The Institute of Internal Auditors

TONE at the TOP

Issue 60 | February 2013

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

Risk Management: Easy as 1 … 2 … 3

The variety and complexity of risks facing today's organizations is rising rapidly, due in part to emerging technologies, globalization, and increased regulation. How can audit committees and other governing bodies get their arms around these growing risks? How can they ensure that each one is carefully considered and that "somebody" in the organization is looking out for each risk area? Moreover, how can they ensure that the people charged with responsibility for these various risk areas are working together to avoid gaps in risk management or duplication of efforts?

Seeking answers to these very questions, more and more company leaders are beginning to pay attention to a risk management and control model that many European organizations have been using successfully for years: Three Lines of Defense.

The premise of the Three Lines of Defense model is that each area within the company has a clearly defined and specific role to play. And when each does its assigned task effectively, the likelihood that a risk will slip past all of the defense lines and penetrate the organization diminishes. Not only that, but with a structure like this in place, the audit committee or other governing body can be confident that it's getting impartial information about the organization's most significant risks — and it knows whether management is responding to them appropriately.

The Model

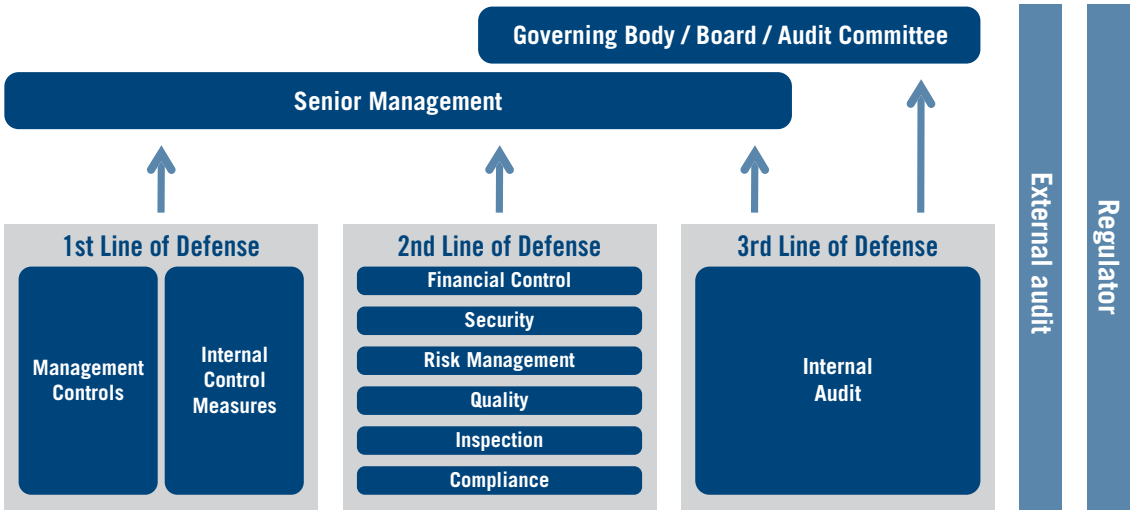
Aptly titled, the Three Lines of Defense model depicts three groups on which senior management and the board can rely to detect and address risk:

1. Operating management.
2. Risk and compliance functions.
3. Internal audit.

As the first line of defense, operational management manages the organization's risks by implementing and maintaining effective internal control procedures on a day-to-day basis. This line encompasses the mid-level and front-line managers who are responsible for identifying control breakdowns and inadequate processes and fixing whatever problems they find.

The second line of defense is made up of a number of specialty risk management and compliance functions

The Three Lines of Defense Model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

that work to make sure the first-line-of-defense controls are designed appropriately and operating as intended. Second-line professionals collaborate with operations managers to develop and monitor processes and controls to mitigate identified risks. They conduct their own risk assessments, develop risk management programs, and alert management to emerging issues and changing regulatory risk scenarios.

The composition of the second line varies depending on the organization's size and industry. A large publicly traded manufacturing company, for example, may have a number of specialized departments that oversee targeted risk and compliance areas like quality, inspection, safety, and financial reporting. In a smaller private company, some of these functions may be combined or nonexistent.

