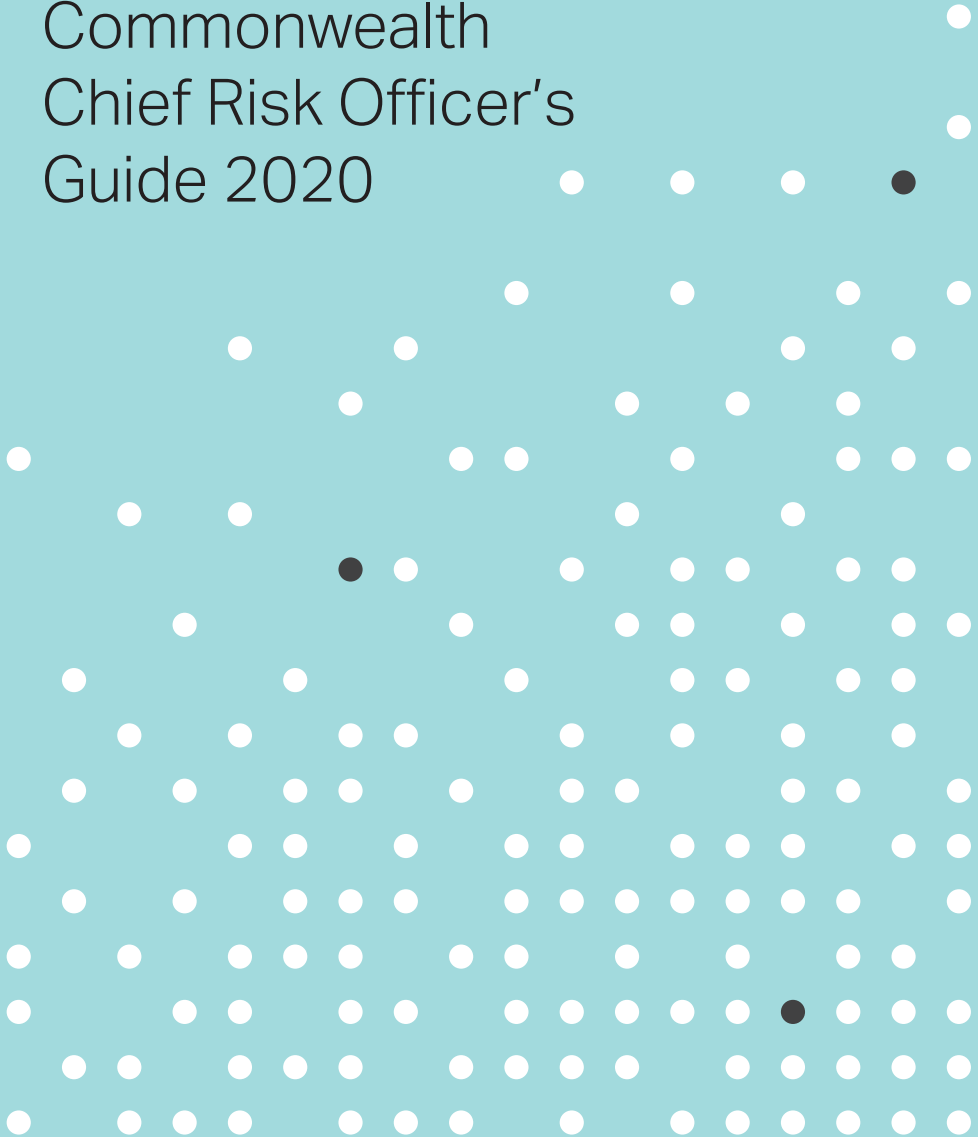




Australian Government
Department of Finance

Commonwealth Chief Risk Officer's Guide 2020



Copyright Notice

This publication is protected by copyright. Copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia.



With the exception of the Commonwealth Coat of Arms, the Department of Finance logo all material presented in this publication is provided under a Creative Commons Attribution 3.0 licence. A summary of the licence terms is available on the Creative Commons website at <https://creativecommons.org/licenses/by/3.0/au/legalcode>

Attribution

Except where otherwise noted, any reference to, use or distribution of all or part of this publication must include the following attribution:

© Commonwealth of Australia 2020.

