources study said executive perks (like company cars and club memberships), stock options, signing bonuses, and performance bonuses. The financial executives said these items weren't being offered anymore because of the economy and an emphasis on cost cutting.

Job candidates should be prepared to negotiate but not make unrealistic demands, says Paul McDonald, executive director of Robert Half Management Resources. He cites the five most common mistakes job candidates make and offers advice on how

continued on next page

OFFERS cont'd

to avoid them:

Not knowing what you want. Know your "must haves," such as a minimum base salary, and what you're willing to sacrifice, such as NBA season tickets.

Failing to do your homework. Thoroughly research the market before the interview, including salary and benefits for similar positions, so you'll know how your offer stacks up.

Playing hardball. Be flexible, and don't issue an ultimatum. Have confidence in yourself, but don't display arrogance, which isn't attractive to employers.

Being shortsighted. Before turning down an offer, evaluate the long-term rewards such as career advancement and growth potential.

Not calculating the total costs. Make sure you can afford to accept the position. If you'll have to relocate, make sure the salary covers the costs of living in the new place, and factor in moving-related expenses if they aren't part of the offer. ■

[ETHICS]

10 Steps to an Effective Ethics and Compliance Program

Curtis C. Verschoor, CMA, Editor

IN TODAY'S BUSINESS CLIMATE, ETHICS ARE *NOT* OPTIONAL. STUDIES SUCH as the 1999 Hudson Institute and Walker Information National Business Ethics Study (www.walkerinfo.com) show that companies that pay attention to ethics receive the direct benefits of customer loyalty and enhanced employee retention. Ethics focuses on what we *ought* to do and provides a framework for making decisions.

On the other hand, compliance is a legal discipline describing the rules for determining whether business conduct is acceptable. It concentrates on what we *ought not* do and is based on minimum standards, not those that will bring the benefits of moral consideration. Consequently, today's trends in business ethics emphasize a values-oriented approach rather than a more rules-focused approach.

I have developed 10 steps, with accompanying diagnostic questions, for an effective ethics and compliance program. Based on earlier work by my colleagues, Dawn-Marie Driscoll and Mike Hoffman of the Center for Business Ethics at Bentley College, these steps will help you review your own implementation efforts and determine what activities should be started, continued, or stopped.

Step 1: Conduct a Rigorous Self-Assessment

- What are our company's values?
- What do employees believe are our real values?
- What elements of an ethics and compliance program are already in place?
- What must we create anew?

Step 2: Ensure Commitment from the Top of the Organization

- What outcomes does senior management want to achieve?
- How do they describe what will be different once this program is in place?
- How does senior management demonstrate its dedication?
- Are our leaders ethically neutral or ethically committed?

Step 3: Publish and Distribute a Code of Ethics

- Do we have written guidance that explains our rules and expectations for all employees and stakeholders?
- Do employees know what they can expect from their organization?
- Can employees find, read, and apply this guidance?
- Are the policies and procedures that employees need to do their jobs readily available?
- Are they written at the average employee's reading level?

Step 4: Communicate, Communicate, and Communicate Once Again

- How are our messages communicated?
- Do employees hear and believe us?

continued on page 4

[GOVERNMENT]

