



The Bulletin

Volume 4, Issue 8

Refocusing the Internal Audit Agenda: Capitalizing on Changing Expectations

Years ago, The Institute of Internal Auditors (IIA) formally defined internal auditing as “an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations.” This definition focused on a broad range of evaluation and improvement activities, namely, “risk management, control and governance processes.” Even now, some view The IIA’s definition as ahead of its time, since many internal audit functions still lack the knowledge and skills required to expand the focus of the audit plan to address all of these activities fully.

Our view is that this definition continues to provide a pathway for refocusing the internal audit agenda in an environment of ever-changing expectations. This issue of *The Bulletin* explores some factors driving higher expectations for internal audit and outlines how chief audit executives (CAEs) – with support from management and the audit committee – can respond to the challenge.

Changing Expectations

To say the least, there is a lot going on that could affect the expectations of internal audit. We highlight some important developments below:

- **Rapidly Evolving Corporate Governance** – Executive compensation, say on pay, Institutional Shareholder Services (ISS) vote recommendations, compensation clawbacks, proxy access, boardroom diversity, the emergence of risk committees and other developments are creating a sea change in the governance landscape. These developments are significant, as they signal the dawn of a new age of shareholder activism and corporate transparency that will foster increased dialogue among boards and management and those who serve the interests of both, including internal audit.
- **The Evolving Board Risk Oversight Process** – Risk oversight is a high priority on the agenda of most boards of directors. Boards are taking a fresh look at the qualifications of their members, how they operate, and the extent to which they avail themselves of the appropriate expertise of officers and others within the organization to understand the enterprise’s risks and how those risks are being managed. A 2010 Protiviti survey of more than 200 directors, commissioned by the Committee of Sponsoring Organizations (COSO), revealed there are mixed signals about the effectiveness of board risk oversight across organizations. While many directors believe they are performing their risk oversight responsibilities diligently and achieving a high level of effectiveness, a strong majority indicated their boards are not formally executing mature and robust risk oversight processes.¹
- **Gearing Up for the Impact of New Regulation** – Regulatory reform is a global phenomenon, placing a premium on company readiness in dealing with new and pending laws and regulatory changes, regulator reviews and other developments. The Dodd-Frank Wall Street Reform and Consumer Protection Act is widely considered to be one of the most comprehensive reforms of the U.S. financial industry in decades. Both regulators and companies are still seeking clarification on its provisions. While the headlines focus on the financial services industry, the legislation includes a variety of provisions that cut across all industries, including improved disclosure relating to pay-for-performance and pay-parity, non-binding shareholder votes, broader clawback provisions, shareholder access, and new whistleblower provisions, among other things. The U.K. Bribery Act 2010 is another example of recent legislation that companies with U.K. operations need to address. With the vigorous pursuit of violators of the Foreign Corrupt Practices Act in the United States, recent new anti-corruption regulations emerging in several other countries, including Russia and China, and the unprecedented collaboration across country borders to combat corruption risk, it is a management imperative to reduce corruption risk to an acceptable level.
- **Raising the Bar for Risk Management** – Traditional risk management practices and check-the-box approaches to satisfying board requests regarding risks and risk management are proving to be inadequate as further surprises and issues continue to arise. Most everyone agrees that an effective risk assessment should never end with just a list of risks and without formulating appropriate risk

¹ See *Board Risk Oversight – A Progress Report: Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities* at www.protiviti.com.

responses, yet that is exactly what happens at many companies. Accordingly, we see organizations enhancing their approach to risk management. Some companies are aligning their competitive and market intelligence functions with their strategy using the critical assumptions underlying the strategy as the bridge between the two. There are organizations recognizing the importance of applying an extended end-to-end enterprise focus on the value chain, looking upstream to the various tiers of suppliers and downstream to customers and the ultimate consumer when evaluating operational risks. Some companies and their boards are recognizing the importance of evaluating the potential impact of culture and compensation on the enterprise's risk profile. There are organizations initiating a dialogue with their boards about risk appetite. There is renewed interest in enterprise risk management as a process for informing the board's risk oversight. And more companies are recognizing the value of considering velocity to impact and persistence of impact when prioritizing risks.²

