TONE at the TOP®

POWERED BY The Institute of Internal Auditors | Audit Executive Center™

Issue 79 | October 2016

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Regulatory Roulette? Best Bets for Managing Compliance Risk

For years, Apple Inc. ran a series of TV commercials advising consumers that, in every situation, "there's an app for that." Companies operating in today's global environment might well think the same thing about regulation. In every industry and geography, for every product and service, there is seemingly "a regulation for that." And the burden of regulation is on the rise. In a 2015 global survey, the International Federation of Accountants (IFAC) found that 83 percent of accountants saw a significant increase in the regulatory impact on their organization compared with five years earlier.

Despite greater regulation and the risk of noncompliance, some companies may not be taking their responsibility for identifying and managing compliance risk particularly seriously. A 2014 survey by Deloitte and *Compliance Week* showed that 40 percent of companies did not perform an annual compliance risk assessment. Further, a 2015 study by The IIA found that 38 percent of chief audit executives (CAEs) did not use compliance or regulatory requirements as a resource to establish the audit plan.

Norman D. Marks, a former chief audit executive, chief risk officer, and chief compliance officer who writes a blog for The IIA's *Internal Auditor* magazine, may have landed on a reason for this behavior: "If organizations don't think of compliance risk as a holistic business risk," he said, "they might underestimate the consequences. But the potential fallout is very real. Constraints can be placed on operating activities, a facility may be shut down, huge reputation impacts can follow, employee morale may suffer, and sales may drop off."

How should directors and executive management who want to better address compliance risks go about making improvements? A good start is to ensure roles and responsibilities related to risk management and control are well-defined and clearly understood across the organization.

The Three Lines of Defense

The Three Lines of Defense model advocates for clearly defined responsibilities over three aspects of risk: risk ownership, risk monitoring, and risk

assurance. Functions that own and manage risks are the first line. Various risk control and compliance functions that monitor risks are the second line. The role of internal audit — the third line of defense — is providing assurance to stakeholders (the board of directors, the audit committee, executives) that compliance risk can be managed at acceptable levels. Finding that "acceptable level" — the balance between the potential cost of risk and the amount of resources to mitigate it — is, of course, part of the challenge.

Internal Audit's Role

Many internal audit departments, Marks says, engage in two types of audits: one that determines if there is appropriate compliance, and one that determines whether there are controls in place to provide reasonable assurance that there is appropriate compliance. Marks says internal audit should focus on the latter and provide an opinion on the management of compliance risk — not an opinion on whether there is compliance. Why? "It's a moving target," he says. "It's possible for the company to be in compliance one day and not the next. In addition, internal auditors are experts in processes and controls, not necessarily in all the nuances and complexities of laws and regulations."

Internal audit's ability to perform its role can be helped or hindered by the structure in which it functions. The IIA recommends that internal audit report functionally to the board and administratively to the CEO to help protect internal audit's independence.

Partnering to Boost Compliance Risk Assurance

Use of combined assurance by the second and third lines of defense can be key for offering effective and efficient assurance for compliance risk. This approach is a coordinated effort by multiple internal assurance functions to combine assurance, which can reduce the nature, frequency, and redundancy of internal audits, thus limiting "audit fatigue" or "reporting fatigue" on the part of the board and executive management. To be successful, internal audit and other internal assurance departments, such as compliance, must partner to ensure both objectivity and quality of combined assurance.

Paul Sobel, CAE of Georgia-Pacific LLC and former IIA global chairman, supports combined assurance, but he also acknowledges that it can present a challenge to obtaining truly objective assurance, notably when compliance reports to internal audit, or vice versa, or when the two lines reside in the same department. "This reporting system requires discussion with management and the board, and consideration of outsourcing or co-sourcing some compliance assurance activities to obtain objectivity," Sobel says.

The Responsibilities of the Board and Audit Committee

The board and the audit committee are key stakeholders in the compliance risk function. What do they need to do to effectively carry out their responsibilities?

While organizations may operate differently, responsibilities of the board should generally include the following:

- Obtain assurance that management is handling compliance risk. Ask to be alerted should there be any significant violations of laws and regulations.
- Ask questions of internal audit, management, and the compliance function about the company's capabilities. Are the right people and the

We're moving *Tone at the Top* exclusively online!

In an effort to be a better environmental citizen, The IIA will soon discontinue the print version of this publication. To subscribe to receive an email notification when each printable electronic copy becomes available, please subscribe for free at **www.theiia.org/tone**. We will continue to provide you with the same great content, in a format that is better for the environment!

right culture in place? Is there a guarantee that, if problems are identified by employees, they will be reported and action taken? Is there a reasonable level of assurance that the company is compliant with the applicable standards and regulations of its industry?

- Obtain training on compliance. Learn the company's compliance-related policies that should be monitored.
- Review across audits the site-level gaps that are perceived as severe, in a context that includes performance, inquiries from external stakeholders, and past incidents. Ask to be made aware of any similar or recurring issues and what efforts executive managers and/or audit committees are taking to address them.

The audit committee's compliance risk responsibilities may also vary from one organization to the next, but they should be clearly outlined in the committee's charter. Many audit committees have responsibility for more detailed compliance updates, though in some organizations, it may be handled by a governance committee. This entails receiving quarterly updates on policy changes, training status, investigations, violations, and other related issues. The committee chair can then update the full board, as appropriate.

