Australian Institute of Company Directors

ORGANISATION

# Risk committee charter

The risk committee assists the board in the oversight of the company's risk management policies and processes.

Principle 7 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*[1] (ASX Principles) states: "A listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework".

The ASX Principles suggest that the role of a risk committee is usually to review and make recommendations to the board in relation to:

- the adequacy of the entity's processes for managing risk;
- any incident involving fraud or other break down of the entity's internal controls; and
- the entity's insurance program, having regard to the entity's business and the insurable risks associated with its business.

Where a company does not have a risk committee, then the audit committee may be tasked with exercising that function and thereby have the responsibilities of a risk committee.[2]

The charter should clearly articulate the committee's role and responsibilities, composition, structure and membership requirements, authority, processes and procedures, as approved by the board. It should also be customised to the needs of the company and reflect its industry, objectives and culture.

For smaller corporations, a combined audit/risk committee is sometimes established. In such a case, the committee's charter will be a combined responsibility to oversee and monitor both functions. Where the entity does not have a risk committee, or a combined committee that satisfies the objectives set out in the ASX Principles, then it is essential that the entity disclose that fact as well as identify the processes that it employs for overseeing the entity's risk management framework.

The sample risk committee charter below is an example of what might be included in a charter.

1. ASX Corporate Governance Council, 2019, *Corporate Governance Principles and Recommendations*, 4th edition, February, **https://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-fourth-edn.pdf**, (accessed 8 May 2019).
2. Refer to the AICD Director Tool *Audit committee charter*

## Points to consider

- The charter ought not be overly detailed or prescriptive, however it ought to contain sufficient power to ensure it can perform its role, notably to have access to information that includes access to management and both internal and external auditors and their reports.
- Consider establishing a formal process to ensure that the charter is regularly monitored and reviewed, so that it remains relevant to the company's needs, reflects current regulatory requirement and risk committee good practice, including maintaining its independent status.
- Refer to the company's code of conduct for expected behaviours and processes, including resolving conflicts of interest.

## Responsibilities of the risk committee

The risk committee will carry out the following responsibilities:

### General risk oversight and monitoring

- Ensure that it is has a charter for the committee; that the committee members are disclosed; and, that at the end of each reporting period, the number of times the committee met throughout that period, along with member attendance, is disclosed.
- Recognise that risk management is essential for effective governance and to enable the committee to be an efficient and effective mechanism in ensuring transparency, focus and independent judgment necessary for sound risk management.
- Review the company's risk appetite and risk tolerance, as determined by the board on a holistic enterprise-wide basis, and with respect to relevant categories of operational risk.
- Review and assess the various categories of risk faced by the company, including any concentrations of risk and interrelationships, between risks.
- Review and assess the likelihood of occurrence, severity of impact of those risks, and any mitigating measure affecting those risks.
- Review the responsibility for risk oversight and management of specific risks to ensure a common understanding of accountabilities and roles.
- Review the risk treatment and mitigation policies and procedures developed by management, including procedures for periodic and critical reporting of matters to the board and risk committee.
- Review management's implementation of the company's risk treatment and mitigation policies and procedures, to assess compliance and effectiveness.
- Review the quality, type and presentation of risk-related information provided to the board.
- Review the objectivity of the company's risk management function and the processes for resolution of differences that might arise.

> The charter should clearly articulate the committee's role and responsibilities, composition, structure and membership requirements, authority, processes and procedures, as approved by the board. It should also be customised to the needs of the company and reflect its industry, objectives and culture.

- Review the utility, effectiveness and efficiency of the company's risk management function in the context of the company's size, scale, complexity and scope of operations, including ensuring that the committee understands and receives from management reports on new and emerging sources of risk and the risk controls and mitigation measures that management has put in place to deal with those risks.
- Review how the company's risk management policy and strategy is communicated throughout the company to ensure it is embedded as part of the company's corporate culture and to make recommendations to the board in relation to changes that will improve the entity's risk management or appetite in line with the board's aims.
- Review internal communication and control systems to encourage the timely flow of risk related information to personnel, including the approval of the internal audit plan and review of the entity's ability to manage risk based on reports from the internal audit.
- Review reports to management, external auditors, internal auditors, legal counsel, regulators and consultants, as appropriate, regarding the risks the company faces and the company's management of those risks, including whether the entity is operating within the risk appetite set by the board.
- Review material incidents, including fraud or breakdown of the entity's risk controls and review the lessons learned from same and review and understand that the entity's insurance program is aligned with the entity's business and insurable risks associated with the business.

