Advisory Services
Internal Audit

Internal Audit 2012*

A study examining the future of internal auditing and the potential decline of a controls-centric approach

Observations

Since 2005, PricewaterhouseCoopers has been conducting an annual “State of the Profession” survey to provide audit leaders with important data and insights into current issues affecting the internal audit community. Given the many forces impacting internal audit in recent years, we thought it would be beneficial to develop a consensus projection of the trends likely to shape the world of internal audit by the year 2012. This report is the result of that effort, and we are deeply grateful to those who participated.

Table of contents

Overview

Internal audit leaders must adopt risk-centric mindsets if they want to remain key players in assurance and risk management.

Throughout the next five years, the value of the controls-focused approach that has dominated internal audit is expected to diminish. As this occurs, internal audit leaders must redefine the function's value proposition and adopt risk centric mindsets if they expect to remain key players in assurance and risk management. These are the central findings of a major survey and interview project PricewaterhouseCoopers conducted to develop a composite picture of internal audit by 2012.

Study results indicate that five identifiable trends—globalization, changes in risk management, advances in technology, talent and organizational issues, and changing internal audit roles—will have the greatest impact on internal audit in the coming years. By understanding these trends and their implications, internal audit leaders can help senior management identify and manage risk, thereby providing added value from the internal audit function.

A changing risk environment

According to our research, companies now view risk management and internal controls as fundamental to their business operations. This means that risk and controls are no longer seen as the technical domains solely of internal audit or other staff functions. Management as well has begun to take ownership of risk to the business and of ensuring the effectiveness of the controls designed to mitigate it.

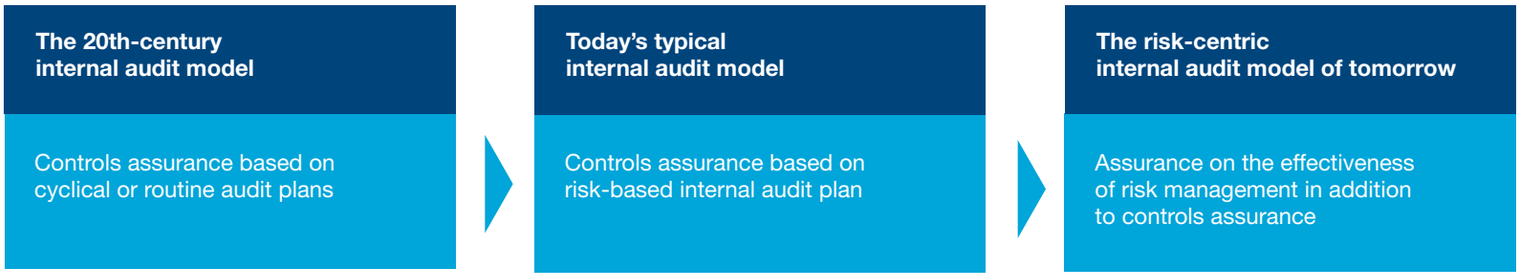
During our study, we observed a range of specific actions to identify, manage, and control risk. Current trend indicators include improved internal controls and better controls monitoring. In addition, we noted that companies are now more likely to assess the merits of a unified approach to governance, risk, and compliance (GRC). Those testing new methods indicated that they were seeking to achieve better balance between risk and opportunity; to control risk and compliance cost; and to enhance planning and forecasting capabilities.

Our research also indicated that globalization and continued advances in technology have begun to influence how companies think about their traditional business models and approaches to assurance and risk management. Changing roles and responsibilities are also influencing corporate efforts to improve risk management, as are the search for audit talent and more effective organizational structures for internal audit.

Accelerated rates of change and the faster pace of business contribute to a more dynamic risk environment, as do increased financial transparency and a 24/7 news cycle that provides consumers and investors near-instantaneous coverage of risk-oriented news around the world. The growing complexity of operations in a global marketplace—including the need to navigate unfamiliar political environments and work with regulators from multiple countries—makes it difficult for management to identify and evaluate new risks.

As our survey and interviews indicate, some internal audit functions have begun to rethink their fundamental value propositions by shifting from an internal audit model focusing on controls assurance to a risk-centric model where risk and control assurance are based on the effectiveness of risk management processes developed by management. For a relative handful of companies, this shift is already under way, as reflected in Figure 1. For other companies, the shift will occur over time as corporate risk management frameworks and control processes reach advanced levels of maturity.

Figure 1: The shifting focus of internal audit



Internal audit at a crossroads: Choosing a new strategic path

As organizations consider new techniques to manage risks and controls, our study suggests they will look to both internal audit and other functional areas to assess risk as well as to perform the more traditional assessments of controls.

Spurred by Sarbanes-Oxley and other reform measures, organizations have taken steps to strengthen controls and expand their controls-related monitoring activities. As a consequence, the value ascribed to traditional controls-focused assurance activities will likely diminish and potentially erode some of the newfound stature that many internal audit functions have attained in recent years. As other risk management functions assume new responsibilities in areas such as controls (and, in the process, enhance their value in the eyes of management), internal audit, with its strong association with controls assurance, could be perceived as being limited in its ability to deliver comparable value.

Internal audit thus finds itself at a crossroads, with two possible paths to the future.

One is to continue doing what it does today and nothing more, a path that brings with it the inherent risk of future obsolescence.

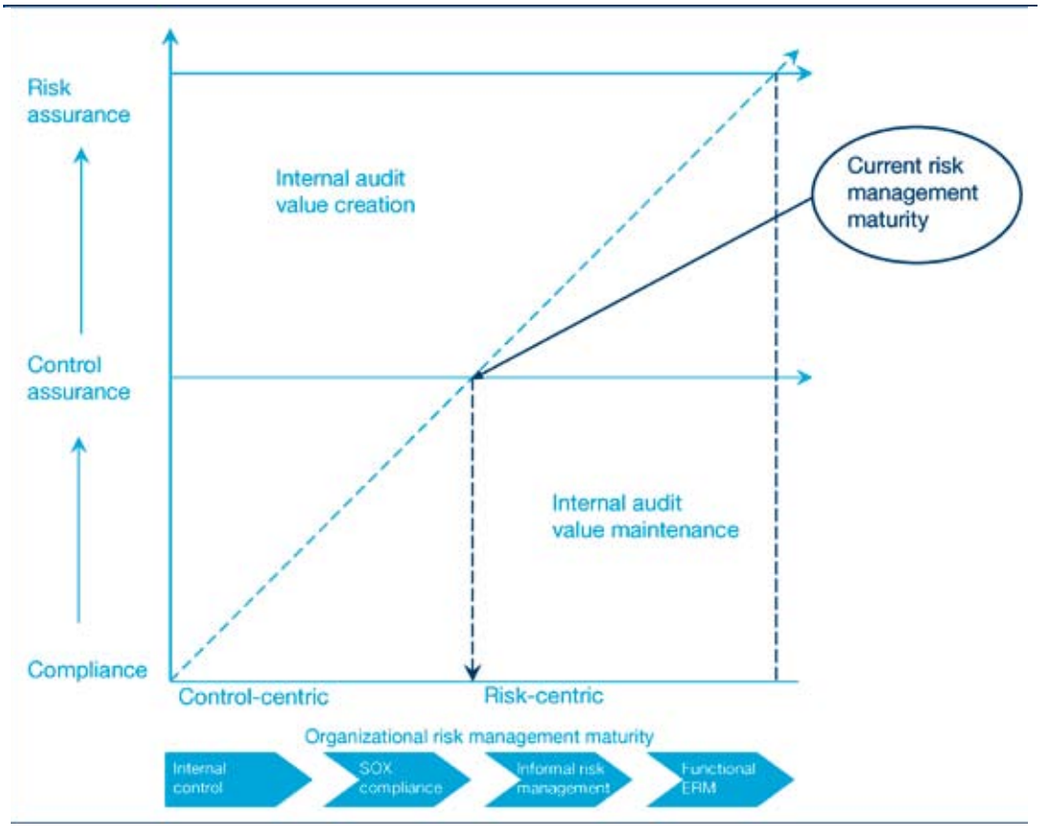
Alternatively, internal audit may choose the path we believe is more likely to lead it to meet the evolving needs of modern organizations, and the rising expectations of senior management and audit committees. This path involves moving beyond the fundamentals of risk and controls to create a new internal audit value proposition.

The new (and inherently more strategic) value proposition would include the provision of risk management assurance along with the traditional responsibility of assurance over controls. Adding risk management capabilities would inevitably help internal audit align itself more closely with an organization's maturing risk management functions. But doing so would require something not always associated with today's internal audit function: a risk-centric mindset.

A risk-centric mindset means that internal auditors adopt an all-inclusive, conceptual approach to audit, risk assessment, and risk management that extends well beyond a narrow focus on controls. With such a mindset, internal auditors would increase their functional value at a time when risk assessment and risk management have become primary stakeholder concerns.

Based on our survey results and interviews, we perceive the potential value of the internal audit function as being dependent on two key factors: the nature of internal audit's primary focus and the relative maturity of the risk management processes at the organization it serves. These correlations are depicted in Figure 2.

Figure 2: Internal Audit 2012 Value Model



Delivering the risk-centric value proposition

As organizations enhance their risk management capabilities, they progress through four stages of risk management maturity, as depicted on the horizontal axis of the Internal Audit 2012 Value Model (Figure 2). The ability of internal audit to provide value stemming from the delivery of risk assurance depends largely on the maturity of a company's risk management organization and structure—the more mature and developed the structure, the more effective internal audit can be in delivering a risk-centric value proposition.

Stage 1: Internal control

At the first stage of risk management maturity, management is focused on providing assurance that selected key internal controls, typically those in higher-risk areas, are functioning as designed. However, the organization probably has not embraced a formal internal control or risk management framework at this stage, and although it has designed controls, these controls are often not well documented.

