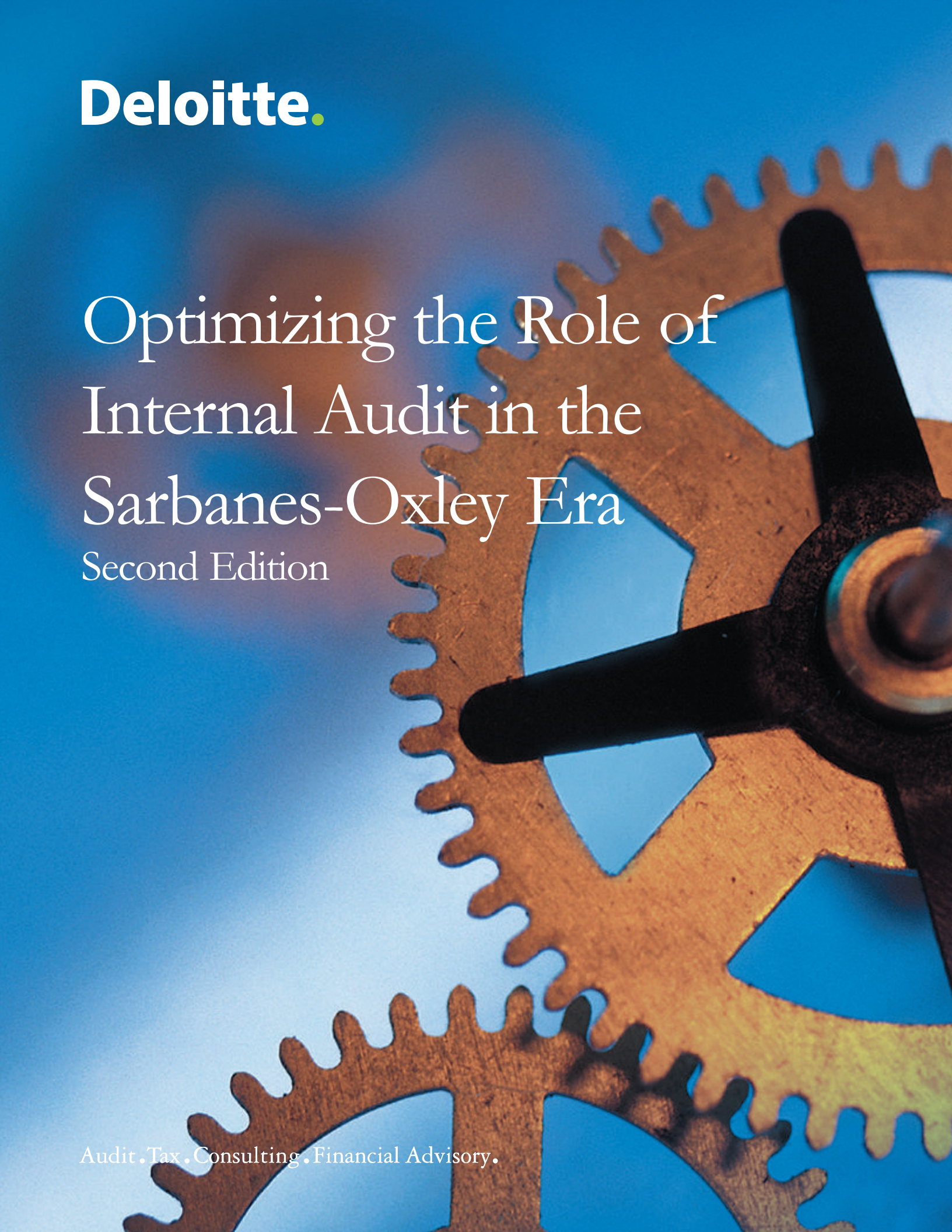
Deloitte.

Optimizing the Role of Internal Audit in the Sarbanes-Oxley Era

Second Edition



Audit . Tax . Consulting . Financial Advisory.

Welcome to the 2nd Edition

Optimizing the Role of Internal Audit in the Sarbanes-Oxley Era

In response to requests for additional guidance, in recognition of the ever-changing business environment, and in light of continual gains in experience and knowledge, Deloitte & Touche LLP is pleased to present this updated whitepaper.

The following is a synopsis of new material contained within these pages:

Table of Contents

Second Edition

Optimizing the Role of Internal Audit in the Sarbanes-Oxley Era

Overview

Few would dispute that the Sarbanes-Oxley Act of 2002[1] has profoundly changed the business environment for companies listed on the U.S. equities markets. The mandated emphasis on corporate governance and internal control has transformed procedures and responsibilities at almost every level of the organization, and the law will likely impact the manner in which business is conducted for decades to come. Whether the benefit will be commensurate with the cost remains an open question in some quarters, but scant argument can be raised against the intent of a law designed to reduce fraud and bring reliability to financial reporting, and to restore confidence to the public markets.

Particularly noteworthy (if not notorious), section 404 of the legislation requires public companies to determine financial reporting risks, identify or establish related controls, assess control effectiveness, fix deficiencies, and then re-test and re-document anew. The challenges posed by this section, and by the Act as a whole, have proven formidable, and the impact has been felt throughout organizations across the U.S. and the world.

Among the business functions most significantly affected by Sarbanes-Oxley section 404, internal audit certainly ranks high. Internal auditors, with their expertise in business process analysis; financial, operational, compliance, and information technology control testing; risk management; the COSO internal control framework[2]; and forensic accounting, faced unprecedented demand for their services during the first years of conformity with the law.

The profession rose to the task. Many internal auditors can claim—with only slight hyperbole—that they played a valiant role in the initial years of Sarbanes-Oxley compliance. Indeed, if not for the internal audit profession, the business landscape would likely be littered with significantly more disclosures of material weaknesses and revelations of noncompliance with the Act.

