Deloitte.

Sample risk committee charter

This sample risk committee charter is based on leading practices observed by Deloitte in the analysis of a variety of materials.

It is important to note that the Risk Committee Resource Guide practices are drawn from Deloitte experiences and our understanding of practices currently being used.

This template is designed for South African public companies; exceptions to the requirements noted below may apply for certain issuers, including investment companies, small-business issuers, and foreign private issuers. All companies should consult with legal counsel regarding the applicability and implementation of the various requirements identified. Further, this template should be tailored on a company-by-company basis to meet the needs and specific situations for each company utilising the tool.

Sample risk committee charter

I. Purpose and authority

The risk committee is established by and among the board to properly align with management as it embarks a risk management program. The primary responsibility of the risk committee is to oversee and approve the company-wide risk management practices to assist the board in:

- Overseeing that the executive team has identified and assessed all the risks that the organisation faces and has established a risk management infrastructure capable of addressing those risks
- Overseeing, in conjunction with other board-level committees or the full board, if applicable, risks, such as strategic, financial, credit, market, liquidity, security, property, IT, legal, regulatory, reputational, and other risks
- Overseeing the division of risk-related responsibilities to each board committee as clearly as possible and performing a gap analysis to determine that the oversight of any risks is not missed
- In conjunction with the full board, approving the company's enterprise wide risk management framework

The risk committee may have the authority to conduct investigations into any matters within its scope of responsibility and obtain advice and assistance from outside legal, accounting, or other advisors, as necessary, to perform its duties and responsibilities.

In carrying out its duties and responsibilities, the risk committee shall also have the authority to meet with and seek any information it requires from employees, officers, directors, or external parties. In addition, the risk committee could make sure to meet with other board committees to avoid overlap as well as potential gaps in overseeing the companies' risks.

The risk committee will primarily fulfil its responsibilities by carrying out the activities enumerated in Section III of this charter.

II. Composition and meetings

The risk committee will comprise three or more directors as determined by the board. The membership will include a combination of executive and non-executive directors. The committee may include non-directors as members. Each member will have an understanding of risk management expertise commensurate with the company's size, complexity and capital structure.

The risk committee will provide its members with annual continuing education opportunities and customised training focusing on topics such as leading practices with regard to risk governance and oversight and risk management.

Committee members will be appointed by the board. Unless a chairperson is elected by the full board, the members of the committee may designate a chairperson by majority vote. Additionally, the risk committee, in conjunction with the full board and with the nominations committee, may do well to consider and plan for succession of risk committee members.

The risk committee will report to the full board. The risk committee will consider the appropriate reporting lines for the CEO, the company's chief risk officer (CRO) and the company's management-level risk committee - whether indirectly or directly - to the risk committee.

The committee will meet at least quarterly, or more frequently as circumstances dictate. The committee chairperson will approve the agenda for the committee's meetings, and any member may suggest items for consideration. Briefing materials will be provided to the committee as far in advance of meetings as practicable.

Each regularly scheduled meeting will begin or conclude with an executive session of the committee, absent members of management. As part of its responsibility to foster open communication, the committee will meet periodically with management, heads of business units, the CRO (if applicable), the chief audit executive (director of the internal audit function), and the independent auditor in separate executive sessions.

III. Responsibilities and duties

To fulfil its responsibilities and duties, the risk committee will:

