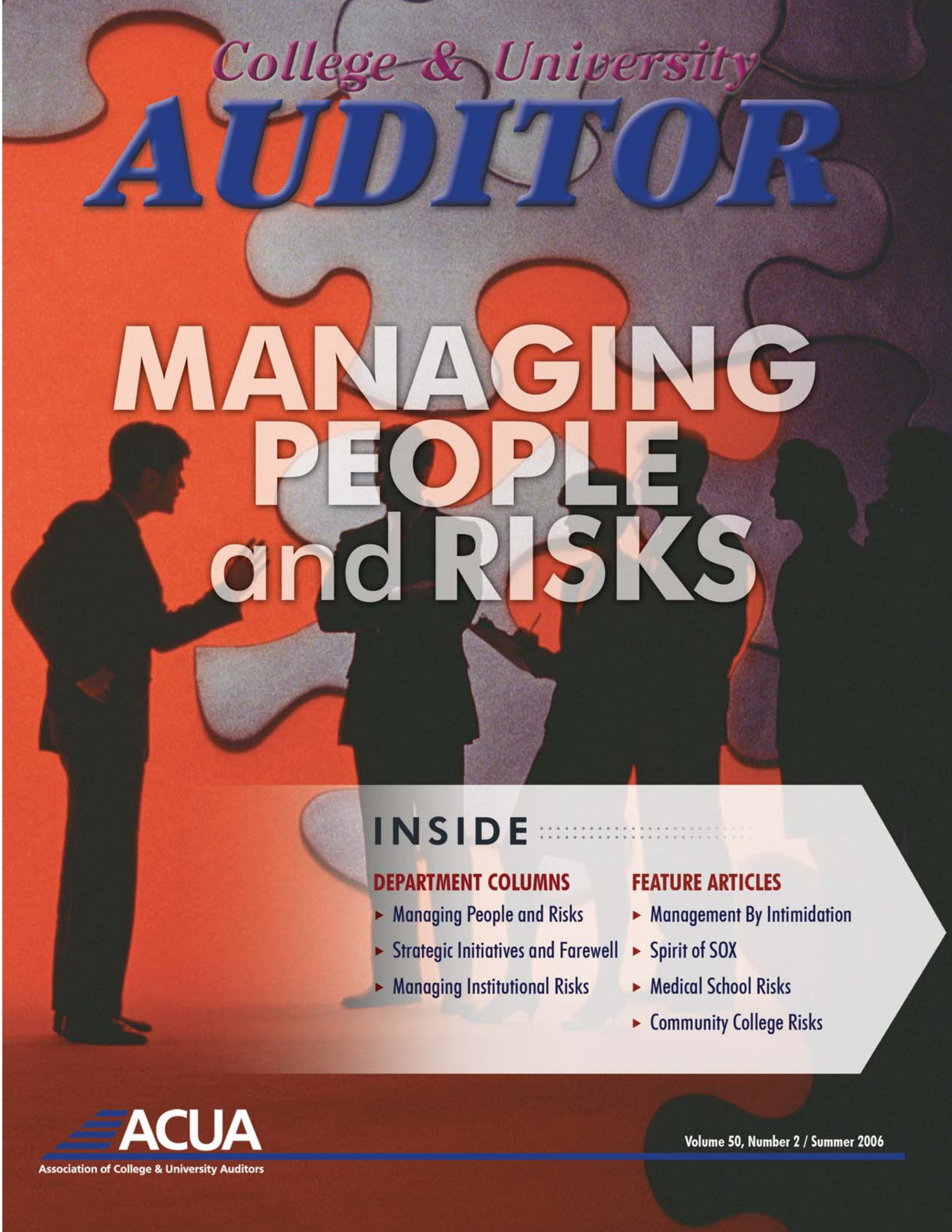


College & University

AUDITOR

MANAGING PEOPLE and RISKS

INSIDE

DEPARTMENT COLUMNS

- Managing People and Risks
- Strategic Initiatives and Farewell
- Managing Institutional Risks

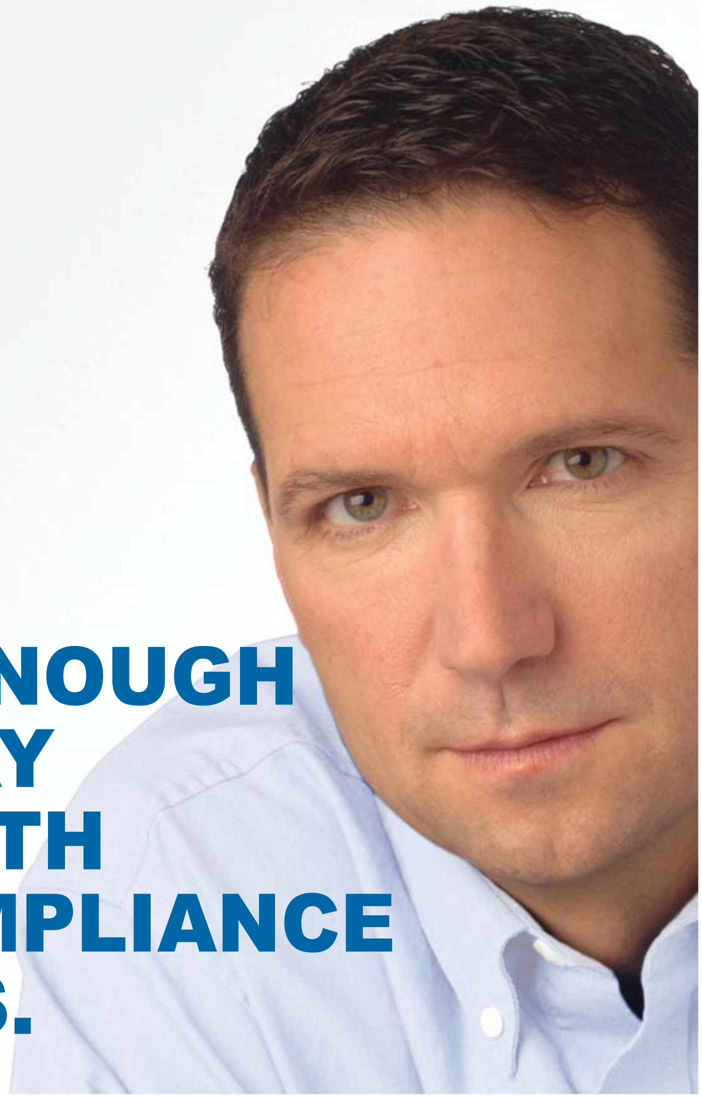
FEATURE ARTICLES

- Management By Intimidation
- Spirit of SOX
- Medical School Risks
- Community College Risks

ACUA

Association of College & University Auditors

Volume 50, Number 2 / Summer 2006



ACUA
Association of College & University Auditors

College & University Auditor is the official publication of the Association of College & University Auditors and is published three times a year in West Hartford, CT. ACUA members are invited to submit letters and original articles to the editor. Go to www.acua.org and click on the "how to" button for further guidelines. The copy deadline for the next issue is **October 4, 2006.** Please send your copy electronically to the editor in Word 95 (or higher) or text file format. The editor reserves the right to reject, abridge or modify any advertising, editorial or other material.

Send address changes to:
ACUA
342 North Main Street, Suite 301
West Hartford, CT 06117-2507

College & University AUDITOR

Vol. 50, No. 2 SUMMER 2006

Contents

Features

Departments

From the *EDITOR*

Managing People **and** Risks

By Slemo Warigon, Editor

Lee Iacocca asserts that "*management is nothing more than motivating people.*" Similarly, Anil Ambani exhorts management to "*work with people*" because managing relationships is "*a question of sharing emotion and feelings*" – not about money.

People are, without any doubt, the most important asset of any organization. They formulate institutional strategies, policies and practices. They transform themselves into effective leaders and productive employees. They also constitute the most important ingredient that transforms an organization from mediocrity to greatness. Given these irrefutable facts, one might feel compelled to ask the burning question: *Why are organizations not doing enough to motivate their employees to be the best they can be?*

People also write *history*, which gives us a good understanding of *past performances* as a basis for predicting the *future*. Niccolo Machiavelli, the Italian statesman and philosopher understood this well when he stated: "*Wise men say, and not without reason, that whoever wished to foresee the future might consult the past.*" This wise saying encapsulates the importance of *risk management* in modern organizations.

Institutions of higher education are facing myriad challenges these days. The market for college-eligible students is becoming increasingly volatile. Competition is increasing. Enrollments are declining. Budgets are shrinking. Academic programs and financial activities are under intense scrutiny by governing and regulatory entities. These environmental factors are pushing institutions to obtain a clearer understanding of the risks they face in order to better protect their human, strategic, financial, physical and intellectual assets.

Institutions of higher education are facing myriad challenges these days. The market for college-eligible students is becoming increasingly volatile.

A risk is essentially anything that prevents an institution from the achievement of its objectives. *Unexamined risks* are quickly opening the gates to hell for many an institution. To avoid this misfortune, institutions are increasingly redefining the role of *risk management* in achieving their strategic objectives. An effective risk management model help institutions to more proactively assess and manage their risks for competitive advantages. This leads to another burning question: *Is your organization really committed to seeking a comprehensive, integrated approach to identifying and managing its risks?*

This issue of *College & University Auditor* sheds some light on these burning questions. The current ACUA president, ***Betsy Bowers***, discusses ACUA's strategic initiatives and reminisces about her presidency. ***Karen Hinen***, ACUA executive director, discusses current issues related to professional development opportunities and management of institutional risks. The first feature article by ***Slemo Warigon*** and ***Betsy Bowers*** addresses the characteristics of *management by intimidation* and positive strategies to minimize their impact on human capital. ***Amy Barrett*** shares her insights about how the University of Texas System has voluntarily adopted the *Sarbanes-Oxley Act* of 2002 in the second feature article that has some implications for other institutions.