But success can carry risk along with reward. The dramatic increase in the workload of internal audit attributable to Sarbanes-Oxley wasn't always accompanied by an equal rise in resources, leading to a predictable outcome: The traditional work of the function—operational, systems, fraud investigations, and special project audit work—often took a back seat to the more pressing needs of regulatory compliance.

For many internal audit departments, this shift toward Sarbanes-Oxley-related duties demands rebalancing. Meeting the requirements of the law is, obviously, important, but not to the detriment of other responsibilities. The function's all-encompassing focus on Sarbanes-Oxley, adopted out of necessity in the early years, should diminish going forward, and in its stead should be a more rational and considered distribution of duties.

This reprioritizing should not be viewed as mere administrative tinkering. Today, more than ever, the fortunes of the company can be tied to internal audit. In fact, a properly structured internal audit function can bring tremendous value to an organization, impacting not just regulatory compliance but also operational excellence. Intelligently utilized, internal audit can help manage risk, prioritize goals and activities, eliminate complexity and redundancy, streamline operations, and drive down cost, which, in turn, can enhance competitiveness while protecting and enhancing shareholder value.

The business world has entered uncharted territory, and optimally structured and high-performing internal audit functions can help shepherd companies through this new terrain.

Defining Effectiveness

In the new regulatory environment, responsibility and liability —both perceived and actual—are elevated to unprecedented levels. Never before have financial statements and disclosures been more carefully scrutinized. And never have the consequences of getting it wrong been more severe.[3]

Demand for heightened accountability resonates especially clearly with two parties: management, most notably CEOs and CFOs, who now must personally certify to the accuracy of the financial disclosures and the effectiveness of controls; and the audit committee, which is compelled to move beyond a reactive to a proactive role in financial reporting oversight. Each of these groups, in turn, relies heavily on an effective internal audit function for objective validation of the effectiveness of control processes and the reliability of financial reporting.

[1] For purposes of this document, the terms "Sarbanes-Oxley," "the Act," and "SOX" all refer to the Sarbanes-Oxley Act of 2002 in its entirety, including all sections of the law enacted by Congress, all associated rules promulgated by the Securities and Exchange Commission, and all related standards issued by the Public Company Accounting Oversight Board. The term "section 404" refers specifically to the "Management Assessment of Internal Controls" section of Sarbanes-Oxley and all the rules and standards that fall under that section.

[2] Committee of Sponsoring Organizations of the Treadway Commission. www.coso.org

[3] Sarbanes-Oxley Act of 2002; Section 906: "Corporate Responsibility for Financial Reports"; Subsection C: "Criminal Penalties": "Whoever certifies any statement ... [that] does not comport with all the requirements ... shall be fined not more than $1 million, or imprisoned not more than 10 years, or both; or willfully certifies any statement ... [that] does not comport with all the requirements ... shall be fined not more than $5 million, or imprisoned not more than 20 years, or both."

But what, exactly, characterizes an effective internal audit function? A baseline definition of internal auditing provides a starting point. The Institute of Internal Auditors (IIA) offers the following description:

> "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."[4]

With this description forming a foundation, the essential characteristics of an effective internal audit function can be framed. Deloitte & Touche LLP sees the following elements as key. An effective internal audit function:

- operates from a clear, updated charter
- adapts its activities to the needs of the organization
- uses a risk-based approach
- reports directly to the audit committee
- enjoys full support of management and the audit committee
- maintains open communication with management and the audit committee
- has "clout" within the executive ranks
- engenders respect and integrity throughout the organization
- teams with other internal and external resources, as appropriate
- provides leadership on issues of internal control, fraud, financial reporting, risk management, and corporate governance
- leverages technology
- deploys best-available methodologies
- engages in continuous education and staff development
- consistently reevaluates its effectiveness
- provides support to the company's anti-fraud programs.

When internal audit reports to management—usually to the CFO—the effectiveness of the function can be diluted.

Organizational Structure

In the days before the harsh light of scrutiny shone on internal audit, its organizational and reporting structure were topics of concern to relatively few. But today, with issues of competence, independence, and objectivity at the fore, many businesspeople are realizing that structure and reporting lines play a critical role in effectiveness.

Complicating the structural issue is the fact that the activities of internal audit serve the needs and/or interests of numerous parties, including:

- audit committee
- board of directors
- executive management
- line management
- shareholders
- analysts and shareholder rating services
- regulators
- external auditors

Of course, despite their vested interest, not all of these parties exert direct supervisory influence over the function. In most companies, lines of reporting usually lead to either of two groups: executive management or the audit committee.

In Deloitte & Touche's view, the latter choice offers clear superiority. When internal audit reports to the audit committee, the function is kept structurally separate from management, a distinction of importance to many, including regulators concerned with independence, external auditors seeking objectivity, and analysts looking for strong corporate governance practices. Such an alignment also encourages the free flow of communication regarding any issues or concerns; allows for direct feedback on the performance of the chief audit executive and the function; ensures that internal audit is staffed and budgeted properly; and permits the audit committee to exert direct influence over the hiring, compensation, and firing of the CAE.

Conversely, when internal audit reports to management—usually to the CFO—the effectiveness of the function can be diluted. If management hires and fires the chief audit executive, controls the budget, and sets the agenda, then the impact on objectivity and independence can be significant. Communication of concerns can become bottled up; the pressure to rationalize questionable practices or to issue favorable reports can intensify.

Although the advantages of reporting to the audit committee are clear-cut, one factor mars what might otherwise be an optimal reporting structure: The audit committee lacks a day-to-day presence in the organization, and therefore may be somewhat out of touch with the culture, issues, and personal ities, as well as the ability to handle required human resource activities.