From time to time it might be necessary for an entity to operate outside of its risk parameters and that is a matter that ought to be disclosed to the board.

### Internal control and risk management

Recommendation 7.2 of the ASX Principles states that the board or its risk committee ought to review the entity's risk management at least on an annual basis to ensure that the entity is operating within the board's set risk parameters and appetite; and, to disclose that this review has taken place.

From time to time it might be necessary for an entity to operate outside of its risk parameters and that is a matter that ought to be disclosed to the board. Identification, understanding of, and operationalisation of strategies to deal with emerging risks, including those relating to technological disruption and privacy.

- Assess the internal process for determining and managing key risk areas, particularly:
  - compliance with laws, regulations, standards and best practice guidelines;
  - important judgments and accounting estimates;
  - litigation and claims;
  - fraud and theft.
- Address the effectiveness of the internal control, risk management and performance management systems with management and the internal and external auditors.
- Assess effectiveness of, and compliance with, the corporate code of ethical conduct and compliance with internal plans, policies and procedures.
- Obtain regular updates from the management and company lawyers about compliance matters.
- Ensure the CEO (or equivalent) and the CFO (or equivalent) are reasonably able to state that their declarations under S.295A of the *Corporations Act 2001*, relating to financial statements and reports of the company, are founded on a sound system of risk management and internal control, and that the system is operating effectively in all material respects in relation to the financial reporting risks.

### Risk transfer and insurance

- Review how certain risks of the company have been mitigated by risk transfer strategies.
- Review and analyse the extent to which any risk transfer strategies give rise to new risks which may be material.
- Review the company's insurance arrangements including:
  - type of cover;
  - scope of cover;
  - duration of cover;
  - adequacy of cover;
  - cost of cover;
  - terms and conditions of cover including exclusions and limitations; and
  - counter party risk of insurer, including through engaging professional insurance broker services.

### Corporate governance

- Assist the board to ensure appropriate corporate governance is in place within the scope of its remit.
- Ensure that the internal audit function is clearly set out and understood within the entity.
- Disclose any material exposure to environmental or social risks and the strategy for managing same.

### Other responsibilities

- Perform other activities related to this charter as requested by the board.
- Institute and oversee special investigations as needed.
- Review and assess the adequacy of this charter annually, requesting board approval for changes and ensuring appropriate disclosure, as may be required by law or regulation.
- Confirm annually that all responsibilities outlined in this charter have been carried out.
- Regularly evaluate the performance of the risk committee and its members.

## SAMPLE RISK COMMITTEE CHARTER

### Role and responsibilities

The risk committee assists the board in carrying out its duties by providing independent and objective review, advice and assistance in developing board policy and monitoring corporate activity within the scope of its remit and making recommendations to the board for resolution. It is not a policy making body, nor does it have substantive executive function in its own right.

The role of the committee includes assisting the board in the company's governance and exercising of due care, diligence and skill in relation to risk assessment, treatment strategies and monitoring.

Consistent with the company's determined appetite for risk, it includes assisting the board to understand risks, that may:

- impede the company from achieving its goals and objectives;
- impact on the company's performance;
- affect the health, safety or welfare of employees, visitors and others in relation to the company's operations;
- threaten compliance with the company's regulatory and legal obligations;
- impact on the community and the environment in which the company operates;
- impact on the company's reputation and that of its people; and
- result in personal liability for company officers arising from the company's operations.