The third feature article by ***John S. Ricaud*** of Piedmont Healthcare delineates a robust risk assessment approach for medical schools in particular and institutions of higher education in general. Similarly, ***Imad A. Mouchayleh*** describes the immense benefits of implementing a comprehensive, integrated and process-oriented risk management framework by institutions of higher education in the fourth feature article.

These timely and informative articles help us make trenchant distinctions between the *right* and *wrong* ways of managing *people* and *risks*. An increasingly competitive global marketplace behooves organizations to better manage their human capital. It also behooves internal auditors to assist their organizations in deploying a *systemic solution* for the proactive identification and management of *institutional risks*. We can facilitate the emergence of more *risk intelligent institutions* by ensuring that our *risk management processes* are appropriately embedded into *management practices* at all levels. After all, an institution is only as good as the *people* it keeps and as successful as the *risks* it manages.

From the *PRESIDENT*

Strategic Initiatives **and** Farewell

By Betsy Bowers, President

Where are the *Windows of Opportunity* on your campuses? Are you able to take advantage of opportunities to be of service to your institution? While I hope you have had a great academic year and are enjoying a rejuvenating summer, keeping your eyes open for such opportunities should be a constant.

From a broader perspective, it is always encouraging to see ACUA highlighted in other professional arenas. Recently, ACUA was present at CAUBO (Canadian Association of University Business Officers) and *Campus of the Future* conferences, with the latter hosted by NACUBO (National Association of College and University Business Officers), SCUP (Society for College and University Planning), and APPA (Association of Higher Education Facilities Officers). It has been a busy and exciting time for ACUA. Our strategic plan is also further materializing through the success of task forces on the *Risk Dictionary* and *Internal Auditing Start-Up Kit*. Activities are ongoing with the Web page update, as well as our working with professional firms for our listserv operations, investments and future conference planning. By including these professional services in our mix, we will achieve greater accountability and responsiveness as well as enhance our fiduciary responsibilities to you.

We Want to Hear From You!

Let us know what you think of this issue. Were our pages filled with timely and useful information, or do we have room for improvement? E-mail your comments to khinen@acua.org. E-mails will be edited for clarity and length.

We also had a marketing firm help redesign our image and you will be seeing some interesting things unveiled at the Annual Conference in September. Recently, the ACUA Board met at ACUA Headquarters to update our *strategic plan*. No, ACUA's strategic plan is not a nice, tidy document we prepare every few years and leave on a shelf to collect dust. Your ACUA Board is committed to being responsive to our members and the industry. Therefore, we have decided to reassess, at least annually if not more frequently, the strategic plan and modify it accordingly. We updated it in May to recognize our tactical achievements (e.g., start-up kit, movement of the listserv, etc.), to update our objectives and to place additional tactical goals before us. The plan now reads:

Strategic Goal A: *ACUA will be its members' indispensable resource for education, knowledge exchange, best practices and networking.* {same}

- Objective 1: Continually seek to understand our members' wants and needs. {new}
- Objective 2: Enhance information, navigation and tools on the ACUA Web site. {new}
- Objective 3: Cultivate networking opportunities that encourage camaraderie among members. {new}
- Objective 4: Enhance ACUA-L (e.g., improve search capabilities). {revised}

Strategic Goal B: *ACUA will be the recognized resource for internal auditors in higher education and a principal advocate of higher education internal auditing.* {revised}

- Objective 1: Develop platforms and opportunities for increasing visibility. {new}
- Objective 2: Create a marketing plan to promote higher education internal auditing. {new}
- Objective 3: Create a process for understanding issues and positions that grassroots members want ACUA to advocate for them. {new}

As I write this last column as your ACUA president, I am reminded of how quickly time passes. It seems like only yesterday that I wrote in my first column about our need for your

Continued on page 17

Maximizing **Educational Opportunities** for Audit Effectiveness

By Karen Hinen, CAE, Executive Director

It seems unbelievable that summer is already upon us! Normally, we think of summer as a little slower and more laid back. With summer classes gearing up, campuses are usually a little quieter and many campus staffers take summer vacations. Your ACUA board of directors is, however, in full swing with a whirlwind of activity.

In May, we met to review and refine the *Strategic Plan* and develop a major marketing initiative that will reexamine and redefine ACUA's relevance to its members. We will be looking at everything from logo to Web site. Committees are working feverishly over the summer months to present these initiatives to the membership at the Annual Conference in Louisville this September.

Our 50th Annual Conference in Louisville, KY on September 10-14, 2006 promises to make a big splash! The conference committee and ACUA staff are really going all out to make this a special conference from a *content* standpoint as well as with our *special events* and *outside activities*. Make plans now to attend! Louisville has completely redone its entertainment district and our hotel is brand new. There will be exciting things to see and do in Louisville both at the ACUA conference and in the city itself. For hotel rooms, call the Marriott Louisville Downtown at (502) 627-5045 or (800) 533-0127, and make sure you use our conference code "ACUA" and ask for the $124 daily rate.

John Alston, nationally acclaimed speaker and founder of the *Stress Management Institute of America*, will deliver a humorous, interactive and thought-provoking presentation designed to uplift and empower participants. No one escapes without a good laugh; audiences enjoy John's entertaining style, and people walk away with a new set of skills and techniques for managing change. John offers an energetic perspective, infusing a new spirit and influencing performance amid changing environments.

Learn from a reformed criminal about white collar fraud. *Sam E. Antar*, former CPA and former Chief Financial Officer of Crazy Eddie, Inc., helped mastermind with his cousin Eddie Antar and Uncle Sam M. Antar (co-founders of the company) one of the largest securities frauds of its time. Sam welcomes tough and probing questions, which are what auditors should ask! His presentation provides straight talk and facts as to the dangers of fraud, lack of internal controls, lack of careful auditing, and how criminals take advantage of human nature and the weaknesses of others, including auditors.

> "A campus is like a small community — it faces the same risks as a city or state. It is paramount to understand today's shifting risks and be prepared."
>
> *Ann Franke, Esq.*

Mark "Tenacious" Towers wraps up the conference with his presentation: *Communication Is Everything and Everything We Do Communicates: Strategies That Get Results.* There are three kinds of skills—technical, organizational and people. In a do-more-with-less-and-do-it-faster world, *people skills* loom more important each day. This educational, motivational and entertaining presentation will provide people skills that can be immediately applied at work and at home. Fasten your seat belts and come join us for a one-of-a-kind session.

Webinars: Within the last few months, ACUA has been able to gain NASBA sponsorship for CPE credit for our *webinars*. We have also developed a seminar program from 2006 and to date, the *webinars* have been wildly successful.

Earlier this year, ACUA, in partnership with *EthicsPoint*, offered our members a webinar on the subject of Risks on the Campus of the Future. The topic was so well received that a second session was run. The two sessions, with nearly 250 attendees, covered a number of topics from the relevance of risk management to possible future trends that higher education institutions will continue to face. Additionally, the *webinar* included a DePaul University case study on effective crisis

Continued on page 21

Impact of Management by Intimidation on Human Capital: Is It Destroying Your Organization?

By Slemo D. Warigon, CIA, CISA, CICA, MBA, Director of Audit and Management Advisory Services, Gallaudet University, Washington, DC, and Betsy Bowers, CIA, CFE, CGFM, Associate Vice President, Internal Auditing & Management Consulting, University of West Florida, Pensacola, FL

Introduction

We have read so much about buzzwords such as *management by objectives* and *management by the seat of your pants* and their impact on organizations. Studies have recently addressed "management by fear" and its impact on organizations. This was briefly discussed in the literature as the eighth of *Fourteen Points of Management* by W. Edwards Deming in 1986.

"Management by fear" is synonymous with the new coinage, *management by intimidation* (MBI) – the focal point of this article. Internal auditors are charged with identifying the risks to their institutions, as well as assisting management with positive strategies to minimize the impact of such risks by addressing these salient questions: What are the effects of MBI? What is the cost to your institution? Is it destroying your organization? This article addresses the characteristics of MBI and their negative impact on an organization's human capital. The article also presents a framework for the effective management of such human capital. Finally, this article presents a framework for the preventive maintenance approach to enhance the organization's human capital.

Overview

Management by Intimidation (MBI) is the practice of managing or governing people based on *fear*. MBI affects the overall financial health of an institution. Costs increase, productivity diminishes and revenue decreases. It also has adverse effects on the morale of employees and ethical climate of an organization.

Most organizations have managers or leaders who employ *MBI practices*. Such practices are inconsistent with Deming's eighth point of management, which behooves contemporary management practitioners to "drive out fear" to make employees feel secure enough to express ideas and ask questions. Deming has steadfastly viewed *management by fear* as counter-productive to the long-term health of an organization because it prevents employees from acting in the organization's best interests.

Management by Intimidation **(MBI) is the practice of managing or governing people based on** *fear*. **MBI affects the overall financial health of an institution.**

MBI is not a new concept. Recently highlighted in the *New York Times* (January 23, 2006), Alexis de Tocqueville's *Democracy in America*, originally published in 1835, indicated that the greatest threat to the USA during the Jacksonian Age was the tyranny of the majority occurring. His book described his fear that the majority would use tyranny of opinion to create fear and limit the independence of mind and true freedom of discussion. That was *management by intimidation* in action back then, and it still rings true today!