Trends are moving steadily toward audit committee oversight of internal audit. Several years ago, better than 90 percent of internal audit departments reported to the CFO. Today, according to surveys by the Institute of Internal Auditors, that number falls between 40 and 50 percent.[5]

While there are no easy answers, two points are unambiguous: The CAE must have a strong and direct reporting relationship to the audit committee; and the audit committee must take responsibility for certain supervisory activities, including approving internal audit's budget, risk assessment, and audit plan, and for hiring, evaluating, and, if necessary, firing the CAE. Having a dual reporting relationship to the CEO or perhaps general counsel can facilitate the required administrative activities associated with operating the function within the company.

[4] Institute of Internal Auditors, "Defining Effectiveness," http://iia.org.au/htdocs/tech_info/code.htm

[5] Institute of Internal Auditors, "Internal Audit Independence and Corporate Governance," 2003, http://www.theiia.org/iia/download.cfm?file=234.

Figure 1

Transforming Internal Audit - Internal Audit Maturity Model

	Baseline	Cumulative or Evolutionary?*	Mainstream	Cumulative or Evolutionary?*	Leading Edge
Philosophy					
Perspective	focus on the past: retrospective look at what happened	cumulative	focus on the present	cumulative	focus on the future: proactice approach toward risk mitigation and development of controls
Defining Effectiveness					
Focus	audit entity based on rotation plan	evolutionary	audit entity prioritized based on inherent risk	evolutionary	focus on strategic, business, and process toward risk
Style	corporate police	cumulative	supportive	cumulative	advisor
Organizational Structure					
Responsibility	auditing for compliance	evolutionary	auditing and suggesting	evolutionary	auditing and consulting
Existence of Chief Audit Executive	not likely	evolutionary	occasionally	evolutionary	member of "C" suite
Internal Audit Reporting Lines	controller	evolutionary	CFO/COO	evolutionary	audit committe chair
Role of Internal Audit in the Sarbanes-Oxley Era					
Objectives and Mandate	compliance to (financial) policies and procedures	cumulative	assurance on financial control, compliance	cumulative	business assurance
Sarbanes-Oxley "Ownership"	N/A	evolutionary	participating in the Sarbanes-Oxley effort	evolutionary	management ownership/IA validation
Independence and Objectivity	hopefully	cumulative	generally	cumulative	absolutely
Technology					
Toolkit	automated workpapers	cumulative	sampling programs and standalone data analysis	cumulative	real-time monitoring
IT Auditing	ill-defined	cumulative	GCC, security, applications	cumulative	consulting to improve IT infrastructure
Fraud Detection					
Fraud Prevention and Detection	generally not addressed	evolutionary	reactive	cumulative	proactive
Risk Management					
Risk Focus	operational	cumulative	operational and financial	cumulative	all enterprise risks

* Cumulative: The past practices of the internal audit function are absorbed into and become part of new, expanded practices.
Evolutionary: The past practices of internal audit are discarded as new practices are adopted to take their place.

The First Years of 404: Lessons Learned

No point sugarcoating it: The first couple of years under Sarbanes-Oxley section 404 were tough. But today, internal audit functions have advanced sufficiently along the path to benefit from the journey. The learning curve, while steep, provided numerous insights on ways to improve the function. Here are a few lessons learned:

Relationship with the Audit Committee: As noted previously, an optimally organized internal audit function reports directly to the audit committee. Of course, setting up the proper reporting structure, in itself, guarantees neither open lines of communication nor strong relationships with the chair and members. Those items take effort. But it's effort worth expending, because the audit committee (AC) can be internal audit's strongest ally.

The IA/AC relationship can be strengthened in various ways. For example, audit committee education programs can help members better appreciate the realities and potential of the function. If expectation gaps exist, education can help bridge them.

Charter: Another area for potential improvement concerns the internal audit charter. Most IA functions have one, yet in some cases, it is not used to align activities with IA mission. The advent of Sarbanes-Oxley provides an opportunity to update the charter; moreover, it offers a chance to enhance or even redefine the function with full participation and approval from the audit committee and management. The more integrated these constituent

groups are in the process, the better support they will provide when audit activities need to be prioritized, hard decisions made, and budget and staffing requests acted upon.

Employee Education: New demands call for new talents, and with the enhancement and redefinition of the role of internal audit comes a need for a broadened skill-set. Sarbanes-Oxley, enacted to address internal control over financial reporting, has exposed a weakness in the traditional internal audit lineup—call it a gap in GAAP expertise. Some IA functions do not have sufficient financial reporting skills, including an understanding of the importance of information technology in enabling proper control over financial reporting. Until recently, many internal auditors have been more business process oriented. Today, a broader spectrum of talent is required, which can be obtained through staff education as well as focused hiring programs.

Areas of Inquiry: A heightened role for many internal audit functions in the Sarbanes-Oxley era is the need to conduct governance reviews. Specific areas of inquiry that might benefit from the attention of internal audit include the appropriateness of audit committee oversight; the adequacy and enforcement of codes of conduct; the sufficiency of documentation, design, and operating effectiveness of entity-level controls; and the effectiveness of fraud risk assessment.

Uncorrected Deficiencies: As quarter-to-quarter and year-to-year compliance data is compiled, the issue of how to handle uncorrected deficiencies can arise. The PCAOB has stated that deficiencies left unremedied may be indicative of a poor control environment and inadequate tone at the top. Further, such uncorrected deficiencies may, either individually or in the aggregate, escalate into significant deficiencies or material weaknesses. To address this issue, IA should evaluate management's ongoing process for monitoring and remediating prior year deficiencies in internal control over financial reporting.

Role of Internal Audit in the Sarbanes-Oxley Era

While the upheaval of the last couple of years has surely roiled the profession, certain principles remain unaffected. Most notably:

The traditional role of internal audit—to assess controls, bring value, and improve operations—is as applicable today as it ever was.

