Chartered Institute of Internal Auditors

**01 February 2023**

# Position paper: Risk management and internal audit

## Chartered Institute of Internal Auditors

### Effective risk management - joint internal audit and risk management functions

- Ensuring that internal audit provides independent and objective assurance on risk management and risk control is vital for risk to be managed effectively.
- Combining risk and internal audit activities raises issues about the objectivity of internal audit's assurance on risk management. Boards will need to address these issues if the two in any way overlap.
- In the case where separate internal audit and risk teams are managed by a joint Head of Audit and Risk (HAR) there needs to be a mechanism, appropriate to the organisation, to ensure that the audit committee and senior management are getting separate, clear and objective messages from each function.
- In cases where internal audit is asked to give advice or assistance on risk management, e.g. as part of its consultancy role, safeguards are needed to ensure that boards are still receiving the objective assurance on risk that they require.
- Where the internal audit and risk functions are fully combined (e.g. in smaller organisations, those that are not risk mature or whose risks are low level and not complex), the board will also need to ensure that the internal audit role is not undermined.

---

Boards need assurance that the risk culture in the organisation is robust and that risks are being managed effectively. This is particularly important following the financial and economic crisis and a series of scandals across other sectors. These risks include not only financial and operational risks but also IT, social, environmental, ethical and regulatory risks, to name but a few.

Risk committees and separate risk functions are required by regulation in some sectors, notably financial services. In others, where risks are complex or high, separate oversight of the executive's risk management structures and activities may still be essential. A firm commitment by the organisation's leaders to risk management through the creation of a risk function can ensure there is adequate professional expertise to maintain and develop best practice, sending a clear message to managers at all levels that they need to take responsibility for mitigating risk.

In all cases it is important that boards consider how they receive assurance on risk across their organisations from all sources, both internal and external, and ensure that there are no gaps or overlaps.

Many organisations find the three lines of defence model useful in explaining the role of internal audit. Under the three lines of defence model, operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks. The second

line consists of the activities of specialist control functions, which monitor and facilitate effective risk management by the first line and ensure the flow of information on risk up and down the organisation. The third line is internal audit.

However experience shows that even this model cannot guarantee success, especially if there is inadequate effective challenge between the lines. The Parliamentary Commission on Banking Standards' concluded in 2013 that the model failed in part because the lines were blurred and the status of the front-line, remunerated for revenue generation, was dominant over the compliance, risk and audit apparatus. Their recommendations were aimed at making the three lines separate, with distinct authority given to internal control, and particular non-executive directors being given individual personal responsibility for protecting the independence of those responsible for key internal controls. They also recommended that this be buttressed with rigorous scrutiny by the regulators of the adequacy of firms' control frameworks.

The key for internal audit as the third line of defence is that it is able to give independent and objective assurance to the board on the effectiveness of the risk management activities of the first two lines and support the audit committee and board in challenging the executive on risk. A dedicated risk management function can help preserve the clear principles of the three lines of defence model, enabling internal audit fully to provide independent assurance upon the design of risk processes, their application and effectiveness. But this alone is not necessarily a sufficient condition for success.

While the Institute regards this framework as one all organisations can aspire to, it recognises that in many organisations, for example where risks are low or relatively straightforward, or where there is lower risk maturity, there may be reasons why internal audit takes on some of the roles normally carried out by the second line of defence. This may be a practical and cost effective proposition given that risk and internal audit skill sets are complementary and secondments or guest appointments can bring new insights and valuable expertise. It may also help keep alignment of audit assurance to business risks where there is a danger that the audit work program and the risk register bear too little relationship to each other. In smaller businesses it can also ensure that both audit and risk get operational representation at the top table.