When an organization is at Stage 1, its management has yet to formally conduct and document an enterprise-wide risk assessment. In fact, its internal audit function may be the only organizational entity to have developed a comprehensive risk assessment. At this stage, the testing and monitoring of internal controls is often viewed primarily as an audit activity as opposed to a management activity. In addition, controls are largely people-dependent, with little or no formal training or communication of control activities taking place.

Stage 2: Sarbanes-Oxley compliance

The Sarbanes-Oxley Act of 2002 requires companies to adopt a common definition of internal control, such as the one promulgated by COSO, and to formally document their internal control activities. The Act also provides the impetus for many companies to formalize their approach to the management, monitoring, and testing of internal controls.

Initially, most companies dedicated significant resources to Sarbanes-Oxley compliance. This changed over time as organizations streamlined their compliance processes and improved their abilities to document and monitor internal control efficiency and effectiveness.

At Stage 2, the focus of internal controls has broadened beyond that of an audit activity to embrace management ownership of controls. In addition, some corporate management groups have begun to develop formal enterprise-wide risk assessments to strengthen their Sarbanes-Oxley compliance efforts.

Stage 3: Informal risk management

At the third stage of risk management maturity, management develops its own enterprise-wide risk assessment and seeks to define ERM for the organization. Management may be setting risk appetites, developing risk management processes, and reporting to the board on its risk management activities. The organization likely has standardized controls, with periodic testing and reporting of results, and it may be employing automated tools to support enterprise-wide reporting of risk and control activities.

Stage 4: Functional enterprise-wide risk management

At the final stage of risk management maturity, management defines and implements formal risk management processes. Management has adopted a formal definition for ERM, such as the COSO enterprise risk management framework, and it has conducted a comprehensive, enterprise-wide risk assessment. Management also sets risk appetites for the organization, manages and monitors responses to risk management issues, and provides assurance to the board as to the effectiveness of the organization's risk management processes.

A Stage 4 organization might have a chief risk officer. It might have real-time management and monitoring of risks and control activities. And it might have automated tools in place to support control activities and allow the organization to make rapid changes to those activities in anticipation of emerging risks.

CAE views on strengthening internal audit's value proposition

Advice from audit leaders interviewed for this report:

- Be relevant, not redundant.
- Partner with other risk and control functions within the company.
- Stay in front of the business rather than lagging behind it.
- Focus on start-ups and other future-oriented activities that have relatively few core controls and thus carry higher risks.
- Focus on new issues and types of audits, such as post-acquisition reviews.
- Determine what audits to perform to strengthen corporate objectives; ensure that management has developed effective processes for managing risk.
- Use the COSO ERM model to improve the ability of internal audit to understand and manage risks.
- Take a flexible approach to the work: do not be too constrained by the annual plan; ensure there is flexibility and sufficient unallocated time to address developing issues.

As organizations enhance their risk management activities, they move from left to right along the horizontal axis of the Internal Audit 2012 Value Model. It is not known how many organizations will eventually have fully functional enterprise-wide risk management systems, and will thus attain the highest level of risk management maturity. However, the results of our survey and interviews indicate that numerous organizations across a range of industries have begun to strengthen their enterprise risk management (ERM) capabilities. Risk management discussions at these organizations frequently involve internal audit leaders as well as audit committee representation.

In an environment characterized by a heightened focus on risk management, it is imperative that the risk management initiatives of internal audit functions match those of management. When they do, internal auditors are able to strengthen their focus on risk assurance and thus move up the vertical axis of the Internal Audit 2012 Value Model to demonstrate more value. Some proactive internal audit groups have already taken the lead in the area of risk, helping senior executives refine corporate risk practices while ensuring that internal audit's approach to risk management is in synch with that of top management.

For internal audit functions, the proactive path to providing greater value requires that internal audit evolve in a manner that complements the company's approach to governance, risk, and compliance oversight. Failure to do so could detract from the growing levels of respect being accorded internal audit by senior management and audit committees.

But first, internal audit needs to determine how best to contribute to the organization's ability to improve risk management activities. With a risk-centric mindset, internal audit may be asked to play a leadership role or serve as catalyst and facilitator, coordinating with members of other risk and control functions to ensure that organizational risks are appropriately controlled and managed.

Our 2012 research shows that leading chief audit executives (CAEs) increasingly expect audit committees and senior management groups to pressure internal audit functions to step up their performance in risk management or face being absorbed or pushed aside by other, potentially more effective, players in the risk management discipline. When discussing these possibilities, a number of CAEs interviewed for this report said they could foresee potential consolidations among various corporate functions currently performing internal audit, risk and control management, and compliance activities. How internal audit would fare with such consolidations is unclear. What is clear is that it must move quickly to change and redefine its fundamental value proposition in order to remain a strategic contributor to the organization.

If internal audit is to remain vital and strong, its fundamental value proposition must shift.

Trends

Our study suggests that the continuing migration toward a more risk-centric approach to internal audit is driven by five key trends, which are all likely to re-shape internal audit by 2012:

1. Globalization
2. Changing internal audit roles
3. Changes in risk management
4. Talent and organizational issues
5. Technological advancement

Results of the study reflect an expectation among participants that in the coming years, globalization, talent, and technology will have a particularly significant impact on the internal audit profession. Yet all five trends appear to be closely related: increased globalization and advances in technology will have a direct impact on talent, and there are notable ties between what participants had to say about the role of internal audit and the changes they expect to see in organizational approaches to risk management.

Leading CAEs already have developed strategic platforms to capitalize on opportunities and manage risks associated with globalization, technological advancement, and other organizational issues. This report reflects the risk-centered, future-oriented thinking of these leading CAEs, as well as our experience and continued study of the profession.

1. Globalization

The pursuit of international growth via new or expanded markets and the hunt for lower-cost suppliers abroad create a unique set of issues for multinationals, according to our study. Among the most common:

- The economies of Brazil, Russia, India, and China (known collectively as BRIC) are reordering world markets. China and India in particular will be even stronger economic centers by 2012.
- The globalization of securities markets and the internationalization of accounting standards are forcing companies to rethink a U.S.-centric approach to business and accounting. And in the United States, the internationalization of accounting standards may lead to a change in the language of accounting.
- The growth of outsourcing and an upsurge in the offshoring of services and manufacturing have made global supply chains more interconnected and more vulnerable and have increased financial market volatility.

Our research identified globalization[1] as a significant and growing trend impacting internal audit today and in the future. As organizations expand to take advantage of global markets and supply chains, internal audit faces a burgeoning need for its services. A majority of survey respondents expect globalization, outsourcing, and offshoring to have a significant impact on internal audit roles and responsibilities over the next five years.

- Nearly 75 percent expect globalization to have a moderate to very strong impact on the roles and responsibilities of internal audit, with 43 percent anticipating a strong or very strong impact and 31 percent projecting a moderate impact.
- Seventy-seven percent believe that the wide-scale outsourcing of corporate or enterprise-wide functions or operations will have a moderate to very strong impact on internal audit roles and responsibilities. On the topic of outsourcing in general (which, in the survey, addressed a broad range of services including but not limited to internal audit), 40 percent of respondents anticipate a strong or very strong impact, while 37 percent project the impact to be moderate.
- Nearly 7 in 10 respondents expect offshoring of corporate or enterprise functions or operations to have a moderate to very strong impact on internal audit in the near future, with 37 percent anticipating a strong to very strong impact and 32 percent projecting a moderate impact.

[1] *Globalization* is an umbrella term that refers to increasing global connectivity, integration, and interdependence in the economic, social, technological, cultural, political, and ecological spheres. Outsourcing and offshoring are key elements of globalization that involves cross-border transactions, the movement of capital, and the integration of financial markets.

When asked where internal audit responsibilities are likely to increase the most over the next five years, 75 percent of respondents chose auditing of outsourced or offshored operations, with 15 percent indicating these responsibilities would increase “much more” and 60 percent saying “somewhat more.” In addition, 39 percent projected likely increases in the number of internal audit resources devoted to globalization.

On balance, most of the CAEs we interviewed agree that globalization is a significant trend that will gain further momentum over the next five years. “Taking advantage of globalization is all about speed and fluidity,” said the audit leader of a global chemical company. “Offshoring [to relocate business processes] is easier to do than ever; joint ventures are happening constantly, and change is a constant. To deal with these challenges, companies must develop governance processes that are capable of responding to change.”

Experienced global players share concerns

While members of the survey population see internal audit responsibilities expanding as a result of globalization, CAEs from seasoned global companies pointed out that risks associated with the pursuit of global markets could be difficult for internal auditors to identify and assess. “Internal audit is vastly unprepared for the risks of global expansion,” said a media company CAE. A number of other CAEs added that inexperienced internal audit groups might lack the insight needed to adequately support the global aspirations of their organizations.

Audit leaders interviewed for this report also expressed concern about a range of other topics, including the following:

- They expect compliance demands to grow in both amount and complexity, with one CAE noting that non-U.S. regulators and regulations, in general, would increase in importance. Compliance with the Foreign Corrupt Practices Act (FCPA) is a concern, as are political risks and risks to reputation borne by organizations active in international markets.
- Cultural issues ranked as an important topic, evidenced by CAE awareness of the need to be sensitive to how people think and act in China, India, and other key trading-partner areas.

- The CAE of a global defense and aerospace company that buys parts from around the world said that vendor quality and standards are of primary concern to all global companies. She said that when she assesses key risks during the annual internal audit planning process at her company, she can clearly identify potential risks in terms of the quality of components and parts for the equipment manufactured by her company. At the same time, she finds it challenging to identify and execute the audits needed to determine how effectively such risks are mitigated.

