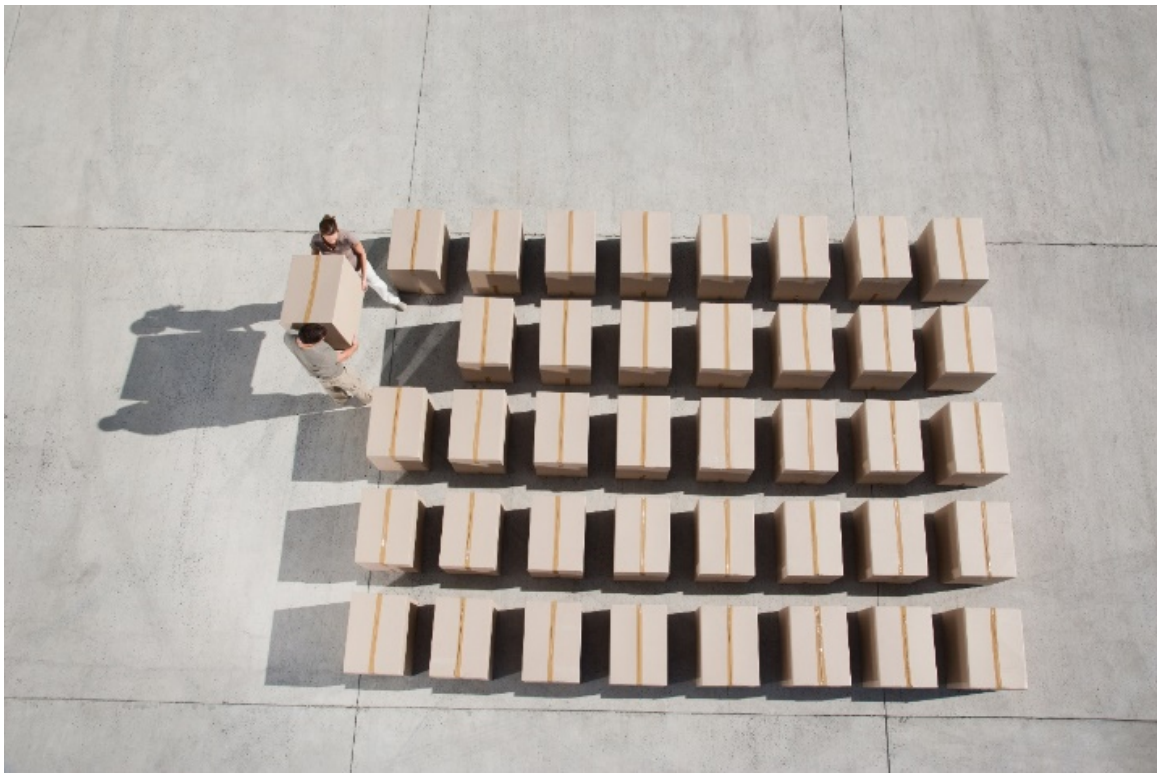


ELEGANT ALIGNMENT

ISO Guidance and the Three Lines Model

By Michael Parkinson, CIA, CRMA, PFIIA

The Institute of Internal Auditors | Global

GOOD GOVERNANCE REQUIRES COLLABORATION

ISO 37000 and the Three Lines Model

The Institute of Internal Auditors (IIA) participated closely in the development of the latest guidance on governance by the International Organization for Standardization (ISO). This robust new guidance and The IIA's Three Lines Model — two accounts of governance — are closely aligned, and the Three Lines Model fits elegantly alongside the more detailed and systems-oriented ISO guidance.

International Standard[1] ISO 37000 *Governance of organizations — Guidance*, published in September, says that governance, "lays the foundation for the fulfilment of the purpose of the organization in an ethical, effective, and responsible manner in line with stakeholder expectations." To put it more simply, good governance helps the organization achieve its objectives in the best way possible, in keeping with cultural and societal norms.

This same thinking is reflected in the 2017 ERM framework (*Enterprise Risk Management — Integrating with Strategy and Performance*) by The Committee of Sponsoring Organizations of the Treadway Commission (COSO). It expects the board to define the desired culture and behaviors of an organization, as well as its performance objectives. There is a further expectation that the board will demonstrate its commitment and hold members of the organization to account for their behavior.

Audit Focus

Internal Auditing Standard 2110: Governance

The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for:

- **Making strategic and operational decisions.**
- **Overseeing risk management and control.**
- **Promoting appropriate ethics and values within the organization.**
- **Ensuring effective organizational performance management and accountability.**
- **Communicating risk and control information to appropriate areas of the organization.**
- **Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.**

The mission of internal audit, "to enhance and protect organizational value," is fully aligned with this thinking. It is achieved through internal audit's work to provide independent assurance over governance, risk

1 The term "International Standard" refers to a publication of the International Organization for Standardization.

management, and control processes. Internal Auditing Standard 2110: Governance addresses internal audit's obligation to improve the organization's governance processes, as well.