- **Sotegai: Preparedness Is the Name of the Game** – The scope of the tragedy in Japan and the nuclear disaster at the Fukushima Daiichi plant has captured the attention of people across the globe. In the debate around whether these tragic events should have been anticipated and planned for, one Japanese executive used a new buzzword, *sotegai*, or “outside our imagination,” to describe what actually occurred.³ The extent of interconnectivity of supply chains, marketing channels, business-to-business transactions and people-to-people interactions has been spawned by globalization, competition, lean manufacturing and other drivers and is increasing the speed of business and the reliance on infrastructure. With this trend toward interconnectivity, it is not difficult to envision how almost every company will be tested by a crisis at one time or another.⁴ Simply stated, more people and more things are potentially in the path of misfortune, and this increased complexity gives rise to fresh security and privacy issues.

Response readiness is gaining more attention at the highest levels of organizations. A crisis management perspective disregards likelihood assessments for “high-impact, low-likelihood” events and asks the fundamental question, “What will we do if the event occurs?” To this point, some companies are considering velocity to impact, persistence of impact and response readiness when evaluating high-impact, low-likelihood

risks in the assessment process to provide greater insights to management on where to improve preparedness. As events and crises continue to demonstrate time and again, the speed and quality of the enterprise's response to a crisis will often determine the speed and quality of its recovery. Therefore, building a strong crisis management capability is a management imperative for unlikely risks with a high velocity and reputation impact.⁵

- **IFRS – Believe It or Not, It's Coming** – While the adoption of International Financial Reporting Standards (IFRS) may not be imminent in the United States and certain other countries, the convergence of U.S. generally accepted accounting principles (GAAP) and IFRS is well under way. This convergence process affects financial reporting in all countries, and while certainly a form of emerging regulation, we think it merits separate mention. As this process unfolds, there are choices to be made about the extent of adoption of new accounting principles and changes needed in important areas. Convergence will affect many financial reporting areas, including fair value accounting, M&A accounting, non-controlling interests, and financial derivative transactions, and will require expanded skill sets to evaluate and apply.
- **Changes Attributable to the Economic Downturn** – Tone at the top and ethical and responsible business behavior have never been more important. During and since the recession, most companies have reduced costs and sized their organizations according to market demand, resulting in increased expectations on employees to do more with less. Now that there is appetite for growth, it is possible for even further stress to be placed on the internal control environment. Historically, we have learned that control breakdowns occur in these types of situations. This is why vigilance is the order of the day to ensure essential compliance and risk management functions remain intact and key control activities essential to financial reporting are not compromised.

The above discussion summarizes some of the developments driving higher expectations for everyone, including internal audit. The level of change spells out a stark reality – continue “business as usual” at your own risk. Everyone, including internal audit, is in the same mode: How do we reinvent ourselves such that we can maximize the value of our contribution to the organization's success?

Capitalizing on Changing Expectations

There are many opportunities for CAEs and their functions to thrive in this brave new world. We discuss some in the following sections.

² See Issue 2 of *The Bulletin*, “Making Your Risk Assessments Count: A Strategic Perspective,” and Issue 3 of *The Bulletin*, “Making Your Risk Assessments Count: An Operational and a Compliance Perspective,” for a discussion of the limitations of traditional risk assessments and why velocity, persistence and response readiness add more value in the way of insights. Both issues are available at www.protiviti.com.

³ “Japanese Nuke Plant Downplayed Tsunami Risk,” by Yuri Kageyama and Justin Pritchard, Associated Press, MSNBC, March 27, 2011: http://www.msnbc.msn.com/id/42295720/ns/world_news-asia_pacific/t/japanese-uke-plant-downplayed-tsunami-risk/.