"The promise of globalization may not be all that great," said the CAE of a global systems integrator. Echoing this point, the audit leader of a large global insurance company believes offshoring and outsourcing could actually decrease if companies failed to achieve expected returns on investment. The CAE of a financial services company added that there would be less interest in offshoring when labor costs were more balanced. "It is the larger organizations that are considering offshoring," he stated. "In the short run, there may be cost advantages. But over time, companies will notice that the cost of labor will equalize."

Organizing global internal audit operations

As companies expand globally, internal audit functions need to determine whether to provide audit coverage from a central location or from a satellite or branch operation aligned geographically with the expanded business operations. Survey respondents generally expect that the internal audit organizational structures for U.S. companies will remain U.S.-centric, albeit with a growing global dimension.

When asked to describe the likely predominant structure for internal audit groups within five years, 54 percent of our study respondents indicated a core internal audit function based in the organization's home country, with some of the internal audit function existing internationally. Another 37 percent expect the predominant model to be one central internal audit function based in the organization's home country. Only a small minority, 8 percent, expects to see most internal audit staff operating internationally.

Interviewees also provided insights about global staffing and organizational issues, and about how to approach the auditing process itself when operating outside the home country. A number of CAEs discussed the importance of maintaining a physical presence in foreign locations and described how they hire internal audit professionals abroad to supplement their ranks. For example, the CAE of a global retailer said she is weighing the pros and cons of establishing a permanent internal audit presence in China following her company's acquisition of a major subsidiary in that country. Another audit leader, the CAE of a leading systems integrator, said his company has a "hub and spoke" organizational model for its global internal audit operations, with the corporate hub in North America and spokes in Asia, Australia, Europe, and the United Kingdom. To improve its ability to do business in China, the company recently opened an office in Singapore, where the internal audit staff understands English, GAAP accounting, the nuances of Chinese culture, and the primary language of China, Mandarin. As the company expands internationally, its internal audit activities will continue to shift to the "spoke" countries.

The more that companies grow internationally, the more they need to identify and develop potential leaders, advised the audit leader of a global consumer products company. "Ideally," he said, "internal audit will train high-potential employees in key areas such as business controls, risk management, and IT audit—and then send them back into the field."

Perspective: Addressing political risk[2]

Both our 2012 research and our experience indicate that political risk in global markets warrants the close attention of internal auditors as well as audit committees and senior management. At a time when risk-based auditing has become a driving force within business circles, political risk considerations should be considered during internal audit risk assessments when the company has global operations.

When it comes to making key decisions about global investments, political considerations can be just as important as economic ones. Elements that make emerging markets so attractive—including pent-up demand in a country opening itself up to foreign trade, investment, and cultural influence—also contribute to potential economic instability in those markets.

Companies operating abroad in unfamiliar political environments can be exposed to new types of risks and complexities that threaten business performance and mask new opportunities. Such risks and complexities range from regulatory and compliance changes lowering barriers to market entry, to practices that violate the Foreign Corrupt Practices Act (FCPA). If a company has a presence in foreign markets, or if it is thinking about making major investments in infrastructure or operations abroad, it needs timely, accurate, and objective assessments of the political environment. Economic analysis alone fails to tell the whole story, particularly in situations where statistical data is either difficult to collect or subject to manipulation for policy interests. To base global investment decisions solely on economic data without understanding the political context is risky business. Given the scope of such challenges, executives of global companies need to know certain things about political risk: the best ways to assess it, how to factor it into investment decisions, and how to use the knowledge gained to help improve global business performance. As companies become more familiar with global expansion challenges, they are more likely to make political risk a key component of enterprise-wide risk assessments. They can also be expected to assess political risk on a more formalized basis.

How can chief audit executives help? They and their internal audit groups need a solid grasp of how political factors affect corporate governance and regulatory compliance as well as operating performance and bottom-line earnings. By monitoring organizational exposures to political risk, internal audit groups will help strengthen corporate risk management efforts.

[2] This material includes excerpts from "Assessing Political Risk," an article by Richard Chambers of PricewaterhouseCoopers and Rachel Jacobs of the McGraw-Hill Companies, which appear in the August 2007 issue of *Internal Auditor*, published by The Institute of Internal Auditors, Inc., www.theiia.org. The excerpts are being used with permission from the IIA.

Political risk management requires a systematic framework to evaluate the impact of individual risks on stability and to ensure that political risk information is available when needed to enhance corporate decision-making. Internal audit can implement a formal program to assess and monitor political risk across business lines, including procedures to gather, interpret, and evaluate political information from multiple sources.

If management's existing enterprise-wide risk assessment includes political risk, internal audit should consider the impact of this assessment on the internal audit plan. Conversely, if political risk has not been addressed in management's enterprise-wide risk assessment, then internal audit should consider including it within its own auditing and risk-assessment activities. Some techniques for this include the following:

- In the risk-assessment process, internal auditors should gather objective information about political risks, factor the information into risk-based audit planning activities, and communicate findings to the audit committee and management.
- For a company's new or existing investments or operations, and for sales or supply chains in international markets, it is wise to monitor rapid economic growth, instability or deterioration, increasing levels of foreign investment, and significant changes in governmental leadership.
- Potential changes in regulations or trade agreements should also be addressed, as should any indications of social unrest or other looming security issues.

Another technique, a process known as political risk analysis (PRA), can help an organization:

- Make better and more timely decisions about international operations, protect existing global investments, improve business performance, and exit unstable markets.
- Anticipate business-risk implications of political change as well as identify both opportunities and risks stemming from political shifts and instability.
- Improve measurement using risk-adjusted evaluation of international performance.
- Create a comprehensive picture of both the risks and opportunities associated with global investment decisions.
- Take steps to mitigate risks, such as recruiting local partners or limiting R&D activities in countries where intellectual property is not well protected.

Bottom line: Until political risk analysis is firmly embedded in a company's management activities and internal audit can assess the overall effectiveness of these PRA activities, political risk should be considered during an annual risk assessment for organizations with global operations.

Perspective: Focusing on the Foreign Corrupt Practices Act

Without question, potential corruption poses serious risks that internal audit and other corporate watchdog groups need to examine on a proactive, systematic basis. Although the FCPA was enacted in 1977, there has been a surge in FCPA enforcement activity against U.S.-based companies in recent years. Factors behind this surge include an increase in globalization, elevated whistleblower activity, growing cooperation among international government regulators in anticorruption, and a dramatic increase in the scrutiny of emerging markets.

In addition to being subject to the FCPA, U.S. companies are now covered by the United Nations Convention Against Corruption (UNCAC), the first anticorruption agreement to be applied on a global level. Parties to UNCAC, including the United States, agree to criminalize corrupt conduct, to actively deter corruption, to cooperate internationally on law enforcement, and to take steps to facilitate international efforts to recover assets. The United States, which approved the UN measure in late 2006, is actively promoting UNCAC as the cornerstone for regional multilateral anticorruption activities.

The crackdown on questionable business practices under both the FCPA and the UNCAC is forcing many companies to implement complex mitigation measures, to develop more stringent internal guidelines, and to conduct costly investigations of their foreign operations. At this point, a substantial number of multinational companies are dealing with one or more allegations of FCPA violations or with ongoing FCPA investigations. What's more, it's not unusual for senior internal audit staff at major multinational corporations to spend a significant amount of time on FCPA investigations.

The core challenges faced by management and internal audit alike in assessing FCPA risks deal with identifying officials who might have received questionable payments from the company and the routes through which such payments were made. As previously mentioned, political risk analysis can help auditors develop roadmaps to link individuals and government-owned companies with a given entity. Areas of particularly high risk include governmental decision-making regarding pricing, reimbursements, and contracts with third-party agents. Political analysts can develop "power maps" to illustrate the linkages between government officials and private industry as well as the subsidiary relationships through which payments could be transmitted.

How to strengthen global FCPA compliance: a ten-step plan

1. **Evaluate the compliance requirements of the Foreign Corrupt Practices Act of 1977 and the UN Convention Against Corruption (UNCAC).** Determine their applicability to your company. For instance, many companies do not contract with foreign governments and are therefore outside the scope of the FCPA. At other companies, only certain subsidiaries deal with foreign governments.
2. **Ensure that corporate standards address FCPA compliance issues and establish minimum thresholds for compliance.** Update corporate documents, policies, and communications relating to anti-bribery and anticorruption activities, internal controls, payments to government officials, and other pertinent subjects. Develop a formal communications and certification plan covering online access, web-based training, and messages from senior management.
3. **Evaluate corporate policies to ensure that they cover high-risk activities.** Develop a set of global standards and basic expectations for processes and controls involving high-risk business activities, specifically regarding books and records requirements.
4. **Provide management training on FCPA compliance.** Promote compliance by educating local management on key tenets of the FCPA and UNCAC, regulatory communications, laws and corporate policies dealing with whistleblowers, and investigative activity by local regulatory agencies.
5. **Assess FCPA compliance and document processes and controls in select/higher-risk subsidiaries.** Address the Leverage Transparency International Corruption Index as well as anecdotal information. Conduct risk assessment by affiliate, produce detailed process maps for each high-risk business activity, and create recommendations for corrective action/remediation.
6. **Develop a global FCPA compliance implementation program.** Develop a formal, standard set of processes and model policies and procedures to be implemented locally. Create an implementation "tool kit" with recommended monitoring controls and internal reporting protocols.
7. **Conduct subsidiary pilot programs focused on testing the execution of the FCPA compliance implementation program locally.** Test and refine Step 6 deliverables.
8. **To support global rollout of the FCPA compliance implementation program, conduct global training on FCPA, company policies, the FCPA compliance implementation program, and the implementation tool kit.** Conduct webcasts and selective live meetings designed to train local management on FCPA, on company expectations for FCPA implementation, and on the tools necessary to promote implementation.
9. **Implement FCPA compliance program globally.** Develop target dates for subsidiary implementation of the FCPA compliance program.
10. **Perform post-implementation validation reviews at select subsidiaries (focusing on those that did not receive implementation assistance) to assess management's implementation of the FCPA compliance program.** Develop reports on the results of post-implementation reviews for each subsidiary. Include recommendations for improvement. Provide for ongoing FCPA compliance monitoring.

