Australian Government
Comcover

Chief Risk Officer's Guide

Risk and Control Operating Model

Implementing the commonwealth risk management policy

The Commonwealth Risk Management Policy

Section 16 of the *Public Governance and Accountability Act 2013* (PGPA Act) provides that accountable authorities of all Commonwealth entities **must establish and maintain appropriate systems of risk oversight, management and internal control for the entity.**

- Non-corporate Commonwealth entities must comply with the Commonwealth Risk Management Policy.
- **Corporate Commonwealth entities are not required to comply but should align** with this policy as a matter of good practice.

Establishing a risk management policy

Entity requirements to meet policy	**Role of the risk function** *Chief Risk Officer / Head of Risk* *Independent review of PGPA Act 2013 Rec 13 "Accountable authorities, particularly of large Commonwealth entities, or entities with complex risks, should consider appointing a Chief Risk Officer to support the accountable authority to implement a strong risk culture and behaviour across all levels of the organisation"*	**Role of the business / function** *Executive Team (Head of Division / Business Unit / Function)* The first line of responsibility for owning and managing risk is the day-to-day decisions of officials in all roles and at all levels.	**Independent and objective oversight** *Audit Committee /Internal Audit/ANAO/Regulators* S45 PGPA Act. Each entity must have an Audit Committee. Functions must include the appropriateness of the entity's system of risk oversight, management and internal controls (PGPA Rule S17(1)).
MUST establish and maintain an entity specific risk management policy that: • defines its approach to the risk management and how it supports strategic plans and objectives • defines the entity's risk appetite and risk tolerance • outlines key accountabilities and responsibilities for managing and implementing the risk management framework • is endorsed by the entity's accountable authority.	The CRO is responsible for maintaining the risk management **policy that links the entity's risk management framework to its strategic objective(s).** The risk management policy and supporting risk management framework should: • **inform, empower and guide the entity and its officials on how to identify and manage risks** in their daily activities and decision making • **protect the soundness of the entity and its resilience to risk events** • **clearly identify the accountabilities and processes for assessing, monitoring, reporting and managing the strategic, emerging and material risks** facing the entity • support **forward looking and insightful risk management across the entity Top Down and Bottom Up.**	Business areas are responsible for: • **proposing an entity's risk appetite, aligned to Corporate and Business Plans,** for approval and ensuring that this is aligned to the entity's risk appetite as cascaded to it • **the Executive Team review and approve Business Plans and associated risk appetite proposed by Businesses and Functions.**	Review and advise the accountable authority on the entity's compliance with the Commonwealth Risk Management Policy.

Establishing a risk management framework

Entity requirements to meet policy	**Role of the risk function** *Chief Risk Officer / Head of Risk* *Independent review of PGPA Act 2013 Rec 13 "Accountable authorities, particularly of large Commonwealth entities, or entities with complex risks, should consider appointing a Chief Risk Officer to support the accountable authority to implement a strong risk culture and behaviour across all levels of the organisation"*	**Role of the business / function** *Executive Team (Head of Division / Business Unit / Function)* The first line of responsibility for owning and managing risk is the day-to-day decisions of officials in all roles and at all levels.	**Independent and objective oversight** *Audit Committee /Internal Audit/ANAO/Regulators* S45 PGPA Act. Each entity must have an Audit Committee. Functions must include the appropriateness of the entity's system of risk oversight, management and internal controls (PGPA Rule S17(1)).
MUST establish a risk management framework which includes: • the risk management policy andthe entity's approach to managing risk • risk reporting (internal andexternal) • the desired risk management culture and how it is being encouraged • the approach to embedding risk management into business processes • how it contributes to managing any shared or cross jurisdictional risks • measuring risk management performance and the oversight • the review and development of risk management framework and risk profile. The risk management framework **must** be endorsed by the entity's accountable authority.	**Working collaboratively with the business to design a risk management framework** ensures that the risk management activities of the entity are: • **proportionate** to the level of risks faced by the entity • **aligned** to the other activities undertaken by the entity • structured, **comprehensive and embedded** across the entity • dynamic and **responsive to emerging and changing risks** or **entity strategy and activities.** (ISO 3100-2018) *Risk Management Framework should address the following risk management activities:* *1. Strategic Thinking* *2. Risk Identification* *3. Risk Management* *4. Risk Appetite* *5. Controls, Data, Systems* *6. Monitoring & Reporting* *7. Governance* *8. Role Profiles* 9. *Customer Outcomes*	Where mandated the business is **responsible for implementing and embedding the entity's risk framework in** its area, including: • the **efficiency and effectiveness of risk controls, processes and procedures** • **the identification, management and reporting of strategic, material and emerging risks** to its business • **working collaboratively** with the Risk Function. • **compliance with policies, processes, legal and regulatory** requirements.	Review and advise the accountable authority on the **appropriateness of the entity's:** • risk management policy • risk **appetite** • internal controls for risk identification and risk **management** • articulation of **roles and responsibilities for risk** management • internal controls framework and processes for assessing **compliance with policies, processes, legal and regulatory** requirements.

