Submission 1.1
Attachment A
18 March 2014

Commonwealth Risk Management Policy

Purpose

1. The Commonwealth Risk Management Policy (the Risk Management Policy) has been developed to support the accountable authorities of non-corporate Commonwealth entities to effectively discharge their responsibilities under the Public Governance Performance and Accountability Act 2013 (PGPA Act) by ensuring they:

   - establish and maintain an appropriate system of risk oversight and management for the entity; and
   - establish and maintain an appropriate system of internal control for the entity.

2. For the purposes of this Risk Management Policy, 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]

Introduction

3. An innovative, productive and efficient public sector requires a focussed approach to managing risk in order to achieve the strategic objectives of Government and the outcomes of individual Commonwealth entities. Effective risk management can enhance the Commonwealth’s capacity to identify, manage and derive maximum benefits from new challenges and opportunities.

4. One of the four guiding principles of the PGPA Act acknowledges that engaging with risk is a necessary step in improving performance. This policy supports this principle and confirms that prudent risk-taking, based on sound judgement and the best information available, is crucial to facilitating innovation and improvements in policy development, program and service delivery.

5. To achieve a consistent Commonwealth approach to managing risk, the Risk Management Policy:

   - is principles based in order to provide sufficient flexibility, given the diverse operations of Commonwealth entities;
   - encourages entities to develop internal risk management frameworks, systems and processes that are commensurate with the scale and nature of their risk profiles; and
   - sets out the risk management attributes necessary for entities to meet government expectations for managing risk under the PGPA Act.

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

6. An entity's risk management framework and systems should be aligned with existing standards and guidance such as AS/NZS ISO 31000:2009-Risk management – principles and guidelines, and the seven policy elements detailed in this policy. This policy is not intended to replicate standards or approaches but rather acknowledge and share better practice within the context of the Commonwealth.

7. The Risk Management Policy also allows a level of flexibility for entities to tailor existing risk systems and practices to achieve the diverse policy or statutory objectives of non-corporate Commonwealth entities.

Scope

8. The Risk Management Policy applies directly to all non-corporate Commonwealth entities, however all Commonwealth entities should review and align their risk frameworks and systems with this policy as a matter of good practice.

Key Principles for Managing Risk in the Commonwealth

9. In discharging their duties under sections 16 (a) and (b) of the PGPA Act, the accountable authority[2] of a Commonwealth entity must consider the following principles of establishing and maintaining appropriate systems of risk oversight and management, and internal control for the entity.[3] These principles are to ensure that an entities framework for managing risk are:
   - **Principle 1—structured** and linked to the strategic business objectives of the entity;
   - **Principle 2—**an **integral** part of the entity's overarching governance, financial, assurance and compliance frameworks;
   - **Principle 3—tailored** to the needs of the entity and proportionate to its risks;
   - **Principle 4—dynamic** with a focus on continual improvement and maintaining better practice; and
   - **Principle 5—managed transparently** with the accountable authority being accountable for the risks of the entity and the responsibility for risk managed by those best able to control the risks.

[2] Accountable authorities are as defined under section 12 subsection (2) of the *Public Governance, Performance and Accountability Act 2013.*

[3] The principles represent fundamental norms, rules, and values that define what is desirable from a risk management perspective.

Elements of the Commonwealth Risk Management Policy

10. The Risk Management Policy contains seven policy elements which include both mandatory requirements and non-mandatory better practice guidance.

11. The mandatory requirements, or '*musts*', are the minimum requirements of the Risk Management Policy and are set out in a box following each policy element.

12. The non-mandatory requirements, or 'shoulds', provide guidance to improve entities risk management capability and performance. Commonwealth entities are encouraged to follow these as a matter of better practice.

Policy Element One - Risk Management Policy and Objectives

- Each entity *must* develop and maintain a written risk management policy.
- This policy *must* be endorsed by the entity's accountable authority and contain a statement expressing this support.
- The policy *must* define the linkage between the entity's approach to the management of risk and its strategic plans and objectives.
- The policy *must* contain an outline of key accountabilities and responsibilities for managing risk and implementing the entity's risk management framework.

13. Developing and communicating a risk management policy is a crucial step in ensuring that risk is managed effectively. A risk management policy is an integral part of an entity's risk management framework and defines how the entity's risk management objectives and philosophy are enacted within its risk framework.