2. Changing internal audit roles

By 2012, strategic internal audit groups will be providing risk assurance as well as controls assurance as part of coordinated efforts to keep in step with corporate advances in risk and control processes. To cope with increased time pressures and competing priorities, internal auditors will devote more time to risk management, fraud, internal controls, and process flows.

Technology expected to have major impact on internal audit

Business trends expected to have the most impact on internal audit roles, responsibilities, and functions between now and 2012 are technology, new regulations, risk management, corporate governance, and ethics and compliance. Of these, technology is projected to have the greatest impact.

The table in Figure 3 reflects the percentage of respondents expecting a particular trend over the next five years to have either a strong or very strong impact on internal audit roles and responsibilities, or a moderate impact on internal audit functions. The last column combines total percentages by trend.

Figure 3: Trends impacting internal audit roles, responsibilities, and functions

Trend	Impact on role and responsibility Strong or very strong (%)	Impact on function Moderate (%)	Combined total: Impact on role and responsibility and Impact on function Moderate to very strong (%)
Technology	60	35	95
New regulations	51	37	88
Risk management	58	29	87
Corporate governance	58	26	84
Ethics and compliance	56	21	77

Technology, enterprise risk management, antifraud measures, and globalization predicted to boost internal audit responsibilities

Between now and 2012, technology, risk management, fraud prevention, and globalization are expected to produce significant increases in responsibility for internal audit functions, according to survey respondents.

Continuous auditing or monitoring is the top factor predicted, with 90 percent of respondents anticipating that such activities will produce additional responsibilities for internal audit over the next five years. Of that percentage, 37 percent expect much more of an increase from continuous auditing and monitoring activities, while 53 percent predict somewhat more of an increase.

Auditing the enterprise risk management (ERM) process is the second-ranked factor, with a total of 77 percent of respondents projecting a boost from ERM activities. Nearly as many respondents see sharp increases ahead linked to globalization, with 75 percent foreseeing additional duties relating to the auditing of outsourced or offshored operations.

Fraud detection, fraud risk assessments, and fraud investigations—three key aspects of a comprehensive antifraud program—are also expected to generate significantly greater responsibilities for internal audit groups.

Other factors include auditing IT security, auditing executive compensation and disclosures, auditing operational efficiency and effectiveness, auditing or evaluating compliance with laws and regulations, and providing training and education to management and staff.

The table in Figure 4 shows leading responsibility factors and reflects the degree to which respondents expect a particular factor to generate either somewhat more or much more responsibility for internal audit.

Figure 4: Factors driving greatest projected increases in responsibility

Factor	Much more responsibility (%)	Somewhat more responsibility (%)	Combined total: Somewhat more to much more responsibility (%)
Continuous auditing or monitoring	37	53	90
Auditing the ERM process	15	62	77
Auditing outsourced or offshored operations	15	60	75
Fraud detection	13	53	66
Fraud risk assessments	8	58	66
Auditing executive compensation and disclosures	11	54	65
Auditing operational efficiency and effectiveness	6	58	64
Auditing IT security	11	44	55
Auditing or evaluating compliance with laws and regulations	6	46	52
Fraud investigations	7	37	44

Sarbanes-Oxley impact expected to plateau or decline

Respondents believe that internal audit responsibilities related to Sarbanes-Oxley will remain level or will decline over the next five years.

Evaluating compliance

With regard to evaluating overall compliance with the Act, 18 percent expect to have somewhat more responsibility than today, 61 percent expect neither more nor less responsibility, and 21 percent anticipate less responsibility than they have now. Overall, most respondents expect the level of evaluation responsibility to remain the same, but a growing number expect a decline.

Section 404 testing

We saw a leveling off and decline in projected responsibilities relating to Section 404 testing, with 7 percent of respondents expecting to spend more time on testing, 47 percent expecting to spend about the same amount of time, and 46 percent indicating less time.

Section 404 project management

Respondents projected leveling-out or declining responsibilities with regard to Section 404 project management, with 7 percent expecting to spend somewhat more time in this area, 56 percent expecting to spend about the same amount of time with project management, and 37 percent projecting less time.

Leaders share opinions on roles and value perception

Audit committees and senior management are placing greater pressure on internal audit to provide more clear-cut strategic value, according to the audit leader of a systems and technology company, who suggested that internal auditors can create such value by taking a risk-based approach to auditing based on ongoing risk assessments.

"The role of the chief audit executive is to bring relevant issues to the attention of both the audit committee and executive management in an objective, transparent manner," said the CAE of a global financial services company. Other interviewees expressed similar viewpoints, with one suggesting that internal auditors need to place a high priority on keeping audit committees informed. A financial services CAE warned that if chief stakeholders of internal audit believe an internal audit function does little more than test controls, that function is likely to experience a loss of stature and resources. CAE advice related to changing internal audit roles included the following:

- **Provide assurance over risk management:** The time is ripe, said a number of audit leaders, for internal audit to expand beyond controls assurance and into assurance over risk management. A large airline CAE told us that audit committees now ask internal audit groups to evaluate enterprise risk management process effectiveness in order to help audit committee members address their responsibilities. "In the future," noted another audit leader, "internal auditors should expect to be asked to check on those responsible for risk management in addition to monitoring risks."
- **Integrate IT audit:** Several interviewees talked about the need to incorporate IT audit within traditional audit programs. The CAE of a communications and entertainment company said he expects the lines separating IT and non-IT audits will continue to blur over the next five years, given the need to leverage the power of technology to enhance audit efficiency. Another CAE reported that his company provides IT training for internal auditors on a global basis.
- **Coordinate with related risk and control functions:** In a new risk management environment, interviewees said, internal audit needs to coordinate and cooperate with related risk and control functions in the organization. Advised one CAE, "Internal audit needs to figure out how to 'partner' with other related risk and control functions."

Perspective: The risk-centric mindset

In recent years, many internal audit groups have achieved unparalleled levels of success and respect. Although demands on internal audit have been extraordinarily high, rewards for strong performance have never been better.

As management groups continue to expand their risk and control responsibilities, it is not enough for internal audit merely to assess the effectiveness of financial and operational controls and to provide assurance on compliance with laws and regulations. Internal audit cannot expect to be a key player in risk management with such a limited approach.

For internal auditors who have not done so already, it is time to adopt a strong, risk-centric mindset and redefine IA's role and value proposition accordingly; to broaden IA's focus to include risk management as well as controls; and to determine how to harness and manage the power of data in order to audit better, faster, and at lower cost.

As we approach the strategic crossroads, internal auditors should focus on the following strategic initiatives:

- Embrace risk assurance as a primary objective.
- Expand assurance activities to cover overlooked areas of risk.
- Anticipate the needs of the audit committee and senior management.
- Identify emerging trends and bring them to the attention of key stakeholders.
- Strengthen risk coverage of technology, fraud, and strategy areas of high priority in which traditional internal audit groups typically lack confidence in their performance.
- Coordinate with other risk and control functions to ensure that risks are appropriately controlled and managed.

Legal and regulatory actions shape antifraud environment

Although antifraud roles vary in business today, top management generally owns the antifraud responsibility, the audit committee oversees antifraud efforts, and internal audit provides a critical line of defense against the threat of fraud by focusing on risk monitoring in addition to fraud prevention and detection. Ideally, risk assessments and fraud audits are part of internal audit's risk-monitoring efforts.

This overview of primary antifraud roles reflects a number of legal, regulatory, and standards-setting actions that have served to broaden the definition of fraud, expand antifraud responsibilities, and place greater emphasis on preventive and detective measures.

- Sarbanes-Oxley and corresponding regulatory changes raised the stakes for senior management and the board of directors, who must now view fraud and misconduct as a broad-based threat and address fraud issues in far greater detail. Sarbanes-Oxley requires management to evaluate and test its internal controls over financial reporting on an annual basis, a requirement that includes antifraud activities. Securities and Exchange Commission (SEC) rules implementing Section 404 of Sarbanes-Oxley refer explicitly to controls related to the prevention, identification, and detection of fraud. These regulations require corporate management to evaluate and test the design and operating effectiveness of antifraud controls on an annual basis.
- Auditing Standard No. 5 (AS5),[3] which was approved by the Securities and Exchange Commission in July of 2007, will enable management to use a top-down, risked-based approach to its evaluation of internal controls. It emphasizes both the need to audit high-risk areas such as the financial statement close process, and controls designed to prevent fraud perpetrated by management. At the same time, AS5 provides auditors with a range of alternatives for addressing lower-risk areas.
- For the most part, antifraud programs and controls need to meet each of the five key components of the COSO internal control framework—control environment, risk assessment, control activities, information and communications, and monitoring—to avoid finding a significant deficiency in internal controls or, worse, a material control weakness. Most companies and auditors in the United States use the COSO framework, authored by PricewaterhouseCoopers, to assert and audit the effectiveness of internal controls.

[3] On May 24, 2007, the Public Company Accounting Oversight Board (PCAOB) voted to adopt Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements, to replace its previous internal control auditing standard, Auditing Standard No. 2. AS5, which was approved by the SEC on July 25, 2007, applies to audits of all companies required by SEC rules to obtain an audit of internal control. The SEC said it expects AS5 will make Sarbanes-Oxley Section 404 audits and management evaluations more risk-based and scalable to company size and complexity.

3. Changes in risk management

Over the next five years, according to our study, internal auditors will be sharpening their focus on continuous auditing and assessment concepts in an effort to streamline and improve the audit process. As risk assessments and risk monitoring assume a more real-time dimension, audit timing will become more dynamic. Audits will be conducted on an as-needed basis, triggered more by changes to organizational risk profiles than by set plans or schedules dictated by traditional auditing practices.