⁴ “The Century of Disasters,” by Joel Achenbach, *Slate*, May 13, 2011: <http://www.slate.com/id/2294013/>.

⁵ See Issues 2 and 3 of Volume 4 of *The Bulletin* for further explanation of velocity, persistence and response readiness.

MANAGE AUDIT COMMITTEE EXPECTATIONS

It is vital to stay close to the audit committee chair and understand his or her committee's expectations as they evolve over time. In general, audit committees:

- Still want internal audit to provide assurance that the organization's internal controls over financial reporting are strong;
- Desire more insights as to the risks companies are facing, including emerging risks;
- Are noting that risk-mapping assessments developed to drive a risk-based audit plan do not suffice in addressing the question, "Do we know what we don't know?";
- Are recognizing the importance of preparedness and seek more insight on the impact of potential future events; and
- Expect internal audit to broaden its value added by addressing risk management processes in the audit plan.

If internal audit can take a lead role in helping the rest of the organization become more risk aware, initiate improvements in risk management throughout the company, and identify emerging risks, it will add value the audit committee will recognize.

Underlying the broader discussion around managing expectations is the question of whether internal audit serves management or the board. For example, is internal audit's delivering of value to management and providing assurances to the board mutually exclusive or either-or propositions? Or are they complementary? In many companies, this complex topic may merit discussion at the highest levels to determine if any change in direction, structure or reporting is in fact warranted. In some industries, the concept of more separation or increased independence of internal audit from management is an emerging issue with regulators and may be appropriate to consider in certain organizations.

In the United States, for instance, clients have told us that regulators consider rotational CAE programs as evidence of weaker governance than programs with long-term, career auditors at the helm. The perception is that if heads of the internal audit function are looking for their next role at the company, they may not be willing to take on hard issues that may be uncomfortable for management and raise those issues to the board.

EVALUATE IT SECURITY AND PRIVACY

As the IT environment becomes more complex, it is also intensifying security and privacy concerns for organizations. The advent of social media, increasing reliance on cloud computing and mobile devices, the WikiLeaks phenomenon, and recent high-profile breaches affecting both private and public companies underscore the potential for data loss that could affect millions of people. And with each significant breach reported, it would seem that no organization is safe from a determined, capable hacker. As a result, uncertainty is increasing in the boardroom and among the ranks of executive management.

IT is a high-risk area, which is why internal audit should be involved to provide an independent layer of additional

assurance. For example, internal auditors should ascertain whether someone in the organization is asking questions such as:

- Who can get into our systems?
- When they get in, what can they do? What might they want? Could they get it?
- Is the risk acceptable? If not, what can we do about it? At what cost?
- If we are mitigating the risk currently, how do we know what we are doing is working?
- Do we understand what information is private by law and what is not?
- Are we considering security and privacy issues when new IT systems are installed?

CONDUCT VALUE-ADDED RISK ASSESSMENTS

To manage risks effectively, they must first be identified. As changes occur to the organization's risk profile, risk assessments must be updated. Otherwise, risk management grows stale.

Regardless of who is responsible for risk management and strategic planning within the organization, internal audit should be involved in identifying emerging risks. The focus should be on obtaining insights as to what management needs to do differently, rather than shuffling known risks around on a risk map. Internal audit should ensure that management is focusing on four things to make risk assessments more value-added:

- Linking the risk assessment process to the critical assumptions underlying the strategy
- Understanding the impact of risk on the extended enterprise
- Considering velocity, persistence and response readiness in the assessment process⁶
- Considering the risk and impact of changes occurring and expected to occur, both inside and outside the organization

USE ASSURANCE MAPS TO IDENTIFY VITAL ASSURANCE PROCESSES

In 2009, The IIA issued Practice Advisory 2050-2 on "Assurance Maps." This release states that one of the board's objectives is to gain assurance that processes are operating within the parameters established to achieve specified objectives. To that end, it is necessary to determine whether risk management processes are working effectively and business-critical risks are being managed to an acceptable level. This point of view spotlights the organization's assurance activities.

