The Governance Institute

Sample Committee Charter:
Enterprise Risk Management Committee[1]

Purpose

The principal purpose of this committee is to task management with the development of a risk management program, oversee and approve the organization-wide risk management practices, and assist the board in ensuring that the risk management infrastructure is capable of addressing risks faced by the organization.

Responsibilities

In fulfilling its charge, the enterprise risk management committee is responsible for the following activities and functions:

- Help to set the tone and develop a culture of the enterprise vis-à-vis risk, promote open discussion regarding risk, and integrate risk management into the organization's strategic goals and compensation structure.
- Provide input to management regarding the enterprise's risk capacity and tolerance and approve the statement of risk capacity and tolerance developed by management.
- Monitor the organization's risk profile—its ongoing and potential exposure to risks of various types.
- Approve the risk management policy, plan, infrastructure, and framework developed by management. The risk management plan should include:
    - The organization's risk management structure
    - The risk management framework and/or approach
    - The standards and methodology adopted—measurable milestones such as tolerances, intervals, frequencies, frequency rates, etc.
    - Risk management guidelines
    - Details of the assurance and review of the risk management process
- 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 or service lines), and transactions and exposures (e.g., by amount) and prioritize them prior to being sent to the board's attention.
- Regularly review information provided by the Chief Information Security Officer (or top executive responsible for cybersecurity) to assess the organization's risk profile for cyber attacks and sufficiency of management's handling of data storage, security protocols, and response to cyber attacks.

---

[1] This committee charter was adapted from a sample corporate risk committee charter based on leading practices developed by Deloitte, with input from Hunterdon Healthcare and ACCORD LIMITED.

- Conduct an annual performance assessment relative to the risk committee's purpose, duties, and responsibilities.
- Oversee and assess the risk program/interactions with management and obtain regular assurance from management that all known and emerging risks have been identified and are being mitigated/managed.
- Periodically review and evaluate the organization's policies and practices with respect to risk assessment and risk management, including the effectiveness of management's corrective actions for deficiencies that arise, and annually present to the full board a report summarizing the committee's review of the organization's methods for identifying, managing, and reporting risks and risk management deficiencies.
- 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 organization's internal audit work plan is aligned with the risks that have been identified.
- Perform an annual committee self-assessment; review the committee charter and advance recommendations for any changes to the board for approval.

Composition

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 organization's size, complexity and capital structure. The chief risk officer or senior executive in charge of risk will serve as staff for the committee.

Recommended skills and competencies:

- Laws and regulatory policy
- Legal implications related to risk management
- Enterprise risk concepts in relation to the healthcare industry and the organization itself
- Familiarity with identification of risk and insurance models
- Conflicts of interest and confidentiality

Meeting Schedule

Quarterly or as needed.