In the ongoing drive for greater efficiency and effectiveness, internal auditors will leverage technology along with their own innate analytical abilities to pinpoint key risk indicators (KRIs) that can more effectively monitor risk conditions. Auditors will use KRIs to identify changes in organizational risk profiles in advance of breakdowns in internal control and will initiate audits in lower-risk areas when KRIs point to significant variances from expectations.

Throughout these pursuits, our experts warned, it is important that internal auditors keep in mind the need to provide timely risk and control assessments and to ensure that audit resources are directed toward areas of greatest or emerging risk.

Risk assessments growing in importance

More than half (51 percent) of our survey respondents expect that an audit planning process focusing on an annual risk assessment will be more important in 2012 than it is today. A total of 15 percent expect it to be far more important, while 36 percent believe it will be somewhat more important.

When we asked respondents to describe what they expect their internal audit planning processes to look like in 2012, we learned the following:[4]

- Nearly half (47 percent) expect to have an ongoing risk assessment conducted with an annual audit plan that is revised and updated throughout the year.
- Fourteen percent expect to see a single, comprehensive annual risk assessment that is used to develop an annual plan.
- Thirteen percent believe their organizations will be conducting an ongoing enterprise-wide risk assessment with an audit plan that leverages that assessment.
- Another 13 percent expect to employ continuous auditing or risk assessment methodologies without a formal audit plan as part of an ongoing continuous audit and risk assessment process.
- Eleven percent expect to be conducting a single, comprehensive annual risk assessment with a rolling audit plan.

[4] Due to rounding, these figures total 98 percent.

A broad spectrum of risks

Audit leaders contend with a broad spectrum of risks, according to our interviewees, who cited as examples risks relating to Sarbanes-Oxley compliance and breaches of information security.

Enterprise-wide risk management and fraud are also of particular concern. At one global airline, the audit committee looks to internal audit to tell them whether the company's ERM processes are working properly, according to the company's chief audit executive. Another CAE reported greater focus on ERM at his company than on Sarbanes-Oxley.

Several of our interviewees said their internal audit groups are increasingly asked to aid fraud investigations. One global software company has gone so far as to develop an investigative unit to examine potential high-risk fraud situations. At the same time, many of the CAEs we interviewed did not believe that internal auditors in general are well prepared to deal with fraud-related risks. "No one [at our company] is readily able to educate, find, and resolve fraud issues," said one CAE.

Threats to reputation are another key concern, interviewees told us. "There is greater likelihood of losing your job or your CEO from threats to your organization's reputation than from a negative business performance," said the audit leader of a global chemical company.

Internal audit's risk assessment and monitoring activities need to consider the risks associated with smaller, future-focused start-up activities, cautioned a CAE. Although these areas are usually not "material," they frequently have fewer controls and thus pose relatively higher risks.

In raising other pertinent issues, the CAE of a financial institution urged internal auditors to consider macro trends such as health and wellness, workforce issues, and product safety as they assess management's risk management practices. The audit leader of a large insurance company cautioned that internal audit's traditional skill sets and experience do not lend themselves to becoming more risk-based, noting that internal audit coverage of operational risks in particular are not well developed. Other CAEs mentioned the need for more strategic risk evaluations and for greater cooperation among functions within the organization. "Sarbanes-Oxley requirements, for example, are addressed by multiple compliance functions," said one audit leader. "There are a lot of questions about who owns and speaks on what risk, especially in reference to governance structures."

Pondering the future, the CAE of a U.S. airline advised internal audit functions to provide stakeholders systems-based dashboards displaying key risk indicators for finance, sales and marketing, IT, and fraud.

Perspective: Risk assessment and the audit cycle

To achieve greater audit efficiency and effectiveness, companies seek to streamline audit cycles and risk assessment procedures so they can analyze significant risks more frequently than current audit cycles typically allow.

With the traditional approach to internal audit, the audit cycle generally includes an annual risk assessment followed by a series of planning, auditing, and reporting activities spread out over a year-long period. Audit resources are assigned well in advance, and the audit schedule changes only when significant matters arise (often a fire-drill situation). Testing is normally conducted in accordance with the audit schedule established in the annual audit plan. Reports are issued only after an audit has been properly completed, reviewed, and approved, often by several layers of management.

Given the highly structured nature of these procedures, the traditional auditing process can be said to be more reactive than proactive. Once the annual risk assessment process is completed, auditing activities generally proceed according to plan, with new issues being addressed on an ad hoc basis only if time and resources permit. While it is not unusual for internal audit plans to be modified, such modifications tend to produce relatively minor changes to the annual plan.

Perspective: Beyond cyclical auditing

To remain relevant in 2012, internal auditors need to move beyond a static, cyclical audit approach and adopt a continuous, comprehensive approach to audit and risk assessment—one that optimizes the use of technology. The ability to identify and analyze emerging risks and trends, and to conduct audits on a more targeted basis in response to specific risk concerns, will be essential.

Future internal auditors will move away from a traditional approach to auditing centered on an annual audit plan and will operate within a faster, more flexible scheduling and planning model. By operating with a "rolling" audit plan, auditors should have enough unallocated time throughout the year to address emerging issues on an as-needed basis.

Many auditors believe that continuous auditing and assessment concepts can strengthen those processes. As our annual surveys of the internal audit profession reflect, these concepts are already in use at a high percentage of organizations with internal audit functions. However, current continuous auditing operations are often piecemeal and fall short of facilitating the type of strategic change required to satisfy stakeholder demands for more timely and continuous assurance and risk assessment.

Contrary to most perceptions, continuous auditing is seldom truly continuous and rarely done in real time. Nor is it a fully automated process, for the audit cycle can be accelerated using manual processes alone, without any elements of automation. Much of what is referred to as "continuous" auditing is, in fact, a blend of automated and manual processes applied on a more frequent basis than traditional auditing procedures.

Within internal auditing circles, continuous auditing is often viewed narrowly as a "silver bullet" (a single tool, software application, or technique designed to accelerate audit cycle times and build repetitive audit programs) or as a means to audit more transactions in a given population. Such a viewpoint typically leads to a focus on computer-assisted audit techniques (CAATs) and data extraction and analysis. Silver-bullet applications also tend to concentrate on either monitoring or auditing, and are often "bolted on" to an existing methodology—factors that limit the impact of an application on overall cycle times.

To date, the net effect of so-called silver bullet approaches to continuous auditing has been incremental change at a time when transformational change is needed.

Perspective: Leveraging the power of technology

Over the next five years, internal auditors will be able to draw on a variety of technologies to assist with data extraction and analysis, computer-assisted audit techniques (CAATs), KRI and control monitoring, audit reporting, and work flows. They will have the means to monitor access controls, observe the close process, or analyze important ratios and KRIs. They will be able to focus on KRIs to identify changes in organizational risk profiles well in advance of breakdowns in internal control. And they will be able to add an anticipatory element to audit reports by providing for the ongoing monitoring of significant risks.

When KRI analyses raise warning flags, auditors may initiate a targeted audit to investigate a particular risk or control area in greater detail. This provides the opportunity to combine interviews with data analysis to pinpoint risks, assess exposures, and develop tailored responses to specific risk concerns.

By conducting audits on a more targeted basis, internal auditors will be able to concentrate on higher-risk areas and increase the likelihood of identifying problems at an early stage. Targeted audits facilitated by technology allow internal auditors to achieve more effective coverage of lower-risk areas, deploy audit resources more effectively, and conduct random audits in search of likely areas of fraud. A targeted audit also helps produce more timely information about changes in risks and controls than can be achieved from the traditional audit cycle's more rigid schedules.

4. Talent and organizational issues

CAEs are clearly concerned about their ability to address strategic and business risks as well as risks relating to fraud and technology, according to our research. At a time of rising stakeholder expectations, CAEs consider a lack of capacity and capabilities to be their primary challenge.

Although traditional accounting and auditing skills are expected to remain highly important in 2012, these skills alone are unlikely to provide the types of risk monitoring and analysis needed for a risk-centric auditing environment. To operate effectively going forward, audit leaders must develop a mix of capabilities, competencies, and experience levels, survey participants said.

From a technical perspective, CAEs will need access to a critical mass of auditors who, on a collective basis, could access, assess, and analyze risk data as well as help prevent and detect fraud. CAE interviewees said consistently that the ability to conduct data analysis was an essential skill for the future. Talented audit professionals able to evaluate and test internal controls, audit and assess complex IT environments, and address both enterprise-wide risk and governance issues will be essential. Finally, internal audit will need people with the financial expertise to assess the adequacy of financial controls.

CAEs interviewed for this report also talked about a broader set of non-technical yet highly desirable characteristics for the internal auditors of tomorrow. They cited the need for personable, well-rounded professionals who could “think beyond the project” and who had the business knowledge and confidence to engage in substantive conversations with senior management, line-of-business executives, and even the audit committee. CAEs also stressed the need to achieve cultural diversity within their audit ranks to address the changing needs of an increasingly global marketplace.

Figure 5: Importance of skill sets by 2012

Total %	Category
89	Data mining and analysis
76	Risk assessment
72	Information technology
70	Risk management
69	Fraud detection
64	Information security
57	Analytical skills
56	Fraud investigation
53	Enterprise resource planning (ERP) systems
53	Project management
50	Knowledge management
50	Privacy
47	General business
45	Regulatory
44	Verbal communications
40	Six Sigma
40	Multi- or bilingual
38	Written communications
38	Financial accounting
23	Social responsibility

Technology hiring expected to soar

Nearly two thirds of our survey respondents expect the number of internal audit professionals to increase over the next five years, with a particular jump occurring in the technology area. Rating skill sets, respondents gave the highest priority to the areas of technology and risk management. At the same time, 22 percent of respondents believe that the number of professional staff will remain about the same, and 15 percent predict a decline in internal audit staff between now and 2012.