### Other committee objectives

The company's risk policy objectives will be achieved by company-wide implementation of effective risk identification, management and mitigation programs, including:

- monitoring and reviewing issues that may impede the goals, objectives and performance of the company;
- maintenance of an enterprise risk management framework and appropriate operational risk management frameworks based on industry accepted standards;

SAMPLE RISK COMMITTEE CHARTER *continued*

- maintenance of internal control systems in order to provide accurate, relevant, timely and reliable financial and operational information;
- monitoring and reviewing safety systems throughout the company's operations;
- monitoring of operations and maintenance of records to ensure compliance with company policies and regulatory requirements;
- the reporting to the risk committee and board on significant circumstances and risk related issues, which may materially affect the company;
- implementation of management systems and loss prevention and control measures directed at managing the potential for loss and damage to the company;
- management of insurance programs to ensure appropriate coverage by reputable insurers at competitive premium levels with regard to the company's circumstance and need; and
- ensuring an appropriate risk-aware culture has been embedded throughout the company.

## Authority

The board authorises the risk committee, through the risk committee chair, to:

- retain independent risk, actuarial, insurance or other consultants to advise the risk committee or assist in the conduct of risk related issues; and
- seek any information it requires from employees, who are directed to co-operate with the risk committee's requests, or from external parties.

## Composition

The risk committee will consist of at least three, and usually no more than five, members of the board. The board, usually on the recommendation of its nomination committee, will appoint risk committee members and the chair of the committee.

Membership of the risk committee will be reviewed annually, and members are eligible for reappointment. Membership will be confirmed annually by the board in alignment with the annual general meeting.

The risk committee should comprise both non-executive and executive directors, although the majority should be non-executive independent directors. Members should be conversant with risk management principles and standards, with the majority of members having a sound understanding of the business, operations and affairs of the company and the industry in which it operates.

The chair of the committee must be non-executive and independent and should not also be the chair of the board.

## Invitees

Non-members may attend meetings by invitation of the risk committee, including the:

- chief executive officer;
- chief financial controller;
- company secretary;
- the head of internal risk or other person charged with compliance assurance; and
- chief operating officer.

These people may take part in the business of, and discussions at, the meeting but have no voting rights.

## Meetings

The risk committee will meet a minimum three times a year and, additionally, as the committee considers necessary.

A quorum will be more than half the members. In the chair's absence from a meeting, the members present will select a chair for that particular meeting.

All Risk committee members are expected to attend each meeting in person, or through other approved means, such as teleconference or video conference.

The risk committee may invite other people to attend as it sees fit and consult with other people, or seek any information it considers necessary, to fulfil its responsibilities.

The notice and agenda of a meeting will include relevant supporting papers.

SAMPLE RISK COMMITTEE CHARTER *continued*

### Voting

Any matters requiring decision, will generally be decided by consensus, or if consensus is not achievable, then by a majority of votes of members present.

### Conflicts of interest

Committee members will be invited to disclose conflicts of interest at the commencement of each meeting. Ongoing conflicts of interest need not be disclosed at each meeting once acknowledged. Where members or invitees are deemed to have a real or perceived conflict of interest, they will be excused from committee discussions on the issue where a conflict exists.

### Secretariat duties

The company secretary (or other appropriate designated person) will act as secretary to the risk committee. The secretary will assist the chair to develop and distribute agendas, papers, minutes and calendar.

### Minutes

Minutes must be prepared, approved by the chair and circulated to the members within two weeks of a meeting. They must be ratified and signed by the chair, at the next meeting of the committee.

### Reporting to the board

The chair of the risk committee is to report to the board following each committee meeting. Such reporting may be by distribution of a copy of the minutes, supplemented by other necessary information, including recommendations requiring board action and/or approval. The chair is to organise the supply of information regarding the risk committee and is to be included in the company's annual report.

### Reviews

The risk committee will review its performance on an annual basis. The review may be conducted as a self-assessment and will be coordinated by the chair. The assessment may seek input from any person. Training needs will be monitored by the chair.

The risk committee will review this charter and its composition annually, to ensure that it remains consistent with the board's objectives and responsibilities. The board should consider the committee's review and either approve or further review the committee's charter and/or composition.

## About us

The Australian Institute of Company Directors (AICD) is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and the not-for-profit (NFP) sectors.

For more information **t:** 1300 739 119 **w:** companydirectors.com.au



07236-3-23