The concept is also addressed in Dr. Robert Bransom's *Coping with Difficult People…in Business and Life* (1981). Bransom describes a *hostile-aggressive trio* of Sherman tanks, snipers and exploders, which is really MBI by another name. The Sherman tank's demeanor expresses "attack," which reflects their strong need to prove their view is always right. They want to put you out of commission through fear and rage. Conversely, the sniper maintains a cover from behind and takes pot shots at you through innuendos, *sotto voce* remarks, not-too-subtle digs, non-playful teasing, and the like. They have an "I'm superior" attitude, which limits them from seeing things from others' perspectives. The third in this trio is the exploder, who exhibits an adult tantrum, much like a small child would. They respond to perceived threats by losing control and feel their outbursts still "work," at least on the surface.

Finally, Cherie Carter-Scott in *The Corporate Negaholic* (1991) drives the MBI theory home. Per Carter-Scott, a *negaholic* is addicted to negativism. Accordingly, negaholics unconsciously limit their own innate abilities by convincing themselves they cannot have what they want, and therefore sabotage the organization's goals. Their behavior spreads like a virus within the organization and leads to a dysfunctional organization. Hopefully, your institution will avoid this "pandemic."

Continued on page 6

Continued from page 5

Warning Signs of MBI

After years of consulting and management reviews, the authors discovered patterns of behavior that characterize MBI. Do you see these common characteristics of MBI in your organization?

- **Use of Threats:** MBI practitioners *threaten* or *intimidate* people to perform, rather than *inspire* people to do their best. Letters of warning, informal threats of dismissal, and informal requests to resign are some of the popular tactics used by MBI practitioners in organizations. A show of unchecked power is the basis for their operating philosophy.
- **Ineffective Oversight Body:** Members of the oversight body (e.g., board of directors) are carefully screened and hand-picked. The intent is to ensure that members who do not habitually question the activities of management are selected and retained. Such an ineffective oversight body gives MBI practitioners a *carte blanche* to act administratively with unchecked powers. The body views auditors as *necessary evils*, rather than *partners* who assist its members in discharging their oversight responsibilities. The need to avoid *micro-management* is used as an excuse for this kind of hands-off oversight philosophy.
- **Censored Communications:** MBI practitioners do not like employees to communicate openly and frankly about their views on organizational matters. They manipulate communication channels to ensure that only positive things are said and written about the organization to external parties. Employees who express unfavorable opinions about the working conditions are routinely reprimanded by superiors who subscribe to the MBI philosophy. *Commitment to truth* is nonexistent. Board members, external auditors, and regulators receive communications censored or sanitized by MBI practitioners to conceal the real organizational climate and culture.

MBI practitioners *threaten* or *intimidate* people to perform, rather than *inspire* people to do their best. Letters of warning, informal threats of dismissal, and informal requests to resign are some of the popular tactics used by MBI practitioners in organizations.

MBI practitioners do not like employees to communicate openly and frankly about their views on organizational matters.

- **Self-Centeredness:** MBI practitioners are self-centered leaders. They make decisions that are usually best for them, their favorite subordinates, their friends, and their business partners. Personal agendas are disguised as organizational agendas.
- **Unchallenged Authority:** MBI practitioners do not like their authority challenged or questioned by anyone. They have no compunction whatsoever in eliminating people who habitually challenge their authority.
- **Lack of Accountability:** MBI practitioners are the least accountable people in organizations. They are quick to take credit for successful initiatives, and equally quick to apportion blame on others for organizational failures. They are meticulous in building cases – real or imagined – against dispensable employees or scapegoats. MBI practitioners last long in organizations mainly because the *culture of accountability* is nonexistent.
- **Lack of Transparency:** MBI practices are not transparent to people who are not directly and indirectly impacted by such practices. We either experience or learn about them from colleagues who were affected by the practices. MBI practitioners are so concerned about leaving *audit trails* that they have adopted the practice of *not* documenting their activities as much as possible and tacitly asking their subordinates to do the same.
- **Questionable Hiring Practices:** MBI practitioners tend to ignore good personnel policies and resort to *cronyism* and *nepotism* in their hiring decisions. Covert tactics are used to ensure that friends and relatives are given preferential considerations. Ruse interviews are occasionally conducted just to satisfy legal requirements.
- **Lack of Diversity:** MBI practitioners preach but do not practice *diversity*. They develop policies, procedures, and plans that merely extol the virtues of diversity. They organize events intended to create the illusion that their organizations believe in diversity. A closer look will reveal that

Continued on page 7

Continued from page 6

the people they surround themselves with in key leadership positions are not diverse. Lucrative positions, contracts and bonuses are typically awarded to people who look, think and act like them.

- **Double Standards:** Activities that are acceptable to MBI practitioners are not necessarily acceptable to ordinary employees. Double standards are consistently applied in organizations. It is acceptable for MBI practitioners to circumvent rules if it suits their whims, but employees who commit the same acts are involuntarily terminated.
- **Disdain for Independent Reviewers:** MBI practitioners treat internal auditors, external auditors and other independent reviewers with open disdain. They do not want anyone to review and criticize their activities, or the activities of their "trusted" employees. They operate under the illusion that their actions are beyond reproach and not subject to audit. MBI practitioners prefer to have "other people" audited or investigated so that they can get the ammunition to eliminate certain people and show that certain conduct cannot be tolerated. The philosophy of "trust but verify" is foreign to MBI practitioners.
- **Management Myopia:** MBI practitioners are inherently *reactive* managers. They like status quo. They dislike people who rock the boat or think outside the box. They rarely communicate their expectations to employees in a clear, unambiguous manner. They conduct periodic performance evaluations based on their moods at a particular time. Disliked employees are harshly criticized and "trusted" employees are richly rewarded. MBI practitioners manage to survive for as long as possible to aggrandize themselves – not to ensure the long-term health of their organizations.
- **Bliss in Feigned Ignorance:** MBI practitioners find bliss in feigned ignorance. The less they know about bad things in their organization, the better for them. That is why they harbor visceral hatred for whistleblowers or employees they perceive as "bad news" messengers. They work hard to erect corporate buffers that will deter unfavorable news from reaching their attention. When confronted by the reality of things in their organizations, they are quick to use the standard excuse of "I didn't know" or "I was not aware" of the problems and their associated risks.

Stress, insecurity and "fear of getting caught" are common factors contributing to the adoption of MBI practices in organizations.

Traditional managers might have employed some or most of these MBI tactics in their leadership roles. Stress, insecurity and "fear of getting caught" are common factors contributing to the adoption of MBI practices in organizations.

The Consequences of MBI Practices

As auditors, we often see some consequences or impacts of MBI practices on human capital in our organizations. How many times have we reported the following issues during a management review or audit?

- **Unmotivated Employees:** Employees will not be sufficiently motivated to give their best or walk extra miles. They will do just enough to get by, giving their required 8 hours daily. Unmotivated employees will not feel bad about engaging in unproductive activities or sabotaging work to make their MBI superiors look bad.
- **Overstressed Workforce:** Employees will operate under enormous stress. They will work in constant fear of their MBI superiors, making it difficult for them to be consistently productive. Increased stress will adversely affect their health, family and work habits.
- **Non-enterprising Employees:** Employees will get the feeling that they are not empowered to think and accomplish anything without the blessings of MBI practitioners. They will be fearful of expressing opinions or suggestions in meetings intended to solicit frank and helpful input. Corporate stances on employee empowerment will be viewed with skepticism. Employees will eventually start finding excuses to avoid involvement in synergistic corporate initiatives.
- **High Employee Turnover:** There will be high turnover of competent employees, especially from the middle management to the frontline staff positions. Affected employees will be those who were made scapegoats by MBI practitioners and those who decided to leave the organization's unhealthy corporate culture to preserve their integrity, health, sanity and/or careers.
- **Inequitable Compensation:** The "favored" or "trusted" employees will always get paid more than employees who are deemed expendable by MBI practitioners. Experience and qualifications will be irrelevant. The perception that some people are more equal than others will eventually percolate in the organizations – causing *bitterness* and *divisiveness* among employees.
- **Climate of Distrust:** Employees will not trust MBI practitioners and vice versa. The climate of distrust will escalate to the point that working conditions become unhealthy and disruptive.
- **Climate of Vindictiveness:** Employees who dare to think outside the box or engage in whistleblowing activi-

Continued on page 8

Continued from page 7

ties will be called names and punished by vindictive MBI practitioners. Such practitioners and their cohorts will not be afraid to flaunt their powers when it comes to exacting punishment on people they view as "disgruntled employees." The absence of a system of checks and balances will promote this climate of vindictiveness in the organization.

It usually takes *front-page news* of organizational problems associated with MBI practices before an organization feels the need to change its culture.