However, as noted previously, the department's workload has dramatically increased with the advent of Sarbanes-Oxley.

Finding the right balance of activities will be key to future success, both for internal audit as a profession, and for the companies that internal audit serves.

Unfortunately, that balance cannot be neatly summarized in a few paragraphs. Each company presents unique circumstances and distinctive needs. Myriad factors complicate the equation and impact the result, including company size, industry, location(s), budget, profitability, IT infrastructure, competence of personnel, preferences of the board and management, and more.

One way to parse the proper role of internal audit is through the use of a maturity model (see figure 1). The various activities of the department can be charted along a descriptive continuum that begins with "baseline," proceeds through "mainstream," and concludes with "leading edge."

In applying the maturity model to their own circumstances, companies will find variability to be the norm. Only the rare internal audit department will see all its data points plotted neatly under any one category. Rather, depending on goals, philosophy, and other factors listed above, the function may classify its risk management activities under, say, "leading edge" while its technology description falls under "mainstream." Virtually unlimited combinations are possible, with none necessarily being right or wrong. What works best and makes sense for one organization may be entirely inappropriate for another.

But regardless of how the data points fall on the maturity model, clearly the optimal role of internal audit extends far beyond internal control over financial reporting. The imperative to attain compliance in the first years distorted that perspective, but the time has come to reestablish a broader view. Internal audit needs to play a role in Sarbanes-Oxley compliance—indeed, one of the most essential roles—however, that should not be its sole responsibility.

A more expansive view of internal audit's optimal role asks the question, *What needs to be done to address stakeholders' needs?* Some of those stakeholders and the issues they have are described in figure 2.

A fair amount of confusion exists within and outside the profession regarding the challenges posed by Sarbanes-Oxley. What are the proper parameters of involvement by internal audit? At what point does the function's independence and objectivity become impaired? To answer these and other questions, Deloitte & Touche convened a meeting of its leading practitioners to debate the issues and reach consensus. The following Sarbanes-Oxley-related activities were found to be allowable and appropriate for internal audit:

- consulting on internal control
- consulting on internal control in relation to enterprise-wide risk management (see page 9, "Risk Management," for more information on this topic)
- assisting the organization in identifying, evaluating, and implementing risk and control assessment methodologies
- recommending controls to address related risks
- assisting with designing systems of internal control (however, designing is not the same as implementing; see page 5)
- drafting procedures for systems of internal control
- assisting with maintenance of the controls repository
- conducting effectiveness testing on behalf of management (but without concluding for management)
- aiding management in the design of tests for control effectiveness (however, in all cases, management should make the final decision on control design and operating effectiveness)
- taking on the role of lead project manager for all or part of the efforts related to complying with section 404

Is Internal Audit Addressing Stakeholders' Needs?	
Board/Audit Committee	How are we managing business risks? How are we assured they are being managed appropriately? Are we dedicating enough resources to manage our risks?
CEO/COO	What unforeseen events might disrupt our strategy and prevent achievement of our goals?
CFO	What risks could materially impact our financial results?
General Counsel	What could we do to further minimize our legal and regulatory liabilities and ensure compliance with laws and regulations?
General Managers	How much risk am I allowed to take? What is our corporate risk appetite? What are my risk management responsibilities?
Risk Managers	How efficient is our current risk financing strategy? Does the current risk management strategy adequately capture the key risks?
Regulators	How comprehensively is the company addressing the interests of stakeholders?
Rating Agencies	How well does senior management understand risk? How great is management's risk awareness? What is their ability to manage risks as they emerge?

Figure 2

- providing training and/or information on internal control identification and assessment, risk assessment, and test plan development
- providing information, training, and/or facilitating a control self-assessment.

The following Sarbanes-Oxley-related activities were found to be inappropriate for an objective internal audit function:

- concluding on the effectiveness of internal controls on behalf of management
- making or directing key management decisions regarding internal controls, remediation activities, and Sarbanes-Oxley compliance
- implementing systems of internal control
- performing control activities.

The overriding factor concerning appropriate activities hinges on decision-making and responsibility. Under the provisions of Sarbanes-Oxley, management is solely responsible for the system of internal control over financial reporting. Internal audit may serve management in many capacities, including advisory, testing, training, and development, so long as that work doesn't cross the line into a decision-making role. Vigilance by all parties can maintain this critical distinction.

Readers should note that the term "allowable" activities is not necessarily synonymous with "optimal" activities. That is, just because a particular activity *could* be performed by the internal audit function, does not mean that it should. In Deloitte & Touche's view, internal audit groups that are involved in the "inappropriate" section 404 activities cited above should strive to transition away from these activities and move toward independent evaluation, validation, and testing. Of course, this recommendation assumes sufficient and competent resources to take over the section 404 responsibilities previously handled by internal audit.

Reconciling Traditional and Contemporary Responsibilities

Long before the advent of Sarbanes-Oxley, internal audit had an important role to play. Its operational audits, systems work, fraud investigations, and other activities provided an invaluable service to management and a major boost to the company's fortunes.

Nothing that has transpired since that time has changed these basic facts. The traditional role of internal audit remains as critical as ever, even as new demands expand the workload.

How can an internal audit group balance its traditional work with its new duties? Here are a few ideas:

Expand staff: With new responsibilities piled upon the old, resources have become strained in many IA organizations. If management continues to utilize internal audit for intensive section 404 and 302 compliance-related work, then an infusion of personnel to accommodate the additional workload should be provided.

Increase funding: Historically, there has been a tendency in some organizations to under-invest in internal audit, despite the fact that chief audit executives have often tried to make the case for increased budgets. Today, however, the dynamic has shifted. The potential ramifications and sanctions around regulatory noncompliance have gotten the attention of those with budgetary authority, and, as a result, the time has never been better to command the resources necessary to perform the job well.