Use of the Coat of Arms

Terms for the use of the Coat of Arms are detailed by the Department of Prime Minister and Cabinet at https://www.pmc.gov.au/sites/default/files/publications/Australian_Government_Branding_Design_Guidelines.pdf

Third party copyright

To the extent that copyright subsists in third party materials, where noted, it remains with the original owner and permission may be required to use the material. Finance has made all reasonable efforts to:

- clearly label material where the copyright is owned by a third party
- ensure that the copyright owner has consented to this material being presented in this publication.

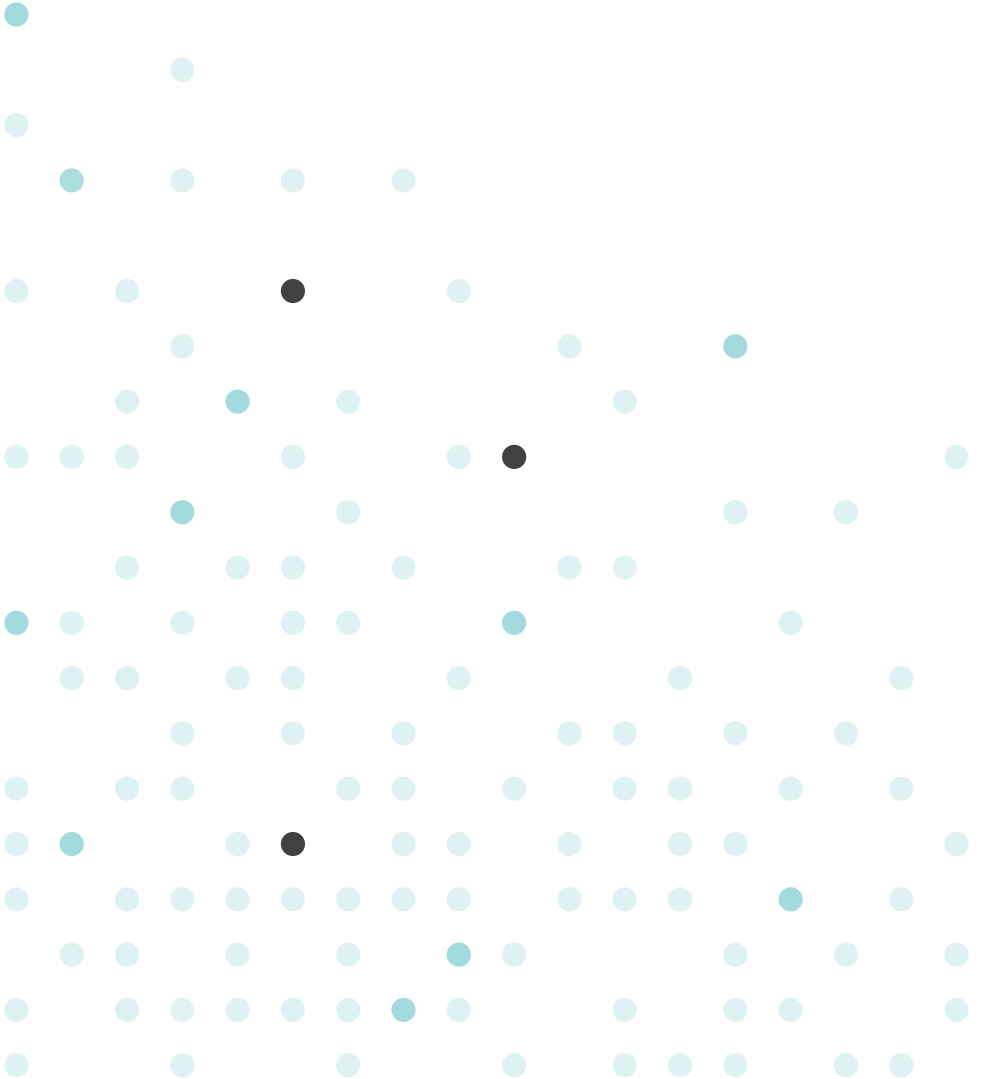
Contact us

Enquiries about the licence and any use of this publication can be sent to:

