Australian Government
Department of Finance

Benchmarking Survey 2019 – Risk Management Capability Maturity Levels

Risk Management Capability Maturity Model

The Comcover Risk Management Maturity Model has been designed to assist entities to determine their current level of risk management maturity across each of the nine elements of the Commonwealth Risk Management Policy. The model assists entities to identify a target level of risk management maturity by providing high level descriptors of capability or competency for each level of the maturity model.

By measuring an entity's current risk maturity, and tracking its progress to its target maturity state, entities will better understand the actions they need to take to improve their level of risk management efficiency and effectiveness.

In determining your entity's target risk maturity, you need to consider the model as progressive. That is, where a competency has been achieved in a previous level it is assumed in the next level of maturity.

ELEMENT ONE: Establishing a risk management policy

Fundamental

- The entity has a risk management policy which has been endorsed by the accountable authority.
- The policy defines the approach and rationale for managing risk within the entity.
- Communication and understanding of the policy and its objectives for managing risk vary across different levels of the entity.
- Understanding of the entity's appetite for risk is inconsistent across the entity.

Developed

- The entity's risk management policy has been communicated throughout the entity.
- There is an innate understanding of the entity's risk appetite by senior executive and the accountable authority that is implied in the entity's risk documentation, in particular its consequence and likelihood tables.

Systematic

- The entity's risk management policy outlines the required accountability and responsibility for managing risk.
- A common definition of risk exists and is applied throughout the entity.
- The entity's risk appetite statement is high-level and qualitative.

Integrated

- The entity's risk management policy includes a vision for the continuing development of its risk management programme.
- The policy contains a high level risk appetite statement with both qualitative and quantitative elements, which is linked to the entity's business strategies.
- The policy is reviewed and updated to reflect changes in the internal and external environment as they occur.

Advanced

- The entity's risk management policy defines the linkages between risk and strategy within the entity.
- The policy is reviewed and updated on an annual basis or more regularly if circumstances change.
- The entity's risk appetite is articulated through individual risk appetite statements developed for each source or category of risk. These statements are supported and operationalised by measures that enable effective monitoring and review.

Optimal

- The entity's risk management policy considers the management of risk as an integral part of the entity's governance systems, and this reflects the link between risk and realising the entity's strategic objectives.
- The policy contains information for all staff and stakeholders on the resources and processes dedicated to the management of risk.

ELEMENT TWO: Establishing a risk management framework

Fundamental

- The entity's risk management framework (framework) is articulated at a high level but not integrated with the entity's operations and overarching governance practices.
- Resources allocated to manage risk are limited and are often shared across other responsibilities.
- The framework and systems used to manage risk may not be widely understood or practiced.

Developed

- The entity's risk management framework articulates the methodology and processes required to manage risk within the entity.
- The effectiveness of the entity's framework is reviewed on an ad hoc or informal basis.

Systematic

- The entity's risk management framework has been implemented and supports a consistent approach to the identification, assessment, evaluation and treatment of risk.
- Resources have been allocated to implement, monitor and review the framework.
- The framework has performance measures that are reviewed on an annual basis.
- The framework explains the requirements for reporting the status of key risks including how an entity contributes to managing shared or cross jurisdictional risk.

Integrated

- The entity's risk management framework is embedded in the operations of the entity and is part of its overarching governance and management framework.
- The techniques for the 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 on a quarterly basis.

Advanced

- The entity's risk management framework includes measures for the accountability and management of risk and controls at both a business unit and programme/project level.
- Key risk indicators are used to measure the overall performance of the entity's risk management framework.
- There is a hierarchy of tools to guide decision making and support regular reporting and the escalation of risks.
- Risk management documentation and data is centrally stored and readily available to officials.

Optimal

- The entity's risk management framework includes techniques to identify, analyse and measure current, future and emerging risks through the collection and analysis of data including loss event, near-miss data and root cause analysis.

- Real time risk information is readily available from a centralised source to support decision making.
- The appetite for managing risk in the entity is understood and informs discussions on the changing profile of individual risks or themes.
- Performance reporting requirements are in place to measure and monitor risk exposures.
- There is no duplication of risk management activities for different risk related functions across branches or business units, resulting in the effective flow of information across the entity.