Many CAEs have found that by having a quality assessment performed they are able to not only identify improvement opportunities but are also in a better position to support the need for additional resources and funding. (It must be noted, of course, that infusions of money and people can help internal audit attain optimal performance, but they alone will not magically transform an underperforming function. Resources must be thoughtfully and methodically deployed in the proper areas of greatest need and most potentially beneficial impact.)

Solicit buy-in: With a varied constituency and additional duties, internal audit must operate from a clear and vetted agenda. All of the major parties—management, audit committee, and independent auditors—should be apprised of and, to the extent that it is appropriate, weigh in on the audit plan.

Combine and integrate duties: Internal audit groups should look at combining traditional duties with section 404 testing. That is, in many instances, operational, systems, and special project audit work can be conducted concurrently with Sarbanes-Oxley-related evaluation, validation, and testing. Not only can this provide cost and time efficiencies, but should also eliminate the need to knock twice on management's door, thereby minimizing the inevitable disruptions caused by internal audit activities.

Given its unique skill-set, internal audit is often at the fore when it comes to rooting out fraud-related problems.

Fraud Detection

Financial statement fraud generates more attention than its prevalence might warrant—significantly more misstatements can be attributed to innocent mistakes and misjudgments. But perception often trumps reality, and sensational acts of fraud defined many of the recent corporate scandals, providing compelling news headlines and fodder for forceful political speeches. When carried out on a large scale, fraud can wipe out billions of dollars of investor wealth in a short timeframe. And, of course, financial statement fraud was the impetus behind the Sarbanes-Oxley Act itself.

Thus, given its prominence and potential magnitude, fraud—both financial statement fraud and the misappropriation of assets—needs to be on the radar screen of every internal audit function. Not that the function should become the sheriff of the organization; rather, internal audit ensures that reasonable activities are in place to help prevent and detect fraud and support company anti-fraud programs.

Indeed, given its unique skill-set, internal audit is often at the fore when it comes to rooting out fraud-related problems. Some cases are first uncovered by the function, and internal audit is frequently the primary option for investigating allegations of fraud.

That said, it must be noted that no company, no matter how vigilant, can eliminate fraud with 100 percent certainty. Determined and deceptive individuals, especially those acting in collusion, can sometimes subvert even the most carefully and conscientiously constructed anti-fraud program.

But the lack of ironclad assurance is no excuse for inaction. A number of activities and programs to combat financial statement fraud are recommended for every public company, not solely because their presence helps to minimize risk, but also because their absence may result in an adverse opinion on the effectiveness of internal control over financial reporting. Steps that address the misappropriation of assets, although not required under Sarbanes-Oxley, are also highly recommended.

A few of the essential elements of an effective antifraud program are noted below:

Control Environment: Strong antifraud activity, just like strong internal control itself, begins with the control environment. The executive management team should continuously demonstrate, through words and actions, that ethical and legal behavior is the only acceptable mode of conduct in the company. This principled "tone at the top" must diffuse itself through everything the organization says and does: in regular communications; company literature; codes of conduct and ethics; hiring, promotion, and termination practices; vendor and customer relations; and much more. Some internal control experts contend that establishing this culture of "doing the right thing" represents the most important component of effective internal control.

While the control environment does not necessarily lend itself to easy assessment, internal audit can gauge its strengths and weaknesses through a cultural survey given to employees throughout the organization. The survey measures hard-to-quantify components such as employee attitudes, corporate culture, communication practices, and more.

Whistleblower Hotlines: Perhaps the most critical piece of an effective antifraud program can be found in the whistleblower hotline, for two reasons: (1) such hotlines are required by section 301 of Sarbanes-Oxley; and (2) whistleblower hotlines uncover more verifiable cases of fraud than any other method, according to a study by the Association of Certified Fraud Examiners.[6]

An effective hotline should be anonymous and continuously available. A detailed procedure for the timely handling of reports should be developed and followed faithfully. Employees should receive guidance and encouragement on its use. And the hotline should be advertised widely, through posters, wallet cards, intranet sites, periodic communications, and other means.

Fraud Risk Assessment: Simply stated, any risk assessment process that doesn't include financial statement fraud considerations will be deemed ineffective by the company's independent auditor, and the consequences will be far-reaching. According to the Public Company Accounting Oversight Board (PCAOB), "if the risk assessment function is ineffective, this should be regarded as at least a significant deficiency and as a strong indicator that a material weakness in internal control over financial reporting exists."[7]

Thus, it clearly behooves companies to appropriately consider the risk of material misstatement due to fraud, and to subsequently design and implement appropriate programs and controls to prevent, detect, and deter relevant fraud risks and schemes.

Areas that deserve special attention during the fraud risk assessment process include management override of controls, revenue recognition, segregation of duties, significant and unusual journal entries, accounts involving judgment and estimates, and complex accounting procedures.

While internal audit has a significant role to play in fraud detection and prevention, the function should not be charged with sole responsibility in this area. The job is simply too large and too important to be left to a single business unit. Rather, the obligation should be shared by every facet of the organization, including executive management, employees, boards and committees, and augmented by oversight and assistance from the external auditor, regulatory agencies, and others.

[6] Association of Certified Fraud Examiners, "2002 Report to the Nation: Occupational Fraud and Abuse." http://www.cfenet.com/pdfs/2002RttN.pdf

[7] Public Company Accounting Oversight Board, Auditing Standard No.2, paragraph 140.

Human Resources for Internal Audit

With the advent of Sarbanes-Oxley, internal audit staffing challenges frequently became acute due to the demands imposed by the Act. Issues such as recruitment, deployment, and professional development took on heightened importance.