- **Ineffective Disputes Resolution:** Employee complaints and disputes will escalate. Offices established to handle such complaints or disputes in compliance with the equal employment opportunity and labor laws will be ineffective in achieving satisfactory resolutions. Such offices will usually report to MBI superiors who are themselves the subjects of escalating employee complaints. The feeling that wolves are set up to guard the henhouse will eventually pervade the organizations until employees sense that it is pointless to file formal grievances. Lawsuits will become the only recourse for victimized employees and costly out-of-court settlements will be the standard solutions for the affected organizations.
- **Fire-fighting Management:** MBI practitioners will operate constantly in a crisis mode – putting out one fire after another in their organizations. All the organizational problems they attempt to hide under the carpet will eventually come back to haunt them and their organizations.
- **Hostile Audit Environment:** When auditing MBI practitioners' activities, some internal auditors will feel like risking their job security and external auditors will feel like risking their engagement contracts. The environment will be decidedly hostile for quality assurance work. MBI practitioners will be tenaciously uncooperative and obstructive. Poor audit trails will make the review process a Herculean task. Equally, auditors' access to members of the audit committee will be significantly curtailed.
- **Disregard for Established Controls:** MBI practitioners feel that controls are established to be conveniently circumvented. They will consistently exhibit little or no regard for established controls. They view preventive and detective controls as major threats to their jobs. Thus, opportunities to commit occupational frauds will abound, and anti-fraud measures will not find fertile ground in the organizations.
- **Unethical Culture:** The environment will foster a corporate culture where anything goes. Ethical misconduct will be widely tolerated. *Tone from the top* will essentially be perceived to mean that trusted employees can get away with anything except murder. Employees caught and prosecuted for unethical and illegal acts will rationalize that their MBI superiors were engaging in similar improprieties. This will eventually attract the keen eyes and ears of local, state, and federal regulators.

It usually takes *front-page news* of organizational problems associated with MBI practices before an organization feels the need to change its culture. In some cases, the efforts to change are genuine. Conversely, in some cases, the efforts to change are purely cosmetic. If anything, the recent corporate scandals involving Enron, WorldCom and others have taught us that MBI practices are inconsistent with the 21st century's *management best practices*. Any benefits from MBI practices will always be short lived.

Why Organizations Need to Address MBI Practices

As auditors, we desire preventive controls rather than detective or corrective controls. We strive to help ensure that our organizations are not infected with widespread MBI practices by introducing preventive controls that reduce the likelihood of such practices pervading our workplace. *Why do we need to identify and eliminate MBI practices?* The answer is threefold.

First, MBI practices do not (1) maximize employee productivity, (2) ensure operational efficiency, or (3) enhance organizational effectiveness. Such practices tend to turn employees into major destabilizing forces for organizations.

Second, MBI practices do not promote an ethical climate and can result in noncompliance with the established policies, procedures and regulations. For instance, Section 406 of the *Sarbanes-Oxley Act* of 2002 (SOX) requires the adoption of a code of ethical conduct or formal performance standards with the necessary controls to help organizations in promoting: (1) honest and ethical conduct; (2) accurate and timely disclosure of public financial reports; (3) compliance with regulations; (4) internal reporting of ethics code violations; and (5) accountability for adherence to the code of ethical conduct. Similarly, Sections 301, 806 and 1107 of SOX address the following regulatory matters:

- Require organizations to establish procedures for the receipt, retention, and treatment of complaints and the confidential anonymous submission by employees on accounting, internal controls and auditing matters.
- Grant employees the right to sue their employers for retaliation by filing a formal charge with the US Department of Labor.
- Provide for criminal penalties, including up to 10 years in prison, for retaliation against employees or whistleblowers.

In addition, the *Federal Sentencing Guidelines* enacted in 1991 by the US Congress state that organizations are liable to sentencing and fines for federal offenses connected with

Continued on page 9

Continued from page 8

Teamwork is the key to success in any worthwhile endeavor. Nobody has all the skills it takes to be successful.

securities, bribery, embezzlement, fraud, money laundering and other criminal business activities. The Guidelines hold that an organization operates only through its agents – usually managers – and is, therefore, liable for the offenses committed by its managers. The Guidelines are intended to achieve (1) just punishment; (2) sufficient deterrence; and (3) encourage the development of internal mechanisms to prevent, identify and report on criminal behaviors in organizations. Furthermore, a recent bill/study initiated by Senator Grassley made specific formal recommendations for strengthening transparency, governance and accountability in the non-public, not-for-profit sector.

Third, MBI practices pose a significant risk to the financial health of the organization. Such practices are inefficient and add significant operating costs to the organization. As noted previously, MBI practices lead to increased absenteeism and turnover, which increase costs to the bottom line. Additionally, MBI practitioners usually lack the awareness of their own accountability or possess blatant blindness to their foibles. All these lead to cost overruns and other additional expenses to the organization.

Tips for Dealing with MBI Practices

A review of existing leadership literature indicates that *outstanding leadership* is more of an *art* than a *science*. It is all about using one's education and experience to inspire people to love their work, love learning, reach their potential, serve others selflessly, adapt to changes gracefully, manage conflicts effectively, and achieve the desired results. It is also about managing complex *people management issues* with a caring heart.

As internal auditors, we are often asked for solutions to complex organizational problems. MBI is no exception and our skill set should include ideas to counter the MBI practices. To effectively dismantle MBI, we believe that the use of proven management philosophy and principles would help in countering insidious MBI practices. These can be summarized as follows:

- The primary *goal* of an organization is to have an environment where people, when they get up in the morning, look forward to going to work and/or study.
- People have *integrity* and value. It is vitally important to maintain the integrity of the organization and employees.
- Each employee is *unique*, comes from a different background, and has peculiar interests, capabilities, skills, and family responsibilities. Recognizing such distinctive individual characteristics helps in effective people management.
- Respecting people for talents is of paramount importance. It implies that the senior leadership continually strives to forgive people's weaknesses. This entails seeing the glass half full by focusing on their strengths and capabilities, rather than seeing the glass half empty by focusing on their weaknesses and faults.
- Only people who *enjoy work*, achievement, and teamwork are employed. Each individual is provided the *opportunity* to maximize his/her achievements, contribution, and personal potential without regard to age, race, gender, national origin, disability, marital status, or sexual orientation.
- Teamwork is the key to success in any worthwhile endeavor. Nobody has all the skills it takes to be successful. If you are a great administrator, you cannot be a creative person looking for new ways to do things. Administrators work to a schedule, creative people do not. It takes a team to have a successful organization. Put differently, good team players recognize that a team's success is the real measure of organizational success.
- People who consistently exhibit a positive attitude in support of the performance and objectives of the organization, management, employees, and clients are always respected and appropriately rewarded.
- The primary *objective* of management is to identify, nurture, and develop the strengths and skills of employees. A good manager does not take lightly the accomplishment of this objective.
- The primary *responsibility* of management is to ensure that all problems are addressed and resolved while they are small problems. A good manager does not abdicate or shirk this responsibility.
- Satisfied clients consisting of external customers, employees, and vendors are the foundation of the company's future. Corporate success is measured by how well the needs of such stakeholders are being met.
- Synergy is vital to the survival of an organization. The organization must have a minimum of two people in charge. There are four major roles to be played, namely (1) administration, (2) entrepreneurial, (3) communica-

Continued on page 10

The primary *responsibility* of management is to ensure that all problems are addressed and resolved while they are small problems.

Continued from page 9

tion, and (4) productivity. All these roles must be done well for an organization to succeed, and they require several people to do it. It is virtually impossible to be an administrator and be thinking creatively as an entrepreneur. It is possible to be a productive entrepreneur and a communicative administrator.

- The most difficult thing to do in management or business is to find good people, and to let them go when it just does not work. The decision to let them go is generally easy, but telling them is extremely hard, regardless of the justification.

Great leaders use these management principles in their ***Statement of Values*** document, which is typically made available to all stakeholders. Such principles are the building blocks of a framework for the effective management of an organization's human capital in the 21st century.

Implications for Auditors

Internal auditors must realize that MBI practices are detrimental to organizational effectiveness. Their risk-based reviews should assist their organizations in identifying and eliminating such practices. This entails performing assurance and consulting engagements with *independence* and *objectivity*. *Job security* should be made secondary to compliance with the audit standards and professional code of ethics.

The most difficult thing to do in management or business is to find good people, and to let them go when it just does not work.

Given the hostile environment in which they operate, internal auditors should be prepared to resign from their positions if it is the only option to make their audit observations known to the internal and external stakeholders. Of course, cultivating a good working relationship with members of the audit committee is of paramount importance in the fight against pervasive MBI practices.

Similarly, external auditors should not let contracts or monetary issues cloud their independence and professional judgment. They should know that weak internal controls contributed by pervasive MBI practice can generate fraudulent financial statements and opportunities for other types of occupational frauds.

In addition, internal and external auditors should avoid credibility problems by not engaging in MBI practices or appearing to turn a blind eye to such practices during internal control reviews. Thus, *self-assessment* is a critical step toward conducting objective reviews and fighting effectively against MBI practices. Lack of credibility has been known to hamper quality audit work.

Finally, the Enron and WorldCom cases showed that internal and external auditors can pay heavy prices if they know but fail to act on red flags in auditable areas.

Conclusion

We live in a democratic society. MBI practices are not in harmony with our democratic ideals or with the principles that undergird our hard-fought democracy. Such practices benefit a few self-centered leaders at the expense of organizational effectiveness. Thus, it is time to take a *reality check*. Three important questions to ask are:

(1) Is our organization engaged in widespread MBI practices?

(2) Are we contributing to such practices?

(3) What can we do to help eliminate such harmful practices?

The evils of MBI practices reinforce the importance of proper management of employees as human beings with feelings, and compliance with governmental regulations. Internal and external stakeholders who value successful organizational performance, ethical culture and social responsibility should join hands in fighting against such practices in their organizations. This requires a proactive mindset because *a stitch in time saves nine*.

Perception about direct or indirect involvement in MBI practices will not allow anyone or any group of individuals to wage an effective fight against MBI practices. Credibility is, thus, an important weapon in the anti-MBI fight. Organizations that are decisively proactive in rooting out MBI practices will be the ones left standing on a solid footing in the 21st century where only the fittest survive in an increasingly competitive global marketplace.

The framework for effective management practices discussed in this article is one that can help organizations in building an environment conducive to a highly motivated workforce, transparent accountability, ethical decision-making, a shared governance process, proactive problem-solving, cost efficiencies and satisfied customers. These will, in turn, contribute to a vibrant *corporate culture* that helps in building and sustaining a healthy bottom line for the organization.