ELEMENT THREE: Defining responsibility for managing risks

Fundamental

- Responsibility for the management of risk has been articulated in the entity's accountable authority instructions.

Developed

- The entity's accountable authority instructions and risk management policy articulate who is accountable and responsible for the management of risk, and the implementation of the entity's risk management framework.
- The management of risk is not specified in individual's performance agreements.

Systematic

- The entity has a risk manager or team responsible for implementing the entity's risk management framework and these roles and responsibilities are defined in the entity's accountable authority instructions and risk management policy.
- Accountability and responsibility for managing risk is clearly defined and linked to the performance of staff at each level of the entity.
- Accountability and responsibility for managing, or oversighting, risk is included in the charters of executive committees including audit and or risk committee.

Integrated

- There is a formalised governance structure to assess and oversight the management of risk at business unit and executive levels.
- The entity has a clear definition of what constitutes a new policy, programme and/or service and there is a formal governance structure in place for the assessment of the risks associated with the development or implementation of these.
- The entity's risk manager or team coordinates the implementation of the entity's framework, its risk profiles and action plans as well as evaluating risk planning to ensure consistency and accuracy of practice.

Advanced

- Senior leadership supports the entity's risk manager or team to facilitate, challenge and drive risk management capability in the entity.
- The risk management team report to senior executive, the audit committee or the accountable authority at regular intervals on the performance of the entity's risk framework.
- The entity's Executive approves the entity's risk appetite, including its risk profile, and the management of significant and critical risks, as well as overseeing the continual improvement of the entity's risk framework.

Optimal

- Managers and supervisors monitor the risks and risk profiles of their areas of responsibility and ensure staff adopt the entity's risk management framework as developed and intended.

ELEMENT FOUR: Embedding systematic risk management into business processes

Fundamental

- Branch and Business unit risks are reviewed annually however these risks do not inform the entity's business planning, budgeting and reporting processes.
- The definitions used to manage risk are inconsistently understood throughout the entity as there is limited guidance for identifying risk processes or differentiating between risk classes.

Developed

- Enterprise-wide risks are considered in the entity's 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.

Systematic

- The entity's risk management framework is embedded in its operational, process and reporting frameworks ensuring greater coordination of risk activities.
- The entity's approach to managing risk is a part of its overarching governance framework and recognised as key to effective business planning.
- The processes of identification, assessment, monitoring, communicating and reporting risk are consistent across the entity.
- The entity's risk profile enables the prioritisation of an entity's audit and assurance activities.

Integrated

- The process of managing risk occurs at the policy, program and/or service delivery level and is evident in the collation and analysis of management information.
- The entity's risk appetite has been defined and communicated to all staff to ensure an appropriate level of risk identification is undertaken when developing strategic and operational plans.
- Specialist risk programs are documented and included in regular reports to senior executive and/or the accountable authority.

Advanced

- The entity's approach to managing risk is fully integrated with its overarching governance framework and recognised as key to effective business planning.
- The entity identifies opportunities for improvement that arise as a result of analysing risk information and identifying good risk management practice.
- The entity has developed a comprehensive set of risk appetite and tolerance statements including KPI's that cascade from high level down to the detailed level.

Optimal

- The entity's risk management processes are utilised at enterprise, business unit, programme and project levels and for all risk activities including specialist areas such as information technology, fraud, security, business continuity, crisis management and business continuity.
- Formal mechanisms exist to build and maintain organisational resilience.
- The entity's risk appetite statement, including its tolerances and limits for different categories of risk are used consistently across the entity to inform decision making.

ELEMENT FIVE: Developing a positive risk culture

Fundamental

- Officials understand and agree the need and value of effective risk management.
- Senior executives and line managers demonstrate the importance the entity places on managing risk in line with the entity's framework and systems.

Developed

- The entity's risk management framework is integral to its operating model.
- Lessons learnt are communicated to staff.
- There is a common understanding of the meaning of good risk management and as a result a consistent use of language and understanding of risk related concepts.

Systematic

- Surveys and external reviews undertaken (such as the annual state of the service report or capability reviews) are analysed to provide insights into the risk culture of the entity.
- The entity analyses loss incidents and identifies areas for improvement. This includes acknowledging good risk management practice and speaking with staff regularly about opportunities to better manage risk.