14. An entity's risk management policy should include:

a. the objective and rationale for managing risk in the entity;

b. a commitment to the effective management of risk; and

c. a commitment to ensuring that appropriate authority and resources are available to manage risk.

15. The entity's risk management policy should explicitly consider uncertainty and opportunity. The nature of uncertainty, and how it should be addressed as part of managing risk, should be recognised as a tool for identifying opportunities.

16. In addition to a risk management policy, an entity's risk management framework should provide:

- **a.** an expression of the agency's tolerance and appetite for risk;
- **b.** an overview of the agency's approach to managing risk;
- **c.** requirements to communicate and report risks both within the entity and with relevant external stakeholders;
- **d.** a description of how the management of risk interfaces with other governance and assurance programs within the entity;
- **e.** the attributes of the risk culture that it seeks to develop;
- **f.** an overview of the entity's approach to integrating risk management into its existing business processes;
- **g.** how the entity appropriately contributes to managing shared or cross-jurisdictional risks;
- **h.** the rationale by which risk management performance is measured;
- **i.** a commitment to, and a summary of, the arrangements for, ensuring the risk framework and entity risk profile are kept current and relevant;
- **j.** a definition or reference to the objectives, strategies, legislative requirements and obligations against which it seeks to manage risk; and
- **k.** a statement highlighting the important role risk management can play in shaping the entity's strategies and business plans to support evidence-based decision making.

Policy Element Two - Accountability and Responsibility

- An entity *must* clearly define responsibility for managing risk, including:
  a. responsibility for the implementation of the entity's risk management framework;
  b. the roles of, and expectations for, staff within the entity with accountability for managing individual risks;
  c. how responsibility for the management of risk controls is determined, assigned and monitored;
  d. the role of those entity functions with specific responsibilities for supporting and reviewing the effectiveness of the entity's risk management framework, e.g. audit and/or risk committees; and
  e. responsibilities for building risk capability through the implementation of development and training programs (e.g. risk training).

17. Ultimate accountability and responsibility for an entity's performance lies with the accountable authority of the entity. This accountability includes providing advice to staff on the entity's approach to the implementation of appropriate frameworks, processes and procedures.

18. The practical management of risk lies with officials at all levels. The clear definition and understanding of these responsibilities is essential to ensure that all officials recognise their role. The senior executive of an entity can assist by providing top-down guidance to staff managing risks throughout the entity, ensuring they understand the entity's priorities, key obligations, objectives and their broader role in contributing to the effective management of risk.

19. The timely communication and transparent reporting of risk is essential to its shared understanding and management. Recognising the increasingly interdependent nature of shared risk, the accountability and responsibility for managing shared risks may require entities to adopt a collaborative approach to managing risk that stretches across a portfolio or jurisdiction.

Policy Element Three - Integration

- An entity *must* ensure that their risk management framework is integrated with other business processes.

20. The objective of good risk management is to improve organisational performance. Commonwealth entities should regard the systematic management of risk as an integral part of strategic planning, governance and evidence-based decision making.

21. An entity should align and integrate its approach to managing risk with its overarching governance framework as a core component of organisational processes. Such an approach will strengthen the relationship between the risk management activities and the entity's outcomes and objectives.

22. Different Commonwealth entities will be exposed to different risks. In some cases, different categories of risk may have their own management requirements and may be subject to particular regulatory or compliance obligations. Examples of risk categories include business continuity, fraud, workplace health and safety, procurement and security. Entities should define how individual categories of risk are considered and managed as part of the entity's overall organisational risk profile.

23. The integration of risk management with other business processes should include mechanisms to ensure that:

- **a.** risk assessment outcomes inform strategic planning and the development of strategies, policies and programs;
- **b.** consideration of how strategies, policies and programs affect an entity's risk exposure when designed and implemented;
- **c.** risks are not solely managed within business units or organisational silos, but are managed at an aggregated or entity level, with interdependencies and shared responsibilities fully considered;
- **d.** performance reporting is accompanied by an assessment of individual risks to inform entities and their stakeholders of the level of risk exposure;
- **e.** the financial assessment of significant (or material) risks, including their mitigating strategies, are considered by undertaking a cost-benefit analysis on impact and likelihood;
- **f.** key service delivery and outcome programs explicitly consider the management of risk throughout their lifecycles; and
- **g.** insights generated from risk management processes systematically inform and help prioritise assurance activities such as audit.