The premise of 2050-2 is that there are three classes of assurance providers, which are differentiated by the stakeholders they serve, their level of independence from

⁶ Ibid.

the activities over which they provide assurance and the robustness of that assurance. These classes are:

1. Those who report to management and/or are part of management;
2. Those who report to the board (including internal audit); and
3. Those whose reports are of interest to, and relied upon by, external stakeholders (such as the external auditor).

In this context, there are many assurance providers internally within an organization – including line management, employees, senior management, functional management, internal audit and compliance.

This IIA advisory is ahead of its time. An assurance map clarifies “who does what” at the different levels of assurance, and identifies gaps and overlaps against the various risk-based expectations set by the board and executive management. It allows internal audit to identify focus areas for evaluating whether the assurance process is functioning effectively. Therefore, as more boards ask internal audit for “assurance” while not really knowing what that request entails, an assurance map provides a basis for educating the board as to where the accountability lies and refocuses the audit plan to assess the quality of the internal assurance processes across the organization.

More important, assurance maps create the opportunity to emphasize a “defense-in-depth” concept, with line management and employees providing the first line of defense. Depending on the industry, compliance management, risk management, VaR review, EH&S, the CIO organization, Sarbanes-Oxley PMO, ORM and other corporate-level functions offer the second line of defense. Executive management provides the third line of defense, and internal audit, the fourth. The defense-in-depth concept is an integral part of the internal control structure.

KEEP PRIORITIES UP TO DATE

All internal audit groups prioritize their projects. The question is: How up to date are these priorities, particularly in the context of the organization’s ever-changing risk profile? The CAE should be looking at his or her function’s priorities when significant changes occur, and at periodic intervals based on the entity’s risk profile and as circumstances dictate. Following are areas to consider when prioritizing points of focus in the audit plan:

- Tone at the top issues and key components of the control environment – for example, corporate governance issues (e.g., executive compensation), effectiveness of monitoring activities, and ethical and responsible business behavior.
- IT matters – such as IT governance, security and privacy, spreadsheets, e-discovery, and Payment Card Industry Data Security Standard compliance (where applicable).
- Corruption risk issues – for example, consider the risk profile of the countries in which the company operates (including

the cultural, political and regulatory environment); foreign and commercial relationships; and the nature of payments made in order to conduct business (e.g., business licenses, permits, certifications and inspections), among other things.

- Other regulatory matters – such as implications of Dodd-Frank legislation (including its impact on banks the company works with) and other regulatory changes.
- Process issues – for instance, intellectual property issues (e.g., identification, management, protection and control); strategic suppliers and business partners; royalty payments, construction and capital projects; and implementation of “Lean Six Sigma” across the organization.
- Risk management – such as the implementation of enterprise risk management (ERM) using ISO 31000, COSO ERM or another suitable framework; foreign currency and liquidity management; enhancements to the risk assessment process; and improvements in risk reporting.
- Sustainability – such as the enterprise’s focus on “walking the talk” with its public disclosures around managing its carbon footprint and balancing environmental, economic and social issues in executing its business model.
- Financial reporting matters – for example, high-risk areas such as revenue recognition; implications of IFRS convergence; and opportunities to make Sarbanes-Oxley compliance more cost-effective.

For many internal audit groups, prioritizing what’s important means directing attention to a more balanced focus on strategic issues, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

LEVERAGE TECHNOLOGY TO EXPAND COVERAGE

By improving the use of technology in the audit process, continuous auditing and continuous monitoring become reality. Better use of technology and the data in existing systems can drive more use of monitoring in the business and more preventive, automated controls. Data mining techniques can be far more effective than testing a sample of 30 items. With company information digitized, why not test 300,000 transactions? If the auditor tests more high-risk transactions, the chances of discovering problems increase. Greater reliance on technology can also support more effective use of self-assessment techniques to achieve more coverage over time.