Defining responsibility for managing risk

Entity requirements to meet policy	**Role of the risk function** *Chief Risk Officer / Head of Risk* *Independent review of PGPA Act 2013 Rec 13 "Accountable authorities, particularly of large Commonwealth entities, or entities with complex risks, should consider appointing a Chief Risk Officer to support the accountable authority to implement a strong risk culture and behaviour across all levels of the organisation"*	**Role of the business / function** *Executive Team (Head of Division / Business Unit / Function)* The first line of responsibility for owning and managing risk is the day-to-day decisions of officials in all roles and at all levels.	**Independent and objective oversight** *Audit Committee /Internal Audit/ANAO/Regulators* S45 PGPA Act. Each entity must have an Audit Committee. Functions must include the appropriateness of the entity's system of risk oversight, management and internal controls (PGPA Rule S17(1)).
An entity's accountable officer **MUST** (within the risk management policy) define the responsibility for managing risk by: • defining who is responsible for determining risk appetite and tolerance for risk • allocating responsibility for implementing the risk management framework • defining roles and responsibilities in managing individual risks.	The CRO provides oversight of the effectiveness of the Three Lines of Defence Model in the entity **that ensures that roles and responsibilities for risk management, risk activities and risk Governance** are clearly understood across the entity and that they **align with, and are complimentary to, delegations and authorisations.** Risk Accountabilities (Individual & Collective) *1. Regulatory / Legal* *2. Internal (3LOD)* *3. Governance* *4. Role Profiles* 5. *Performance and Remuneration.*	The Head of the Business/Function must ensure that roles and responsibilities for risk: • are meaningfully **understood and cascaded to all staff** and included in their role profiles and performance objectives • **are assessed as part of individuals' performance review** processes.	Review and advise the accountable authority on the **appropriateness of the entity's articulation of roles and responsibilities for risk management.**

Embedding systematic risk management into business processes

Entity requirements to meet policy	**Role of the risk function** *Chief Risk Officer / Head of Risk* *Independent review of PGPA Act 2013 Rec 13 "Accountable authorities, particularly of large Commonwealth entities, or entities with complex risks, should consider appointing a Chief Risk Officer to support the accountable authority to implement a strong risk culture and behaviour across all levels of the organisation"*	**Role of the business / function** *Executive Team (Head of Division / Business Unit / Function)* The first line of responsibility for owning and managing risk is the day-to-day decisions of officials in all roles and at all levels.	**Independent and objective oversight** *Audit Committee /Internal Audit/ANAO/Regulators* S45 PGPA Act. Each entity must have an Audit Committee. Functions must include the appropriateness of the entity's system of risk oversight, management and internal controls (PGPA Rule S17(1)).
MUST ensure that the systematic management of risk is embedded in key business processes.	Provides objective **oversight and challenge** of the: • **entity's systems and controls in respect of risk management, noting risks are owned by the business** • **effectiveness of risk management across the entity by the business** including compliance with risk appetite, risk policies, controls, processes and procedures • **risks inherent in any proposed business strategy and plans are consistent with the entity's risk appetite and tolerance.** Where **appropriate, provide guidance to the business on consideration of risk** in business decisions.	Within their area of accountability: • effective implementation of risk controls and processes • own and manage risks within risk appetite, and evidence consideration of risk in decision making • remediate weaknesses in risk controls or processes • escalate breaches of risk appetite or risk concerns • **collaborate with, and seeks guidance from, risk SMEs** to inform consideration of risk in decision making.	• Provide independent assurance over the adequacy, effectiveness and compliance with risk policies, internal controls and processes within the business, and the adherence to them by officials of the entity. • Conducting **thematic and post incident reviews** at the Entity / Business /Functional level as required.