The audit committee may also ask the internal audit department to audit the second line of defense, focusing on significant strategic risks. For instance, that might include site-level gaps and initiatives requiring capital expenditures. The committee should also identify gaps in program knowledge and implementation by reviewing issues that are similar or recurring across many sites.

Further, the audit committee and the board should thoroughly review and approve internal audit's plan and ensure it is focused on both appropriate compliance and operational risks, particularly when industry standards may not reflect all the risks to the business. For instance, businesses in many industries use the International Organization for Standardization's (ISO) international standards, which, according to the ISO, "provide requirements, specifications, guidelines, or characteristics that can be used consistently to ensure that materials, products, processes, and services are fit for their purpose." Peter Montagna, head of the environmental, health and safety (EHS) audit and assessment area at Henkel Corporation, says, "The audit committee and/or senior management team commissioning audits must make it clear that identifying gaps against the published standards is secondary to identifying risk. By doing so, operations can take appropriate actions and management can be assured that environmental, health and safety risk is controlled."

The board's and audit committee's increasing responsibilities are clear indicators that compliance risk is assuming greater prominence among an organization's business risks. This involves internal audit as well. But Marks also cautions about an exclusive emphasis on compliance risks: "Audit committees and executives need to understand that compliance risk is only one area of risk among many that internal audit focuses on. Internal audit should place the majority of its resources on the risks that affect the success of the organization and achievement of its objectives. Not all compliance risks are significant enough to be on the audit plan."

Quick Poll Question

Please rate your level of agreement with the following statement: I am confident that there is sufficient assurance over compliance risk at my organization.

Visit **www.theiia.org/tone** to answer the question and learn how others are responding.

About The IIA

The Institute of Internal Auditors Inc. (IIA) is a global professional association with more than 185,000 members in more than 170 countries and territories. The IIA serves as the internal audit profession's chief advocate, international standard-setter, and principal researcher and educator. www.globaliia.org

Complimentary Subscriptions

Visit **www.theiia.org/tone** or call +1-407-937-1111 to order your complimentary subscription.

Reader Feedback

Send questions/comments to **tone@theiia.org**.

Content Advisory Council

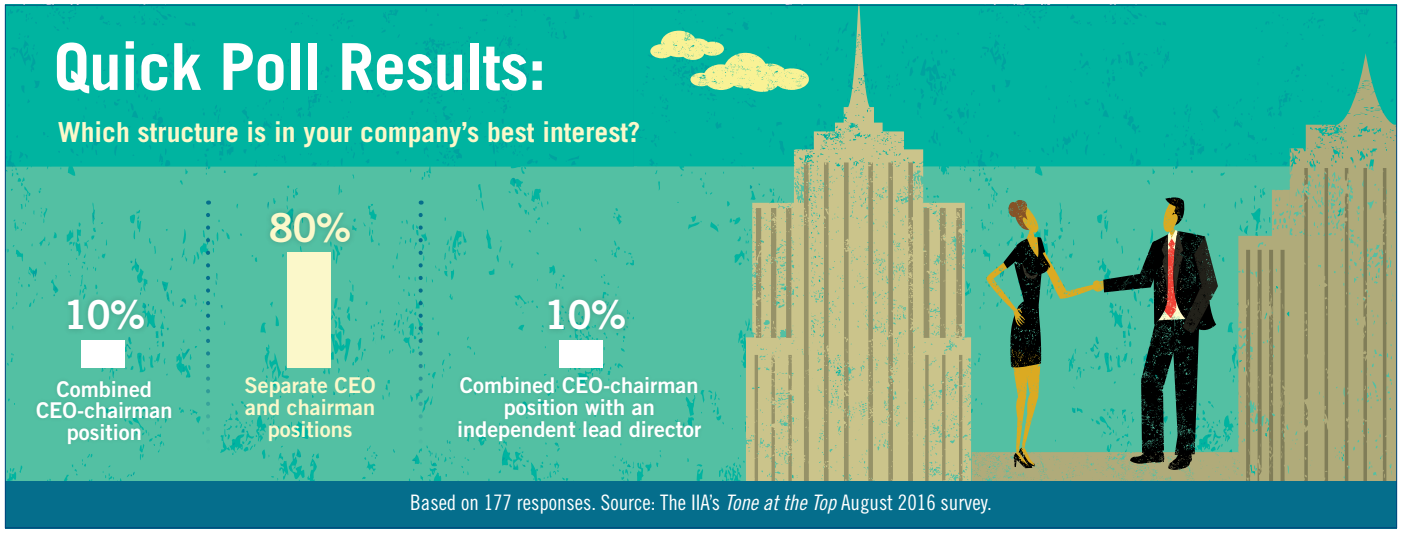
With decades of senior management and corporate board experience, the following esteemed professionals provide direction on this publication's content:

Martin M. Coyne II
Michele J. Hooper
Kenton J. Sicchitano

TONE at the TOP®

247 Maitland Ave.
Altamonte Springs, FL 32701-4201 USA

NONPROFIT ORGANIZATION
U.S. POSTAGE
PAID
THE INSTITUTE OF
INTERNAL AUDITORS



10/2016-1300