Policy Element Four - Positive Risk Culture

- An entity *must* determine and describe the attributes of the risk culture that it seeks to develop. To encourage a positive risk culture, an entity's risk management policy and framework needs to emphasise the benefits and opportunities of managing risk in achieving its objectives.

24. Risk culture is the set of shared attitudes, values and practices that characterise how an entity considers risk in its day-to-day activities. For those entities that do not explicitly define and shape their risk culture it may form haphazardly, resulting in significantly different risk cultures within an entity.

25. As risk is inherent in everything that organisations do, entities should adopt a consistent approach to how risk is communicated and managed to enable an organisation-wide culture of transparency and appropriate risk taking. Accountable authorities are encouraged to adopt a risk based approach to decision making that assists officials to make informed choices, prioritise actions and distinguish between alternate courses of action.

26. An entity's commitment to managing risk should be demonstrated by its senior executives to the extent it is reflected in the entity's leadership, communication, accountability, and incentive structures. This can be supported by the development and enforcement of policies in areas such as codes of conduct, delegations, disclosure, whistle blowing, fraud control, security and information management. Appropriately managed, each of these contribute to the development of a positive risk culture.

27. An entity's risk management framework should support the development of a 'risk aware' culture—where risk is appropriately identified, assessed, communicated and managed across all levels of the organisation.

Policy Element Five - Communication and Consultation

- Each entity *must* implement arrangements to ensure the effective communication and reporting of risk, both within the entity and with relevant external stakeholders.

28. Effective communication and consultation underpin the successful management of risk. Good risk communication requires active consultation with relevant stakeholders and the transparent, complete and timely flow of information to and from decision-makers.

29. Proactive and systematic engagement with stakeholders, both internal and external, throughout the risk management process is key to identifying, analysing and monitoring risk effectively.

30. The consideration of risk and the consultation process with stakeholders should include a discussion of risk management methodologies, the financial impact of individual risks and the determination of the effectiveness of the controls required to treat individual risks. This approach is of a higher importance where entities have an obligation to work together to determine and manage shared risk exposures.

31. As the Commonwealth and State/Territory jurisdictions undertake a range of joint programs for improved policy development and program and service delivery the issue of shared risk becomes more apparent. The appropriate jurisdiction or entity best able to manage each risk should take responsibility for its management within the joint program. Responsible entities should be clearly defined in a strategy agreed upfront by each of the entities and jurisdictions involved in any joint program.

32. To encourage effective risk management, the risk management framework and a shared understanding of relevant risks should be supported by appropriate training and communication programs. These should consider:

a. the requirements of the Risk Management Policy;

b. the entity's risk management policy and framework;

c. the need to promote risk management good practice across a broad spectrum of management and staff. This should span the senior executive to operational staff, including staff from a range of locations, roles and business areas;

d. both internal and external stakeholders;

e. the importance of frank and honest disclosure of risk and the courage to make risk broadly visible without fear of reprisal or blame; and

f. the interdependent nature of many risks, where individual work groups of an entity, or multiple entities, can influence or be impacted by a single risk event.

Policy Element Six - Risk Management Capability and Resourcing

- Each entity *must* assess and maintain sufficient capability and resourcing to both implement the entity's risk management framework and manage its risks.

33. Effective risk management requires an entity to adopt an appropriate level of capability and resources to mange their risk. The nature and scale of these should be commensurate with the characteristics and complexity of the entity's risk profile.

34. In assessing an entity's risk management capability requirements it should consider its risk appetite, key stakeholders and those risks shared with others. Similarly, entities should collaborate to make best use of shared risk management capabilities where sensible to do so.

35. To determine the appropriate level of risk management capability and resources entities should consider:

a. engaging people with the appropriate competence, experience and authority and where appropriate subject matter expertise or specialist advice;

b. documenting processes, methods and tools for managing risk; and

c. establishing review, evaluation, continuous improvement programs and reporting mechanisms that provide information for recording and monitoring risks.