Asking where staff increases would likely occur, we found that technology and regulatory developments garnered the most nods. Fifty percent of respondents indicated technology; 42 percent said increases would be linked to regulatory developments; 39 percent said globalization; and 35 percent indicated risk management. In addition, 32 percent indicated corporate governance, ethics, and compliance, while 26 percent selected outsourcing and 21 percent chose offshoring.

Data mining/analysis and risk assessment predicted highest gainers in skill set importance

Data mining and analysis was the front runner when we asked survey respondents to indicate which skill sets they expected would be either far more important or somewhat more important than they are today—a finding that audit leaders may want to keep in mind when assessing future needs for internal audit skills and methodologies. CAE interviewees agreed, with some reporting that they had already hired non-auditors with data mining skills in an effort to enhance internal audit's ability to conduct more complex data analyses.

Figure 5 shows which skill sets rose to the top of our survey and how they ranked.[5]

[5] We asked respondents to indicate which skill sets they expected would be either far more important or somewhat more important than they are today. The percentages in Figure 5 are equal to the total respondents who indicated "far more important" or "somewhat more important" than today.

"We need people who have worked on the business side and who know the ins and outs of operating a business effectively," said the audit leader of a large financial services company. Both assurance and consulting competencies are critical, said the CAE of a global software provider, who added that it is becoming increasingly important to find people with integrated skills in finance and technology. "IT skills are a must, and the ability to conduct data analysis to test outliers is critical," said another CAE.

The audit leader of a systems integrator said a mix of "raw energy with experience" works best for him. His ideal staffing blend would include 40 percent experienced people who "know the business and may not be interested in travel," while the other 60 percent would be "fresh talent with natural energy who are eager to learn." With such a model, he believed he could develop a successful internal audit staff within six to nine months.

"Stronger communication skills are a must," said the CAE of a global airline. "Auditors need training in public speaking and written communications if they expect to deal effectively with executive management and audit committees." Another CAE stressed the need for more cultural and geographic diversity on global internal audit staffs, stating, "Such diversity presents unique opportunities to mix staff and cross-pollinate cultures across internal audit organizations."

Staffing shortfalls and talent competition predicted

With large numbers of baby boomers expected to retire over the next decade, CAE interviewees anticipate shortages of both middle managers and internal auditors having 8 to 10 years of experience. Rotational staffing models are on the rise, they said, while the career-auditor path continues to diminish in popularity. CAEs reported hiring more staff internally to leverage preexisting knowledge of their particular companies and the markets they serve.

According to the CAE of a global software company, the supply of traditional internal audit skill sets is much smaller than marketplace demand, suggesting that competition for well-qualified internal audit talent extends beyond the ranks of IT, finance, and risk management. The same audit leader also reported difficulty in attracting talent because of what he described as a "significant increase in salary levels at Big Four accounting firms."

Similar comments were made by the audit leader of a global media and entertainment company, who said public accounting firms promote staff at a much faster rate than does industry. “A talented person could be a manager within five years at an accounting firm [in the United States], while it might take twice that long to be promoted to manager in industry,” he said. Citing such pay differentials, he surmised that it might be more advantageous for industry to hire college graduates than people from major accounting firms.

Maybe so, agreed the chief audit executive of a global insurance company, but he cautioned that while new hires direct from school might come with sought-after IT skills, they probably lack ideal levels of business knowledge and expertise. Another CAE, the audit leader for a large beverage company, said he used to hire about 90 percent of his workforce from public accounting firms and from outside the company. Now, with the help of a rotational staffing model, his department has reduced its level of external hiring to about 60 percent. At another company, a communications and entertainment concern, the internal audit department employs a staggered rotational model to help preserve its knowledge base. According to the model, the longer an individual remains in the internal audit department, the higher that person ranks in the department.

CAEs noted that building staff and retaining talent, even when they are part of a rotational model, puts a premium on career development and planning. To attract talent, interviewees said, internal audit needs to be viewed as a function that offers talented people multiple opportunities for development as well as varied experiences. The CAE from a financial services organization reported urging her staff to consider the following questions when exploring career opportunities:

- What is my career direction?
- What is my Achilles’ heel (point of vulnerability)?
- Outside of internal audit, on whose radar screens do I want to appear?

Organizational considerations

A majority of survey respondents (64 percent) foresee an increase in the number of internal audit functions reporting administratively to the CEO rather than the CFO, a common benchmark for the relative independence of an internal audit group. Of note, the same percentage of respondents predicted that the organizational stature of chief audit executives would be enhanced by 2012.

Respondents were also asked to describe the types of internal audit organizational structures they would expect to find in five years. Fifty-four percent predict a core internal audit function based in the home country with some of the function existing internationally. Another 37 percent expect to see one central function based in an organization's home country, while 8 percent foresee a core internal audit function based in an organization's home country with most of the function operating internationally.

A number of CAEs spoke positively about integrating traditional corporate auditing operations with those of IT audit. One chief audit executive declared IT and other specialized skills to be an essential complement to traditional auditing skills. Another cited the need for internal audit to gain an understanding of actual IT risks, suggesting that integration would achieve that objective. The audit leader of a financial services company said IT coverage should be embedded in lines of business as well as being available in a common function.

Taking an opposing viewpoint was the CAE of a global insurer, who said there would continue to be a divide between IT audit and the rest of the audit world because of the specialized skills involved.

Flexible scheduling was a subject that drew conflicting viewpoints from our CAE interviewees. The audit director for a technology and outsourcing company said simply, "Working from home will not work. Your staff has to bond with each other to be able to work together and grow. And new members of your staff need constant coaching to make them truly successful." Another CAE acknowledged that he couldn't see the flexible-schedule, work-from-home approach working for his staff because, he said, the model is inherently difficult to manage.

Other chief audit executives are upbeat about the potential for flexible working arrangements in the world of internal audit. "A flexible workplace and work schedule is essential in the future," said the CAE of a large insurer, who felt that video conferencing, in particular, could reduce travel time for internal auditors and help improve the work/life balance. His belief was that internal audit functions are more than ready to try flexible approaches to service delivery and, in fact, would do well to help facilitate such a change within their organizations.

Perspective: Talent and organizational issues

Internal audit groups need people who are strong in both data extraction and analysis to evaluate key risk indicators (KRIs) and compare them with industry norms. Risk analysts need to understand risk factors and related control implications in order to provide more timely risk and control assurances and update organizational risk profiles. Risk analysts also need the skill sets and training to analyze a business process and determine which controls, if any, are effective or necessary and which can be removed with little or no negative impact.

By building a strong core of risk analysts within the group, internal audit leaders create the capability for their staff to monitor an established set of KRIs for primary risk concerns. In addition, many organizations find it helpful to develop teams of specialists, including risk analysts, to focus on fraud and other areas of significant risk.

To excel at business analysis and specialized auditing, risk analysts need solid backgrounds in audit, data analysis, and research, as well as the ability to interview others well. They also need a deep understanding of their company and of the industry or industries that company serves, and a thorough grounding in the analytics they will use to monitor risks and controls across the organization. In addition, risk analysts should have sufficient industry knowledge to identify industry trends (and the risks associated with these trends), as well as the confidence and communication skills to discuss these trends and perceived risks with management.

To put together an effective team of risk analysts, internal audit leaders need to first determine the probable scope of risk analyst activities and then identify the skills needed to perform them. For example, risk analysts might spend 80 percent of their time analyzing business risks and 20 percent conducting targeted audits. They might gather intelligence in a variety of ways—from audits and data analysis to meetings with business-unit management or experts in IT or compliance. In addition, they might look at new and emerging risks stemming from acquisitions, changes in personnel, or operations.

Roles associated with fraud prevention and detection

Given the spate of corporate scandals in recent years, fraud and misconduct have evolved into mainstream risks. Both regulators and investors are demanding proactive antifraud programs characterized by a strong focus on the prevention and timely detection of fraud.

To conduct an effective antifraud effort, an internal audit department ideally needs a broad range of specialized skills, knowledge, and expertise, including:

- Solid understanding of measures intended to prevent and detect fraud
- Awareness of financial fraud schemes and scenarios and knowledge of forensic investigations
- The ability to detect financial statement fraud, which requires a firm understanding of financial reporting standards

Every member of an internal audit staff needs to have some level of fraud training, even if the department retains specialized resources to target fraud. Such training should address common fraud schemes and scenarios and provide the grounding needed for an internal auditor to assess fraud risk and identify fraud indicators. In particular, internal auditors need to be aware of potential schemes and scenarios affecting the industries and markets in which their organizations do business, and they need to be able to identify signs of these schemes.

For many internal audit functions, these skill sets may be relatively new, for little emphasis has been placed on fraud prevention and detection until recently. Running investigations into "what happened" differs substantially from performing fraud risk assessments, testing antifraud control activities, and conducting fraud audits. Yet, simply hiring an investigator or former law enforcement agent doesn't provide all of the necessary skills and expertise.

To strengthen a company's antifraud effort, internal audit leaders should consider forming a dedicated unit to focus on the prevention, detection, investigation, and remediation of fraud and issues stemming from forensic investigations. Alternatively, IA leaders may gain access to such capabilities through a co-sourcing relationship.

