Australian Government

Comcover

2025 Comcover Risk Management Benchmarking Program

Risk Management Capability Maturity Model – Overview

Purpose of the Maturity Model

The Comcover Risk Management Maturity Model has been designed to assist entities with determining both their current and target level of risk management maturity against five identified areas of focus.

These areas of focus leverage fundamental risk management principles outlined in the Commonwealth Risk Management Policy (CRM Policy).

How to use the Maturity Model

- The model provides the framework by which entities measure their level of risk management maturity.
- The maturity model is progressive (i.e. where a competency has been achieved in a previous level, it is assumed in the next level of maturity and as such may not be referenced in subsequent descriptors). This provides entities with the opportunity to identify areas where existing processes can be strengthened, or where new processes can be implemented in order to enhance risk capability.
- Given the interrelated nature of risk management activities, capability descriptors may be relevant to multiple components of the maturity model.
- An entity's risk management capability must be fit-for-purpose in respect to the entity's size, complexity, operating environment and strategic goals and objectives. In determining a desired target risk maturity, entities are encouraged to evaluate the investment required to achieve the desired maturity and the intended benefits this will bring. As such, not all entities should necessarily be striving for an 'advanced' risk maturity in one or all of the five areas of focus.

1. Risk Maturity Model

1 Simple

- The risk management framework has been communicated across the entity, however it is not implemented consistently across operations and broader governance
- There are no formal arrangements in place to define the entity's desired risk culture
- Staff are able to develop risk management skills through access to ad hoc training
- Informal processes exist to support the management of shared risk
- Formal mechanisms to build and maintain organisational resilience have not been established.

2 Established

- Accountability for managing risk is articulated within the governance framework at business unit levels, and is recognised as key to effective business planning and decision making
- Formal activities are undertaken to obtain insights on the entity's current risk culture levels
- The risk management framework has been implemented and supports a consistent approach to risk identification, assessment, treatment, communication and reporting across current, emerging and shared risks
- The risk appetite statement is high-level, and has been linked to business strategies
- Mechanisms to build and maintain organisational resilience are conducted infrequently.

3 Defined

- Formal governance structures assess the risks associated with the development or implementation of new policies/programs/services
- Leadership actively demonstrate the entity's desired risk culture
- Communicating and escalating risk issues is considered in the day-to-day activities of staff
- Risk terminology is understood by all staff, providing a consistent approach to managing risk
- Defined processes exist to periodically monitor and report on risk management performance across the entity.

4 Embedded

- The risk management framework is integrated with strategic and business planning processes and reviewed and updated in accordance with the risk landscape
- A defined process exists to formally assess the effectiveness of risk culture change initiatives
- A consistent approach to communicating risk enables staff to understand how risk management contributes to achieving the entity's objectives
- Agreed governance arrangements and desired risk culture levels allow for effective management of current, emerging and shared risks
- Accountability is assigned to actively monitor and manage key risk controls and treatments.

5 Advanced

- Risk is considered as an integral part of the entity's governance systems, identifying the link between risk and the entity's strategic objectives
- Risk thinking is integrated into day-to-day operations to create a environment where open discussion is embraced
- The risk appetite statement, including tolerance limits linked to strategy, are used consistently to inform decision making
- Data sensing and analytics techniques are used to inform the identification, assessment and treatment of emerging risks
- Formal mechanisms exist to build and maintain organisational resilience, enabling the entity to have robust plans to respond to and recover from adverse events.

2. Areas of focus descriptors for the Maturity Model

RISK GOVERNANCE	Risk governance encompasses the organisational structures including risk ownership, responsibilities, and accountabilities across all levels for managing risk day-to-day, as well as the defined protocols for reporting and communicating risk information. Effective communication requires consultation with relevant internal and external stakeholders to enable transparent, complete and timely flow of information between decision makers. Information presented in a fit-for-purpose manner will allow risk to be applied to strategic (corporate) planning.
RISK CULTURE	Risk culture is the set of shared attitudes, values and behaviours that characterise how an entity considers and communicates risk in its day-to-day activities, where officials are supported to engage with calculated risks. A positive risk culture promotes an open discussion on current and emerging risks that considers both threat and opportunity, allowing risk to be appropriately identified, assessed, communicated and managed across all levels of the entity. Effective collaboration and communication enables clear accountabilities and measurement techniques to be implemented, allowing the entity to move towards its desired risk culture.
RISK CAPABILITY	Risk capability focuses on maintaining an appropriate level of capability across its people, systems, tools and processes to manage risk effectively across the entity. The nature and scale of this capability must be considered in the context of the entity's vision for risk and its current resource profile to enable timely and efficient communication of risk information.
RISK MANAGEMENT FRAMEWORK AND PRACTICES	Effective risk management practices should include (and not be limited to): strengthening the link between risk and strategic objectives, actively leveraging risk appetite as a decision-making tool, utilising appropriate tools to identify and analyse risk, developing effective risk treatments, and enhancing management of shared risk.
ORGANISATIONAL RESILIENCE AND AGILITY	Organisational resilience is maintained and strengthened through regular review and evaluation of risk performance and control effectiveness. Detailed analysis of internal and external data supports the identification of trends to equip the entity to be better prepared for emerging risks and future unknowns by adapting risk profiles, processes and tools in accordance with the changing risk landscape.

