Australian Government

Comcover

Commonwealth Risk Management Capability Maturity Model

This document summarises the high level descriptors of capability defined in the Risk Management Maturity Model against the following:

1. Each of the six states of maturity to determine overall maturity (described below)
2. Across each of the nine elements of the Commonwealth Risk Management Policy (described overleaf).

The model can be used to assist entities to determine both their current state of risk management maturity and the appropriate state of maturity or capability (target state) that an entity aspires to achieve to support its operations and the achievement of its business objectives. Setting a target maturity state is designed to drive future investment in risk management capabilities. Entities should remember that the model is fit-for-purpose, and not all entities should strive for optimal. Entities are encouraged to adopt an appropriate risk maturity that is reflective of their size, complexity and risk culture.

1. Overall Maturity Attributes

Fundamental	Developed	Systematic	Integrated	Advanced	Optimal
• Risk management policy and framework have been endorsed by the accountable authority, however the framework has not been integrated with operations and broader governance • Inconsistent appetite for risk across the entity • Absence of common risk language • Communication and understanding of risk may not be widely understood • Ad-hoc processes to discuss and understand shared risks • Limited and/or shared resources allocated to manage risk.	• Risk management policy and framework have been communicated and implemented across the entity • A common risk language is used, however not consistently understood • Risk management policy defines shared risk. Informal processes are in place to discuss shared risk • Accountable authority instructions and risk management policy articulate responsibilities and accountabilities for risk management, however these are shared with other responsibilities.	• Risk management framework is fully embedded • Risk appetite statement is high-level and qualitative • A common understanding of the importance of managing risk exists • Formal arrangements exist for to discuss and understand shared risk • Accountability and responsibility for managing risk is clearly defined within the overarching governance framework • Dedicated staff are responsible for implementing the risk management framework.	• Risk management framework is part of the overarching governance and management framework • Risk appetite statement contains both quantitative and qualitative elements which are linked to strategy and communicated to all staff • The risk management program is reviewed regularly to identify improvement opportunities and assess the level of investment in risk management activities • Risk information and data is stored in a readily accessible central repository.	• Risk management policy is integrated with strategic and business planning processes and reviewed and updated annually (or as changes arise) • Formal arrangements facilitate identification of current, future, emerging and shared risks. These are clearly articulated across the entity • A senior executive sponsor leads, promotes and drives risk management capability • The risk management framework includes measures for the accountability and management of risk controls at business unit and program levels.	• Risk management policy considers management of risk as an integral part of the entity's governance system • Risk appetite statement, including tolerances and limits for risk categories are used consistently to inform decision making • Governance framework facilitates recording, monitoring and reporting on shared risk • Performance reporting identifies examples of good risk management practices, which are communicated and rewarded • Real-time risk information is readily available and used to identify, analyse and measure risks & trends • Costs of risk management activities are managed within the operational budget. Risk resources are allocated based on informed analysis.