Copyright Coordinator
Department of Finance
One Canberra Avenue
Forrest ACT 2603 AUSTRALIA

Commonwealth
Chief Risk Officer's Guide
2020





Introduction

The Minister for Finance is responsible for the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). To support the implementation of risk management in the Commonwealth, the Minister issued the Commonwealth Risk Management Policy (the Policy) in 2014. The PGPA Act, and 2018 independent review of the operation of the PGPA Act, recognises that effective risk management is essential for Commonwealth entities.

Purpose of the Guide

The Guide was developed for Chief Risk Officers (CROs), accountable authorities and executive teams of Commonwealth entities.

It articulates the value of a CRO in the Australian Public Service, sets out a better practice approach to how entities can ensure a CRO is successful in their role, and outlines the desired attributes, roles and responsibilities of a CRO.

The Guide acknowledges there is no one size fits all approach to the role of the Commonwealth CRO. It outlines how the role of a CRO can provide critical capability within an entity in the Commonwealth's dynamic landscape.



A Chief Risk Officer

A CRO plays an important advisory role in supporting the accountable authority to achieve a positive risk culture within an entity. They are most effective when they have:

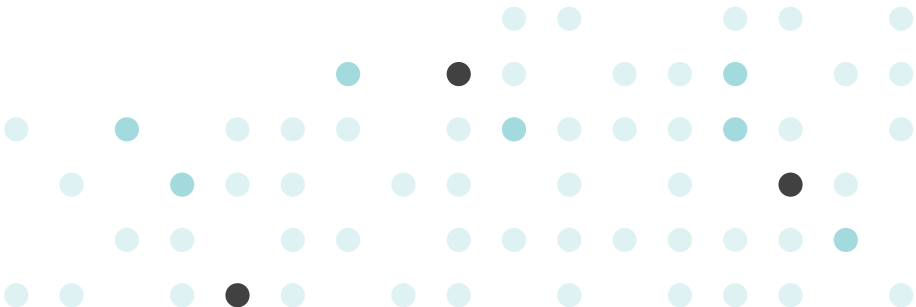
- a sound understanding of their entity's business related processes
- informed judgement on how to engage in risk as part of the business process, not as an add-on or discretionary process.

CROs should be sufficiently senior and have a good understanding of the operations of their entity and the government's objectives in relation to the entity's purpose.

CROs should have the authority to effectively challenge decisions that may affect the entity's risk profile, and lead discussions across the entity on what risk can be accepted and managed.

Critical success factors that assist a CRO to meet their role and responsibilities include having:

- direct access to, and the trust of, the accountable authority and senior management in notifying them of any significant breach of, or material deviation from, the risk management framework of the entity
- access to all parts of an entity that have the potential to engage in or generate material risk
- the respect of staff when highlighting relevant factors for risk assessment and management
- appropriate delegation and sufficient resources to support the effective execution of their responsibilities.



The value of a Chief Risk Officer

To realise the value of an effective CRO, the following section summarises the support a CRO can provide in an entity.

Defines how an entity views risk management

A CRO assists an accountable authority establish how officials view risk and the risk taking behaviours in an entity. This includes defining how officials in an entity:

- view risk as an opportunity as well as a threat
- develop an appropriate risk culture, encouraging desired behaviours such as speaking up and learning from mistakes
- achieve an appropriate level of risk management maturity that reflects the entity's risk profile and emphasises that risk is about continuous learning and embracing opportunities.

An influencer of decision making

A CRO is an advisor on the management of risk, they are not the owner of an entity's risks. CROs provide a critical role in guiding and influencing risk-based decisions.

To realise the value of a CRO, the accountable authority should reinforce the CRO's role:

- is one of risk oversight, not ownership
- applies insight to decisions. For example, an effective CRO is involved early in conversations on issues that may impact the achievement of an entity's objectives
- works across an entity to ensure consistency in the approach to risks and the quality of risk information to support robust decision making
- is a trusted advisor to the accountable authority and while they may not necessarily be part of the executive team, they have the authority to support the executive in making risk informed decisions.