3. Capability descriptors for the Maturity Model

	1. SIMPLE	2. ESTABLISHED	3. DEFINED	4. EMBEDDED	5. ADVANCED
RISK GOVERNANCE	• Responsibility and ownership for managing risk and implementing the risk management framework is defined for limited roles across the entity • Communicating and escalating risk issues is limited to senior leaders, and may not be widely understood across the entity • Timely communication of risk information is acknowledged as important • A standard risk reporting format has been agreed with reports produced on an ad hoc basis.	• The risk management framework includes accountabilities and processes to enable the identification and management of risk and controls at business unit and program / project levels • Managing risk is part of the entity's overarching governance framework and recognised as a key component of effective business planning • Tailored reporting formats and set reporting frequencies have been agreed for target audiences, including both internal and external stakeholders.	• Formal governance structures assess and oversee risk management across business units, and for the development or implementation of new policies / programs / services • Communicating and escalating risk issues is considered in the day-to-day activities of all staff, including as an agenda item in internal meetings • Accountability and responsibility for managing risk is clearly defined and linked to staff performance.	• Centralised real-time risk information is readily available • A consistent approach to communicating risk enables staff to understand how risk management contributes to the achievement of goals and objectives • Managers and supervisors actively monitor the risk profiles of their areas of responsibility and ensure staff adopt the risk management framework as developed and intended • The entity communicates and engages with all required stakeholders (both internal and external) to enable effective risk management.	• Management of risk is fully integrated with the entity's overarching governance framework and recognised as vital to effective business planning • Risk information including strategic, operational, emerging and shared risks are reported regularly with consideration for the entity's risk appetite and desired risk culture • The importance of communicating risk is apparent across the entity via a common understanding of risk management principles, escalating risk issues as they arise and informing internal and external stakeholders in a timely manner.
RISK CULTURE	• Officials understand and agree on the need and value of effective risk management, with lessons learned communicated to staff • 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 • Senior executives (including the accountable authority) and line managers demonstrate the importance of managing risk in line with the risk management framework and systems • There are no formal arrangements in place to define desired risk culture.	• A common understanding of the meaning of good risk management results in a consistent use of language and understanding of risk-related concepts • Formal activities are undertaken to obtain insights on the entity's current risk culture levels • Good risk management practice is acknowledged by senior leaders who will informally speak with staff about opportunities to better manage risk • The desired risk culture of the entity has been articulated, however, has not been integrated with broader governance and operations.	• The behaviours and actions of leaders promotes an open and proactive approach to managing risk that considers both threat and opportunity • Risk terminology is understood by all staff, providing a consistent approach to managing risk • A maturity roadmap has been developed to support the achievement of the entity's desired risk culture, which defines assessment techniques and the required reporting structures • The entity's desired risk culture has been integrated into the risk management framework and communicated to staff.	• Desired risk culture has been articulated in accordance with strategic objectives, risk appetite and tolerances • The entity's current risk culture is formally and regularly assessed against the desired risk culture, with recommendations identified for improvement • Initiatives to uplift risk culture are in place and are monitored and reported on an ad hoc basis.	• The maturity roadmap includes considerations of the governance, communications, measurement techniques, desired leadership behaviours and resources required to support progress towards the desired risk culture • Demonstration of good risk management practices are communicated and rewarded, with consequence management processes established for non-compliant behaviours • Performance against desired risk culture is regularly assessed and reported, including monitoring intended benefits of risk culture change initiatives.