Tactics to address a talent shortage

1. **Conduct a gap analysis.** To determine resource needs, internal audit leaders first need to compare the current state of their internal audit functions with where they would like them to be. With a gap analysis of the current and future states, they can determine what changes need to be made to processes, skill sets, systems, and technologies in order to achieve internal audit's objectives. Once resource gaps are pinpointed, IA leaders can determine the steps needed to address these gaps. They might, for example, decide to increase risk analyst capabilities. They might also seek to develop a rapid-response team of auditors and analysts who could quickly conduct targeted audits or address situations in which key risk or performance indicators have exceeded acceptable values.
2. **Explore both internal and external sources for talent.** To strengthen capabilities in critical areas such as risk analysis, fraud detection, and technology, IA leaders should consider the use of capacity multipliers, such as strategic co-sourcing, to acquire needed skills. Tapping third-party internal audit service providers will gain them access to particular skill sets, expand geographic coverage, and provide the flexibility needed to deliver a responsive audit plan. Consider guest auditor programs to recruit subject-matter experts (SMEs) from within the company to conduct specific audits leveraging SME areas of expertise. Such programs can serve as an excellent means of auditioning and/or recruiting individuals who demonstrate a strong aptitude for internal audit.
3. **Adopt a rotational staffing model.** Rotational staffing has moved well beyond best-practice status to become the prevalent staffing model for large corporate internal audit groups. With leading companies relying on internal audit as a major source of talent for lines of business, corporate internal audit groups are turning to rotational staffing models to recruit staff from within and outside their companies. Such models provide internal audit with attractive career paths for recruiting purposes, and the professional experiences offered by internal audit are highly valued by other corporate functions. Typically, recruits are offered career opportunities in company business units after a two- to three-year rotation within internal audit.

5. Technological advancement

Our survey respondents and interviewees clearly appreciate the potential value and likely impact of technology. Most respondents expect technology to have a significant impact on internal audit in the years ahead, and 100 percent predict that their use of technology will increase over the next five years.

Despite the high regard for technology among participants, our study suggests that optimizing the potential of technology would require different skill sets for internal auditors, more sophisticated tools and applications, and a move beyond traditional internal audit methodologies.

Technology's anticipated impact on the profession

Survey respondents expect technology to impact business in general and their own ability to strengthen the internal audit process in particular. Not surprisingly, survey participants predict that technology will affect internal audit roles and responsibilities more than any other business trend.

Over the next five years, 95 percent of respondents expect technology to have a significant impact on internal audit responsibilities, with 60 percent anticipating the impact to be either strong or very strong. In addition, all of our survey respondents predict that their use of technology will increase over current levels, with 46 percent expecting the increase to be dramatic and 43 percent projecting a moderate increase.

Increased technology risks seen

A strong majority (79 percent) believes technology risks will pose a higher or significantly higher degree of risk to the organization by 2012. How internal audit will organize to address this risk is variable:

A slight majority (57 percent) expects to maintain a separate IT audit group to support audit teams as they address technology risks. By comparison, 26 percent expect internal audit to maintain a separate IT audit group within internal audit to address technology risks, and 14 percent expect to embed auditors with IT audit skills within internal audit rather than within a separate IT audit group.

To address technology risks and the need for IT audit resources, survey respondents intend to employ a variety of infrastructure, human resources, and organizational strategies. These range from acquiring more sophisticated technology tools to embedding auditors with IT audit skills into a core internal audit function while maintaining a separate IT audit group to help address technology risks. The table in Figure 6 ranks strategies in the order respondents felt those strategies were most likely to be used. Of note, respondents expect CobiT to remain the most commonly used IT controls framework over the next five years.

Figure 6: Strategies for addressing technology risks and IT resource needs

Projected usage (%)	Strategy to address HR & organizational needs in IT audit
76	Increase the core skill level of the general internal audit staff for understanding and auditing technology risks
68	Acquire more sophisticated technology tools to address technology risks
60	Increase the use of third-party experts
57	Embed some auditors with IT audit skills in the larger internal audit function while maintaining a separate IT audit group to support audit teams in addressing technology risks
54	Deploy higher-level/more experienced IT auditors
49	Increase the number of IT auditors with relevant certifications
47	Increase the percentage of total staff who are IT auditors
37	Deploy technology professionals who are not auditors
26	Maintain a separate IT audit group within internal audit to address technology risks
14	Embed auditors with IT audit skill sets within larger internal audit function without maintaining a separate IT audit group to address technology risks

When it comes to skills and capabilities, respondents anticipate that six IT skills/capabilities will grow in importance between now and 2012. These six are listed here, with each skill/capability followed by the percentage of respondents who believe that it will be somewhat or far more important in 2012:

- Privacy-related risks (60 percent)
- Offshored technology operations (60 percent)
- Automated controls (60 percent)
- ERP systems (53 percent)
- Network penetration (51 percent)
- Data warehouse controls (50 percent)

Increased importance placed on continuous monitoring, data analysis, and fraud-detection technologies

When we asked survey respondents to project the relative importance of specific technologies related to internal audit over the next five years, nearly 9 in 10 rated continuous monitoring and auditing software applications as most important, with data extraction and analysis, fraud detection, and risk analysis software following close behind. In addition, respondents predict a sharp surge in the importance of continuous monitoring and fraud detection when compared with current usage patterns. Figure 7 shows the differences between today's use of technology and respondents' predictions for 2012.

Figure 7: Changes in importance of internal audit technologies

Current usage (%)	Technological application	Projected usage by 2012 (%)
37	Continuous monitoring/auditing	89
94	Data extraction and analysis	83
25	Fraud detection and prevention	81
29	Risk analysis/management	71
33	Knowledge management/best-practices databases	67
13	Predictive modeling tools and capabilities	60
57	Network security assessment	57

Increased responsibilities predicted from continuous auditing and monitoring, fraud prevention, and auditing IT security

In our study, we sought to predict which aspects of technology were most likely to create an increase in internal audit responsibilities over the next five years. Ranked first is continuous auditing or monitoring, with 90 percent of our survey respondents projecting an increase in responsibilities relating to such applications by the year 2012. Of this total, 37 percent of respondents anticipate much more of an increase from continuous auditing and monitoring activities. Activities relating to fraud detection and auditing IT security are also expected to generate significantly more responsibility for internal audit over the next five years.

Nearly half (49 percent) of our respondents expect continuous auditing to be fully operational at their organizations by 2012, while another 35 percent anticipate that continuous auditing will be a work in progress but not fully developed by then. Another 10 percent of respondents expect that continuous auditing will be in various stages of planning and development.

Of those respondents who expect their continuous auditing operations to be fully implemented within five years, 64 percent expect their operations to be largely automated, while 32 percent foresee employing both manual and automated processes.

Respondents were asked to project the primary focus of their continuous auditing operations in 2012. A quarter of them expect their focus to be on monitoring key performance indicators (KPIs) to identify deteriorating business activities. Another 24 percent expect to focus on monitoring risk attributes to identify changes in risk profiles. Searching for fraud and control deficiencies also ranked high.

Although 2012 survey respondents appeared bullish about the prospects for continuous auditing and monitoring, opinions on the subject varied among our interviewees. One CAE told us he does not think continuous auditing exists—period. His belief, he said, is that every time internal audit identifies something that should be continuously monitored, management can or should assume the responsibility. Another CAE said he believed continuous monitoring was a concept that needed to be embraced by management, but not by internal audit. Still another CAE said he avoids using the word *continuous* to describe his company's auditing operations because, he said, none of [his company's] auditing activities are really continuous. He believes that the term builds unrealistic expectations in the eyes of management.

On the plus side, a number of audit leaders spoke positively about the prospects for continuous auditing and monitoring activities: “Whether it’s called continuous monitoring or data mining, technology enables us to do a better job of extracting data and auditing more effectively,” said a global airline CAE. Another CAE, the audit leader of a global defense contractor, views data mining and continuous monitoring as the enterprise risk management of the future, suggesting that both management and internal audit would play key roles in the advancement of these activities as companies achieved further integration of their IT infrastructures. The CAE of a global insurance company said continuous auditing is a must for the future of internal audit as part of the general movement toward more extensive testing of all transactions.

Introduction of the topic “technology as a trend” led to vigorous discussion among study participants. In the words of one CAE interviewed for this report, “Stop talking about technology. Instead, talk about the need to do large-scale data analysis and data mining.” Another CAE advised his fellow internal auditors to use technology to monitor what is occurring in the business and to tell the audit committee and senior management what did happen as opposed to what might happen.

A seven-step plan for continuous auditing and assessment

Internal audit groups could benefit from a continuous approach to auditing, assessment, and reporting. To optimize the potential benefit, we recommend the following seven-step approach:

1. Assess risk assessment needs and specifications.
2. Inventory technology applications already available within the company.
3. Identify KRIs to track and check their viability.
4. Explore how to track target KRIs by utilizing the multiple legacy systems most organizations have in place.
5. Reach out to others within the organization to determine if they are trying to obtain similar information, possibly for use as KRIs. If so, consider how best to leverage collective efforts, possibly working together on a common platform.
6. Determine how vendors could help internal audit calculate, integrate, and present target KRIs to analysts for review.
7. Consider risk dashboards and other options for presenting KRIs to the board and management for review.

Perspective: Internal audit's use of technology for a continuous approach to auditing, assessment, and reporting

Technology can be applied to a range of audit activities, from planning, testing, and risk assessment to data analysis and visual reporting. Given that technological applications tend to have a relatively narrow focus (and are thus not silver-bullet solutions), internal auditors typically employ multiple applications in order to address the broad scope of their activities. For example, some applications will help audit segregation of duties across the enterprise, while others will address reporting work flows.

Companies now combine continuous auditing and assessment concepts with technological applications to improve assurance quality, enhance audit management and testing, and increase the timeliness and relevance of their internal auditing operations. They apply technology-enabled risk analysis to accelerate the audit process, assess emerging trends, report "outliers," and analyze entire populations of data rather than samples alone. Companies now leverage technology to extract data and capture knowledge relating to business risks and controls. They increase efficiency by combining standard computer-assisted audit techniques with manual procedures and inquiries performed at regular intervals. In these pursuits, auditors must always be wary of crossing the fine line separating the roles of auditor and management.