Many chief audit executives grappled with the question: How can my department maintain an on-demand, flexible workforce without incurring burdensome fixed costs? The problem defies easy answer. Maintaining the high level of staffing necessary to respond to peak demands, such as Sarbanes-Oxley work, can be costly; yet most internal audit functions need to deliver on those demands.

No single solution can solve the staffing quandary, but multiple approaches, in combination, can ease the burdens imposed on the function. Consider the following:

- External consultants and contractors can be utilized to cover the workload peaks and specialized skill needs.
- Recruitment activities can be stepped up, with an eye towards building a multi-disciplinary team with a healthy mix of CIAs, CISAs, CPAs, CFEs, MBAs, and specific industry experience.
- The CAE can work with the executive management team to determine a practical philosophy for moving employees in and out of the function, i.e., should internal audit be considered a career path, a stepping stone to management, or a combination of the two?
- Internal audit heads should consider the benefits of increasing education and training for their employees to enhance not only job performance but prospects for retention.
- Internal audit should stay current on the latest PCAOB guidance. IA practitioners can "network" through the Institute of Internal Auditors and other professional associations, identifying leading practices and lessons learned, which should be brought back to management for enhancement of their Sarbanes-Oxley processes.

Utilizing Internal Audit to Optimize Section 404 Compliance

Internal audit can help management develop a program of sustainable compliance and generate tangible business improvements by focusing on three areas: people, process, and technology.

People: Internal audit can serve as a catalyst, through education, for the company and its internal control program. Training can be delivered in the areas of codes of conduct, business ethics, and communications to create organization-wide awareness and support the effort to achieve overall compliance and sustainability. Such an activity supports a strong control environment and ordinarily will not escape the notice of the external auditors, who will factor it into their assessment of the effectiveness of internal control.

Process: Internal audit can be a driving force behind the efficiency and effectiveness of testing activities. The function can head up a control rationalization effort to weed out duplicative and immaterial controls from the test plan. Redundant processes across and within business units can be identified and eliminated by management.

Just as a person requires regular medical check-ups to remain in peak health, so too can internal audit benefit from a thorough evaluation.

Technology: Forward-thinking executives will strive to leverage existing technologies to create efficiencies in testing, documenting, monitoring, and other compliance functions. In the early years of compliance, companies were able to identify and reduce inefficiencies that resulted from non-standardized information technology systems in different units and business locations. Internal audit, in its consulting and advisory role, is in a position to promote other ways to reduce inefficiencies through the use of continuous monitoring technology.

The Pursuit of Quality

With so much riding on internal audit—both from a regulatory and competitiveness standpoint—the optimal functioning of the department becomes a vital concern. Every stakeholder cited previously, but especially management and the audit committee, relies heavily on internal audit. How can these parties be sure that the function is up to the task?

The answer comes in the form of quality assessments—an examination of the effectiveness and efficiency of the function. Just as a person requires regular medical check-ups to remain in peak health, so too can internal audit benefit from a thorough evaluation.

Three models exist, two internal and one external; forward-thinking companies will utilize all of them:

1. **continuous quality assurance:** Built into the job descriptions and operating routines of the department should be continuous quality assurance activity. In some respects, this program could be considered internal audit's own set of controls that provide a window into work performed and quality of operations.

2. **self-assessments:** Conducted every two years, this process deploys internal staff to examine the operations of the function. Has the charter been updated to reflect current conditions? Does a comprehensive risk assessment serve as the basis for planning and execution? Are stakeholder needs met in a timely fashion?

3. **external quality assessment:** The Institute of Internal Auditors strongly encourages chief audit executives to subject their internal audit departments to independent scrutiny. The IIA's Standard 1312, issued in 2002, states that "...every internal audit department [must] have an external quality assessment at least once every five years by a qualified independent reviewer from outside the organization." In certain circumstances—such as rapid turnover of staff or a change in internal audit leadership—a more-frequent assessment schedule may be warranted.

Whether internal or external, a quality assessment reviewer will look at the function for certain characteristics and performance indicators, including the following:

- independent and objective
- dynamic and flexible
- proactive
- risk focused
- knowledgeable about company and industry
- innovative and consultative
- catalyst for change
- aligned with management and audit committee expectations
- aligned with corporate objectives
- leverages technology and leading practices
- communicates effectively
- maintains constructive relationships
- emphasizes continuous learning.

It should be acknowledged that quality assessments can be time-consuming and costly. Yet the rationale is compelling:

- As Sarbanes-Oxley-related activities become less of a fire drill and more part of standard operating procedure, realignment of internal audit's duties becomes essential. A quality assessment can help the function, audit committee, and management fully understand the needs of the business and how internal audit should be organized to meet these challenges.

- Yesterday's leading practices are today's outmoded methodologies. A qualified external quality assessment team that is continually exposed to the full spectrum of approaches and techniques can bring up-to-date knowledge to the function.

- Business moves at a breakneck pace, and to keep up, companies require continuous improvement—a fact that holds as true for internal audit as any other business function. A quality assessment can provide that edge. As an ongoing process, the quality assessment will result in a periodic list of improvement areas that the chief audit executive can include in his/her evaluation metrics to encourage continuous improvement.

Deploying Technology

While technology will never replace an intelligent, inquisitive, and well-trained internal auditor, certain tools can improve efficiency and enhance productivity. Two categories of tools predominate: supporting technologies and enabling technologies.

The former category is fairly commonplace and not particularly revolutionary. For example, electronic spreadsheets serve as an aid in recordkeeping; automated work papers remove some of the drudgery from documentation.