2. Maturity against the nine elements of Commonwealth Risk Management Policy

	Fundamental	Developed	Systematic	Integrated	Advanced	Optimal
Element 1: Establishing a risk management policy	• A Risk management policy (policy) has been endorsed by the accountable authority • The Policy defines the approach and rationale for managing risk • Communication and understanding of the policy varies • Understanding of the entity's appetite for risk is inconsistent.	• The Policy has been communicated throughout the entity • An innate understanding of risk appetite by senior executives is implied in risk documentation, in particular its consequence and likelihood tables.	• The Policy outlines the required accountability and responsibility for managing risk • A common definition of risk exists and is applied throughout the entity • Risk appetite statement is high-level and qualitative.	• The Policy includes a vision for the continuing development of its risk management program • The Policy contains a high level risk appetite statement with both qualitative and quantitative elements, linked to business strategies • The Policy is reviewed and updated to reflect changes in the operating environment as they occur.	• The Policy defines linkages between risk and strategy • The Policy is reviewed and updated on an annual basis or more regularly if needed • Risk appetite statements for each source or category of risk exists, and include measures that enable effective monitoring and review.	• The Policy considers the management of risk as an integral part of the governance system, reflecting the link between risk and realising strategic objectives • The Policy contains information for all staff and stakeholders on resources and processes dedicated to the management of risk.
Element 2: Establishing a risk management framework	• The risk management framework (framework) is articulated at a high level, but not integrated with the operations and overarching governance practices • Resources allocated to manage risk are limited and often shared across other responsibilities • The Framework and systems used to manage risk may not be widely understood or practiced.	• The Framework articulates the risk management methodology and processes required to manage risk • The effectiveness of the framework is reviewed on an ad-hoc or informal basis.	The Framework: • Has been implemented and supports a consistent approach to risk identification, assessment, evaluation and treatment • Has annually reviewed performance measures • Has resources allocated to implement, monitor and review • Explains requirements for reporting the status of key risks including managing shared risk.	• The Framework is embedded in the operations of the entity and is part of its overarching governance and management framework • Techniques for identification, assessment, evaluation and treatment of risk are applied consistently across all business units • Reporting on the status of key risks and control performance including effectiveness of the framework occurs quarterly.	• The Framework includes measures for accountability and management of risk and controls at business unit and program/project levels • Key risk indicators measure the overall performance of the framework • Tools exist to guide decision making and support regular risk reporting and escalation • Risk management data is centrally stored and accessible.	• Techniques exist to identify, analyse and measure current, future and emerging risks • Centralised real-time risk information is readily available • Risk appetite informs risk related discussions • Performance reporting measures and monitors risk exposures • Information flows effectively as a result of no duplication of effort in risk roles.
Element 3: Defining responsibility for managing risk	• Responsibility for the management of risk has been articulated in the accountable authority instructions.	• The Accountable authority instructions and policy articulate who is accountable and responsible for the management of risk, and the implementation of the framework • The Management of risk is not specified in individual's performance agreements.	• A dedicated risk manager or team is responsible for implementing the framework • Accountability and responsibility for managing risk is clearly defined and linked to staff performance • Accountability and responsibility for managing, or oversighting risk is included in the charters of executive committees or audit and/or risk committee.	• Formalised governance structures assess and oversee risk management at business unit and executive levels • Formal governance structures assess the risks associated with the development or implementation of new policies/programs/services. • The Risk manager or team coordinates the implementation of the framework, risk profiles and action plans.	• Senior leadership supports the risk manager or team to facilitate, challenge and drive capability • The Risk management team regularly report to senior executive, the audit committee or the accountable authority on the performance of the framework • Executives approve the entity's risk appetite and oversee the continual improvement of the framework.	• Managers and supervisors monitor the risks and risk profiles of their areas of responsibility and ensure staff adopt the framework as developed and intended.
Element 4: Embedding systematic risk management into business processes	• Branch and business unit risks are reviewed annually, however do not inform business planning, budgeting and reporting • Risk definitions are inconsistently understood as there is limited guidance for identifying risk processes or differentiating between risk classes.	• Enterprise-wide risks are considered in business planning, budgeting and reporting processes • There is No evidence of the identification of specialist categories of risk, such as fraud, or business continuity in these processes.	• Framework is embedded in operational, process and reporting frameworks • Managing risk is part of the overarching governance framework and recognised as key to effective business planning • Risk identification, assessment, monitoring, communicating and reporting processes are consistent • Risk profile enables the prioritisation of audit and assurance activities.	• Risk management occurs at policy, program and/or service delivery level • Risk appetite has been defined and communicated to facilitate strategic and operational planning • Specialist risk programs are documented and included in regular reporting to senior executive and/or the accountable authority.	• The Entity's approach to managing risk is fully integrated with the overarching governance framework and recognised as key to effective business planning • Opportunities for improvement and good practice are identified through analysing risk information • A comprehensive set of risk appetite and tolerance statements, including KPI's, that cascade from high level down to detailed exist.	• Risk management processes are utilised at enterprise, business unit, program and project levels for all risk activities • Formal mechanisms exist to build and maintain organisational resilience • Risk appetite statements, including tolerance and limits are used consistently across the entity to inform decision making.