A solution seeker and champion for risk taking

The CRO should encourage and develop processes to support appropriate risk taking so all officials in the entity consider:

- new proposals or initiatives in line with the risk appetite and tolerance(s) of the entity
- opportunities to the entity offered by new proposals or initiatives
- consequences, including potential reputational damage to the entity and/or broader Commonwealth, should a proposal fail.

A shared risk awareness steward

A CRO is integral to ensuring shared risks, those where more than one entity, or areas within an entity, have influence or are exposed, are identified and managed. This may involve:

- designing and implementing a tailored approach to support the identification of shared risks, the relevant stakeholders and the mitigation strategies to adequately manage these risks
- establishing appropriate governance structures to identify and manage shared risk
- tracking improvements on how shared risks are managed in the entity.

An advocate of emerging risks

The CRO informs their executive of emerging and future risks by:

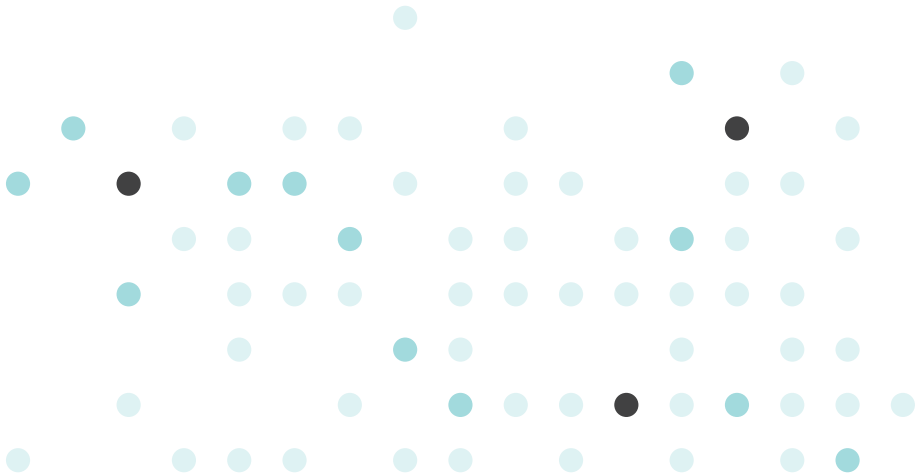
- monitoring the Commonwealth's dynamic and constantly changing operating environment
- optimising the use of risk sensing tools such as
 - environmental scanning
 - workshops
 - scenario modelling.

The attributes, roles, responsibilities and accountabilities of a CRO

This section provides guidance to accountable authorities, and officials assisting them, on key attributes, roles, responsibilities and accountabilities of a CRO to assist how they define and embed the role within an entity.

A CRO is not the owner of the entity's risks but rather an advisor on risk management matters. A CRO provides a critical role in guiding and influencing risk based decisions, working closely with the accountable authority to identify, measure and evaluate all key current, emerging and future risks.

A CRO role is a position of significant influence and provides critical capability to an executive team. A CRO supports the accountable authority to influence the culture of an entity by providing objective advice on the performance and behaviours of people, processes and systems in their entity.



Attributes of a CRO

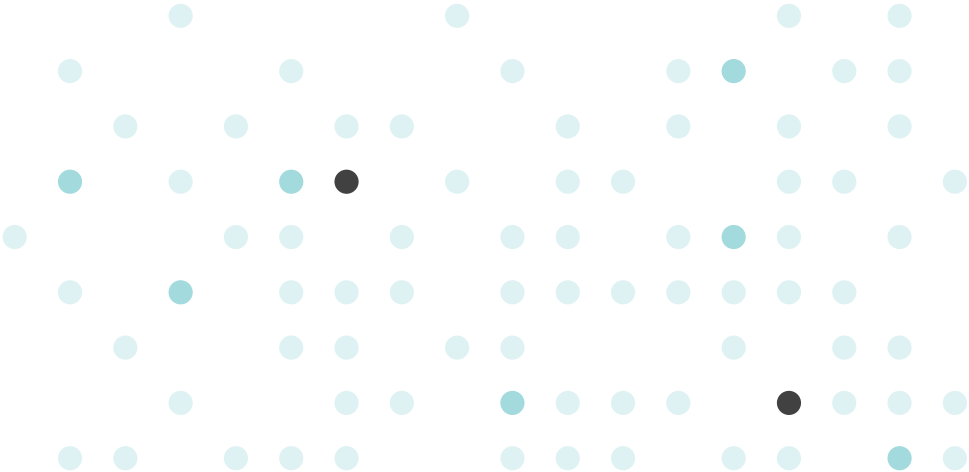
A CRO, in conjunction with other executives, should define, articulate and model attributes and behaviours which help drive and, where necessary, change the culture of the entity.

