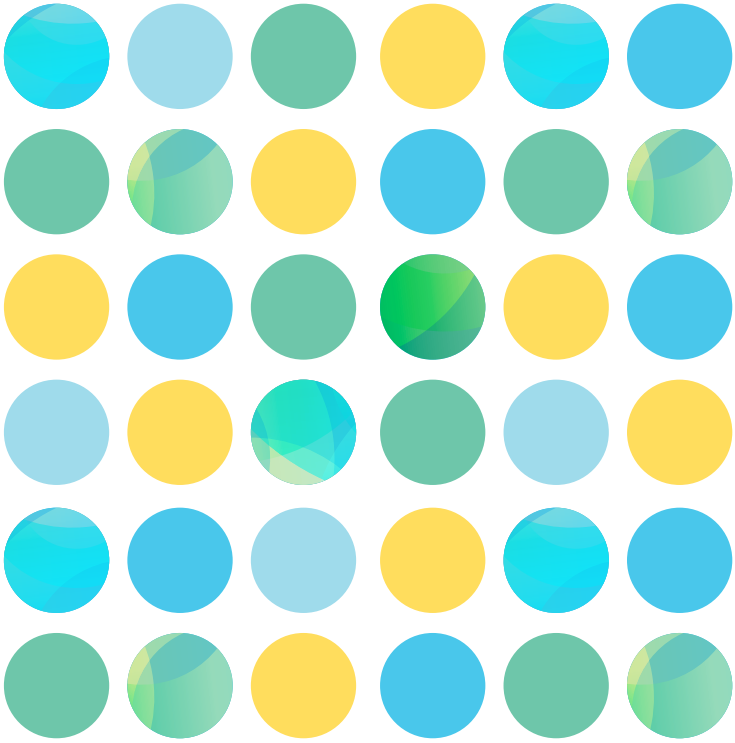
Australian Government

Department of Finance



Commonwealth Risk Management Policy

1 July 2014

Department of Finance
Business, Procurement and Asset Management

978-1-922096-51-7 (Print)
978-1-922096-50-0 (Online)

Contact us
Inquiries regarding the licence and any use of this work are welcome at:

Business, Procurement and Asset Management
Department of Finance
John Gorton Building, King Edward Terrace, Parkes ACT 2600
Email: governmentadvertising@finance.gov.au

Foreword

I am pleased to issue the Commonwealth Risk Management Policy.

This policy sets out the Government's expectations for Commonwealth entities in undertaking the business of Government. It supports the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) framework, which provides that the accountable authority of a Commonwealth entity must establish and maintain appropriate systems and internal controls for the oversight and management of risk.

A more productive, innovative and efficient public sector requires a focussed approach to managing risk in order to achieve the Commonwealth's strategic objectives and to limit unnecessary red tape. Effective risk management, based on sound judgement and the best information available, enhances the Commonwealth's capacity to identify, manage and derive maximum benefits from new challenges and opportunities.

The nine elements of the policy seek to strengthen the risk management practices of Commonwealth entities by encouraging officials to engage with risk in a positive and transparent way. This new approach to managing risk is crucial to facilitate innovation, and in turn, improved policy development and service delivery.

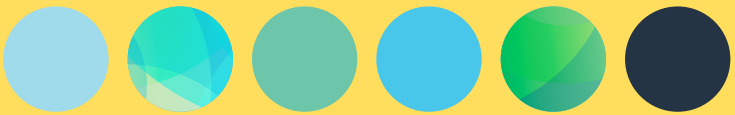
These nine elements will assist accountable authorities to build on their existing risk management framework, develop more detailed arrangements for risk oversight, and embed them into day to day business practices.

I commend the Commonwealth Risk Management Policy to Commonwealth Government officials.