PCAOB Proposed Standard on Auditing Internal Controls

Stephen Barlas, Editor

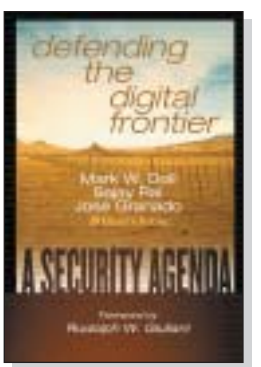
THE PUBLIC COMPANY ACCOUNT-ing Oversight Board (PCAOB) met some of the concerns corporate financial officials have voiced about the upcoming auditors' standard on the "attestation" of corporate internal controls, but it definitely didn't meet all of them. The proposed standard the PCAOB announced in early October says that auditors can rely on the work of corporate accountants some, but not all, of the time. Groups such as the Financial Executives International (FEI) have been arguing that an attestation standard should allow auditors to basically look at the internal controls assessment management is obligated to perform (and comment on in the annual report) under Section 404 of the Sarbanes-Oxley Act instead of testing those internal controls themselves. In the key section of its proposed standard, the PCAOB states, "The proposed auditing standard also would allow the auditor to incorporate into the audit of internal control over financial reporting some of the work performed by others, such as internal auditors or third parties who have performed work under the direction of management." But the auditor has to assess the competence and objectivity of the staff professionals before relying on their work. And the auditor must do certain tasks personally, like work related to company-wide anti-fraud programs and controls, as well as work related to other controls that have a pervasive effect on the company, such as general controls over the company's electronic data processing. The proposed auditing standard also would require that the auditor directly obtain the "principal evidence" about the effectiveness of internal control over financial reporting. As always in federal rulemakings, the devil will be in the def-

continued on next page

BOOKS

Protecting Digital Assets

✷ **IN THEIR BOOK, *DEFENDING THE DIGITAL*** *Frontier*, Mark S. Doll, Sajay Rai, and Jose Granado define the digital frontier as the tradeoff between productivity gains from the use of computer technology and probability of failure of that system due to unauthorized use of the system. Just as physical assets must be protected, digital assets, consisting of operating data, customer information, and gateways to vendors, must be guarded. Instead of providing a technical treatise in computer technology, the authors present a guide to senior management to recognize and plan for the risks of digital failure.



The 1990s saw an explosion in the use of computer technology to increase productivity and increase sales. While the advantage of digital storage and retrieval of information was established well before then, one component of their use changed during that period: the use of the Internet and the World Wide Web. Before that period, companies were connected to vendors and outlying offices by dedicated telephone lines, and communication was relatively secure. Use of the Internet, with its packet-switching technology for communication between offices and for customers completing purchases online, opened up the possibility of not only the interception of data by unauthorized parties but of theft of information from mainframe computers by hackers posing as customers or legitimate users. The Internet also provided a convenient front-end for the

continued on page 6

[ETHICS] cont'd from p. 2

- What are the key messages that must be repeated over and over?
- How well do we handle change?
- Are we using multiple channels to get our messages across?

Step 5: Training

- How are our messages reinforced?
- Do employees get timely training that helps them use our rules and values?
- Are we building a capacity among all employees to exercise moral judgment?

Step 6: Provide Confidential Resources

- Where can employees go with problems, concerns, and allegations of misconduct?
- How reliable and trusted are those resources?
- Must employees channel all concerns through a supervisor, or is there an alternative confidential resource such as a help line or hotline?
- Are confidences maintained?
- Can reports be made anonymously?
- What happens after a call is made?

Step 7: Ensure Consistent Implementation

- Do our processes work smoothly and efficiently?
- Do we work effectively across business unit and organizational boundaries?
- Are roles and responsibilities clear and well documented?

Step 8: Respond and Enforce Consistently, Promptly, and Fairly

- Are we consistent in applying our values, standards, and rules?
- Is appropriate conduct recognized and rewarded?
- How are our internal investigations conducted?
- Is discipline uniformly applied?
- How do we treat high performers who fail to conduct business according to our values?

Step 9: Monitor and Assess

- How do we measure success?
- Do employees receive feedback on our own internal controls?

Step 10: Revise and Reform

- Do we periodically update our values, rules, and program content?
- Are we committed to continuous improvement?

As the overall hallmark of success, when every employee has the courage and ability to talk about ethical dilemmas, we are doing business ethics just right.—*Joan E. Dubinsky*

Joan E. Dubinsky, Esq., directs the Rosentreter Group, a Washington, D.C.-based management consulting practice providing personalized assistance in designing, implementing, and evaluating corporate ethics, business conduct, and compliance programs. She is an Executive Fellow at the Center for Business Ethics at Bentley College, Waltham, Mass.

Curtis C. Verschoor is the Ledger & Quill Research Professor, School of Accountancy and MIS, DePaul University, Chicago, and Research Scholar in the Center for Business Ethics at Bentley College, Waltham, Mass. His e-mail address is cverscho@condor.depaul.edu.