About the Authors

Slemo D. Warigon, CIA, CISA, CICA, MBA, is Director of Audit and Management Advisory Services at Gallaudet University. He has written extensively on information systems control and security, and his work has appeared in numerous professional publications. The Institute of Internal Auditors presented him the 1999 Outstanding Contributor Award for his article "Data Warehouse Control and Security." He can be reached at slemo.warigon@gallaudet.edu.

Betsy Bowers, CIA, CFE, CGFM, is Associate Vice President of Internal Auditing and Management Consulting at the University of West Florida, Pensacola, FL. She is currently the President of the Association of College & University Auditors (ACUA). She can be reached at bbowers@uwf.edu.

Voluntary Adoption of the Sarbanes-Oxley Act: How Far Should You Go?

By Amy Barrett, Assistant Director, The University of Texas System Audit Office, Austin, TX

Overview

A Texas Southern University president is fired for spending $650,000 over seven years in university funds for her personal benefit. The Senate Finance Committee is looking into governing board reform at American University as a result of a $3.75 million severance package provided to the president who was fired for inappropriate expenditures. Ohio State University is investigated for cash payments made to athletic recruits. The University of Texas (UT) System regents receive free athletics tickets valued at over $1 million. Two hundred thousand social security numbers are improperly accessed at Ohio University. The University of California System votes to divest in companies with ties to Sudan.

Such stories and the headlines they make are all too familiar to those of us working at academic institutions. We have difficulty staying in front of the issues and often seem to be operating in crisis mode. Seldom, if ever, do we see headlines about financial reporting issues at educational institutions such as misreporting earnings, improper application of accounting principles, or lack of transparency in financial statement disclosures. Yet, those are the issues that get public companies in trouble. Enron invested in off-balance-sheet partnerships that were buried in incomprehensible footnotes. The company also used aggressive accounting practices such as mark-to-market accounting. WorldCom manipulated earnings by misreporting depreciation expense. The *Sarbanes-Oxley Act of 2002* (the "Act") was written into law to ensure that these types of financial reporting abuses do not happen again. But if the Act is targeted at risks that public companies face because of pressure to report earnings, does the Act have any applicability to colleges and universities where the risks are different?

The Spirit of Sarbanes-Oxley at the University of Texas

The answer to the above question is a definite "Yes," but only in spirit. The *Spirit of Sarbanes-Oxley* is the guidance that the UT System adopted in 2003 for the purpose of increasing awareness of the Act, adopting appropriate provisions and implementing a strategy of not getting ahead or behind subsequent changes in federal and state laws. Many of its provisions stand the test of time. UT based the *Spirit of Sarbanes-Oxley* on NACUBO's *The Sarbanes-Oxley Act of 2002: Recommendations for Higher Education* and issued a paper of its own, *Implementing the Spirit of Sarbanes-Oxley Act of 2002 in The University of Texas System*. Following the publication of the paper, an ad hoc committee composed of chief business officers and internal audit directors from all fifteen system institutions met and issued an action plan. The action plan set forth the following guidance:

Reporting: Similar to the Act's requirement for certification of the financial statements by senior management, one responsible party at each institution and systemwide was designated to ensure accountability and authority over financial reporting and to certify the fair presentation of the financial statements. A systemwide policy was issued to define the duties and responsibilities of the responsible party. Also, a public accounting firm was engaged to perform the first ever audit of the systemwide financial statements (financial statements of state educational entities in Texas are not required to be independently audited).

Governance: The audit committee of the board of regents adopted a charter similar to charters adopted at for-profit organizations. Each institution adopted similar charters for their institutional audit committees (led by senior management of each institution with outside members encouraged). Limitations were placed on the amount of non-audit work allowed to be performed by external auditors and the process for approving their work. Hotlines were established at each institution and a whistleblower protection policy was developed.

Internal Controls: Given the decentralized nature of many of the UT System campuses, controls over segregation of duties and completion and supervision of reconciliations were emphasized. Training was held. Internal audit departments performed departmental audits every three years to ensure these basic controls were in place and reported exceptions to institutional audit committees that met quarterly.

Continued on page 12

Continued from page 11

Section 404 of the Act requires the documentation and testing of both transaction-level and entity-wide controls and is the section that has caused public companies to expend the most time and effort. The ad hoc committee was considering piloting a portion of Section 404 across the system when management at the *University of Texas Investment Management Company* (UTIMCO) volunteered for the pilot. UTIMCO is UT's investment arm and a separate 501(c)3 organization with a staff of just over 40 people and $18 billion in assets under management. Volunteering for the pilot meant that management had to acknowledge their responsibility for establishing and maintaining adequate internal control over financial reporting and had to hire an independent firm to attest to and report on their assessment of internal control over financial reporting. UTIMCO manages several funds on behalf of UT, each of which received an independent audit annually from an outside public accounting firm. UTIMCO selected the Permanent University Fund (PUF) to undergo Section 404 procedures in 2005. UTIMCO staff had to document and test all entity-wide controls according to the COSO model referenced in the Act, including the control environment, risk assessment, monitoring of controls, and information and communication. Next, management had to identify and document processes related to financial reporting and identify key controls associated with these processes. In all, UTIMCO identified 8 processes for the corporation and 24 for PUF, each with 5 to 10 key controls identified. Internal audit performed testing of the key controls on behalf of management and issued a report on the controls to the UTIMCO management and audit and ethics committee in September 2005 (UTIMCO has an August 31 year-end). The outside firm performed an independent assessment of internal control and issued their opinion in January 2006. No material weaknesses or significant deficiencies were identified. Approximately 3,500 hours of work was incurred in the process: 1,200 hours by UTIMCO management, 1,500 hours by UT System internal audit, and 800 hours by the independent auditors. Keep in mind that UTIMCO staff consists of approximately 40 individuals and much of their accounting is handled by a banking institution for which UTIMCO obtains and relies upon a SAS 70 report on internal controls. Now, consider the time it would take your university to implement the Act fully!

Was the process worth it? To UTIMCO staff, it was. They were able to prove to the UT System that they had an adequate financial reporting control system in place. UT System audit staff benefited through developing relationships at UTIMCO, learning the financial controls there, and getting comfortable that their time was better spent addressing non-financial risks in the future. Going forward, the plan is to complete this process once for every fund managed by UTIMCO. In year two, internal audit will work with the external auditors to pare down the cycles and controls internal audit tests for management and in year three, the plan is to eliminate internal audit's involvement in the process altogether. Management will be responsible for updating narratives and testing internal controls.

Where were other pilot programs in the UT System? The UT System has six health institutions, many of which use wholly-owned not-for-profit organizations for services such as medical billing. In 2004, the UT System Office of Health Affairs issued a memo requiring all of these not-for-profits to comply with the *Spirit of Sarbanes-Oxley*. In the memo, the following provisions were discussed (some as requirements and some as best practices):

- Prohibition of non-audit services by an independent auditor
- Lead partner rotation every seven years.

Continued on page 13

Continued from page 12

- Establishment of an audit committee charter.
- Annual training of all audit committee members.
- Requirement for one external committee member and preference for a financial expert.

Attention should remain on financial reporting, strengthening governance, and evaluating high risk internal controls, always with a cost-benefit objective in mind, and always with an eye on the latest legislation and headline.

- Establishment of a confidential reporting line.
- Certification of financial statements and internal controls by the CEO and CFO with subcertifications by others encouraged.
- Requirement of annual ethics training for senior management and the board.

Compliance with Section 404 was required over time; however, the memo was not specific as to what compliance in this area should look like. The service organizations interpreted the memo in various ways. Two hired an external firm to document controls and asked institutional internal audit to test them. Another performed a risk assessment of internal procedures and only recently began documenting higher risk areas internally. All added external members to their audit committees.

Given the haphazard nature of adoption, the Office of Health Affairs and System Audit Office are in the process of reviewing guidance issued since 2004 and will issue a memo in the next few months with more detailed guidance. If the UT System were to issue the guidance today, it would focus on three things:

First, did the not-for-profits implement the non-Section 404 provisions specified in the memo from Health Affairs? The UT System believes these provisions are the most important because transaction-level controls can be overridden by management. A strong tone-at-the-top in the form of an effective audit committee with an independent member is the best deterrent for this type of abuse.

Since the memo was issued, bond rating agencies for nonprofits such as Moody's Investor Service and Fitch Ratings have provided guidance as to which provisions of the Act they view as important to their bond ratings determinations. Additionally, the Panel on the Nonprofit Sector, formed at the encouragement of the Senate Finance Committee, issued a report to Congress on how charitable organizations could best strengthen transparency, governance and accountability. The Panel report focuses on sections of the Act other than 404 and emphasizes the need for an annual audit, an audit committee, a whisteblower hotline and an ethics policy.

Given the more recent guidance, UT System internal audit performed a gap analysis and recommended that the memo be amended to address areas such as the reasonableness of executive compensation, incentive compensation programs, conflict of interest policies, travel and entertainment policies, performance reporting, communications to the audit committee and a risk-based approach to assessing internal controls over financial reporting.

Second, how strong are the entity-wide controls in the organization? In other words, is there a strong tone-at-the-top? Are policies and procedures in place? Is there active monitoring of compliance with these policies and procedures? Entity-wide controls are a better defense across an organization than transaction-level controls. If the tone-at-the-top is not strong, completing monthly reconciliations of cash accounts will not be as important (see the first paragraph on excessive spending by presidents, and you'll see what I mean).