RISK CAPABILITY	• Staff are able to develop risk management skills through access to ad hoc training • Risk information is shared across the entity informally • Informal mechanisms exist to identify systemic or material risks across the entity that require escalation and prioritisation.	• Risk information is centrally stored and accessible to new and existing staff through key risk documents • Dedicated resources are responsible for implementing the risk management framework, with a well-developed understanding of operations • Risk management training is provided to different levels and responsibilities across the entity • An overarching approach to collecting and recording risk information has been defined, however, is not consistently utilised.	• A dedicated risk management team is responsible for assisting branches or business units to identify and evaluate risk in a consistent and structured approach • Resources are allocated to allow for effective implementation, monitoring and review of risks, with risk information consistently recorded and collected across the entity • Tailored initiatives are used to support and develop risk management capabilities across all staff levels of the entity.	• There is 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 • Internal and external information sources are used to inform risk assessment processes that consider both current and emerging risks • Risk information is integrated with key operational systems.	• A central repository is available which enables all personnel with risk responsibilities and accountabilities to view and edit risk information that is used to support organisational decisions • Risks are actively monitored to identify systemic or cross-functional risks which are escalated and prioritised in accordance with the entity's risk management framework • Risk resources spanning systems, tools, processes and people are allocated based on a robust understanding of the risk capability needs of the entity.
RISK MANAGEMENT FRAMEWORK AND PRACTICES	• The risk appetite statement is high-level and qualitative • The risk management framework is not consistently integrated with the entity's operations and overarching governance practices • The risk management framework articulates the risk management methodology and processes required to manage risk • Informal processes exist to support the management of shared risk.	• The risk appetite statement is high-level, and has been linked to business strategies • The risk management framework is actively implemented and supports a consistent approach to risk identification, assessment, treatment, communication and reporting across current, emerging and shared risks • Enterprise-wide risks are considered in corporate planning, budgeting and reporting processes.	• The entity's risk appetite has been defined and communicated to facilitate strategic and operational planning and inform risk-related discussions • The risk management framework includes measures for accountability and management of risk and controls at business unit and program / project levels, and is embedded in operational and reporting frameworks • Senior executives (including the accountable authority) demonstrate a collaborative approach to managing shared risk, with clear accountabilities for all parties defined.	• A comprehensive set of risk appetite and tolerance statements defined across strategic objectives include measures that enable effective monitoring and review • Risk management is embedded in decision making for strategic planning and project and program risks, including business cases • Agreed governance arrangements and desired risk culture levels allow for effective management of both current and emerging shared risks.	• Risk appetite and tolerance statements have been articulated to support the achievement of the entity's strategic objectives and are used consistently across the entity to inform decision making • A comprehensive process that utilises both quantitative and qualitative techniques exists to support the identification, analysis and evaluation of risk (both current and emerging) across enterprise, business unit, program and project levels • Established mechanisms for recording, monitoring, managing and reporting shared risks are embedded in the entity's governance framework, including sharing risk insights across portfolio entities.
ORGANISATIONAL RESILIENCE AND AGILITY	• The effectiveness of the risk management framework is reviewed on an ad hoc or informal basis • Formal mechanisms to build and maintain organisational resilience have not been established • Limited methods are in place to assess control design and performance effectiveness for critical business processes or risks • Risk documentation is reviewed and updated on an ad hoc basis.	• Reviews on the performance of the risk management framework are completed and reported to senior management regularly • A defined program of review occurs to ensure the entity's risk profile reflects the current risk and control environment • Mechanisms to build and maintain organisational resilience are conducted infrequently.	• Scheduled risk reviews and monitoring of plans occurs across all branches and business units to ensure the entity's risk profile reflects the current risk and control environment • Regular reviews of compliance with the risk management framework are undertaken by internal audit and/or external parties with plans developed to support recommendations for improvement • Risk documentation is reviewed and updated in accordance with a defined schedule.	• Formal mechanisms exist to build and maintain organisational resilience • A regular and independent process has been established to assess control design and effectiveness over critical business processes • Tools and techniques exist to identify, analyse and manage emerging risks beyond the current planning horizon • Opportunities for improvement and good practice are identified through analysing risk information.	• The entity has robust, tested plans to respond to and recover from adverse events • Comprehensive data sensing and analysis supports continuous review, monitoring and learning, with a focus on identifying, analysing and preparing for emerging risks • Better practice insights are actively utilised to improve risk management processes, including assessment of control design and effectiveness for critical business risks and active consultation with external parties.