Element 5: Developing a positive risk culture	• Officials understand and agree on the need and value of effective risk management • Senior executives and line managers demonstrate the importance of managing risk in line with the framework and systems.	• The Framework is integral to the entity's operating model • Lessons learned are communicated to staff • A Common understanding of the meaning of good risk management results in a consistent use of language and understanding of risk related concepts.	• Surveys and external reviews undertaken are analysed to provide insights into the entity's risk culture • Loss incidents are analysed and areas for improvement identified. This includes acknowledging good risk management practice and speaking with staff regularly about opportunities to better manage risk.	• Senior executives are held accountable through performance agreements for managing risk including responsibility for strengthening the risk culture of their teams • Risk culture is formally and regularly assessed with recommendations identified for improvement • The Framework is integrated with its overarching governance framework.	• Officials are comfortable raising concerns with senior managers and those being challenged respond positively • A senior executive level sponsor leads and promotes the management of risk • Lessons learned from positive and negative situations.	• Culture demonstrates and promotes an open and proactive approach to managing risk that considers both threat and opportunity • Demonstration of good risk management practices are communicated and rewarded.
Element 6: Communicating and consulting about risk	• No common risk language is used with limited risk reporting • Branches and/or business units communicate with their stakeholders, but this information is not shared across the entity • Communication of risk issues is as requested which may lead to a duplication of information across the entity.	• Communication with senior executive and/or the accountable authority is limited to specialist risks • A Common risk language is used and understood by the risk management function and senior leadership teams, but these terms are not consistently understood across the entity.	• A common understanding of the principles and importance of managing risk exists • Timely communication of risk information is acknowledged as important • While areas for improvement are identified, feedback is not commonly used to improve • External communication occurs to inform stakeholders of the management of key risks and the risk management approach.	• Risk terminology is understood by all staff, providing a consistent approach to managing risk • Communicating and escalating risk issues is considered in the day to day activities of staff • Reporting formats have been agreed and are tailored to target audiences.	• A consistent approach to communicating and discussing risk enables staff to understand how risk management contributes to achieving the objectives • Staff are informed of the entity's risk appetite • Evidence of the integration of risk information with key operational systems exists.	• The importance of communicating risk is apparent across the entity via - common understanding of risk management principles, escalating risk issues as they arise and informing internal and external stakeholders in a timely manner.
Element 7: Understanding and managing shared risk	• There are no formal arrangements in place to discuss and understand shared risks.	• The Policy defines shared risk • The Framework reflects the requirement to consider shared risk in supporting guidance and documentation • Informal arrangements are in place to discuss and understand shared risks.	• The Framework provides guidance on how to identify, assess, communicate and contribute to the management of shared risk • Formal governance arrangements are in place to discuss and understand shared risks.	• Senior executive champion shared risk behaviours by demonstrating a collaborative approach to managing shared risk • A common understanding of accountabilities and responsibilities for managing shared risk exists.	• The culture of the entity is one where identifying and managing shared risk is considered important • Agreed governance arrangements are in place to discuss, understand and effectively manage both current and emerging shared risks.	• Shared risk and the arrangements for managing it, are reflected in the governance framework and business processes • Established mechanisms and protocols for recording, monitoring and reporting on managing shared risk exist.
Element 8: Maintaining risk management capability	• There are limited resources available for the management of risk • Key individuals are provided limited risk management training • Informal processes exist to exchange risk information.	• The role of implementing the framework is shared with other responsibilities • Staff are able to develop risk management skills through access to regular training • Risk information is disseminated and shared across the entity informally.	• Dedicated resources are responsible for implementing the framework with a well-developed understanding of operations • Levels of risk competence are identified for each level of the entity • An effective flow of information through the entity exists • Risk information is stored centrally and accessible for key staff.	• The Risk manager or risk management team is responsible for assisting branches or business units to identify and evaluate risk in a consistent structured approach • A consistent approach to identifying and developing risk management skills internally exists • Real-time risk information is stored centrally, accessible by all staff.	• Operational budget reflects the cost of managing key risks • There is a demonstrated culture of knowledge sharing • Risk management information systems are used to undertake data analysis and inform organisational decisions.	• Risk resources are allocated based on detailed data analysis • Ongoing costs of implementing the framework are identified and managed within operational budgets • Demonstrated understanding of the need to build risk capability, focussing on priority areas for improvement, addressing underlying issues and utilising the skills of existing resources.
Element 9: Reviewing and continuously improving the management of risk	• There is limited oversight of the effectiveness of the framework • The reporting and consideration of risk issues is performed in an uncoordinated manner.	• Reviews of the effectiveness of the framework are undertaken on an ad-hoc basis by the internal audit function • Accountability for the oversight of key risks is unclear.	• Reviews on the performance elements of the framework are completed and reported to senior management regularly to establish review and monitoring plans • Regular reviews and evaluation of all material risks are undertaken • Regular risk reporting occurs in an agreed format • Dedicated staff are responsible for implementing the framework.	• Scheduled risk review and monitoring plans occurs across all branches and business units • Risk reporting includes qualitative and quantitative criteria to assess performance • Regular reviews of compliance with the risk framework are undertaken by internal audit • Ongoing oversight and monitoring of the risk function occurs to identify opportunities for improvement.	• The Framework contains real-time validation and assurance processes • Risk processes are independently assessed regularly • Review and monitoring plans are established and monitored independently • The Accountable authority and senior executive agree target maturity states and identify resources and investment to achieve these.	• Comprehensive data supports continuous review, monitoring and learning • The allocation of resources for managing risk is considered in the business unit operating budget, including the treatment of key risks and the costing of opportunities for improved processes or additional programs.