Third, and only after the first two elements are in place, has the organization identified its processes and risk-ranked them? Resources should be focused on high risk, high probability areas. If your organization does not care about whether library books get depreciated over 30 or 50 years, do not put your resources there. UT is considering requiring its not-for-profits to document and independently test key controls for high risk processes every 3 years.

What have UT academic and health institutions done? Beyond the initial action plan, one institution besides UTIMCO that receives an independent stand-alone annual audit, MD Anderson, issued a request for proposal for a firm to develop a reasonable approach to the Act. The reasonable approach has yet to be defined or agreed upon. None of our academic or health institutions has gone beyond the initial action plan. Internal audit at the UT System continues to monitor legislation to determine what impact it would have. States have adopted legislation to varying degrees; so far, none has passed in Texas.

Conclusion

So what does implementing the *Spirit of Sarbanes Oxley* mean to the University of Texas System and what should it mean to other educational institutions? It means that the institution is not only aware of the Act, but that it maintains a strategy for not getting ahead of or behind subsequent changes in laws. It means that the institution takes seriously accountability for controls over financial reporting with a focus that is high-level and risk-based. Attention should remain on financial reporting, strengthening governance, and evaluating high risk internal controls, always with a cost-benefit objective in mind, and always with an eye on the latest legislation and headlines.

About the Author

Amy Barrett is an assistant director at The University of Texas System Audit Office. Previously, she was a senior manager with PricewaterhouseCoopers, LLP.

Medical School Risk Assessment

By John S. Ricaud, MBA, CIA, Director of Internal Audit, Piedmont Healthcare, Atlanta, GA

Overview

According to the Liaison Committee on Medical Education, the nationally recognized accreditation agency for medical education, there are currently 162 medical doctorate academic programs in the United States and Canada. Although a few medical school programs are stand-alone, the majority are offered by universities through a College or School of Medicine as an integral component of a comprehensive mix of undergraduate and graduate academic degree programs and activities.

The challenge facing internal auditors is to accurately assess risk exposures throughout the institution and to address the unique aspects of medical schools, in conjunction with audit responsibilities for all higher education programs and administrative functions. With limited resources, university internal auditors must recognize the primary areas of risk and concentrate exclusively on relevant issues. The purpose of this article is to assist university auditors in identifying the most important risk areas unique to the medical school environment.

The primary universal medical school risk exposures facing academic medical centers include, but are not limited to, the following categories: administration, financial management, research, education, patient care and facilities management. Each of these areas will be reviewed for specific risk exposures that internal auditors should assess within their institutions.

Administration

In the event a university operates a traditional academic campus in addition to a College or School of Medicine, many of the high-level administrative activities are performed for the entire organization and would apply to the medical school as well as the other academic colleges (e.g., Business, Education, Arts & Sciences, etc.). However, in some cases, executive management opportunities and challenges exist that are exclusive to medical education administration. The auditor should be aware of these activities for incorporation into the enterprise risk assessment program.

- **Strategic Planning** – The auditor should assess the degree to which executive management has conducted market research, evaluated growth opportunities, changing trends and the actions of its competitors. Auditors should determine if measurable goals are established and if specific accountability is assigned for task completion with applicable dashboards reported to the Board.
- **Development of New Programs** – Executive management should have an established methodology to evaluate the expansion into new academic and/or clinical programs. The auditor should review the process for effectiveness and verify if the addition of new programs supports the organizational strategic plan.
- **Physician Recruitment** – Senior Management, via Human Resources, should have plans in place to actively recruit clinical faculty and research faculty to the institution and retain quality individuals. Via a turnover and vacancy analysis, the auditor can assess the degree to which staffing goals have been achieved.
- **Policy and Procedure** – Administration is also responsible for establishing effective policies and procedures, as a key component of internal control. Internal Audit should assess the adequacy of the policies and procedures as well as compliance by faculty and staff personnel.
- **Philanthropy** – Donations from benefactors are critical to the success of an academic medical center. Foundation operations are a risk exposure area that warrants internal audit coverage.

In 2003, Medicare spent $126 billion on inpatient and outpatient hospital services and $47.6 billion in benefits for physician services. Operating costs for academic medical centers tend to be greater than traditional healthcare organizations; therefore, additional graduate medical education payments are provided by Medicare.

Continued on page 15

Continued from page 14

Financial Management

For large universities, financial management is usually centralized. However, there are some financial aspects unique to medical schools. For traditional colleges and universities, the primary sources of funding are state appropriations, tuition and fees. In contrast, medical schools derive revenue via patient charging and billing and clinical as well as basic science research funding. The following outlines financial risk exposures specific to medical schools:

- **Reimbursement –** Patient charging and billing to third-party payers serves as the most significant financial risk for the healthcare industry. Auditors should allocate adequate resources to ensure controls are effective to maximize collections and ensure compliance with Medicare and Medicaid regulations, managed care contracts, and commercial insurance requirements for physician billing reimbursement.
- **Expenditure Management** – Medical supplies and equipment represent significant costs for a medical school. The auditor should assess the risks associated with the purchase of lab supplies, clinical supplies and research equipment. Group purchasing plans, product standardization and obsolescence may pose risks.
- **Physician Compensation** – Clinical faculty often receive the bulk of their compensation via salary supplements per the physician practice plan. Since a percentage of patient reimbursement is paid to the physician based on the terms of the practice plan, the auditor should evaluate risk exposures regarding the administration of the physician practice plan.
- **Faculty and Staff Payroll** – The auditor should determine his or her level of reliance on payroll controls. Of particular concern are routine practices associated with charging of research-related salary costs to the applicable grant or contract as well as undocumented faculty leave.
- **Research Participant Payments** – One area of vulnerability involves the payments made to research participants in a clinical trial. The auditor should consider assessing risk as relatively high for research projects involving a large volume of participants. In addition to the financial risk exposures, a signed informed consent must be obtained from each individual participating in a clinical drug study.
- **Student Financial Aid** – The vast majority of medical students finance their tuition and living expenses via scholarships, student loans or grants. Regulatory requirements, especially for federal assistance programs, are substantial with significant consequences for non-compliance. Internal auditors should assess the risk exposure for financial aid operations appropriately.

The average number of National Institutes of Health (NIH) awards for the top five research medical schools was 856.6 projects, amounting to $380.5 million in average funding in fiscal year 2004 for each of the five institutions. The total amount of grants awarded by the NIH in fiscal year 2004 was $22.9 billion.

Research

The clinical faculty consists of physicians who provide supervision to medical students and residents in a clinical setting and their research often involves clinical drug trials. The basic science faculty is interested in pure scientific research. Although they instruct medical students in the classroom setting, the primary focus of basic science faculty is on laboratory research. Total research dollars for a medical school commonly exceed three times that of a traditional university. Consequently, the risk exposures associated with academic medical center grants and contracts are a significant consideration. Specifically, internal auditors should assess the following functions.

- **Research Oversight –** The Institutional Review Board is responsible for reviewing the ethics of proposed and ongoing research projects involving human subjects, while a comparable Animal Resource Committee performs reviews of research projects that use animal subjects. Many granting agencies have strict requirements for the administration of these oversight groups. A risk exposure exists in light of the discontinuance of current and future funding in the event of violations. The auditor should thus assess operation of research oversight groups.
- **Compliance** – Adherence to granting agency requirements is a primary risk exposure area. Non-compliance could jeopardize current and future grant funding. The auditor should assess the necessity of allocating audit resources to research projects based on their volume and post-award management controls. For medical schools receiving an excess of $200 million in annual grant funding, a full-time dedicated auditor may be justified.
- **Time and Effort** – Time and effort reporting will always be a risk area for research institutions. In assessing controls, the auditor should evaluate the need for audits in this area. In an environment in which research faculty and staff are performing multiple projects, errors in time and effort reporting could be problematic.

Education

One of the primary missions of a medical school is education, specifically graduate medical education. For medical students, the latter years of training are conducted in a clinical setting under close supervision by faculty physicians. Upon gradua-

Continued on page 16

Continued from page 15

tion from medical school, new physicians enter a residency program that varies in duration depending on the specialty. The residents, again under faculty supervision, are exposed to a full array of clinical experiences. The following are related risk exposures.

- **Management of Residency Programs** – Accreditation requirements for residency programs mandate clinical rotations and clinical exposure to specific patient diagnoses. Auditors should consider performing compliance testing in this area. Failure to meet accreditation standards may result in the loss of the entire program, which could have ramifications on the overall medical school accreditation. Documentation of faculty supervision in the medical record is critical to meet both accreditation standards as well as Medicare regulations for patient billing. Auditors should assess the validity of internal controls over this process.
- **Admission Requirements –** Medical school admission is highly competitive. Many state schools have residency requirements and minimum Medical College Admission Test (MCAT) standards. Similarly, acceptance to residency programs is equally competitive. Auditors should assess the admission process for the College or School of Medicine as well as for the specific residency programs to ensure equal consideration is afforded each applicant based on reliable and objective criteria.

Patient Care

In addition to research and education, patient care serves as the third component of the mission of a medical school. The diagnosis and treatment of patients in inpatient and outpatient settings are integral to medical education training. Medical students and residents perform clinical activities at a teaching hospital or hospitals associated with the medical school. In addition to physician billing discussed in the financial management section, the following risk exposures should be considered by the internal auditor:

- **HIPAA –** Patient privacy has become a major risk exposure for all healthcare providers. According to federal law, physicians and hospitals must inform patients of their rights, and providers must safeguard protected health information. The auditor should review the compliance program to ensure compliance is maintained and that a process is set out to address privacy breaches promptly and appropriately.
- **Patient Safety** – Healthcare providers, including physicians in training, have an obligation to adhere to patient safety regulations. The auditor should assess the applicable laws and level of compliance. Examples include infection control policies, Joint Commission standards, Food and Drug Administration regulations, etc. Risk exposures are significant and non-compliance could result in a negative patient outcome, medical school sanction or litigation.