Once the audit risk analysis concept picks up steam, more and more internal auditors will use technology to identify and track key risk indicators (KRIs) and facilitate the real-time monitoring of controls. In addition, technology has the potential to strengthen the presentation of audit reporting. For instance, directors and executives alike would benefit from visual portrayals of KRIs as well as from easy-to-grasp charts showing the nature and scope of organizational risks. These areas deserve high priority as internal audit leaders explore ways to maximize the value of technology to their departments and organizations.

We believe internal audit must be proactive and redefine its value.

Imperatives for internal audit success

In working with dozens of high-performing internal audit functions around the globe, we have observed that such organizations share two key attributes: first, the ability to articulate stakeholder expectations; second, the ability to exceed stakeholder expectations on a consistent basis. This finding came as no surprise. The strong alignment of internal audit priorities with key stakeholder expectations is the ultimate best practice.

While primary stakeholder expectations will differ from one organization to another, they typically include a combination of the following:

1. The audit committee and board expect internal audit to:
    - Institute a comprehensive risk-based audit plan
    - Inform directors about the tone of the organization and its control processes
    - Provide expertise and assurance on risks and controls
    - Facilitate greater understanding of the organization's risks and its risk management processes
    - Provide an objective set of eyes and ears across the organization
    - Serve as a trusted advisor
2. Management expects that internal audit will:
    - Provide expertise and assurance on internal controls
    - Offer and provide insight, advice, and assurance on enterprise risks
    - Deliver timely and relevant information to facilitate risk management and business decisions
    - Assist management with identification of emerging risks or events
3. External auditors, regulators, and others expect internal audit to:
    - Identify key risks facing the organization and assess the effectiveness of controls to mitigate those risks
    - Provide insight into the adequacy of financial controls
    - Execute a risk-based audit plan addressing financial risks and relevant IT controls

We believe the following ten imperatives provide the foundation for a high-performance internal audit function in the years ahead.

1. **Achieve sufficient strategic stature for internal audit within the organization.** Ideally, a chief audit executive will report functionally to the audit committee, as is the case with 86 percent of the respondents to the 2007 State of the Internal Audit Profession survey. However, a reporting relationship alone will not create prominence or stature. To be successful, a CAE needs to be perceived as strategic and as a member of senior management or its operating equivalent. Audit leaders who reach these milestones strive continuously to ensure that internal audit's priorities align effectively with those of the audit committee and senior management. They make a point of communicating regularly with the chairman of the audit committee, on both a formal and informal basis. And they position themselves as trusted advisors to their key stakeholders. Such proactive steps are likely to be even more important in the years ahead as pressures mount for internal audit to demonstrate value beyond providing controls assurance.
2. **Develop and regularly update a formal strategic plan aligned with key enterprise-wide objectives and stakeholder expectations.** To navigate the inevitable changes, it will be more important than ever for organizations to have a formal strategic plan in place. To be effective in driving change, a strategic plan should:
   - Describe the organization's vision for the future of internal audit—one that is clearly aligned with the needs of the organization and its stakeholders
   - Serve as a primary basis for change and management of the function
   - Outline the major risks and trends affecting the company and its industry
   - Describe how internal audit is organized to deliver service
   - Suggest specific goals or strategic initiatives to bridge capability gaps and to achieve internal audit's strategic vision
3. **Communicate frequently with key stakeholders on their needs, expectations, and satisfaction with internal audit.** A CAE needs to keep senior management and the board informed about emerging risks to the enterprise as well as systemic risk and control-related trends that are gleaned from audits. The CAE and senior internal audit managers should cultivate active two-way communication channels with the chairman of the audit committee and with the company's external auditors.

4. **Align HR strategies with enterprise and stakeholder needs.** Our research indicates that a number of new and emerging skills will become critical for internal auditors during the next five years. Successful internal audit functions will identify and bridge both existing and projected gaps in expertise. Rotational staffing, which has long been a leading practice within internal audit, is fast becoming the prevalent staffing model for large corporate internal audit groups. The model allows internal audit groups to recruit staff from within and outside their companies and to offer these recruits career opportunities in company business units after a two- to three-year rotation within internal audit. The vast majority of the Fortune 500 respondents to our 2012 survey have some form of rotational staffing in place that affects either all or significant portions of their internal audit staff. When asked to describe their current staffing model for internal audit, 13 percent of our Fortune 500 respondents said they use a pure rotational staffing model, and 57 percent said they use a blend of rotational staffing and career positions. Of note, training and development are key success factors with such programs.

5. **Adopt a risk-centric value proposition that focuses continually on enterprise risks.** To meet rising stakeholder expectations, internal audit needs to embrace a risk-centric approach to delivering value. That requires providing assurance on risks as well as controls, maintaining an ongoing focus on risk, and keeping the audit committee and senior management well informed about changing risk exposures. Ideally, internal audit will conduct an annual enterprise-wide risk assessment and have a robust process in place to update that assessment and will make adjustments to its formal audit plan on a quarterly basis. In addition to including a continuous dimension, risk assessments will be transparent, aligned strongly with business units, and involve external auditors as well as senior management and the audit committee.

6. **Take an integrated approach to IT audit, one designed to strengthen IT capabilities.** IT audit strategies need to lay the groundwork for integrating IT audit expertise within audit teams. An IT audit plan should center on an annual IT risk assessment, reflecting a clear linkage between IT risk assessments and IT audit planning. In addition, it should address risks within individual business processes and provide for continuous enhancement of IT audit capabilities. It's also important for the plan to be clearly articulated, formally documented, and well aligned with organizational IT strategies and objectives.

7. **Leverage technology to optimize audit operations.** High-performing internal audit functions maximize the use of technology to enhance the efficiency, effectiveness, and quality of operations.

   - To increase efficiency, internal audit should automate issues tracking and reporting to achieve paperless audits and reports, and use capacity multipliers to mitigate the impact of constrained resources.
   - To improve effectiveness in the search for errors or unusual transactions, internal audit should test entire data populations automatically.
   - To strengthen quality, internal audit should apply technology to conduct real-time reviews, escalate issues, and ensure compliance with standards.

   Technology solutions deployed in high-performing internal audit functions typically include the following:

   - Integrated internal audit software to streamline the production of work papers, risk assessments, and audit reports, and to automate issues tracking, monitoring, and administrative activities.
   - Data retrieval software to automate testing. Proficiency with such software should be considered a core competency for an internal audit staff.
   - Data mining/analysis software for predictive analysis and modeling.
   - Knowledge tools and databases to provide best-practice insights as well as a source for business-process benchmarking tools.

8. **Strategically leverage internal audit knowledge and expertise.** The internal audit staff has a wealth of knowledge and expertise about enterprise risks and controls that must be captured and shared. This need will become even more pronounced as internal audit expands the scope of its focus to include assurance on risk. To ensure their success going forward, internal audit functions must develop a formal knowledge-management plan to synthesize risk and control knowledge and make it readily available to internal audit management and staff, business-unit managers, senior enterprise management, and other stakeholders, as appropriate. Remember to budget appropriately: significant investments are required to build and maintain such a capability.

9. **Commit to continuous quality assurance and improvement.** High-performance internal audit requires a commitment to quality that extends well beyond conformance with the IIA Standards. A formal quality assurance and improvement program should provide for periodic internal assessments. It should also include periodic external assessments, such as a quality assurance review (QAR)[6] that includes extensive benchmarking and insight into how internal audit compares with its peers.

10. **Link performance measures to strategic goals.** High-performance internal audit groups align their performance measures with stakeholder values and expectations and with their own strategic goals and objectives. They develop a strategic plan in concert with the audit committee and executive management and continually track their performance to plan, often employing balanced scorecards to focus on outcomes as well as outputs. Performance metrics in internal audit will typically assess the number of engagements completed, number of findings, number of recommendations, number of recommendations implemented by management, and number of repeat findings/conditions, as well as average cycle time for engagements, average reporting cycle time, and client satisfaction.

[6] When the Institute of Internal Auditors (IIA) unveiled its International Standards for the Professional Practice of Internal Auditing in 2002, it mandated that internal audit groups conforming to the Standards adopt formal quality assurance and improvement programs that included an external quality assurance review (QAR) performed at least once every five years. With internal audit's enhanced role today in the risk, control, and governance activities of many major corporations, QARs are considered to be particularly important in management and audit circles. In addition to confirming compliance with the IIA Standards, a well-designed external assessment will provide benchmarks and measurements that can be used to improve internal audit performance long after an external QAR report is issued.

Methodology

To gain a broad base of input for this study, PricewaterhouseCoopers surveyed the chief audit executives (CAEs) of Fortune 250 companies about trends likely to affect internal auditors over the next five years and what they expect internal audit to look like in 2012. We also interviewed a number of highly respected CAEs, as well as thought leaders representing the academic and stakeholder arenas to add a qualitative dimension to our study. Through our survey responses and interviews, we obtained input from nearly a third of the Fortune 250. We then drew upon four sources—survey results, interview feedback, our client experience, and internal audit perspectives—to create a composite picture of trends expected to impact internal audit functions over the next five years.

Surveys were sent to the chief audit executives of all Fortune 250 companies in the United States. In addition, we sent surveys to 25 thought leaders within the global internal audit community to seek input from these stakeholders and academics well versed in the challenges confronting the profession.

We received a total of 82 survey responses, 72 from CAEs and 10 from thought leaders. To enhance our research, we also conducted in-depth interviews with 19 individuals who represented a cross-section of our survey population. All of this input has been incorporated in our report.

Contacts

Dennis Bartolucci
Partner
312.298.3584
dennis.d.bartolucci@us.pwc.com

Dick Anderson
Partner
312.298.4814
dick.anderson@us.pwc.com

Richard Chambers
Managing Director
678.419.7004
richard.f.chambers@us.pwc.com

Or visit:

www.pwc.com/internalaudit

pwc.com