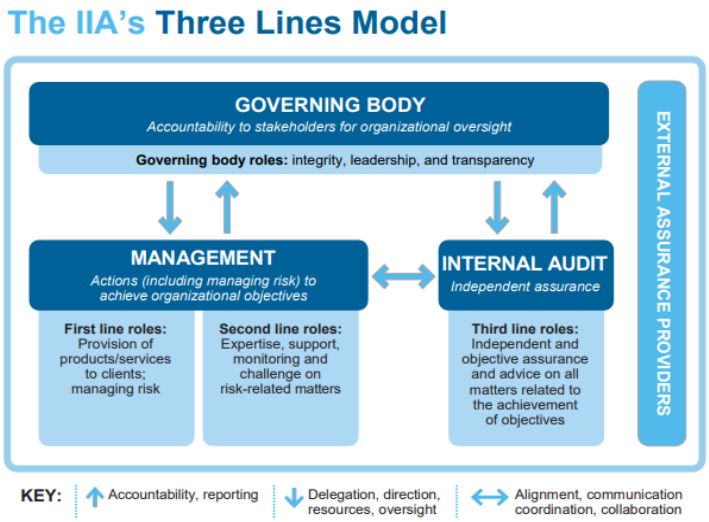
ISO 37000 describes eleven "principles of governance." While all aspects of this international standard will be of interest to internal audit reviews of organizational governance, its principle of oversight should be of particular interest to internal auditors.

Oversight: *The governing body should oversee the organization's performance to ensure that it meets the governing body's intentions for, and expectations of, the organization, its ethical behavior and its compliance obligations.*[2]

ISO 37000 lists multiple ways in which a governing body may exercise this oversight. These include direct inquiry and independent review. The governing body is expected to require reports on all material aspects of operation, make sure that internal controls systems (covering risk management, compliance, and financial management) are implemented, and ensure that the reports being provided are accurate. This implies that management is expected to set up systems to manage critical risks and to report the risk management process. Of particular interest to internal auditors is the emphasis on assurance over management reporting.

The board is expected to hold to account those to whom it delegates authority. This process of accountability requires reliable information. Therefore, top management should seek assurance that the reports it receives are correct and that they accurately analyze the activities of the organization. Consequently, top management creates management systems to provide continual monitoring, analysis, and improvement of operations. To obtain greater assurance, top management sometimes seeks additional external assurance on the accuracy of information it receives. This external assurance, often expressed as a management system certification, is commissioned by management and is part of the second line. Similarly, the board needs assurance on the accuracy of reports from a source independent of top management.

The Three Lines Model emphasizes that good governance requires multiple streams of information, and assurance from multiple, mutually independent sources. This model reflects that while the board may be informed by management (and by external entities such as regulators) it needs an independent, internal review function that it can direct to areas of interest. Similarly, the model reflects the need of top management to obtain reviews of areas of concern to them.



2 International Standard ISO 37000 Governance of organizations – Guidance, International Standards Organization

The roles in the Three Lines Model[3] are directly reflected in ISO 37000:

- First line role – The board should undertake direct verifications.
- Second line role – The board should seek direct reports from risk management, compliance management, and other control functions.
- Third line role – The board should obtain reports from internal audit as an independent provider of assurance.

A valuable suggestion in ISO 37000 is that the board, in addition to the common practice of holding private sessions with the internal auditors, should have private sessions with those who manage critical control functions.

Governance is a whole-of-organization activity, which requires direction, accountability, and an ethical framework. It does not exist simply to provide reports to management and the board. The organization has products and services and the delivery of these are its primary purpose.

Internal auditors have long understood that the delivery of efficient assurance requires cooperation and coordination. IIA Standard 2050: Coordination and Reliance requires that the chief audit executive "share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts."

If we understand where the roles explained in the Three Lines Model are within our organization, we can learn where the review activity takes place. Strategies for the delivery of internal audit services should take into account the roles of the other lines. In smaller organizations, some second line activities may be assigned to the chief audit executive (CAE). In such cases, understanding and utilizing the Three Lines Model can assist in structuring the lines of accountability.

Audit Focus

Internal Auditing Standard 2050: Coordination and Reliance

The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

There is value in internal audit working with other review functions to build an integrated review schedule to provide mutual support and to deliver in the most efficient manner the assurance the board needs.

ISO 37000, together with the understanding that the Three Lines Model provides, allows internal auditors to analyze and use the governance structures of their organizations to deliver efficient and properly targeted assurance that complements other sources of information used by the board. ISO 37000 and the Three Lines Model provide a useful reference point for assessing the quality of organizational governance. These tools also allow for management and the board to better understand governance and the various roles and responsibilities needed for success, including independent assurance from internal audit.

3 The IIA's Three Lines Model helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management. The governing body is ultimately accountable for governance, which is achieved through the actions and behaviors of the governing body as well as management and internal audit.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

Copyright

September 2021

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org