Facilities Management

In academic healthcare, after salaries, the second most significant costs to institutions are the construction and maintenance of physical facilities, the acquisition of diagnostic equipment, the purchase of medical supplies and the information technology infrastructure. The following risk exposures should be evaluated by the internal auditor as an integral component of enterprise risk management.

- **Construction** – Construction is often overlooked as a risk exposure. This area requires special audit training and should be outsourced if the expertise is not available among the audit staff. Construction costs for a typical research or classroom building may exceed tens of millions of dollars. In addition, most campuses are in a constant state of facility renovation. Based on building activities, the auditor should assess the applicable risks and allocate resources accordingly.
- **Fixed Assets –** Medical diagnostic equipment tends to be expensive and becomes obsolete very rapidly. Fixed asset management and depreciation accounting are areas to be considered in risk assessment.

Continued on page 17

Continued from page 16

Periodic inventory observations for high-dollar capital items may be necessary.

- **Facility Security –** Biomedical research is often performed in a sterile environment. The contamination of specimens could destroy or compromise years of research. Access to laboratory or animal care facilities should be strictly controlled. The auditor should determine if physical security controls are adequate and effective.
- **Information Technology –** Much critical research and clinical data are stored electronically. The integrity of data and access to programs and data are vital to the success of the organization. Auditors should assess controls over servers, data files, disaster recovery and communication interfaces. These activities are critical risk exposure areas that should be evaluated in a comprehensive manner.

Conclusion

Developing an annual audit schedule for a comprehensive university that includes a medical school can appear overwhelming. There are thousands of risk exposures to consider; however, if you know where to look, even a limited amount of audit resources is sufficient to address the bulk of the institutional exposures. A comprehensive enterprise risk assessment, incorporating the areas outlined in this article, will enhance the quality of internal audit coverage. In the academic healthcare environment, an effective internal audit function is critical, and opportunities to add value to the university are abundant. Remember, follow a sound internal audit methodology and do not be intimidated by the clinical setting. Follow through with your best professional effort, and you can be sure that executive management and the audit committee will recognize and appreciate your contribution.

About the Author

John S. Ricaud, MBA, CIA is the Piedmont Healthcare's Director of Internal Audit. He has served as an internal auditor for higher education, academic medical center and hospital organizations since 1991. He can be reached at jricaud@hotmail.com.

From the President

Continued from page 3

involvement. My goal for the past year was to encourage more people to take active roles in ACUA operations, whether it was serving on a committee/task force or writing/editing for this publication or *ACUAnews*. By so doing, many of you have stepped forward to open personal *Windows of Opportunity*.

I would be remiss if I didn't pause and express a heartfelt thank you to the many volunteers and leaders of ACUA. I would like to thank the ACUA Board and ACUA Headquarters for being the framework that holds our *Windows of Opportunity*. You have been a source of strength. I know you will strongly support our incoming president, Kim Turner. To those who served as mentors and counselors, you made my job a much easier task, especially when I would call or e-mail seeking your advice. Thank you! For the many ACUA volunteers (committee chairs, conference coordinators, task force members, committee members, proctors, teachers, authors, ACUA-L writers, etc.), your interest in and enthusiasm for ACUA has opened our *Windows of Opportunity* wider. Please continue to work with and for ACUA to make us stronger and stronger.

As the sun begins to set through my windowpane of ACUA life, I also would like to thank my other colleagues for their support, wisdom and integrity throughout the year. Like any organization, we faced challenges; yet by working together to express our ideas, we frequently capitalized on ACUA's *Windows of Opportunity*. Ultimately, the togetherness was essential to our success.

Please put September 10-14, 2006, on your calendars to attend ACUA's 50th Annual Conference in Louisville, Kentucky. I know many *Windows of Opportunities* will open there for organizational and personal success—yours included!

An **Institutional Risk Management** Approach

By Imad A. Mouchayleh, MBA, Director of Internal Audit, Austin Community College, Austin, TX

Introduction

Each organization striving to achieve its goals and objectives faces many challenges and risks. Measured by their impact and probability, these risks are on the rise due to advances in technologies, Internet, global business, global markets, global communication, and free global information sharing. Organizations must identify and manage their risks to be able to compete and survive in this era of global competitiveness. Risk for organizations is the silent killer; the more it goes unidentified and non-mitigated, the more severe, deadly and irreversible its impact becomes.

Overview

Austin Community College (ACC) undertakes activities associated with the identification and management of risks that are embedded in its day-to-day work processes. What ACC lacks is the risk management approach that provides the consistency of a formal discipline, a systematic approach to identify and assess risks, and to seize the opportunity of new initiatives to enhance accountability and internal controls structure.

To address this shortcoming, ACC has decided to:

(1) Identify its risks and manage them before their impact grows beyond the institution's control.

(2) Identify the right systematic process-oriented risk management approach for adoption.

(3) Formalize and incorporate the risk management approach into campus work processes.

(4) Seize opportunities to enhance accountability and the internal controls environment.

The risk management approach at ACC was formally introduced by the Office of Internal Audit. This decision will change forever the way ACC thinks about risks, the risk management process and internal controls.

Risk Management Approach

Finding the right approach is not an easy task. Outsourcing is no longer an option for ACC to consider due to its high cost and the limited framework proposed by the external entities that the Director of Internal Audit contacted. Utilizing *The Committee of Sponsoring Organizations (COSO) of the Treadway Commission Integrated Framework* publication from the Association of College & University Auditors (ACUA) risk management bookstore, the *Director of Internal Audit* (Director) decided to develop a risk management approach suitable for ACC.

Risk appetite is not a topic that previous ACC management invested in much. ACC's risk appetite is embedded in its day-to-day transactions, and is typically seen in the way the college conducts itself. Risk appetite is neither identified nor understood as a *systematic* process that could be formally reviewed and updated. ACC did not have any assurance as to what the areas of risks are, who has the authority to take risks on behalf of the College, and whether managers are taking risks as they should be.

Currently, ACC does not have a ready definition for its risk appetite. However, by introducing the risk management approach, the Director established the foundation to define it. ACC's current risk appetite is seen as the monetary or non-monetary level beyond which a residual risk cannot be accepted.

Planning ACC's risk management approach was easy. In its report "Higher Education – Improving Risk Intelligence" presented to ACUA on September 22, 2005, Deloitte Development LLC proposed five questions for each organization to answer; ACC chose to address these questions and answer them:

(1) What is the policy and process for managing risks on an **integrated** basis?

(2) What are the **key risks** and vulnerabilities, and what is the plan **to address** them?

(3) What is the **risk appetite** and related thresholds where various risks need to be escalated for response?

(4) Who has the **authority** to take risk on behalf of the organization?

(5) What is ACC's **capability** to manage risk on an integrated and sustainable basis?

Continued on page 19

Continued from page 18

Implementing Enterprise-wide Risk Management (ERM) Model

Answering these five questions confirmed ACC's need for a formal and process-oriented discipline to conduct its risk management approach. The COSO model provides a sound, comprehensive, structured, disciplined, integrated, and process-oriented risk management framework that the College was looking for. The framework implemented by ACC includes the following elements:

1. ***Risk Oversight***
   - *Strategic* – Risk must be aligned with strategic framework (risk taking)
   - *Operational* – Effective and efficient use of resources (risk avoidance)
   - *Reporting* – Reliability of the financial and non-financial reporting (risk avoidance)
   - *Compliance* – Compliance with applicable laws and regulations (risk avoidance)
2. ***Risk Areas***
   - *Subsidiaries* – Board and senior management
   - *Business unit* – Directors and managers
   - *Division* – Direct supervisors and operational business units
   - *Entity level* – Contracts and external entities
3. ***Risk Assessment***
   - *Set objectives* – Identify critical risks
   - *Risk assessment* – Assess the risks' impact and likelihood
   - *Risk response* – Management response to mitigate the identified risks
   - *Information and communication* – Timely capture and communication of information to appropriate entities
   - *Monitoring* – Ongoing risk monitoring

The Risk Management Assessment Methodology

ACC adopted the *brainstorming methodology* to assess its risks. The brainstorming methodology consists of:

(1) *Brainstorming activities* (internal, external, consider interaction of events, ongoing, periodic); consolidate the identified activities into processes; prioritize identified processes.

(2) *Brainstorming risks* (what could go wrong, inherent without controls, inherent with unmonitored operating controls).

(3) *Ranking the risk's impact* (High – showstopper; Medium – inefficient and extra work; Low – no effect).

(4) *Ranking the risk probability before controls* (High – will happen frequently; Medium – will happen infrequently; Low – will seldom happen).

(5) *Identifying risk's mitigation measures* or internal controls using the cost-benefit analysis approach.

(6) *Ranking the risk probability after controls* (High – will happen frequently; Medium – will happen infrequently; Low – will seldom happen).

(7) *Producing risk* footprint and risk monitoring sheet.

As the ACC risk assessment methodology progressed, more questions were raised. Some of these questions were:

(1) ***Do controls reduce the impact of a risk or only its probability?*** Some would argue that controls are implemented to reduce the probability or the likelihood of the risk occurring, but the risk's impact remains unchanged. Others would argue that the risk's impact changes after controls. The risk of a hurricane is the best example where the impact changes after implementing controls. The probability of a hurricane cannot be controlled; being well prepared, after a hurricane hits, is controllable. A well developed disaster recovery plan can reduce the impact of a disaster. The question for ACC is whether or not the methodology should be changed to rank the impact after controls.

