Risk committee guidance for audit leaders

Overview

Robust corporate governance is the bedrock of all successful organisations. To provide valued assurance, auditors need to keep up to date with best practice and developments such as the new principles-based guidance for board risk committees and risk functions published by the Risk Coalition in December 2019, with contributions from the Chartered IIA (a former member of the group).

This short thought leadership article provides an overview of that guidance and considers the potential implications of it for audit leaders. Although initially for the financial services sector, there is an intention to extend the reach of this guidance to other sectors in line with other governance codes.

Audit leaders should take note, especially those with responsibility for the risk function, and be aware of the seventeen principles (eight board risk committee/nine risk function) that their audit committee chairs will be demanding, relevant to assurance work for governance and risk management.

No risk committee? The guidance also applies to audit and risk committee or the board itself depending on governance structure.

The role of the Risk Coalition

The Risk Coalition is an association of not-for-profit professional bodies and membership organisations committed to raising the standards of risk management in the UK and strengthening risk governance.

Their first publication targets board risk committees, the chief risk officer and the risk function. It also details how the relationship with internal audit should operate.

The role of a risk committee in corporate governance

A risk committee is an authorised sub-committee of the board, with a similar function to a remuneration and nominations committee. It is most commonly but not exclusively seen within financial services.

In financial services firms, risk committees are established to review and report conclusions to the board. Their activity focuses on how an organisation manages and adheres to its risk appetite and tolerance in addition to reviewing the enterprise risk management framework such as principles, policies, culture, organisation, behaviours, systems, processes and procedures.

To date, there has been no guidance to support this, with organisations left to determine their own criteria. As Martin Stewart, Former Director of the Prudential Regulation Authority, highlights: “Nothing like this currently exists in Europe”.

Fortune Chigwende of Hermes Investment Management, likewise notes: “This guidance has been long

© Chartered Institute of Internal Auditors

awaited by third line functions as it has historically been very difficult to benchmark the effectiveness of the second line function."

In 2015 the Risk Management Society (RIMS) stated that: "One of the greatest advantages to forming a risk committee is its ability to help create a more risk-aware culture throughout the organisation."

It added: "With most or all of the business operations represented on the risk committee, communication about new projects, initiatives and information about other departmental exposures creates a more informed workforce, as well as one that incorporates risk management practices into daily routines."

Principles and guidance

The guidance provides an agreed benchmark for "what good looks like". It is based on eight principles for setting up and running an effective risk committee and nine principles to achieve a robust risk function, as outlined below.

© Chartered Institute of Internal Auditors

Principle	Description
A1. Board Accountability	The board risk committee is primarily an advisory committee to the board. Its aim is to facilitate focused and informed board discussions on risk-related matters. The board retains ultimate accountability for the organisation's principal risks and for the overall effectiveness of its risk management arrangements.
A2. Composition & Membership	The board risk committee should be formed of independent non-executive directors and apply UK Corporate Governance Code guidance on chair, composition, succession and evaluation criteria.
A3. Risk strategy & Risk appetite	The board risk committee should provide the board with advice on the continued appropriateness of the board-set risk strategy and risk appetite in light of the organisation's stated purpose, values, risk culture expectations, corporate strategy and strategic objectives.
A4. Principal risks & Continued viability	The board risk committee should assess and advise the board on the organisation's principal and emerging risks and how these may affect the likely achievement of the organisation's strategic objectives and continued viability of its business model.
A5. Risk culture & Remuneration	The board risk committee should monitor and periodically advise the board on the overall effectiveness of the organisation's risk management and internal control systems.
A6. Risk information & Reporting	The board risk committee should assess and advise the board on the quality and appropriateness of the organisation's risk information and reporting.
A7. Risk management & Internal control systems	The board risk committee should consider and periodically report to the board as to whether the organisation's purpose, values and board-approved risk culture expectations are appropriately embedded in the organisation's risk strategy and risk appetite, and are reflected in observed behaviours and decisions.
A8. Chief risk officer & Risk function independence	The board risk committee should safeguard the independence and objectivity, and oversee the performance, of the chief risk officer and the second line risk function.

In reference, the Risk Coalition "strongly encourages organisations to continually innovate and improve their practices, going beyond the minimum necessary wherever possible".

© Chartered Institute of Internal Auditors

Principle	Description
B1. Independent risk oversight	The chief risk officer, supported by the risk function, is responsible for ensuring robust, independent oversight and challenge of risk-taking activities across the organisation.
B2. Independent perspective	The chief risk officer and members of the risk function should maintain an independent and objective perspective.
B3. Risk governance	The chief risk officer should be of appropriate standing to provide effective challenge at both executive and board level.
B4. Risk reporting	The chief risk officer should provide the board risk committee with appropriate assurance that executive management's reporting of risks is both complete and fairly stated.
B5. Corporate strategy & objectives	The chief risk officer should ensure appropriate consideration of risk during corporate strategy, strategic objective setting and business planning discussions.
B6. Risk function independence & effectiveness	The chief risk officer should ensure the independence and effectiveness of the risk function.
B7. Risk culture	The risk function should monitor, assess and periodically report to executive management and the board risk committee on the organisation's risk culture.
B8. Innovation & change	The risk function should support the organisation in identifying and adapting effectively to material changes or developments in the internal or external environment.
B9. Group risk functions	The group chief risk officer should ensure that risk management arrangements operating across the group are appropriate and effective

© Chartered Institute of Internal Auditors

Considerations for internal audit

Audit leaders in the financial service sector will recognise much of the content as existing good practice. The guidance standardises and formalises expectations so even if your organisation is reasonably risk mature, it is worth checking the detail.