Mathias Cormann
Minister for Finance

Contents

Purpose



Purpose of the Commonwealth Risk Management Policy

1. The *Public Governance Performance and Accountability Act 2013* (PGPA Act) is a principles based Act that seeks to improve the high level accountability of all Commonwealth entities through focusing on their duties, internal controls and the way they engage with, and manage, risk.
2. Risk is defined as the 'effect of uncertainty on objectives' and risk management as the 'coordinated activities to direct and control an organisation with regard to risk'. [1]
3. Key elements of the PGPA Act related to the management of risk include:
   - **a.** Duty to govern the Commonwealth entity (PGPA Act section 15);
   - **b.** Duty to establish and maintain systems relating to risk and control (PGPA Act section 16);
   - **c.** Rules about general duties of accountable authorities (PGPA Act sections 20 & 102);
   - **d.** Corporate plan for Commonwealth entities (PGPA Act sections 35 & 95);
   - **e.** Annual performance statements for Commonwealth entities (PGPA Act section 39);
   - **f.** Audit committee for Commonwealth entities (PGPA Act sections 45 & 92);
   - **g.** Annual reports for Commonwealth companies (PGPA Act section 97);
   - **h.** Rules relating to the Commonwealth and Commonwealth entities (PGPA Act section 102);
   - **i.** Indemnities, guarantees, warranties and insurance (PGPA Act sections 60 to 63); and
   - **j.** Accountable Authority Instructions under the PGPA Act.

1 AS/NZS ISO 31000 Risk management – Principles and Guidelines, p1-2.

4. Section 16 of the PGPA Act provides that, **effective from 1 July 2014,** accountable authorities of **all Commonwealth entities** must establish and maintain appropriate systems of risk oversight, management and internal control for the entity.

5. **Non-corporate Commonwealth entities** must comply with this Commonwealth Risk Management Policy, which supports the requirements of section 16 of the PGPA Act.

6. **Corporate Commonwealth entities** are not required to comply with the Commonwealth Risk Management Policy, but should review and align their risk management frameworks and systems with this policy as a matter of good practice.

Applying the Commonwealth Risk Management Policy

7. The goal of the Commonwealth Risk Management Policy is to embed risk management as part of the culture of Commonwealth entities where the shared understanding of risk leads to well informed decision making.

8. The Commonwealth Risk Management Policy sets out nine elements which **non-corporate Commonwealth entities** (entities) must comply with in order to establish an appropriate system of risk oversight and management.

9. The nine elements of the Commonwealth Risk Management Policy are:

   a. Establishing a risk management policy;

   b. Establishing a risk management framework;

   c. Defining responsibility for managing risk;

   d. Embedding systematic risk management into business processes;

   e. Developing a positive risk culture;

   f. Communicating and consulting about risk;

g. Understanding and managing shared risk;

h. Maintaining risk management capability; and

i. Reviewing and continuously improving the management of risk.

10. The Commonwealth Risk Management Policy enables entities to tailor existing risk management systems and practices to a level that is commensurate with the scale and nature of their risk profile. More detailed guidance on implementing risk management can be found at Comcover's website. [2]

11. While not mandatory, an entity's risk management framework and systems should be aligned with and reflect existing standards and guidance such as *AS/NZS ISO 31000:2009 – Risk management – principles and guidelines.*

12. Following its implementation, the Commonwealth Risk Management Policy will be reviewed to assess its impact and effectiveness.

2 Available at www.finance.gov.au

Policy Elements

Element One – Establishing a risk management policy

13. A risk management policy links the entity's risk management framework to its strategic objective. Communicating the accountabilities, responsibilities and expectations within an entity's risk management policy is important to ensure a common understanding of risk across the entity.

13.1 An entity *must* establish and maintain an entity specific risk management policy that:

- **a.** defines the entity's approach to the management of risk and how this approach supports its strategic plans and objectives;
- **b.** defines the entity's risk appetite and risk tolerance;
- **c.** contains an outline of key accountabilities and responsibilities for managing and implementing the entity's risk management framework; and
- **d.** is endorsed by the entity's accountable authority.

Element Two – Establishing a risk management framework

14. A risk management framework is the set of components and arrangements that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the entity.

14.1 An entity *must* establish a risk management framework which includes:

- **a.** the overarching risk management policy (Element One);
- **b.** an overview of the entity's approach to managing risk;
- **c.** how the entity will report risks to both internal and external stakeholders;
- **d.** the attributes of the risk management culture that the entity seeks to develop, and the mechanisms employed to encourage this;
- **e.** an overview of the entity's approach to embedding risk management into its existing business processes;
- **f.** how the entity contributes to managing any shared or cross jurisdictional risks;
- **g.** the approach for measuring risk management performance; and
- **h.** how the risk management framework and entity risk profile will be periodically reviewed and improved.

14.2 The risk management framework must be endorsed by the entity's accountable authority.

Element Three – Defining responsibility for managing risk

15. The accountable authority of an entity is responsible for an entity's performance in managing risk. The responsibility for the day-to-day management of risk lies with officials at all levels.