ACQUIRE, DEVELOP AND DISTRIBUTE TALENT

As CAEs evaluate risk and skills coverage, gaps in skills can be identified. If positions are open, they should be filled. If necessary, outside help should be sought to address specialized skills. While these activities support the talent acquisition process so vital to internal audit’s success, over time internal audit needs to focus on developing people for other opportunities within the company. Internal audit should be viewed as a place for training strong performers who can be transferred to specific functions within the business. By placing trained former auditors throughout the organization in management

positions, the company raises the quality of its control environment. This approach allows internal audit to recruit better candidates because they see personal growth opportunities. Rotation programs and guest auditors work well within this strategy in augmenting staff positions the CAE must fill.

DEMONSTRATE POSITIVE CHANGE

One of the best ways to gauge the effectiveness of internal audit is to assess its reputation among other groups in the organization. When the internal audit function reports on its work, it's important to know what positive changes were made as a result – that is, the value contributed. For example, did internal audit's recommendations result in cost savings, improve information for decision-making or enhance the effectiveness of internal controls?

Another aspect of positive change is better collaboration. Are internal audit's activities redundant with other functions? Are process owners besieged with the same requests from internal audit and other functions? For example, chief risk officers and CAEs often find themselves struggling to resolve differences between their respective functions' views of business risk and evaluations of the effectiveness of risk management practices. The use of assurance maps, as discussed earlier, can help address overlap issues.

Summary

“Business as usual” is a dangerous practice in a rapidly changing environment. One way to obtain a fresh view is to consider a Quality Assurance Review (QAR), which is required by The IIA's *Standards* every five years. A QAR can be a source of fresh ideas for refocusing the internal audit agenda; however, a recent survey conducted by The IIA indicates that less than half of internal audit groups have conducted one in the past five years.⁷

The CAE must understand the expectations in the company and align the internal audit function accordingly to create positive change within the function itself and the organization at large. Positive change comes from refocusing the internal audit agenda on activities that add value and improve – in the face of ever-changing expectations – the company's operations and its risk management, control and governance processes.

⁷ According to *The IIA's Global Internal Audit Study: Core Competencies for Today's Internal Auditor*, 2010 CBOK Study, on pages 18 and 19, 46.3 percent of CAE respondents indicate their organizations are in compliance with all The IIA *Standards*; however, only 31.3 percent indicate they have an internal audit quality assessment and improvement program in place. Meanwhile, 50.9 percent report they have never had an external QAR.

Protiviti's 2011 Internal Audit Capabilities and Needs Survey

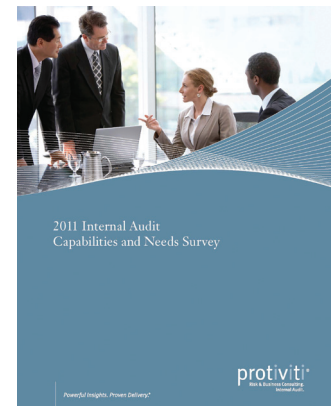
As global markets continue to emerge from several years of economic instability, increased regulatory oversight and greater attention to risk management are monopolizing the attention of boards and executive management. In many ways, the core solutions for operating successfully and growing profitability amid a heightened regulatory and risk management environment include a strong internal audit function. Today's internal auditors are being relied upon to help guide their organizations to compliance while ensuring key operations perform at peak efficiency.

Protiviti's annual Internal Audit Capabilities and Needs Survey assesses the capabilities of internal auditors in areas of priority for today's organizations, along with the competencies that are most in need of improvement.

To learn more about the ever-changing expectations for internal audit functions, download our report and view our video at www.protiviti.com/IASurvey.

For more information about Protiviti's Internal Audit and Financial Controls solutions, please contact:

Robert B. Hirth Jr.
Executive Vice President – Global Internal Audit
+1.415.402.3621
robert.hirth@protiviti.com



protiviti[®]
Risk & Business Consulting.
Internal Audit.