Enterprise responsibilities

- Help to set the tone and develop a culture of the enterprise vis-à-vis risk, promote open discussion regarding risk, integrate risk management into the organisation's goals and compensation structure, and create a corporate culture such that people at all levels manage risks rather than reflexively avoid or heedlessly take them
- Provide input to management regarding the enterprise's risk appetite and tolerance and, ultimately, approve risk appetite and the statement of risk appetite and tolerance messaged throughout the company and by line of business
- Monitor the organisation's risk profile - its on-going and potential exposure to risks of various types
- Approve the risk management policy and plan. Management should develop both the risk management policy and the plan for approval by the committee. The risk management plan should consider the maturity of the risk management of the company and should be tailored to the specific circumstances of the company. The risk management plan should include:
  - the company's risk management structure
  - the risk management framework i.e. the approach followed, for instance, COSO, ISO, IRMSA ERM Code of Practice, etc.
  - the standards and methodology adopted – this refers to the measureable milestones such as tolerances, intervals, frequencies, frequency rates, etc.
  - risk management guidelines
  - reference to integration through, for instance, training and awareness programmes, and
  - details of the assurance and review of the risk management process.

  The risk management policy should set the tone for risk management in the company and should indicate how risk management will support the company's strategy. The risk management policy should include the compa¬ny's definitions of risk and risk management, the risk management objectives, the risk approach and philosophy, as well as the various responsibilities and ownership for risk management within the company.
- The committee should review the risk management plan at least once a year.
- Define risk review activities regarding the decisions (e.g. acquisitions), initiatives (e.g. new products), and transactions and exposures (e.g. by amount) and prioritise them prior to being sent to the board's attention
- Review and confirm that all responsibilities outlined in the charter have been carried out
- Monitor all enterprise risks; in doing so, the committee recognises the responsibilities delegated to other committees by the board and understands that the other committees may emphasise specific risk monitoring through their respective activities
- Conduct an annual performance assessment relative to the risk committee's purpose, duties, and responsibilities; consider a mix of self- and peer-evaluation, supplemented by evaluations facilitated by external experts
- Oversee the risk program/interactions with management
- Review and approve the risk management infrastructure and the critical risk management policies adopted by the organisation
- Periodically review and evaluate the company's policies and practices with respect to risk assessment and risk management and annually present to the full board a report summarising the committee's review of the company's methods for identifying, managing, and reporting risks and risk management deficiencies

- Continually, as well as at specific intervals, monitor risks and risk management capabilities within the organisation, including communication about escalating risk and crisis preparedness and recovery plans
- Continually obtain reasonable assurance from management that all known and emerging risks have been identified and mitigated or managed
- Communicate formally and informally with the executive team and risk management regarding risk governance and oversight
- Discuss with the CEO and management the company's major risk exposures and review the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies
- Review and assess the effectiveness of the company's enterprise-wide risk assessment processes and recommend improvements, where appropriate; review and address, as appropriate, management's corrective actions for deficiencies that arise with respect to the effectiveness of such programs
- Monitor governance rating agencies and their assessments of the company's risk and proxy advisory services policies, and make recommendations as appropriate to the board
- In coordination with the audit committee, understand how the company's internal audit work plan is aligned with the risks that have been identified and with risk governance (and risk management) information needs

Reporting

- Understand and approve management's definition of the risk-related reports that the committee could receive regarding the full range of risks the organisation faces, as well as their form and frequency
- Respond to reports from management so that management understands the importance placed on such reports by the committee and how the committee views their content
- Read and provide input to the board and audit committee regarding risk disclosures in financial statements and other public statements regarding risk
- Keep risk on both the full board's and management's agenda on a regular basis
- Coordinate (via meetings or overlap of membership), along with the full board, relations and communications with regard to risk among the various committees, particularly between the audit and risk committees
- Disclose in the company's Integrated Report how it has satisfied itself that risk assessments, responses and interven¬tions are effective

Charter review

- Review the charter at least annually and update it as needed to respond to new risk-oversight needs and any changes in regulatory or other requirements
- Review and approve the management-level risk committee charter, if applicable
- Perform any other activities consistent with this charter, the company's bylaws, and governing laws that the board or risk committee determines are necessary or appropriate
- Submit the charter to the full board for approval

Queries:

Dr Johan Erasmus – jerasmus@deloitte.co.za

Designed and produced by Creative Services at Deloitte, Johannesburg. (807474/dbn)

Previous