---

But it is important that, where this happens, boards are fully aware of the potential dangers and recognise that safeguards need to be in place:-

- It should be clear that management remains responsible for risk management. Typically the CEO and CFO should have ownership of risk in reporting to the board.
- Internal audit should not manage any of the risks on behalf of management, nor should it be classed as a risk owner (e.g. on risk registers).
- Internal audit should provide advice, challenge and support to management's decision making, as opposed to taking risk management decisions themselves.
- The nature of internal audit's responsibilities should be documented in the internal audit charter and approved by the audit committee.
- The board should be satisfied that dividing the HIA's time between the two functions does not undermine his/her ability to manage internal audit and engage with the audit committee on internal audit issues.
- A joint HAR cannot give objective assurance on any part of the risk management framework for which he/she is directly responsible. Such assurance should be provided by other suitably qualified parties.

- Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

In practical terms, where there is a jointly managed risk / internal audit function, it is important to maintain individuals' integrity. The solution may be for the HAR to have a deputy for internal audit who can put forward an objective internal audit view on risk. Hybrid roles below the HAR and deputy also need to be considered carefully as they are likely to make it even more problematic to distinguish second and third line activities in the day-to-day operations of the joint function. In any case the audit committee needs to be aware of conflicting loyalties, and may wish to consider external validation of internal audit's view on risk from time to time to ensure that it is not compromised.

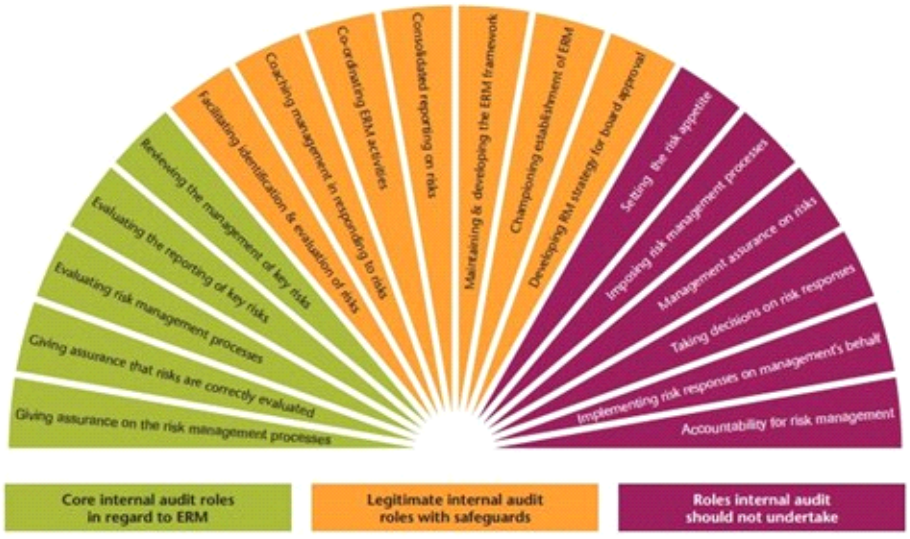
Where a joint audit and risk function reports to a joint Audit and Risk committee, HIAs should strive to ensure that the committee also understands its dual role in relation to both functions and that the committee's Terms of Reference, membership and meetings are structured to enhance the likelihood that both parts are given the requisite focus and attention.

It is also important for boards to understand that internal audit needs to form its own view of risk, both to enable it to focus its audit plan on the higher risk areas of the organisation's activities and also to alert the board if it considers that the risk appetite and risk culture are not in line with the organisation's strategic risk universe. This however is very different to internal audit being directly involved in the management of risk.

---

The diagram below illustrates the sort of roles that internal audit can play in Enterprise-wide Risk Management (ERM) provided the necessary safeguards are in place.

**The role of internal audit in Enterprise-wide Risk Management**




Expand this diagram

Further guidance can be found in:

- The Global IIA Position Paper "The role of internal audit in enterprise-wide risk management", 2009,
- The Chartered Institute guidance paper "Coordination of assurance services", 2010.
- The Chartered Institute policy paper on the Three Lines of Defence.
- The Chartered Institute guidance paper "Annual internal audit coverage plans" 2014