Integrated

- Senior executives are held accountable through their performance agreements for managing risk including responsibility for strengthening the risk culture of their teams.
- The entity's risk culture is formally and regularly assessed with recommendations identified for improvement.
- The entity has a risk management framework that is integrated with its overarching governance framework so that the task of managing risk is not regarded as an additional responsibility or burden.

Advanced

- Officials are comfortable raising concerns with senior managers and those being challenged respond positively.
- There is a sponsor at the senior executive level of the entity that leads and promotes the management of risk across the entity.
- The entity learns from negative and positive situations so that policy and procedural changes are made to improve the management of risk in the future.

Optimal

- The culture of the entity is one that demonstrates and promotes an open and proactive approach to managing risk that considers both threat and opportunity.
- Examples of good risk management practice are communicated by senior executive and individuals that excel in demonstrating good risk management practice in their day to day responsibilities are rewarded.

ELEMENT SIX: Communicating and consulting about risk

Fundamental

- There is no common risk language used across the entity with limited reporting of risks to senior executive, the accountable authority or key stakeholders.
- Branches and or business units communicate with their stakeholders but this information is not shared across the entity.
- Communication of risk issues with senior executive and/or the accountable authority is as requested. As a result, this may lead to duplication of information across the entity.

Developed

- Communication with the senior executive and/or the accountable authority is limited to information on the specialist risks of the entity such as work health safety, security or fraud. Risks are discussed at the senior executive level but it is not apparent how this information is communicated or shared with those responsible for managing specific risks.
- A common risk language is used and understood to communicate risk by the risk management function and senior leadership teams but these terms are not consistently understood across the entity.

Systematic

- There is a common understanding of the principles and importance of managing risk across the entity.
- The entity acknowledges the importance of communicating risk in a timely manner by providing information on the management of key risks and the effectiveness of the entity's risk management framework to senior executive and the accountable authority.
- While the entity analyses incidents and identifies areas for improvement feedback is not commonly used to improve policies, procedures and related communications.
- External communication occurs to inform stakeholders of the management of key risks and to assist them in understanding the entity's approach to managing risk.

Integrated

- The entity's risk terminology is understood by all staff providing a consistent approach to managing risk across all branches and functions internally.
- The importance of 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.

Advanced

- There is a consistent approach to communicating and discussing risk, enabling staff to develop an understanding of how risk management contributes to achieving an entity's objectives.
- Staff are informed of the entity's appetite for risk through a variety of communication and information channels which are regularly reviewed and updated as the entity's context for managing risk changes.

- There is evidence of the integration of risk information with key operational systems such as strategic planning, work health safety and business continuity.

Optimal

- The importance of communicating risk is apparent across the entity with a high level of importance placed on ensuring a common understanding of the principles for managing risk; understanding the need to escalate risk issues as they arise; and the importance of informing both internal and external stakeholders in a timely manner.

ELEMENT SEVEN: Understanding and managing shared risk

Fundamental

- There are no formal arrangements in place to discuss and understand shared risks between the entity and other external entities or stakeholders.

Developed

- The entity's risk management policy defines shared risk.
- The entity's risk management framework reflects the requirement to consider shared risk in supporting guidance and documentation.
- Informal arrangements are in place to discuss and understand shared risks between the entity and other external entities.

Systematic

- The entity's risk management 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 between the entity and other external entities.

Integrated

- Senior executive champion shared risk behaviours by demonstrating a collaborative approach to managing shared risk.
- There is a common understanding of accountabilities and responsibilities for managing shared risk within the entity.

Advanced

- The culture of the entity is one where identifying and managing shared risk is considered important.
- Where an entity shares risk with another entity or organisation there are agreed governance arrangements in place to discuss, understand and effectively manage both current and emerging shared risks.

Optimal

- The concept of shared risk, and the arrangements for managing it, is reflected in the entity's governance framework and business processes.
- The entity has established mechanisms and protocols for recording, monitoring and reporting on managing shared risk.

ELEMENT EIGHT: Maintaining risk management capability

Fundamental

- There are a limited number of resources available for the management of risk. Primary resources include the allocation of staff to support the implementation of an entity's risk framework and a budget to manage specific risks.
- Key individuals, including senior executive, the accountable authority and risk personnel are provided limited training to understand and execute their risk management responsibilities.
- There is an informal process in place to exchange risk information between the senior executive and the accountable authority with individual branches or business units.