[GOV'T] cont'd from p. 3

inition of such terms as "principal evidence."

Senate Moves First on Corporate Tax Cuts

With a threat of European sanctions hanging over Capitol Hill, the Senate moved first to come up with a substitute for the Foreign Sales Corporation-Extraterritorial Income Act (FSC-ETI) regime. That is a tax credit used by U.S. multinationals that saves companies about $5 billion a year. But the World Trade Organization has said the FSC-ETI is illegal, leading to EU threats that the U.S. replace the tax break by the end of 2003 or else. The Senate Finance Committee passed a bill in early October that replaces the FSC-ETI with a number of new tax breaks, chief among them a 3% tax-rate cut for all U.S. manufacturers and a controversial temporary "tax holiday" that would reduce the tax rate on foreign earnings from American companies. Many Democrats and Republicans in both the Senate and House are worried about the manufacturing economy, so a tax-rate cut has wide support. But the Senate bill and a counterpart introduced by Rep. Bill Thomas (R.-Calif.), chairman of the House Ways & Means Committee, contain numerous other provisions that reduce revenue to the U.S. treasury at a time when the federal deficit is growing like a weed. They include an extension of the net operating loss (NOL) "carryback," AMT relief, repatriation of foreign source income, subpart F reforms, and improved availability of foreign tax credits. Those are all things that groups such as the National Association of Manufacturers (NAM) want. But the Senate bill—called the

Jumpstart Our Business Strength Act—also has some less-appetizing provisions, which led to the NAM withholding its support.

House Moves to Thwart Pro-Business Rules on Pension Plans

The House passed an amendment to the Treasury Department appropriations bill for fiscal 2004 that prohibits the department from publishing final rules on cash balance pension plans, which have been avidly sought by U.S. corporations. Treasury issued proposed regulations last January that relieved companies of the obligation to subject cash balance plans to age discrimination rules. A federal court decision last July ruled IBM's application of an age bias to its cash balance plans was illegal and underlined the need, in Treasury's mind, to finalize its proposed rules. ■

[NEWS] *cont'd from p. 1*

The FAF has oversight, funding, and appointment responsibilities for the Financial Accounting Standards Board (FASB), the Governmental Accounting Standards Board (GASB), and their advisory councils.

Robert Denham is an attorney and former investment banking leader. He joined Munger, Tolles & Olson in 1971, then later went to Salomon Inc. in New York City as its general counsel. He served as the firm's chairman and CEO from 1992 through 1997, then returned to his current firm in 1998. He also is a member of the board of directors and chair of the audit committees of U.S. Trust Company and Lucent Technologies, as well as a member of the board of Wesco Financial Corp. and Fomento Economico Mexicano, S.A. de CV (FEMSA).

Ned Regan has been president of Baruch since June 2000. Before that, he was New York State comptroller from 1979 to 1993 and later served as a member of several corporate and nonprofit boards. He is returning to the FAF Board where he formerly served as a trustee from 1997 to 2000.

New Sarbanes-Oxley Guide

Protiviti has just published a new *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements* that updates its previous guide and frequently asked questions regarding Section 404 of the Act to reflect the Securities & Exchange Commission's final rules. The guide contains 40 pages of new material, including 47 additional questions.

Some of the topics covered are how Section 404 relates to Sections 302 and 906, applying the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Controls—Integrated Framework*, getting started with Section 404 compliance, identifying and assessing controls, testing controls, and reviewing the roles of management, internal audit, the independent public accountant, and the audit committee.

To download a free copy of the report, visit www.protiviti.com.

Clear Out Your Inventory

Every year at this time, the National Association for the Exchange of Industrial Resources (NAEIR) reminds companies that if they want to get rid of excess inventory, they can make a donation and receive a tax deduction. NAEIR is a nonprofit gifts-in-kind organization that accepts donations of new, overstocked, or discontinued products and redistributes them to schools and nonprofits nationwide.

Visit their website at www.naeir.org for complete information. ■

[BOOKS] *cont'd from p. 3*
introduction of computer viruses, which can lead to denial of service to outright destruction of information. Failure of the computer system moved from simple mechanical failure to theft of data and sabotage of the entire system.

