Chartered Institute of Internal Auditors

IIA Policy Paper

Internal audit, risk and corporate governance – the Three Lines of Defence Model

Main message

The *Three Lines of Defence Model* is a valuable framework that outlines internal audit's role in assuring the effective management of risk, and the importance for delivering this of its position and function in the corporate governance structure.

Applying the three lines of defence model in an organisation is not a silver bullet for achieving effective internal audit. Much also depends for example on the standing, scope and resourcing of the internal audit function. However if the positioning and governance structure for internal audit are wrong, its ability to support the board or audit committee in their challenging of management can be fatally undermined.

Different parts and levels of an organisation play different roles in risk management, and the interplay between them determines how effective the organisation as a whole is in dealing with risk.

Internal audit's unique role is to provide assurance to the board that is objective and independent of management about the controls in place to manage risk. Blurring internal audit's role can undermine effectiveness. The independence and objectivity of internal audit are vital in its support of the board and audit committee.

Regular and ongoing dialogue by internal audit with the first and second lines of defence is needed so that the function has a more timely perspective of business direction and business issues. Internal audit can therefore play a valuable advisory role to help the executive improve the second line of defence processes with advice, facilitation and training. Internal audit can also identify where there are gaps in the first two lines of defence and advise on how they can be plugged.

Internal audit can also play a valuable role in helping the board ensure that governance structures are effective in identifying and managing wider strategic as well as internal risks.

What do we want?

Changes to governance codes, standards, guidance or regulation should promote internal audit's role as a core part of the third line of defence and must avoid undermining its unique position in monitoring and providing assurance on the management of risk. Demarcation between the third line of defence and the first two lines must be preserved to enable internal audit to provide an objective overview to the Board, independent of management, on the effectiveness of all risk management and assurance processes in the organisation.

In some organisations the role of internal audit is combined with elements from the first two lines of defence. For example some internal audit functions are asked to play a part in facilitating risk management or managing the internal whistleblowing arrangements. Where that happens, boards need to be aware of potential conflicts of interest and ensure they take measures to safeguard the objectivity of internal audit. (See www.iia.org.uk/policy/policy-position-papers/risk-management-and-internal-audit/ and https://www.iia.org.uk/media/565182/iia_whistleblowing_briefing3.3.2014final.pdf)

Background

1. *The first line of defence (functions that own and manage risks)*

   is formed by managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving objectives. Collectively, they should have the necessary knowledge, skills, information, and authority to operate the relevant policies and procedures of risk control. This requires an understanding of the company, its objectives, the environment in which it operates, and the risks it faces.

2. *The second line of defence (functions that oversee or who specialise in compliance or the management of risk*)