Policy Element Seven - Continuous Evaluation and Improvement

- Each entity *must* review its risk management framework, the application of its risk management practices, and its risks on a regular basis.
- Risk management reviews *must* be effectively documented and endorsed at the appropriate level within the entity.

36. The formalisation and implementation of risk management within an entity is not a 'one-off event'. The effective management of risk is a process of continuous improvement. Accordingly, effective and mature risk management frameworks incorporate regular review and evaluation mechanisms.

37. For an entity to identify opportunities to improve its approach to the management of risk a review process is required. These review processes should be scheduled on a annual basis and consider an entity's:

a. risk appetite and tolerance levels;
b. maturity and changing risk profile;
c. level of compliance and consistency across it's risk management framework;
d. effectiveness and quality of risk management practice;
e. accuracy and currency of information used to support it's risk decisions; and
f. risk events, 'near misses' and the entity's internal and external operating environment.

38. The monitoring and review of an entity's risks should be an active process, with clear accountability for identifying indicators which may suggest a risk is changing outside its accepted tolerances. In determining appropriate timeframes for the review of its risk profile, an entity should consider the severity and nature of its risk profile, and the volatility of both the entity and its stakeholders' operating context.

39. Entities should also ensure the review of risk is considered in other business processes. For example, change management processes should contain an explicit requirement to review the manner in which the change activity might affect the risk profile of the entity or its stakeholders. In particular, entities should explicitly consider the impact of organisational and external change on their risk profile and the operation of their risk framework.

Linkages to other elements of reform and other government policies and frameworks[4]

40. The duty for accountable authorities to establish and maintain appropriate systems of risk and control has linkages to the following elements of reform:

- Fraud risk management (PGPA Act sections 15 & 16);
- Fraud (PGPA Act sections 20 & 102);
- Corporate plans (PGPA Act sections 35 & 95);
- Annual performance statements for Commonwealth entities (PGPA Act section 39);
- Audit Committees (PGPA Act sections 45 & 92);
- Annual reports and reporting requirements (PGPA Act sections 45 (3) & 97);
- Commonwealth Procurement Rules and the Commonwealth Grant Guidelines (PGPA Act section 102 (c)); and
- Indemnities, guarantees and warranties by corporate Commonwealth entities (PGPA Act sections 60 & 61).

[4] Insert hyperlinks to relevant sections of the Act and to each supporting rule.

APPENDICES AND INDEX

This section will be further developed in the coming weeks following feedback and consultation it is intended to include:

