Good Governance Guide

Risk management overview

Governance Institute of Australia

Recognise and manage risk

It is **good governance** for an entity to ensure that all directors and senior executives have a shared understanding of risk, which is the effect of uncertainty on an entity achieving its strategic objectives and maintaining its long-term viability and reputation.

The board is responsible for the informed oversight of risk management within the entity and should regularly review and approve the risk management policies and framework. Management is responsible for developing and implementing a sound system of risk management and internal control.

The entity needs to determine the material business risks that it faces, which may include but are not limited to financial reporting, operational (liquidity, interest rate risk, investment risk, commodity prices, project management, supply chain for example), sovereign/political, environmental, sustainability, digital/online and technological, compliance, strategic, ethical conduct, reputation or brand, product or service quality, human capital and market-related risks. Risk management policies need to reflect the entity's risk appetite and tolerance levels as determined by the board, and the directors and senior executives need to have clarity as to the level of risk that the entity is prepared to take in achieving its strategic objectives.

A risk management policy is a document that identifies an entity's approach and direction in relation to risk management. Within this context, it is **good governance** when developing a policy on risk management to consider the following issues:

- the entity's strategy
- the material business risks it faces and its tolerance levels for those risks
- shareholder and stakeholder expectations
- the regulatory framework within which the entity operates
- organisational capacity in relation to managing and monitoring the material business risk that the entity faces and the environment within which the entity operates, that is, does the entity have the relevant resources, skills and time to make such a risk assessment? Entities will need to consider if the assessment of organisational capability needs to be undertaken internally or externally or both
- the extent to which the entity can adapt to changing industry and market conditions and emerging risks (taking into account that 'big' picture, 'black swan' issues may emerge)
- crisis management
- how the entity will monitor and manage risks that arise
- the ability of the organisation to report to the board the management of risk in a timely and reliable manner (consideration needs to be given to the requirement of the board to report against Principle 7: Recognise and Manage Risk of the ASX Corporate Governance Council's *Principles and Recommendations of Corporate Governance*)

A risk management framework defines an entity's processes for managing risk including the implementation, monitoring, reviewing and improvement of risk management. The entity needs to determine whether the risk function can be undertaken internally or requires external support. In addition, consideration should be given as to whether an internal audit function is required and, if so, its interaction with the management of risk within the entity.

When developing the framework, the entity should have regard to *ISO31000/2009: Risk Management Principles and Guidelines* and Principle 7: Recognise and Manage Risk of the ASX Corporate Governance Council's *Principles and Recommendations of Corporate Governance*. It is **good governance** when developing a framework for the management of risk to consider the following issues:

Board matters

- All directors upon induction and thereafter should understand the entity's business and the material business risks it faces.

- Risk forms part of an entity's governance processes with the oversight of risk being part of the regular process of the board.
- Accountability must be clear, for example, who reports to the board (it may be the CEO, or the Chief Risk Officer is one exists) — the size and nature of the entity will determine accountability.
- The processes are in place to ensure the effective reporting to the board so that the board can fulfil its oversight role and meet its disclosure requirements.

Delegations of authority

- The delegations of authority support and are complementary to the risk management framework.
- The entity needs to consider the role of committees and:
  - whether a dedicated risk management committee needs to be established or whether this function is to be combined with the audit committee's responsibilities — consideration of the needs of the entity will determine committee establishment
  - whether, in order to allow the CEO to discharge their responsibilities for risk management, they can establish internal risk management committees comprising key personnel as required.

Systems and monitoring

Management needs to:

- determine the systems that are required to effectively monitor and manage risks
- ensure that any system accommodates a robust response mechanism
- determine the reporting systems and internal controls that are required to effectively report on risk and risk mitigation strategies (and assess whether the reporting is geared to actions and improvements rather than merely noting instances of concern)
- consider the advantages and disadvantages of a certification process and whether it is feasible to implement such a process, taking into account the need for the board of listed entities to receive assurance from management as to whether all risks are being properly monitored and managed
- assess whether the risk assessment data is robust
- consider training programs.

Framework and standards

Management needs to assess:

- the framework to ensure it can take into account external reference points and is not purely internally-focused
- what crisis events are reasonably foreseeable and develop a framework that addresses those events
- how crisis management and business continuity plans interact with the control systems and have clear prior agreement on the respective roles of the chair and the chief executive in the event of a crisis
- whether the entity should have regard to the supplementary guidance to Principle 7 of the ASX Corporate Governance Council's *Principles and Recommendations of Corporate Governance* — this is particularly relevant to smaller and medium-sized entities.

Review

The entity needs to:

- consider the successes and failures of the framework in a regular review, including behaviours as well as metrics
- accommodate an external, independent review where necessary.

External reporting

- If the entity is listed, it must have regard to its continuous disclosure obligations under Listing Rule 3.1.
- If the entity is an authorised deposit-taking institution, it must have regard to its reporting obligations to the Australian Prudential Regulation Authority.
- The entity should be mindful of ongoing developments relating to ESG disclosures and integrated reporting, with consideration given as to how to link reporting on risk to discussions of strategy and the business model.

Compliance is a critical aspect of risk management. Refer to the Good Governance Guide: *Compliance*.

The overview of risk management is an ongoing process. The directors and senior executives of an entity should remain attentive to the business and its internal and external environment and continually monitor the risk management policy and framework.