Developing a positive risk culture

Entity requirements to meet policy	**Role of the risk function** *Chief Risk Officer / Head of Risk* *Independent review of PGPA Act 2013 Rec 13 "Accountable authorities, particularly of large Commonwealth entities, or entities with complex risks, should consider appointing a Chief Risk Officer to support the accountable authority to implement a strong risk culture and behaviour across all levels of the organisation"*	**Role of the business / function** *Executive Team (Head of Division / Business Unit / Function)* The first line of responsibility for owning and managing risk is the day-to-day decisions of officials in all roles and at all levels.	**Independent and objective oversight** *Audit Committee /Internal Audit/ANAO/Regulators* S45 PGPA Act. Each entity must have an Audit Committee. Functions must include the appropriateness of the entity's system of risk oversight, management and internal controls (PGPA Rule S17(1)).
An entity's risk management framework **MUST** support the development of a positive risk culture.	The CRO is responsible for **supporting the accountable officer in the development of a positive risk culture** across the entity. This should include the **assessment of and actions taken to embed positive risk behaviours:** • *Listening, Sharing and collaboration* • *Adherence to policies, processes and procedures* • *Risk is evidenced in **decision making*** • *Continuous improvement* • *Individual accountability and Learning from mistakes* • *Open and constructive giving and receiving of challenge.* The risk culture should promotes a proactive approach that **considers both threat and opportunity.**	• Role model and set a strong **Tone From the Top.** • **Support the development of a positive risk culture** consistent with the **entity's target risk culture,** evidenced by **reinforcing desired risk behaviours** and **appropriate actions taken for detrimental culture risk behaviours.** • Promote **a proactive approach to risk management that considers both threat and opportunity.**	Review and advise the accountable authority on the **appropriateness of the entity's risk culture**.

Communicating and consulting about risk

Entity requirements to meet policy	**Role of the risk function** *Chief Risk Officer / Head of Risk* *Independent review of PGPA Act 2013 Rec 13 "Accountable authorities, particularly of large Commonwealth entities, or entities with complex risks, should consider appointing a Chief Risk Officer to support the accountable authority to implement a strong risk culture and behaviour across all levels of the organisation"*	**Role of the business / function** *Executive Team (Head of Division / Business Unit / Function)* The first line of responsibility for owning and managing risk is the day-to-day decisions of officials in all roles and at all levels.	**Independent and objective oversight** *Audit Committee /Internal Audit/ANAO/Regulators* S45 PGPA Act. Each entity must have an Audit Committee. Functions must include the appropriateness of the entity's system of risk oversight, management and internal controls (PGPA Rule S17(1)).
MUST implement arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders.	• Oversight and **report the entity's aggregate risk profile relative to current and future business strategy and activities and agreed risk appetite:** • reporting should consider all **material risks** • report on **emerging risks to the entity** and plans to mitigate them • **alert the accountable authority** to and provide challenge on, any business strategy, plans or actions that may cause the entity exceed it risk appetite and tolerance • oversight and validation of the **entity's external risk reporting** obligations.	• **Oversight of and report the business risk profile** relative to **current and future business strategy and activities and agreed risk appetite.** • Report **emerging risks and plans to mitigate them.** • **Alert the Risk Function and the accountable officer with regard to current or planned activities that may cause the business to exceed it risk appetite and tolerance.**	Outcomes of oversight activities should: • inform the accountable authority whether the entity's system of internal controls is appropriate to the entity • provide advice to the accountable authority on **major concerns** identified **and recommended actions,** including identification and dissemination on good practice.