Audit leaders in other sectors should note that even where risk maturity is still evolving, once the scope is extended beyond financial services, the guidance should also be applied for audit or audit and risk committees where no dedicated board risk committee exists.

The table below identifies where internal audit is specifically mentioned and suggests questions to consider in respect of the relationship of internal audit to chief risk officers (CRO) and the risk committee outlined in the guidance.

Guidance Paragraph	Internal Audit Considerations
12 - chief audit executive should have a standing invitation to the risk committee	• Does this happen already? • If not, what do you see as the barriers? • Can internal audit be effective at the risk committee?
56 - the chief audit executive must not report to the chief risk officer	• What dialogue does a CAE with responsibility for risk management need to have with the board/audit committee? • Could this statement devalue the CAE role for stakeholders? • Do CAEs need to reinforce that their reporting line is to the audit committee chair?
81 - risk function to share its plan (the risks) with internal audit for comment	• How effective has this been to date? Does it happen? • Is the risk function able to produce a quality plan? • What role should internal audit have the identification of risk?
82 - risk function to coordinate planned work with internal audit	• How integrated is the assurance programme across the three lines of defence in your organisation? • Is coordination to maximise value and efficiency a sustainable model or could it compromise assurance? • Is your audit plan adaptive to new and emerging risks?
82 - risk function to share results of work with internal audit	• Should internal audit rely on the work of the risk function? • Could resource be shared between the two functions? • How will independence be maintained?
82 - chief risk officer maintains open and constructive relationship with chief audit executive	• How effective is the relationship today? • Could there be unintended consequences on independence? • What is the audit committee chair's perspective on this?

In addition to these points, the guidance emphasises the importance of the three lines of defence model: commonly used in the financial services sector.

The guidance assumes but does not require that organisations operate the three lines of defence model. Under this model, which you will be familiar with:

- First line management is responsible for risk-taking. Management therefore owns the organisation's risks and is responsible for managing them in line with the organisation's risk strategy and risk appetite.
- The second line is responsible for providing robust, independent oversight and challenge of first line risk-taking, but is not responsible for managing the organisation's risks.
- The third line (internal audit) is responsible for providing independent assurance over the organisation's governance, risk and internal control arrangements.

Within this section it states that the internal audit function should provide the board risk committee with:

© Chartered Institute of Internal Auditors

- Insight on risks
- Details of significant control weaknesses and audit findings
- Themes/trends to aid understanding of the organisation's principal risks, overall residual risk profile and risk capacity
- Periodic assessment of the quality and reliability of first and second-line risk reporting.

Audit leaders might wish to consider how existing reporting formats meet such requirements. Important questions worth asking include:

Could reporting be enhanced to provide this information now as it is considered good practice?

Do you have the resource to audit risk reporting in the first and second line?

Is this a conversation to have sooner rather than later?

Thoughts for audit committees

Audit leaders should ensure that their audit committee chair is aware of this guidance.

Independence

It raises familiar discussion topics such as the need to assert CAE independence through appropriate reporting lines, membership of the executive and attendance at strategy meetings.

The guidance (paragraph 61) states that the CRO should have a standing invitation to the audit committee. Effort may also be required to ensure that the CAE role is not be perceived as being a subordinate to that of the CRO.

Reports and information

As outlined earlier, internal audit has reporting requirements for the risk committee. There is a risk of potential information overlap or omission between the risk and audit committee which the CAE must manage. There is also the possibility that the CAE and CRO will present different versions of the truth to the committee.

Points for consideration include:

Will reports be previewed to resolve any conflicts or addressed in the meeting?

How does the risk maturity of the organisation sit with this?

Is there clarity over the information required at different governance meetings?

The guidance is a timely reminder for all audit leaders to evaluate their reporting packs. And, in doing so, you should ask yourself this:

Is there differentiation between assurance opinions and risk information?

Does it fit the current governance arrangements?

Does it enhance decision-making?

Risk culture

© Chartered Institute of Internal Auditors

Perhaps not surprisingly the topic of risk culture is also included in the guidance under Principle B7. The risk function should monitor, assess and periodically report to executive management and the board risk committee on the organisation's risk culture. There is a requirement for at least annually, the risk function to provide executive management and the board risk committee with a thematic analysis of the organisation's risk culture based on the consolidated results of its risk culture monitoring and make recommendations for improvement. Where appropriate, the results of the risk function's thematic analysis may be combined with the results of risk culture monitoring performed by the first and third lines.

External audit

The CRO role operates at the same level as the CAE and is required to have access to the same stakeholders, in particular external audit.

From the perspective of the organisation, there are complexities and sensitivities in managing the relationship with external audit.

How should internal audit manage the relationship going forward?

Is it prudent to have joint meetings?

What level of transparency does the audit committee chair expect in the relationship?

What different dynamics does the CRO bring to the table?

Closing thoughts

The guidance clearly outlines best practice for risk governance and further enhances risk maturity within the organisation. It does not however guarantee effective risk management. Ideally, the guidance will prompt dialogue in all sectors, raising expectations and driving action. What are you doing to support the risk governance framework? Does your audit plan provide sufficient assurance on risk management?

"The committee should seek to evidence appropriate values and behaviours at all meetings but more importantly experience first-hand the cultures and environments in operational activities by 'walking the floor'".

Fraser White Chair, Insurance Internal Audit Group

© Chartered Institute of Internal Auditors