Good Governance Guide

Risk framework

Governance Institute of Australia

Risk management

Managing risks is a complex task for any organisation but is necessary to ensure achievement of strategic objectives. It is **good governance** for an organisation to demonstrate leadership and commitment to managing risks by establishing and documenting a formal risk management framework, approved by the board.

There is no prescribed format for a risk management framework. However, guidance is available on developing risk management frameworks in regulatory standards, government department publications and other sources.

The primary risk management reference currently used in Australia defines the purpose of a risk management framework as 'assisting the organisation in integrating risk management into significant activities and functions'.[1]

The key components identified in the ISO guidelines are

- **Design** — when designing the framework an organisation should examine and understand its:
  - external context including: its operating environment, external stakeholders, contractual relationships and commitments and its networks and dependencies.
  - internal context including: vision, mission and values, strategy and objectives, culture, capabilities and internal stakeholders.
- **Implementation** — The framework should be implemented by an appropriately resourced plan including timelines that identifies decision points and accountability. An organisation should ensure that the arrangements for managing risk are clearly understood and practiced.
- **Evaluation** — The organisation should periodically evaluate the framework to determine whether it remains suitable for achieving its objectives.
- **Improvement** — The organisation should continually monitor and adapt the framework to address external and internal changes.
- **Integration** — risk management should be integrated into the governance of the organisation, including decision-making.

A well-designed, implemented and maintained framework will enable organisations to achieve a risk aware culture that is vital to consistently achieve goals within legal and ethical boundaries.

Designing a risk management framework

The systems for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating the risks facing an organisation as well as the structures, policies, processes and people supporting them, are collectively an organisation's risk management framework.

In some instances, organisations will include governance, risk and compliance in their model for a more holistic framework.

Core elements

Risk management frameworks usually consists of the following core elements:

Risk appetite statement — An articulation of the shared views on how much risk the organisation is willing to take in pursuit of its objectives. It is **good governance** that the risk appetite statement be aligned with the organisation's code of ethics, code of conduct, strategic plan and objectives.

© Governance Institute of Australia 2020. This material is subject to copyright. The Good Governance Guides indicate, in the view of Governance Institute of Australia Ltd, one interpretation of good practice. They are not designed to cover or comply with all applicable legislation or case law. We cannot be held liable or accountable to any person who acts or relies upon the information provided. The guides are not a substitute for professional advice.
Visit our website at **governanceinstitute.com.au** to find more **Good Governance Guides** and information on **governance**.

Risk appetite statements typically include risk tolerances, which provide more detailed information about how risk appetite should be considered at a more granular risk category level, such as for health and safety risks or financial risks.

See *Good Governance Guide Risk Appetite Statement*.

Governance structure — that provides for effective board oversight of the organisation's management of its risks, including how the risk management framework integrates with audit, compliance, ethics and other assurance mechanisms.

Risk management policy — is approved and sets out a commitment to the management of risk, responsibilities, objectives, accountabilities and other policy elements.

See *Good Governance Guide Risk Management Policy*.

Roles and responsibilities

It is **good governance** for the board to set the risk appetite for the organisation, 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 **good governance** for management to design and implement the framework and to ensure that the organisation operates within the risk appetite set by the board.

Useful references to consider

There is no 'one size fits' all risk management framework. Any framework should be aligned to the organisation and be capable of integration into its structure and processes.

When considering how best to approach the development of a risk management framework, the following may be useful references:

- *ISO 31000:2018 Risk Management Guidelines and the related handbook, HB 436:2004 Risk management guidelines —Companion to AS/NZS ISO 31000:2009* — the Australian Standard provides non-industry/non-sector specific guidelines which can be customised by organisations.
- ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*, Principle 7: Recognise and manage risk, 4 ed, 2019 — sets out good practice recommendations for recognising and managing risk in listed companies including for the composition and operation of risk committees.
- *Prudential Standard CPS 220 Risk Management*, Australian Prudential Regulatory Authority, July 2019 — requires APRA-regulated institutions and heads of group to have systems for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks that may affect its ability to meet its obligations to depositors and/or policyholders.
- *Commonwealth Risk Management Policy*, Commonwealth Department of Finance, July 2014 — the policy supports the requirements under the Public Governance, Performance and Accountability Act 2013 which requires accountable authorities of entities to establish and maintain systems and appropriate internal controls for the oversight and management of risk.
- 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* — the policy assists agencies fulfil their legislative obligations under the *Public Finance and Audit Act 1983* (NSW), which requires departments and statutory bodies to establish and maintain an effective internal audit function.
- *Risk management for Directors, Governance Institute of Australia.*

Notes

1. *ISO 31000:2018 Risk Management Guidelines*

© Governance Institute of Australia 2020 This material is subject to copyright. The Good Governance Guides indicate, in the view of Governance Institute of Australia Ltd, one interpretation of good practice. They are not designed to cover or comply with all applicable legislation or case law. We cannot be held liable or accountable to any person who acts or relies upon the information provided. The guides are not a substitute for professional advice.
Visit our website at **governanceinstitute.com.au** to find more **Good Governance Guides** and information on **governance**.