(2) ***Can one risk have multiple impacts? If so, how to rank them?*** The risk of a hurricane or a natural disaster can have more than one impact on a higher education institution, including: interruption of business, destruction of facilities and equipment, loss of enrollment (evacuees), and health and environmental problems. Ranking these impacts may vary based on their nature and severity. The brainstorming methodology allows ranking one impact per risk. This means that the multiple impacts are being collectively ranked under one risk.

(3) ***Can the impact be the risk in different situations?*** The risk of bad reputation for a higher education institution is critical. Ranking the impact of such risk "high" is the right way to go. However, during the brainstorming exercise, the interviewees brainstormed risks like fraud, misappropriation of funds, misrepresentation, theft and bad policy among others, and ranked their impact as "high." The overall impact of these risks would be the institution's bad reputation or image. The impact became the risk and vice-versa.

Organizations must identify and manage their risks to be able to compete and survive in this era of global competitiveness.

Continued on page 20

Continued from page 19

(4) ***Who should be the risk owner to mitigate and manage?*** Any risk identified through the ERM approach is an *Enterprise's risk*; hence, it's the management's responsibility to manage it. But who is *management* and who the final recipient of the risk assessment report that should be responsible to manage the identified risks, and also has the authority to do so? When the ERM approach lists the risks identified under the Human Resources Department (HR), it is HR's highest authority that should be responsible for managing the identified risks. At ACC, it is the Associate Vice President (AVP) of HR. Among the duties the President delegated to this AVP is the management of the risks the HR area presents. But this does not eliminate the President's responsibility for managing these risks as well. The President can assign any other authority he finds more adequate to manage part or all of the HR identified risks. It is a dual responsibility and the AVP should be the first to assume the responsibility of the risks their area presents.

(5) ***How can the identified controls be linked to the identified risks in a process oriented way?*** The adopted brainstorming methodology does not provide a *systematic* way to rank the efficiency and effectiveness of the identified internal controls, and how this ranking is linked to and affects the identified risk. Further, this methodology does not consider ranking or scoring the internal controls to disclose how they change the risk's probability. To determine ACC's risk appetite, we combined the brainstorming and the scoring methodologies in a systematic way to establish what the College's net risk is.

The Benefits of ERM Approach

ACC's ERM approach is a living process that evolves and is modified as needed to achieve the institution's goals and objectives. This approach proved that risk is the responsibility of everyone in the College. The Board of Trustees faces many risks and uncertainties while striving to maintain the College's value and mission. The President faces the challenge of determining how much risk and uncertainties to accept while striving to optimize the balance between goals/objectives and risk/uncertainties. Staff faces a wide variety of risks and uncertainties affecting different parts of the College's organizational and operational structures.

How much risk to accept is a management decision, and our College has not yet found the right answer. Each manager or staff member may pursue a *high risk* or *low risk* strategy as appropriate. However, ACC is committed to:

- Developing and maintaining a stronger internal controls environment.
- Making the internal control environment the first line of defense to mitigate risks.
- Formally organizing risk management responsibilities and activities.
- Providing the requisite oversight of risk management.
- Assuring that every employee understands the risks chosen and invests in them with his/her tolerance for potential variations.
- Providing the disciplines and procedures to establish risk management as an integral part of the business strategy setting process.
- Providing a sound, comprehensive, structured, disciplined, integrated and process-oriented risk management framework.

ACC brainstorming interviewees stated that "*this exercise* (the ERM approach) *gave us the opportunity to re-think our areas, document our controls and test their efficiency; monitor our risks; and is a process that we can update internally on an annual basis.*" These comments clearly demonstrate the value of an effective ERM approach. The benefit is great when management and staff understand risks and invest in them, each in his or her own way to achieve the same goals and objectives. A risk management approach makes the institution flat due to the mutual foundation and understanding of risk and risk management between management and staff members. This, in essence, sets up *The Right Tone at the Top*.

The President faces the challenge of determining how much risk and uncertainties to accept while striving to optimize the balance between goals/objectives and risk/uncertainties.

Conclusion

The role of an internal auditor in the risk management approach is the same as that of a musical maestro guiding a big orchestra called organization – directing all the players to perform in an integrated and systematic manner to produce delightful music for the audience. If your organization is not thinking about risk and taking responsibility for risk management, it is a great opportunity for you to take the lead role and be the maestro of your enterprise-wide risk management orchestra.

About the Author

Imad A. Mouchayleh, MBA, is Director of Internal Audit at Austin Community College in Austin, TX. He can be reached at imouchay@austincc.edu.

Continued from page 4

planning. The session brought together different risk perspectives from ***Ann Franke, Esq.*** President, Wise Results LLC; ***Amy Kovalan***, Associate Vice President for Institutional Compliance; and ***Peter Batsakis***, Occupational Safety Officer, DePaul University

The Shifting Risks: Speaking of the shifting risk landscape that colleges and universities face today, Franke provided a global viewpoint and a comparison of today's versus yesterday's *institutional risks*. Institutions today need to be prepared to address *global risks* as well as *local risks*. Institutions are faced with more political risks and evolving laws and liabilities at state and federal levels in addition to facing a wider range of issues such as changing population characteristics, the increased prevalence of drugs and violence, proliferation of technology and access to personal data. These issues are joined by new challenges in such areas as research integrity and campus safety in the face of homeland security risks.

Franke noted that there are more regulations focusing on privacy now than in the past 30 years – FERPA, HIPAA and data security breach laws – and that minimal reporting obligations are now evolving into compliance requirements. The area of privacy interests continue to expand, especially with the use of e-mail and Internet sites such as *FaceBook* and *MySpace* where many personal disclosures and inadvertent disclosures are occurring.

From March 2005 to February 2006 the *Privacy Rights Clearing House* group has tracked 57 college and university data breaches – most resulting from hackers. Other causes include lost or stolen computers and inadvertent disclosure online or via e-mail or dishonest insiders. Of these 57 incidents, over 1.5 million records were compromised. According to Franke, this will cause a shift on the state level to address more closely data breaches.

One-third of participants reported having a breach in data security within the past 12 months. This poll provides a good thermometer of what's happening in terms of data security breaches. Although one-third have had a breach, most have not.

Managing Institutional Risks: Campuses can prepare for and continue to effectively manage constant shifts in risks. DePaul University is managing risks with a two-pronged approach:

- *Managing institutional business risks* approach that addresses the effective management of money or people, and involves developing a management standards handbook and training materials. The goals of these tools are effective communication of key policies and procedures that DePaul University management is required to follow.
- Global assessment and management process for managing institutional risks – an approach that entails identifying high level risks and steps to mitigate those risks. *Executive leadership* and support is key to success as well as a designated *Compliance Officer* and a formal *Executive Compliance Committee*.

One important step for managing institutional risks is to create a list of high risk areas for your institutions. The criteria that DePaul used looked at:

- The likelihood of non-compliance occurring in general due to complexity or inherent risks
- The consequence of non-compliance especially as it relates to the risk of a federal or state audit, financial loss, harm to people and damage to DePaul's reputation
- Special areas of concern identified by Board.

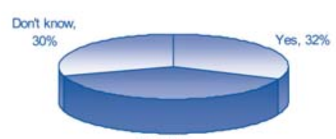
Kovalan explained how to better mitigate those risks and went through the steps that DePaul has taken to meet this detailed level:

- Identify a responsible party – one person that identifies the risk, sets up the controls and executes
- Identify department level risks
- Identify operating controls
- Follow up with oversight and accountability
- Conduct peer review

The webinar concluded with a case study from DePaul University on crisis planning – addressing how institutions can develop a response plan in the case of a pandemic outbreak on their campuses. Watch for announcements of upcoming Web seminars.

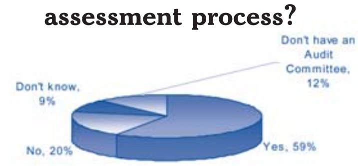
To hear the entire webinar you can view an archived recording by visiting http://info.ethicspoint.com/about/news/archive/event03080601.asp

Has your institution had a breach of data security in the past 12 months involving personal information?



Breach of data security in the past 12 months involving personal information – 1/3 have had a breach, but most have not.

Is your institution's Board of Trustees Audit Committee involved in the institution's risk assessment process?



59% has an audit committee that is involved with the risk assessment process; 20% said no and 12% don't have an audit committee.

ACUA

Association of College & University Auditors

342 North Main Street
W. Hartford, CT 06117-2507

PRSRT STD
U.S. POSTAGE
PAID
HARTFORD, CT
PERMIT NO. 2115

Governance Solutions for **Higher Education**

Building an ethical culture takes more than a commitment – it requires the right tools, processes, and expertise.

EthicsPoint has created a suite of flexible, integrated applications and services that can be tailored to the unique demands of the higher education community. Whether you're taking small steps or giant leaps, we're committed to helping you build a sustainable ethical culture.

We are proud to support the ACUA Distance Learning Program. Mark your calendars for these important seminars throughout the year:

> ***May 18th, 2006*** *Risk on the Campus of the Future*

> ***August 15th, 2006*** *Data Security on College and University Campuses*

> ***November 15th, 2006*** *Conflicts of Interest in Higher Education*

For more information, visit
info.ethicspoint.com/education/events
or call 1-866-297-0224

Online Ethics Training
Hotline/Helpline Reporting
Incident Management
Measurement & Assessment

ethics·point®

Integrity. Information. Insight.