Understanding and managing shared risk

Entity requirements to meet policy	**Role of the risk function** *Chief Risk Officer / Head of Risk* *Independent review of PGPA Act 2013 Rec 13 "Accountable authorities, particularly of large Commonwealth entities, or entities with complex risks, should consider appointing a Chief Risk Officer to support the accountable authority to implement a strong risk culture and behaviour across all levels of the organisation"*	**Role of the business / function** *Executive Team (Head of Division / Business Unit / Function)* The first line of responsibility for owning and managing risk is the day-to-day decisions of officials in all roles and at all levels.	**Independent and objective oversight** *Audit Committee /Internal Audit/ANAO/Regulators* S45 PGPA Act. Each entity must have an Audit Committee. Functions must include the appropriateness of the entity's system of risk oversight, management and internal controls (PGPA Rule S17(1)).
MUST implement arrangements to understand and contribute to the management of shared risks.	• The CRO **provides guidance to the business on how to** collaborate **with other Commonwealth Entities** to **identify areas of shared risks** and to contribute to the aggregate assessment of those risks and, importantly, their effective management, not only for the entity, but on occasion the Commonwealth.	• **Openly collaborates and shares information on current and emerging risk issues** with others.	Where appropriate share outcomes of oversight with other **Commonwealth entities** to **identify areas of shared risks** and to contribute to the aggregate assessment of those risks.

Maintaining risk management capability

Entity requirements to meet policy	**Role of the risk function** *Chief Risk Officer / Head of Risk* *Independent review of PGPA Act 2013 Rec 13 "Accountable authorities, particularly of large Commonwealth entities, or entities with complex risks, should consider appointing a Chief Risk Officer to support the accountable authority to implement a strong risk culture and behaviour across all levels of the organisation"*	**Role of the business / function** *Executive Team (Head of Division / Business Unit / Function)* The first line of responsibility for owning and managing risk is the day-to-day decisions of officials in all roles and at all levels.	**Independent and objective oversight** *Audit Committee /Internal Audit/ANAO/Regulators* S45 PGPA Act. Each entity must have an Audit Committee. Functions must include the appropriateness of the entity's system of risk oversight, management and internal controls (PGPA Rule S17(1)).
MUST maintain an appropriate level of capability to both implement the entity's risk management framework and manage its risks.	• Identify and support the development of the capabilities needed to ensure that risks are managed effectively across the entity, including that the data used to assess its risks is fit-for-purpose in terms of quality, quantity and breadth. • Identify and support learning and training needs needed to effectively manage risk and develop a positive risk culture across the entity.	• The business is **primarily responsible for ensuring staff have the capabilities to manage risk in** their daily activities aligned to their roles and responsibilities • Where appropriate the **business collaborates with the Risk Function for support in building their risk capabilities.**	Identify and **support the development of the capabilities needed to conduct its oversight activities.**

Reviewing and continuously improving the management of risk

Entity requirements to meet policy	**Role of the risk function** *Chief Risk Officer / Head of Risk* *Independent review of PGPA Act 2013 Rec 13 "Accountable authorities, particularly of large Commonwealth entities, or entities with complex risks, should consider appointing a Chief Risk Officer to support the accountable authority to implement a strong risk culture and behaviour across all levels of the organisation"*	**Role of the business / function** *Executive Team (Head of Division / Business Unit / Function)* The first line of responsibility for owning and managing risk is the day-to-day decisions of officials in all roles and at all levels.	**Independent and objective oversight** *Audit Committee /Internal Audit/ANAO/Regulators* S45 PGPA Act. Each entity must have an Audit Committee. Functions must include the appropriateness of the entity's system of risk oversight, management and internal controls (PGPA Rule S17(1)).
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.	Ensure the **continuing efficiency and effectiveness** of the **risk management Function and Risk Management Framework and that it remains fit-for-purpose** in supporting and **enabling the entity to conduct its activities in a safe manner.**	Undertakes regular activities **to assess the effectiveness of risk management within the business** and is responsible for remediating identified weaknesses.	Ensure the **continuing efficiency and effectiveness** of its oversight processes, including the **coverage** of the oversight activities of the entity's key risks and activities.