15.1 Within the risk management policy, the accountable authority of an entity *must* define the responsibility for managing risk by:

a. defining who is responsible for determining an entity's appetite and tolerance for risk;

b. allocating responsibility for implementing the entity's risk management framework; and

c. defining entity roles and responsibilities in managing individual risks.

Element Four – Embedding systematic risk management into business processes

16. The objective of effective management is to improve organisational performance. Considering risk is an integral element of the overall management capability of an entity and must include, and not be limited to, each of the following: strategic planning; the establishment of governance arrangements; policy development; programme delivery; and decision making.

16.1 Each entity *must* ensure that the systematic management of risk is embedded in key business processes.

Element Five – Developing a positive risk culture

17. Risk culture is the set of shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities.

18. A positive risk culture promotes an open and proactive approach to managing risk that considers both threat and opportunity. A positive risk culture is one where risk is appropriately identified, assessed, communicated and managed across all levels of the entity. Such a culture needs to be fostered and practiced by each entity.

18.1 An entity's risk management framework *must* support the development of a positive risk culture.

Element Six – Communicating and consulting about risk

19. Communicating and consulting about risk underpins the successful management of risk. Effective communication requires consultation with relevant stakeholders and the transparent, complete and timely flow of information between decision makers.

19.1 Each entity *must* implement arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders.

Element Seven – Understanding and managing shared risk

20. Shared risks are those risks extending beyond a single entity which require shared oversight and management. Accountability and responsibility for the management of shared risks must include any risks that extend across entities and may involve other sectors, community, industry or other jurisdictions.

20.1 Each entity *must* implement arrangements to understand and contribute to the management of shared risks.

Element Eight – Maintaining risk management capability

21. Effective risk management requires an entity to maintain an appropriate level of capability to manage its own risk management programme and to manage its risks. The nature and scale of this capability must be considered in the context of the entity's current resource and capability profile and be commensurate with the characteristics and complexity of its risk profile.

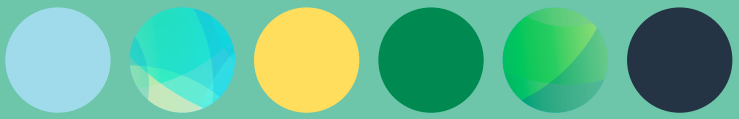
21.1 Each entity *must* maintain an appropriate level of capability to both implement the entity's risk management framework and manage its risks.

Element Nine – Reviewing and continuously improving the management of risk

22. Formalising and implementing risk management within an entity is not a 'one-off event'. The effective management of risk is a process of continuous improvement, requiring regular review and evaluation mechanisms.

22.1 Each entity *must* review its risks, its risk management framework and the application of its risk management practices on a regular basis, and implement improvements arising out of such reviews.

Appendix



Appendix A:
Glossary of terms

Accountable authority - The person or group of persons who has responsibility for, and control over, a Commonwealth entity's operations.

Commonwealth entity - A Commonwealth entity is a:

- **a.** Department of State; or
- **b.** Parliamentary Department; or
- **c.** listed entity; or
- **d.** body corporate established by a law of the Commonwealth

Corporate Commonwealth entity - A Commonwealth entity that is a body corporate and legally separate from the Commonwealth.

Non-corporate Commonwealth entity – A Commonwealth entity that is not a body corporate and legally part of the Commonwealth.

Internal control - Any process, policy, device, practice or other actions within the internal environment of an organisation which modifies the likelihood or consequences of a risk.

Risk – The effect of uncertainty on objectives. An effect is a deviation from the expected — positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence.

Risk assessment – The process of risk identification, risk analysis and risk evaluation.

Risk appetite – The amount of risk an entity is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describes the entity's attitude toward risk taking.

Risk criteria – Terms of reference against which the significance of a risk is evaluated.

Risk management framework – A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk management – Coordinated activities to direct and control an organisation with regard to risk.

Risk oversight – The supervision of the risk management framework and risk management process.

Risk profile – A description of any set of risks. The set of risks can contain those that relate to the whole organisation, part of the organisation or as otherwise defined.

Risk tolerance – The levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk.

Shared risk – A risk with no single owner, where more than one entity is exposed to or can significantly influence the risk.