Examples of Second-line Functions

- Financial control
- Security
- Risk management
- Quality
- Health and safety
- Inspection
- Compliance
- Legal
- Environmental
- Supply chain

Internal audit serves as the organization's third line of defense, reviewing controls and risk management procedures, identifying problems, and keeping the board and senior management informed. What distinguishes internal audit from the other two lines of defense is its high level of independence and objectivity, which is enabled by the chief audit executive's direct reporting line to the board or other governing body. Due to its distinct responsibilities and uniquely independent positioning, internal audit is able to provide reliable assurance on the effectiveness of the organization's overall governance, risk management, and internal control processes.

Safeguarding Objectivity

From time to time, it's not uncommon for management to request internal audit's assistance to establish first-line controls or perform second-line risk management activities such as due diligence. When the U.S. Sarbanes-Oxley Act of 2002 was first enacted, for example, managers were quick to turn to their internal auditors for help establishing adequate internal controls over financial reporting. Although internal auditors may have the requisite skills to perform second-line activities, they must take care to ensure that these ad-hoc projects do not interfere with their primary responsibility of providing independent

assurance to senior management and the board. In reality, muddling the second and third lines of defense can compromise internal audit's objectivity and limit the function's overall effectiveness and reliability.

Clarity Across the Board

The Three Lines of Defense model provides clarity to governing bodies, management, and internal auditors around the roles of each function — particularly those that may appear to have overlapping objectives or responsibilities — and illustrates how they can work together to manage the organization's high-priority risks with the greatest efficiency and effectiveness. Moreover, the model demonstrates how internal audit's separation from management and management duties can benefit the board by enabling unbiased, unfiltered upward communication of the organization's risks and control efforts. The ultimate beauty of this model, however, is that its basic structure can be applied to any organization — regardless of size or industry.

The IIA Endorses Three Lines of Defense

The IIA recently released a position paper on this topic entitled *The Three Lines of Defense in Effective Risk Management and Control*. As part of The IIA's International Professional Practices Framework (IPPF) — the framework that houses IIA authoritative guidance — position papers go through a rigorous vetting process, which is governed by an independent oversight council, to ensure relevancy, consistency, and international applicability.

Visit www.theiia.org/standards-and-guidance to download the complimentary paper.

See our new **Quick Poll** on the back page!

Key Takeaways

- Boards/audit committees can look to internal auditing as a valuable resource to help them carry out their oversight responsibilities.
- The organization's risk management strategy is enhanced with greater efficiency and effectiveness when each group in the organization has clear roles and responsibilities.
- Internal audit's independence enables the function to provide effective assurance to the governing body and senior management on whether the organization's risks are being identified and mitigated adequately.
- When internal auditors perform activities that should fall under management's responsibility, the function's overall effectiveness and reliability as an assurance provider to the board may be compromised.

Questions Boards Should Ask

1. Does the Three Lines of Defense model accurately describe my organization's structure for addressing risk? If not, does something need to be changed?
2. Has management established appropriate resources for the second line of defense?
3. Does internal audit have a direct independent reporting line to the board or other governing body?
4. Does internal audit conduct second-line activities that should be performed by another group?

The Institute of Internal Auditors | TONE at the TOP

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

About The IIA

The Institute of Internal Auditors Inc. (IIA) is an international professional association and standard-setting body that serves as the internal audit profession's global voice, chief advocate, and principal researcher and educator. The IIA has more than 175,000 members in 190 countries around the world. www.globaliia.org.

Complimentary Subscriptions

You, your colleagues, and your audit committee and board members can receive complimentary subscriptions to *Tone at the Top*.

Visit **www.globaliia.org/Tone-at-the-Top** or call +1-407-937-1111.

Quick Poll

What do you think about the Three Lines of Defense model?

- ❏ My organization uses this structure.
- ❏ My organization doesn't use this structure, but I think we should.
- ❏ I'm uncertain whether this model would work in my organization.
- ❏ I'm not interested in this model.

Visit **www.theiia.org/goto/quickpoll** to answer the Quick Poll question and see how others are responding.

Look for the results of this Quick Poll in the next issue of *Tone at the Top*. And, as always, let us know what you think of this issue by emailing the editor at tone@theiia.org.

02/130276/PM/LW