Good Governance Guide

Risk governance

Governance Institute of Australia

Those exercising authority and making decisions within an organisation exercise power to facilitate the strategic objectives of the organisation. In achieving its strategic objectives each organisation will face a range of risks.

The International Standard for risk management ISO 31000:2018: Risk Management— Guidelines, defines risk as 'the effect of uncertainty on objectives'.[1] Accordingly, risk management is a critical area of responsibility for the board and a core component of a governance framework.

Risk governance is concerned with providing assurance to the board that risks are being effectively managed throughout the organisation. This includes the identification of contemporary and emerging risks, a risk-aware culture, effective communication of risks and alignment of risks to strategy.[2]

Organisations need to be aware of the need to consider risk at the forefront of their activities, both day-to-day and over the longer term; also decision-makers need to be knowledgeable about the need for a strategic risk focus as a specific consideration.

It is **good governance** for organisations to recognise and manage risk.[3]

Risk management is part of good corporate governance

Risk management is a critical area of responsibility for the governing body (the board) and a core component of a governance framework.

It is the role of the board to set the risk appetite for the entity, to oversee its risk management framework and to satisfy itself that the framework is adequate and that the organisation is operating with due regard to the risk appetite set by the board.

It is the role of management to design and implement that framework and to ensure that the entity operates within the risk appetite set by the board.

Risk management is the process by which risks are identified, assessed and treated within an organisation. Risk should be considered in terms of upside risk (opportunities) as well as downside risk (threats). Risk is a key governance function not only for the board, but also management and all employees.

It is **good governance** for organisations to design, implement and monitor systems and processes for providing oversight and implementation of the risk management function and its relationship to business value creation.

Risk appetite statements

The board is ultimately responsible for deciding the nature and extent of the risks it is prepared to take to meet objectives. The amount of risk an organisation is willing to accept in the pursuit of its objectives may be documented in a risk appetite statement.

An organisation's board should articulate its risk appetite, to: support decision-making, provide context to management in formulating strategy, and provide a basis for assessing risks requiring treatment.

An organisation's appetite for risk may be different for different categories of risk. For example, there may be a very low appetite for people risks, but a high appetite for growth.

There are links between strategy, risk and budget. Strategic plans should be prepared through the dual lenses of risk appetite and budget, or strategic objectives are unlikely to be able to be achieved.

For more information, refer to the *Good Governance Guide: Risk appetite statement*.

Risk management committees

Board committee

The ultimate responsibility for the oversight of risk management lies with the board. In exercising this responsibility, boards often establish committees with a focus on particular aspects of their governance responsibilities. Boards should consider if their risk oversight function should be delegated to a committee, in order to ensure that an appropriate amount of time

and skills are available to consider risk oversight issues. This may result in a board risk committee being formed or it may be incorporated into another committee such as the audit or finance committee.

Organisations may have more than one committee responsible for the oversight of different elements of risk, such as workplace health and safety, sustainability, investment and environmental impact. Where that is the case, it is important that the board maintains holistic oversight of those risks in aggregate.

For more information, refer to *Good Governance Guide: Issues to consider when constituting an audit and risk committee*.

Executive management committee

The executive management committee generally consists of the CEO and some or all of the CEO's direct reports. It may be called a management committee or an executive committee or an executive management committee, but regardless of title, the membership consists of key executives of the organisation or, where appropriate, key executives of business divisions.

The responsibility of an executive management committee is to make decisions on executing the board-approved strategic objectives in line with the risk appetite set by the board. The executive management committee will have responsibility to report on progress in achieving those strategic objectives. An executive management committee may have delegated authority from the CEO to make decisions within the organisation to deliver the strategic objectives.

Larger organisations may also establish an executive risk committee, which is usually chaired by the chief risk officer.

See *Good Governance Guide: Executive Management committees*.

Risk management committees

It is good governance for management to develop a risk management framework which is reviewed and approved by the board.

This may include:

- policy statement — see *Good Governance Guide Risk Management Policy*
- definitions (risk dictionary)
- functions and delegations
- adopted risk management Guidelines (such as those described in *ISO 31000:2018: Risk Management — Guidelines*).

Larger organisations may also develop risk policies that address specific risks, or are developed at subsidiary level. In these cases, the risk management policy of the parent entity is the overarching one.

Risk register

It is good governance for risks to be recorded in a risk register, which is essentially a table of risks. Information about individual risks may include:

- risk category
- risk ID
- risk description
- risk analysis
- risk controls
- actions.

A risk register should be a dynamic tool and subject to continuous review to ensure it reflects the risks of the organisation in real time.

Risk frameworks to consider

When considering how best to approach the development of a risk management framework for the organisation, reference may be made to:

- *ISO 31000:2018 Risk Management Guidelines* and the related handbook, *HB 436:2004 Risk management guidelines — Companion to AS/NZS ISO 31000:2009*
- ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations*, Principle 7: Recognise and manage risk, 4th ed, 2019
- *Prudential Standard CPS 220 Risk Management*, Australian Prudential Regulatory Authority, effective 1 July 2019
- *Commonwealth Risk Management Policy*, Commonwealth Department of Finance, July 2014
- State-based expectations, for example, TPP 15-03, Internal Audit and Risk Management Policy for the NSW Public Sector, Version 1.0, NSW Treasury, July 2015.

Risk governance structure

There is no one-size-fits-all approach to how an organisation manages risk. The following table sets out a possible functional structure and highlights roles to be considered.

Board
Responsible for oversight and monitoring of the risk management framework, reviews and approves the overall risk management strategy, including setting the organisation's risk appetite within which it expects management to operate.
Board risk management committee
The board may delegate responsibility to a risk management committee to develop and recommend the risk appetite and review and oversee recommended risk management frameworks, policies and procedures. The committee is responsible for monitoring and anticipating changes in the market, industry and community in which the organisation operates.
Executive management committee
The executive management committee is responsible for identifying trends and emerging risks and opportunities facing the organisation, as well as championing an effective risk management culture within the organisation. There may also be an executive risk committee.
Risk management function
Risk management is responsible for designing and implementing a board approved risk management framework that meets the organisational context, supporting line management to embrace and adhere to the framework, conducting independent assurance and providing timely information to the executive and board.
Compliance function
Compliance is responsible for ensuring a robust compliance system is in place to provide additional assurance that compliance risks are being effectively managed and legislation, regulations, standards, policies and contractual obligations are being met. It is important that the compliance function works in close alignment with the risk management function.
Internal audit function
Internal audit is responsible for making recommendations to improve the internal control framework operating within the orgwanisation. It is good governance for internal audit to be independent of the risk management function.
External audit function
External audit is responsible for providing assurance that financial statements are prepared accurately and in accordance with legislation and standards.

Notes

1. *ISO 31000:2018: Risk Management — Guidelines.*
2. See Managing Culture — *A Good Practice Guide, Governance Institute of Australia, 2017.*
3. See *Corporate Governance Principles and Recommendations, 4th edition, Principle 7.*