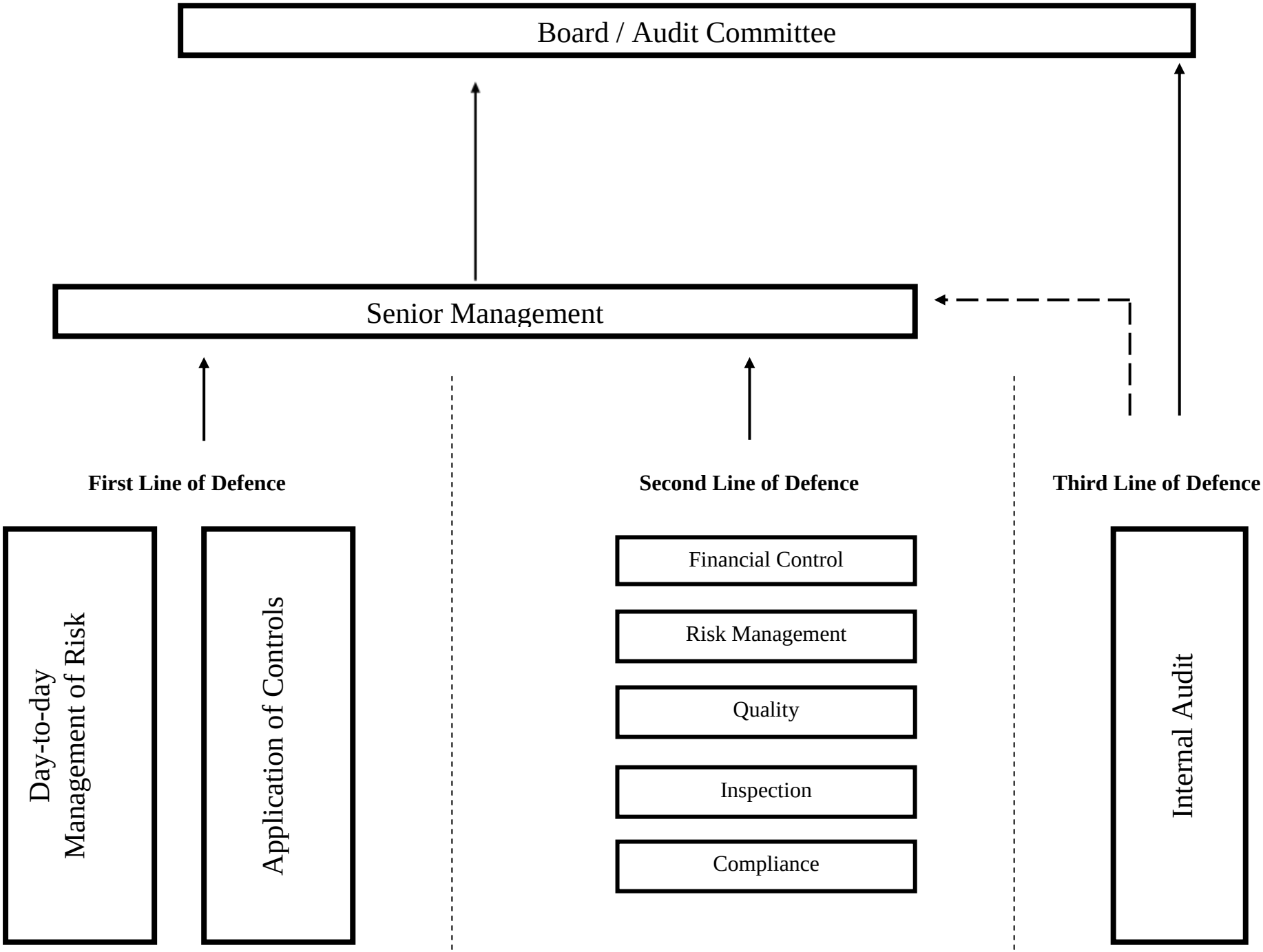
   provides the policies, frameworks, tools, techniques and support to enable risk and compliance to be managed in the first line, conducts monitoring to judge how effectively they are doing it, and helps ensure consistency of definitions and measurement of risk.

3. *The third line of defence (functions that provide independent assurance)*

   is provided by internal audit. Sitting outside the risk management processes of the first two lines of defence, its main roles are to ensure that the first two lines of are operating effectively and advise how they could be improved. Tasked by, and reporting to the board / audit committee, it provides an evaluation, through a risk-based approach, on the effectiveness of governance, risk management, and internal control to the organization's governing body and senior management. It can also give assurance to sector regulators and external auditors that appropriate controls and processes are in place and are operating effectively.

   For a more detailed analysis of the three lines of defence and how to coordinate their activities, please see

   https://global.theiia.org/standards-guidance/Public%20Documents/ippf%20pp%20the%20three%20lines%20of%20defense%20in%20effective%20risk%20management%20and%20control.pdf


Board / Audit Committee
Senior Management
First Line of Defence
Second Line of Defence
Third Line of Defence
Day-to-day Management of Risk
Application of Controls
Financial Control
Risk Management
Quality
Inspection
Compliance
Internal Audit