a. Additional Resources, Guidance and Support

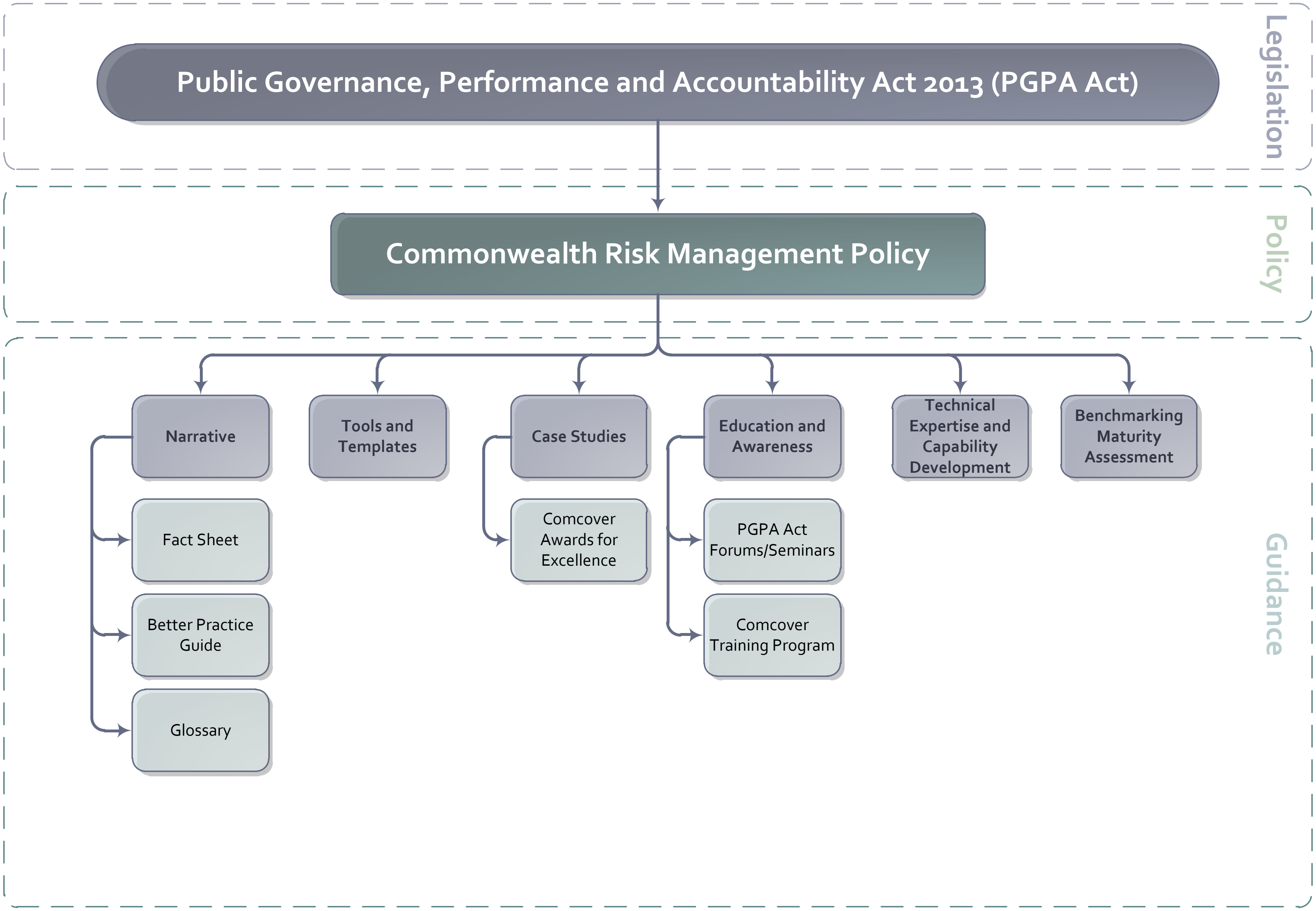
b. Glossary of Terms used and Definitions

Accountable Authority
Commonwealth entity
Corporate Commonwealth entity
Internal control
Non-corporate Commonwealth entity
Risk
Risk assessment
Risk appetite
Risk event
Risk framework
Risk management
Risk oversight
Risk profile
Risk tolerance
Shared risk

c. Glossary of Abbreviations and Acronyms

d. Index

Submission 1.1
Attachment A1
18 March 2014



Legislation

Public Governance, Performance and Accountability Act 2013 (PGPA Act)

Policy

Commonwealth Risk Management Policy

Guidance

Narrative

- Fact Sheet
- Better Practice Guide
- Glossary

Tools and Templates

Case Studies

- Comcover Awards for Excellence

Education and Awareness

- PGPA Act Forums/Seminars
- Comcover Training Program

Technical Expertise and Capability Development

Benchmarking Maturity Assessment

Australian Government
Department of Finance

Submission 1.1
Attachment A2
18 March 2014

FACT SHEET

Commonwealth Risk Management Policy

Audience

The Commonwealth risk management policy applies directly to all non-corporate Commonwealth entities. Corporate Commonwealth entities should review and align their risk frameworks and systems with this policy as a matter of good practice.

At a glance

- Sections 16 (a) and (b) of the *Public Governance Performance and Accountability 2013* (PGPA Act) provide that the accountable authority of a Commonwealth entity must establish and maintain
  - appropriate systems of risk oversight and management for the entity; and
  - an appropriate system of internal control.
- The Commonwealth risk management policy has been developed to assist accountable authorities of non-corporate Commonwealth entities meet their obligations in managing risk, and thereby promote the proper use and management of public resources.
- The Commonwealth risk management policy provides a set of principles and seven policy elements which should underpin an entity's risk management framework.

What you need to do

□ Ensure that the principles and seven policy elements contained in the risk management policy are understood and adhered to in order to meet your obligations in managing risk and promoting the proper use and management of public resources.

□ Ensure the principles of the risk management policy are reflected in your entities' systems and documentation and ensure that your level of capability is measured against each of the elements of systems for risk and control.

Useful resources

[insert link to RMP page here]
[insert link to PGPA page here]

Contacts