Developed

- The role of implementing the entity's risk management framework is shared with other responsibilities such as audit, security or facilities management.
- Staff are able to develop their level of risk management skills through access to regular training.
- Risk information is disseminated and shared across the entity informally.

Systematic

- Staff responsible for implementing the entity's risk management framework are dedicated resources to the risk management function, with a well developed understanding of the entity and its operations.
- Levels of risk competence have been identified for each level of the entity and there is support for the ongoing development of risk management skills appropriate for each level.
- There is an effective flow of information through the entity with a structured approach to the provision of information to senior executive and the accountable authority that consolidates all risk data.
- Risk information is stored in a centralised repository and accessible to key staff.

Integrated

- The risk manager or risk management team is responsible for assisting branches or business units to identify and evaluate risk, ensuring a consistent and structured approach is applied.
- Management regards the resourcing of risk as important therefore the entity has a consistent approach to identifying and developing risk management skills internally.
- Risk information is stored in a centralised repository that is accessible by all staff and provides access to real time data.

Advanced

- The entity's operational budget reflects the cost of managing key risks.
- There is a culture of knowledge sharing with the cost of managing risk appreciated at all levels.

- Risk Management Information Systems are used to undertake data analysis and inform organisational decisions. This includes historical data such as near misses and loss events as well as predictive data that includes the identification of new and emerging risks and the potential costs of these risks.

Optimal

- Risk resources are allocated based on detailed analysis supported by data on current, future and emerging risks.
- The ongoing costs associated with the implementation of an entity's risk management framework, such as risk treatment, resourcing, education and communication, are identified and managed within an entity's operational budget.
- The entity demonstrates an understanding of the need to build risk capability through the effective allocation and use of risk resources. This is achieved by focusing on priority areas for improvement, addressing underlying issues, and utilising the skill of existing resources.

ELEMENT NINE: Reviewing and continuously improving the management of risk

Fundamental

- There is limited oversight of the effectiveness of an entity's risk management framework.
- The reporting and consideration of risk issues is performed in an uncoordinated manner.

Developed

- Reviews of the effectiveness of the entity's risk management framework are undertaken on an ad-hoc basis by the internal audit function.
- Accountability for the oversight of key risks is unclear.

Systematic

- Reviews on the performance elements of the entity's risk management framework are completed. Results are reported to senior management and the entity's accountable authority so that review and monitoring plans are established for future periods in select functions.
- Regular reviews and evaluation of all material risks are undertaken in the entity.
- Reporting of risk occurs on a regular basis enabling the consideration of key issues in a timely manner by the senior executive and accountable authority.
- The risk management framework includes a process by which individuals certify the performance of their responsibilities.
- Reporting formats have been agreed and are tailored to the target audience.

Integrated

- Scheduling of risk review and monitoring plans occurs across all branches and business units.
- Risk reporting to the senior executive and the accountable authority includes the use of qualitative and quantitative criteria to assess performance against appetite and tolerance levels.
- Regular reviews of compliance with the risk framework are undertaken by internal audit.
- Ongoing oversight and monitoring of the risk function occurs on a regular basis to identify opportunities for improvement in the framework and processes of the entity.

Advanced

- The entity's risk management framework contains validation and assurance processes on a real-time basis with performance considered by senior executive.
- Risk processes are assessed on a regular basis by an independent party.
- Review and monitoring plans are established for future periods across all functions. These plans are independently monitored to determine progress and outcomes.
- The accountable authority and senior executive discuss and agree target maturity levels for each critical component of risk management and a conscious decision is made about the allocation of risk management resources and the necessary investments to achieve an agreed future vision.

Optimal

- Comprehensive data collection supports continuous review, monitoring and learning from outcomes (e.g. internal audit, near misses, loss event data, independent reviews).
- The management of risk is reflected in branch and business unit budgets, with the cost of risk being identified and managed effectively. The entity considers the cost of managing risk at all levels and reports on this to the senior executive and accountable authority on a regular basis. As a result, the allocation of resources for managing risk is considered in the entity's operating budget. This includes the treatment of key risks and the costing of opportunities for improved processes or additional programmes as a result of the identification of opportunities from the risk management process.