Attributes listed below are not exhaustive and, dependent on the size and risk complexity of the entity, should be considered when appointing and designing the role of a CRO.

Key areas of focus	Attributes of a CRO
Policy and Framework	<ul style="list-style-type: none">• have a deep understanding of risk management principles and effective risk management• have a comprehensive understanding of the operations of the entity and the entity's purpose
Implement and Embed	<ul style="list-style-type: none">• challenge decisions that may affect the risk profile of the entity, or cause officials to act outside the risk appetite and tolerance of the entity• be able to develop and promote a vision for risk that adds value• possess good judgement regarding key risks to an entity and those that require focused attention• facilitate and promote an environment whereby informed risk-based decision making can occur
Risk Culture	<ul style="list-style-type: none">• foster a positive risk culture• have the ability to influence others• be sensitive to the complexities of government and relationships with ministers and stakeholders• exemplify and model integrity, ethics, values and the desired cultural behaviours• be innovative and bring a holistic and objective lens to decision-making conversations



Key areas of focus	Attributes of a CRO
Communication and Consultation	<ul style="list-style-type: none">• communicate acceptable risk taking across the entity• be a good communicator across all levels of the entity to deliver targeted messaging• have the ability to communicate complex matters with clarity and succinctness• be able to present information in easy to understand formats and communication methods
Organisational Capability	<ul style="list-style-type: none">• be committed to developing the capability of the entity to harness opportunities through effective risk management



Roles and responsibilities of CROs

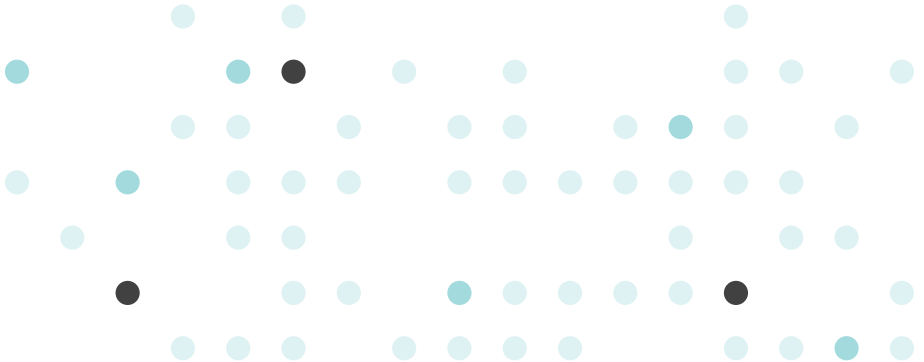
CROs play a key role supporting accountable authorities to deliver their strategic objectives and purpose. This includes the allocation of responsibility for implementing the risk management framework for the entity, and making it clear that all officials have a responsibility to actively manage risk as part of their daily duties, regardless of their role or position.

