Chartered Institute of Internal Auditors

07 October 2019

Governance of risk: Three lines of defence

Chartered Institute of Internal Auditors

Internal audit has a key role in the corporate governance structure to assure on the effective management of risk:

The board provides direction to senior management by setting the organisation's risk appetite. It also seeks to identify the principal risks facing the organisation. Thereafter, the board assures itself on an ongoing basis that senior management is responding appropriately to these risks.

The board delegates to the CEO and senior management primary ownership and responsibility for operating risk management and control. It is management's job to provide leadership and direction to the employees in respect of risk management, and to control the organisation's overall risk-taking activities in relation to the agreed level of risk appetite.

To ensure the effectiveness of an organisation's risk management framework, the board and senior management need to be able to rely on adequate line functions – including monitoring and assurance functions – within the organisation. The IIA and the IoD endorse the 'Three Lines of Defence' model as a way of explaining the relationship between these functions and as a guide to how responsibilities should be divided:

1. the first line of defence – functions that own and manage risk
2. the second line of defence – functions that oversee or specialise in risk management, compliance
3. the third line of defence – functions that provide independent assurance, above all internal audit.

1. First line of defence

Under the first line of defence, operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks.

2. Second line of defence

The second line of defence consists of activities covered by several components of internal governance (compliance, risk management, quality, IT and other control departments). This line of defence monitors and facilitates the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate riskrelated information up and down the organisation.

3. Third line of defence

Internal audit forms the organisation's third line of defence. An independent internal audit function will, through a risk-based approach to its work, provide assurance to the organisation's board of directors and senior management. This assurance will cover how effectively the organisation assesses and manages its risks and will include assurance on the effectiveness of the first and second lines of defence. It encompasses all elements of an institution's risk management framework (from risk identification, risk assessment and response, to communication of riskrelated information) and all categories of organisational objectives: strategic, ethical, operational, reporting and compliance.

The role of the three lines of defence

Internal audit is uniquely positioned within the organisation to provide global assurance to the audit committee and senior management on the effectiveness of internal governance and risk processes. It is also well-placed to fulfil an advisory role on the coordination of assurance, effective ways of improving existing processes, and assisting management in implementing recommended improvements. In such a framework, internal audit is a cornerstone of an organisation's corporate governance.

The use of the three lines of defence to understand the system of internal control and risk management should not be regarded as an automatic guarantee of success. All three lines need to work effectively with each other and with the audit committee in order to create the right conditions.

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.

Four key issues for directors monitoring internal audit's effectiveness

Before considering the detailed recommendations of this guidance, it is important to stress the four fundamental issues that should be considered by directors in order to ensure that internal audit maximises its contribution to good governance:

1. Internal audit should have a functional reporting line to the board or one of its committees, making it independent of the executive, able to make objective judgements, and giving it the authority to conduct its work across the whole organisation without constraint. To work effectively it also needs a close relationship with the Chief Executive and should have access to management information going to the executive committee and board.

2. Internal audit must be properly resourced, including ensuring a consistently high level of professionalism and quality based on the International Standards, plus appropriate knowledge, skills and experience.

3. Internal audit should use a risk-based approach in developing and executing the internal audit plan in order to focus on the greatest threats to the organisation.

4. Internal audit's scope should be unrestricted, including all areas of risk – such as key corporate events, culture and ethics, reputation, new products and the outcomes of processes. The following recommendations for directors are consistent with the globally recognised International Standards.

Further reading

IIA Global's Three Lines of Defense in Effective Risk Management and Control

Next: Sample audit committee charter