KPMG

Oversight of risk

Audit Committee Questions
Audit Committee Institute part of KPMG Board Leadership Centre

Companies have become much more risk conscious and their management and oversight more risk-driven. Not surprisingly, the audit committee's time commitment in this respect has increased substantially over the last few years. A thorough review of the effectiveness of the audit committee's review process deserves a dedicated place on its agenda.

Operational risks | **Reputation risks** | **Financial risks** | **IT and Cyber risks** | **Emerging risks**

Audit committee oversight essentials …

Reviewing the effectiveness of internal control and risk management systems is an essential part of the board's responsibility but the review work is often delegated to the audit committee. The audit committee's precise role in the review process will depend upon factors such as the size and composition of the board; the scale and complexity of the company's operations, and the nature of the significant risks the company faces.

A company's risk management and internal control system should be designed to effectively manage the risks that threaten the achievement of the company's objectives. To this end, a company needs to (1) identify its objectives and assess the risks that threaten the achievement of those objectives, (2) design internal controls and strategies to manage/mitigate those risks and (3) monitor the controls and strategies to help ensure that they are operating effectively.

The audit committee should review the process by which the company's significant risks are identified and ensure that the board is fully apprised of the significant risks facing the business. It is important to ensure that the risk identification process:

- has a sufficiently broad perspective – external risks such as macroeconomic risks as well as internal risks such as weak controls.
- Is dynamic – the importance of giving due consideration to both those risks "flying under the radar" and early warning indicators.
- extends sufficiently far into the future – including consideration of various risk scenarios and "what-if's".

When assessing the company's risk processes, the audit committee should help ensure that proper consideration is given to the underlying gross risks (i.e. before any form of control or mitigation) and not merely to the net risks (i.e. after controls have been exercised). For each identified risk, a value judgment must be made as to the impact it would have and the likelihood of the risk occurring. It is particularly important to consider the reputational impact as well as the direct financial or operational impact (The effect on a company's reputation may have a far greater cost than the perceived initial impact).

Internal controls should be used to maintain the risks facing the company within the defined risk tolerance levels set by the board, bearing cost-benefit considerations in mind. The audit committee should be satisfied that proper control policies, procedures and activities have been established and are operating as intended.

Successful risk management requires the right tone set at the top of the company – the board and audit committee should send out a clear message that risk and control responsibilities must be taken seriously.

Indications that risk information is weak and therefore the system of internal control is compromised

Symptom	Warning signs
Risk information is produced, but not used	- Strategies, plans, budgets and processes do not change as new risks emerge
Inconsistent risk data is delivered from a number of competing risk functions	- There is no single, accepted risk process and management cannot give a united, single view of risk
The risks on the register do not reflect business reality	- Risk assessments rarely change
Risk information is not escalated to the right person at the right time	- Lack of strategic or emerging risks - Risks are materialising, but were not on the risk register
Quantity has the upper hand over quality	- Risk reports run to many pages, and are in fact risk registers - There is little analysis of key themes or interactions between risks

Key questions for audit committees to consider:

Risk identification and assessment

- Can management articulate a clear understanding of (say) the 5-10 major risks within the company?
- What are the company's key business objectives? Do these objectives include measurable performance targets and indicators?
- How is the company's risk strategy linked to the key business objectives?
- Do management and others have a clear understanding of the company's risk appetite? What risks are acceptable?
- What information sources are used to define the key risks facing the company? Are internal and external forces being considered?
- How is risk information consolidated and presented and does this provide consistent visibility of the key risks across the company?
- Are the criteria to evaluate the impact and probability of the identified risks meaningful, and aligned with the company's specifications (e.g. amount of turnover, number of employees, etc.)?
- What processes are in place to identify emerging risks affecting objectives and the related changes in risk prioritization?
- Does the company have a proactive approach to improving risk management processes?
- Are interrelationships of risks clearly identified, understood and integrated in risk assessment procedures?
- Does the company have the right risk professionals and are they integrated with both operations and assurance functions?
- Is the company's risk management policy clearly articulated and communicated throughout the company?

Risk mitigation

- Does management have clear strategies for managing the significant risks that have been identified? What kind of assurance is obtained that risk mitigating systems, policies, processes and controls are working effectively?
- To what extent are costs of strategies and action plans evaluated against benefits and incremental risks exposure?
- Does the company's culture, code of conduct, human resource policies and incentive systems support its objectives and the risk management and internal control system?
- Does the company have one view of risk, a common language that drives effective risk management actions and decisions?
- Is authority, responsibility and accountability defined clearly such that decisions are made and actions taken by the appropriate people? Are the decisions and actions of different parts of the company appropriately coordinated?
- Do employees have the knowledge, skills and tools to effectively manage risk?
- Are there formal reporting and/or key risk indicators set up to monitor the key risks and mitigating actions? Does this reporting provide consistent visibility of the key risks across the organization?
- How are processes/controls adjusted to reflect new or changing risks or operational deficiencies?
- How does risk management information influence key decision making? Who prepares this information?

www.kpmg.com/globalaci