Significantly more valuable, however, are enabling technologies, which allow internal auditors to attain new levels of testing assurance. For example, instead of developing sampling procedures, internal audit can now, through technology, test a higher percentage (or the entire population) of transactions and processes. Additionally, the department can perform exception-based and fraud-related procedures with far greater levels of reliability.

Leading the way are a number of enhancements to enterprise resource planning (ERP) systems. This latest generation of software can acquire data from different repositories within the network, and can help validate whether internal controls are operating effectively.

Other examples of enabling technology include data acquisition, analysis, and monitoring tools; and administrative tools.

In the modern internal audit environment, enabling technologies are no longer a luxury, but a necessity, as they promote continuous monitoring of risk in a cost-effective fashion. Chief audit executives can and should make a compelling case to include such tools in their budgets.

Key Business Relationships

Efforts to spur corporate growth and improve operational efficiency have led to a proliferation of contract-based business arrangements, such as outsourcing (payroll, benefits administration, order fulfillment, etc.), joint ventures (shared R&D, pooled manufacturing, etc.), strategic marketing alliances (companies with complementary services or products going to market together), and licensing of intellectual property (sharing patents and copyrights with business partners and customers in exchange for royalties). The beneficial impact of these business arrangements can be substantial, of course, but new risks and responsibilities also become important considerations.

Companies need to perform periodic contract compliance activities to assess the integrity and reliability of extended business relationships. By playing an active role in contract compliance activities, internal audit can not only achieve bottom-line results (such as revenue recovery or cost reduction), but can also play a critical part in identifying and mitigating significant risks throughout a company's extended business network.

Where does internal audit fit into the picture? In various areas:

- defining control objectives and identifying related control activities
- assessing the validity and completeness of any information provided by the contracting party
- validating integrity assumptions and contract compliance with business partners, including customers, suppliers, and licensees
- identifying specific monetary and non-monetary risks present in important relationships
- recommending steps to mitigate the risks of those relationships
- evaluating whether the company's own internal control environment is sufficient to identify and monitor key relationship risks.

Risk Management

As noted in the early pages of this document, proper risk management lies at the heart of an effective internal audit function. The specific role the department assumes in regard to risk will depend on its placement in the maturity model cited previously (figure 1, page 3). A "baseline" approach may deal only with operational risk, while a "leading edge" practice may include a broad universe of enterprise risks. Many functions will fall in the middle of the two extremes, depending on philosophy, charter, goals, and other factors. Some departments may limit themselves to the identification of risk; others may participate in the mitigation of risk.

Surprisingly, during the first years of Sarbanes-Oxley compliance efforts, many companies failed to develop and deploy a comprehensive financial accounting risk assessment process, an outcome both unexpected—because risk assessment is an essential component of internal control over financial reporting—and unfortunate—because without proper risk assessment, some of the time and dollars devoted to documenting and testing controls may have been misspent. Clearly, this situation needs rectifying going forward. Internal audit should play a prominent role in helping management realize that without a comprehensive risk assessment process, internal control over financial reporting can never be considered effective.

It should also be noted that if an organization does not have a formal risk management process in place, the Institute of Internal Auditor's practice advisory No. 2100-4 says that "the internal auditor should bring this to management's attention along with suggestions for establishing such a process."

An aid to proper risk management may be found in a recent publication from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Entitled "*Enterprise Risk Management—Integrated Framework*," the document defines and discusses key enterprise risk management (ERM) principles, concepts, and components. Although not solely directed at the internal audit profession, the COSO ERM framework can provide a clear blueprint for anyone seeking more effective risk management. (Visit www.coso.org for ordering information.) (See also the enterprise risk management section of Deloitte website for additional materials and publications: www.deloitte.com/us/risk.)

Augmenting the COSO ERM document is guidance from the Institute of Internal Auditors, which reviewed the publication for applicability to the profession and deemed much of the information relevant and useful. According to the IIA, "Internal auditing's core role with regard to ERM is to provide objective assurance to the board on the effectiveness of an organization's ERM activities to help ensure key business risks are being managed appropriately and that the system of internal control is operating effectively."[8]

Thus, according to the IIA, a risk-focused internal audit function will engage in the following basic activities:

- providing assurance on risk management processes
- providing assurance that risks are correctly evaluated
- evaluating risk management processes
- evaluating the reporting of key risks
- reviewing the management of key risks.

[8] Institute of Internal Auditors, "The Role of Internal Auditing in Enterprise-wide Risk Management," Sept. 29, 2004.

During the first years of Sarbanes-Oxley compliance efforts, many companies failed to develop and deploy a comprehensive financial accounting risk assessment process.

Some companies may wish to have their internal audit department take on a more active role regarding risk management. In such cases, the IIA considers the following roles permissible:

- facilitating identification and evaluation of risks
- coaching management in responding to risks
- coordinating ERM activities
- consolidating the reporting on risks
- maintaining and developing the ERM framework
- championing establishment of ERM
- developing risk management strategy for board approval.

While participation in risk management activities is clearly a desirable role for internal audit, care should be taken to maintain independence and objectivity. The board of directors and the management team should retain full responsibility for risk management; internal audit should diligently strive to limit itself to an advisory role.

Leveraging Outside Perspective and Leadership

How can chief audit executives keep their internal audit function at the top of its game? Where should CAEs turn for thought leadership, fresh ideas, and leading internal audit practices? Many avenues can lead to improvement:

- Conducting a quality assessment of internal audit (see page 7) can help ensure that the function is performing optimally. Having an outside, objective party perform an evaluation can infuse new thinking and provide perspective.
- Inviting a guest auditor to join the function for a period of time can help share leading practices and promote thought leadership throughout the internal audit function. These "guests" can be drawn from other departments within the organization, which can help diffuse institutional knowledge, or can be brought in from another organization, which can provide valuable outside perspective.
- Developing training and education programs can improve internal audit and internal control skills. Using outside trainers can provide new perspectives.
- Adopting more formal programs that rotate internal auditors from different regions in the company can bring in new viewpoints and skill-sets.
- Benchmarking the practices of internal audit units at other companies may inspire internal auditors to adopt new practices or look at old problems in new ways. Developing relationships with other CAEs can lead to the sharing of new ideas and approaches.