Doll, Rai, and Granado identify nine components of a first-class digital security system. The system must be aligned with company objectives. The extent of application of computer technology and commensurate productivity gains are often inversely related to increased risk of failure of that computer system. Senior management must compare these probable costs of system protection and failure—a cost that can't be measured in dollars and cents—to the increased advantage in productivity and market share which the firm gains—a cost that can be measured.

Defense of the digital frontier must be enterprise-wide, extending from the most remote workstation to computers of customers and suppliers, whose networks are often linked to those of their customers. The key phrase is "authority of use." Any workstation that is authorized to connect to a firm's network should be included in its plans of defense.

An organization's digital security system should be updated continuously since hazards, mainly presented by the Internet, change every day. Too, the actual curve of a firm's digital frontier may shift as corporate objectives change or manufacturing technology is updated. Just as installation of security patches is a never-ending process due to newly discovered software flaws and new viruses, the executive entrusted with maintaining the digital security system must be ever vigilant to changing digital security risks.

The security system must be proactive. This means paying attention to what makes the firm's computer system a potential target for unauthorized entry, determining what a potential intruder or disgruntled employee might want to damage or destroy, and taking measures to protect against loss before an attack occurs. In this case, an ounce of prevention is worth more than several pounds of cure.

A security system must be validated, which means actually tested and compared to third-party standards, such as ISO 17799, CISSP, Common Criteria, or other recognized models. Testing a security system for the first time when an incident occurs is a poor alternative to independent validation.

A digital security system must be formal. Policies, standards, and guidelines must be documented and communicated to every member of the organization. Relying on the memory of the head IT manager in the face of business disruption caused by a security incident is a sure recipe for disaster, especially if that person is on vacation when the event happens. And if the security system isn't formalized, there's little chance that the system can be validated against third-party standards.

These components of a world-class digital security program are based on three organizational pieces of any firm: people, processes, and technology. "People" refers to training and how well employees understand their roles in incident recovery. "Processes" refers to the routine tasks of monitoring, validating, and authorizing as well as the specific steps to be followed when a system is hacked or infiltrated. "Technology," of course, is software such as firewalls and intrusion detection programs, but it also includes planning for and configuration of operating systems and alternative input devices such as Wi-Fi and various types of routers. Without the dedication of employees, repeated and understood processes of digital security, and up-to-date technology to electronically protect information, the best world-class security system based on the foundations above will fail.

The authors stress that installation of an effective digital security system must begin with the CEO because only he or she can evaluate the risks the firm takes as increased productivity—made possible with the use of computer technology—bumps up against the probability of unauthorized use of that technology. The CEO's approach and that of other top executives should be similar to their evaluation of any other opportunity the firm faces. Digital security may be in the domain of the IT department per se, but loss of customer lists, operating data, and other digital assets should be considered in a multidiscipline approach in consultation with human resources, legal affairs, business operations, internal audit, finance,

and (physical) risk management because such loss has widespread repercussions across all areas of the firm. The CEO must establish a digital security system in concert with other management from every area of the organization that can be affected by a digital incident. Only the top executive can evaluate the tradeoff between investment in digital security and restricting system access (thus limiting productivity gains) and potential loss of digital assets.

Management typically evaluates an expenditure that benefits more than one accounting period as return on investment (ROI). The CEO may be able to determine the investment required to install an effective digital security system, but the ROI he or she is trying to evaluate is the probability of loss of customer lists, financial information, or the denial of critical Web service to customers. These losses may be expressed in dollars and cents, but loss of customer confidence that personal data is no longer safe can't be. Loss of market share caused by wholesale customer defection to another vendor may lead to economic hardship or eventual failure for the firm. As noted earlier, management can't put a dollar value on loss of sensitive data or market share due to computer theft or introduction of a damaging virus, but the risk is still real and must be planned for. Every CEO whose firm is invested in computer technology or is planning to be in the future should read *Defending the Digital Frontier.—Mike Osheroff*