Key roles and responsibilities of a CRO should include the following:

Key areas of focus	Roles and responsibilities
Policy and Framework	<ul style="list-style-type: none">• lead the design of the risk framework for the entity• ensure the risk framework and function is proportionate to the scale and complexity of the activities undertaken by the entity• provide clarity around risk ownership and responsibility• undertake continuous reviews of the entity's risk management policy and framework to ensure it remains fit for purpose
Implement and Embed	<ul style="list-style-type: none">• ensure risk management is part of corporate planning and reporting processes• oversee the implementation of the frameworks and policies to manage risks• develop and review risk appetite and tolerance statement(s)• embed systematic risk management into business processes• create, review and implement simple and risk management tools• analyse and report at an enterprise level on the risk profile and the risks of the entity• design and ensure operational effectiveness of key controls of the entity's risk framework• identify new and emerging risks relevant to the entity



Key areas of focus	Roles and responsibilities
Risk Culture	<ul style="list-style-type: none">• contribute to the development of the culture for managing risk in the entity• define the expected behaviours for risk taking in the entity, as articulated by the accountable authority
Communication and Consultation	<ul style="list-style-type: none">• ensure the executive receives the information required to assess the risk profile of the entity so informed decisions can be made• articulate a whole of entity view on risk
Organisational Capability	<ul style="list-style-type: none">• implement and ensure the use of a common risk language• identify and implement appropriate training and awareness programs to build the capability of officials to appropriately manage risk



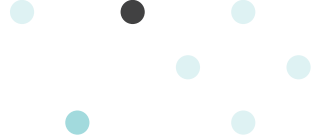
Accountabilities of a CRO

A CRO is accountable for the design and implementation of effective systems of risk management within the entity.

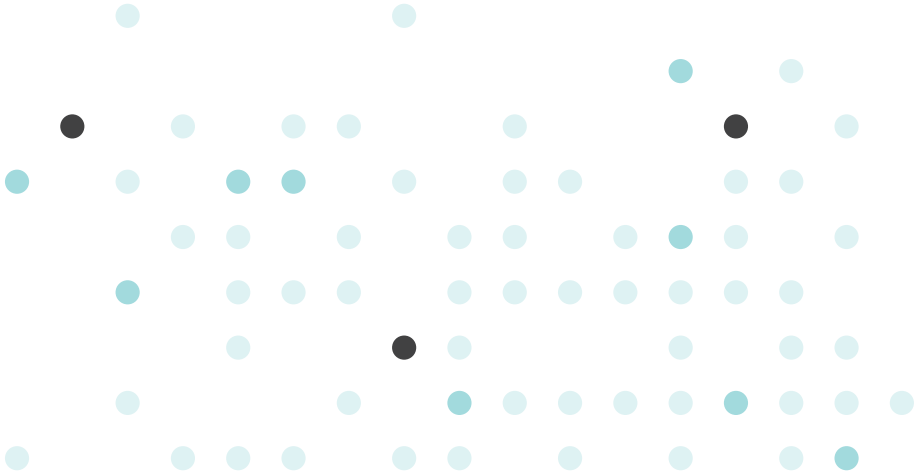
Key accountabilities for a CRO should include the following:

Key areas of focus	Accountabilities
Policy and Framework	<ul style="list-style-type: none"> design and implement a fit-for-purpose governance model for risk management within the entity ensure that roles and responsibilities for risk management are clearly understood across the entity and they align with delegations
Implement and Embed	<ul style="list-style-type: none"> provide support to the accountable authority on external risk reporting support the accountable authority and executive to determine their appetite and tolerance for risk ensure the data used by officials to assess risks is fit-for-purpose ensure the executive have a comprehensive understanding of the whole of entity risk profile embed the risk framework into the business operations of the entity be accountable to the executive for oversight of the risk framework provide oversight of the systems and controls, noting risks are owned by the respective business areas
Risk Culture	<ul style="list-style-type: none"> measure and report on the risk culture of the entity





Key areas of focus	Accountabilities
Communication and Consultation	<ul style="list-style-type: none">• make risk information available throughout the entity to inform decision making• encourage the executive to communicate the importance of managing risk• report to the accountable authority on the entity's risk profile relative to its risk appetite and tolerance(s)
Organisational Capability	<ul style="list-style-type: none">• identify the capability required by officials to appropriately manage risk• report on the risks in any proposed business initiative that are not consistent with the agreed risk appetite and tolerance(s)



Contact

If you have any questions or feedback in relation to this Chief Risk Officer's Guide, please contact Comcover at comcover@comcover.com.au.