Beyond Sarbanes-Oxley

Pre-Sarbanes-Oxley, internal audit faced no shortage of worthy projects. Today, it's time to place many of them back on the agenda. Here are a few that merit consideration:

Evaluating New Business Initiatives: Dynamic companies constantly seek out new opportunities; those that don't may soon find their fortunes lagging. However, each new opportunity also brings new risk, and internal audit should take a significant part in identifying and helping the company control that exposure. Obviously, anything as monumental as a merger or acquisition requires due diligence on the part of internal audit. However, less weighty initiatives, such as a new product design or new services, could also benefit from internal audit's wisdom and guidance.

Managing Information Technology (IT): IT usually presents significant risk management challenges to an organization, whether the computer systems are static, undergoing an incremental upgrade, or in the midst of a complete migration. Section 404 compliance has also inspired many companies to consolidate disparate IT systems to bring more efficiency and reliability to internal control; in such cases, management should be drawing heavily on internal audit expertise.

Contributing to Corporate Growth: Bringing value to the organization has always been a prime concern of internal audit, and building top line revenue growth certainly falls under that rubric. Specific activities in support of the growth objective will vary by company. If corporate growth is attained through acquisition, then the function should participate in due diligence. When organic growth defines the strategy, either through expansion into new regions, distribution channels, or customers, internal audit should be involved in all the "auditable" processes. In other words, internal audit plans and activities should be skewed towards the company's areas of focus and risk. If the company is thinking about "betting the farm" in a particular area, internal audit should be calculating the odds.

Other Activities: Certain other areas are prime for internal audit involvement:

- research and development effectiveness
- decision-making processes
- inventory management
- ethics compliance.

Peak Performance Indicators

How does internal audit measure success? The particular method employed is less important than the act itself. Performance of the function should be constantly monitored and rated. Here are some critical performance indicators:

- recommendations adopted
- recommendations implemented within a certain time period
- stakeholder surveys
- reports issued on time
- staff training and certifications
- cost-saving opportunities and actual cost recoveries
- internal audit turnover
- internal audit transfers (with employees moving to other units within the business considered a positive outcome)
- internal audit employee survey measuring professional staff satisfaction
- internal audit staff utilization
- hours of training.

Conclusion

For companies listed on the U.S. equities markets, the regulatory environment stands in a state of unprecedented flux. Internal audit can and should take a leading role in restoring equilibrium.

But before it takes on that enterprise-wide challenge, the department must first be sure its own house is in order. The distortion caused by the first years of Sarbanes-Oxley compliance must be clarified. Charters and job descriptions should be updated. Traditional roles must be reconciled with new responsibilities. Audit work should be judiciously balanced between financial, operational, strategic, compliance, and information technology. Risk must be carefully weighed. And the needs of stakeholders should figure prominently in the action plan.

Moving forward, Sarbanes-Oxley-related work should become a visible and permanent part of internal audit's job description. Helping to sustain compliance with section 404 of the Act will remain a critical responsibility. Providing objective assurance to the board and management on the effectiveness of the company's enterprise risk management activities will deliver significant value to the organization. But the organizational structure and specific activities of any particular internal audit department will vary considerably by company.

Adaptability and flexibility will stand out as key characteristics of successful internal audit functions. "One size fits all" was probably never an accurate description of an ideally structured department, but it certainly doesn't apply today. Rather, an optimized internal audit function will tailor its activities to areas of greatest risk and opportunities for greatest value. Their companies will reap the benefits of sustainable compliance and enhanced competitiveness.

Deloitte & Touche LLP Internal Audit Professionals

Eric Hespenheide
Global Managing Partner
Internal Audit Services
+1-313-396-3163
ehespenheide@deloitte.com

Wayne Rose
U.S. Deputy Managing Partner
Internal Audit Services
+1-214-840-7268
wrose@deloitte.com

Global Regional Leaders

Darryl Butler
Regional Leader - Asia Pacific
+61-3-9208-7000
dbutler@deloitte.com.au

Jean-Pierre Garitte
Regional Leader - EMEA (Europe/Middle East/Africa)
+32-2-800-23-11
jpgaritte@deloitte.com

Jane Kinney
Regional Leader - Canada
+1 416-601-6317
jkinney@deloitte.ca

Marcelo Alcantara
Regional Leader - Latin America
+55 115186-1566
malcantara@deloitte.com

Michael Jones
Regional Leader - United Kingdom
+44-20-7303-6401
mijones@deloitte.com

U.S. Regional Leaders

Tony DeVincentis
New York
+1-516-918-7750
tdevincentisjr@deloitte.com

Mike Corcoran
Atlanta
+1-404-220-1729
micorcoran@deloitte.com

John Morgan
Dallas
+1-214-840-7287
jomorgan@deloitte.com

Adam Regelbrugge
Chicago
+1-312-486-2165
aregelbrugge@deloitte.com

Todd McGowan
Detroit
+1-313-396-3407
tmcgowan@deloitte.com

Darrin Kelley
Los Angeles
+1-213-688-5420
darkelley@deloitte.com

David Zechnich
San Jose
+1-408-704-4560
dzechnich@deloitte.com

Item#6049

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas – audit, tax, consulting and financial advisory services – and serves more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

In the U.S., Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP and their subsidiaries), and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting and financial advisory services through nearly 30,000 people in more than 80 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's Web site at www.deloitte.com/us.

Member of
Deloitte Touche Tohmatsu