Australian Government
Department of Finance

Implementing the Commonwealth Risk Management Policy – Guidance

2016

Resource Management Guide 211

Department of Finance
Commercial and Government Services

978-1-925205-46-6 (Print)
978-1-925205-45-9 (Online)

Contact us
Inquiries regarding the licence and any use of this work are welcome at:

Commercial and Government Services
Department of Finance
One Canberra Avenue, Forrest ACT 2603
Email: governmentadvertising@finance.gov.au

Contents

Introduction

Purpose of this Guide

This Guide provides practical advice to assist Commonwealth officials in implementing the requirements of the Commonwealth Risk Management Policy.[1]

The Guide is designed to be used as a learning resource and is not mandatory. It is important that entities develop risk management frameworks and systems that are tailored to the needs of their organisation. Entities may elect to adapt the concepts contained in this Guide to suit their specific needs or use alternative methodologies.

The mandatory elements of the Commonwealth Risk Management Policy are repeated in this Guide in the boxes at the beginning of each element.

What is risk management?

Risk is the effect of uncertainty on objectives. Risk is the possibility of an event or activity preventing an organisation from achieving its outcomes or objectives.

Risk management is the activities and actions taken to ensure that an organisation is conscious of the risks it faces, makes coordinated and informed decisions in managing those risks and identifies potential opportunities.

What are the benefits of risk management?

- improved ability to identify, evaluate, and manage threats and opportunities
- improved accountability and better governance
- better management of complex and shared risks
- improved financial management
- improved organisational performance and resilience
- confidence to make difficult decisions
- decreased potential for unacceptable or undesirable behaviours such as fraud and harassment.

[1] The Commonwealth Rick Management Policy and section 16 of the PGPA Act set out a framework that encourage Commonwealth entities to engage with risk, demonstrate innovative thinking and establish and maintain appropriate systems of risk oversight and internal control.

Policy Elements

Element one - Establishing a risk management policy

Commonwealth Risk Management Policy

An entity must establish and maintain an entity specific risk management policy that:

a. defines the entity's approach to the management of risk and how this approach supports its strategic plans and objectives
b. defines the entity's risk appetite and risk tolerance
c. contains an outline of key accountabilities and responsibilities for managing and implementing the entity's risk management framework
d. is endorsed by the entity's accountable authority.

The key elements of an entity's risk management policy

Overview of the approach to risk management

Entities are encouraged to include in their risk management policy a statement of intent to embed risk management into their decision making and performance management processes. The inclusion of a risk philosophy statement or key principles can be useful in conveying to officials the tone for risk management in the entity.

Risk appetite and tolerance

Risk appetite is the amount of risk an entity is willing to accept or retain in order to achieve its objectives. Risk appetite is usually set out in a statement or series of statements that describe the entity's attitude toward risk taking.

Risk tolerance is the specific level of risk taking that is acceptable in order to achieve a specific objective or manage a category of risk. Risk tolerance represents the practical application of risk appetite and will be most effective when it is easily understood by all officials.

A risk appetite and tolerance statement provides officials with an understanding of the entity's acceptable risk levels for all significant risk categories. In cases where risk appetite is low, this statement provides guidance to officials on what decisions they cannot make. Where the entity is prepared to take increased levels of risk, a statement reflecting this empowers officials to make acceptable risk-based decisions.

Risk tolerance statements often include quantitative measures to enable monitoring and review. For example an entity with a low risk appetite for IT system outages may define their risk tolerance as no more than five days of system outages per annum.

While the inclusion of a risk appetite and tolerance statement in a risk management policy can be useful in setting the tone for risk taking in the entity, this may not always be practical due to the level of detail required. In such circumstances, it may be more practical to refer to it or link to other document/s detailing the entity's risk appetite and tolerance.

Key accountabilities and responsibilities

While the accountable authority is ultimately responsible for maintaining systems of risk oversight, management and internal control, an entity's risk management policy can be a useful means of communicating more specific risk management responsibilities to officials. Aside from those requirements set out in element three of the Commonwealth Risk Management Policy, think about what additional responsibilities and accountabilities you would like to communicate.

A statement noting that all officials in the entity are responsible for managing risk can be a useful way of communicating to staff that it is not just the risk management area that is responsible for managing risk.

Accountable authority endorsement

A key role of the policy is to provide a clear and meaningful mandate for the entity's risk management framework. It is critical that the accountable authority understands and endorses the policy as this signifies to all officials the expectation that the policy is an essential part of their day-to-day work.

A written statement or personal message from the accountable authority (or senior leadership) that summarises the entity's risk management policy can also effectively and clearly express the intentions and requirements of the organisation. The way in which such messages are distributed and publicised are also important factors in how successfully risk management issues are communicated.[2] Options can include circulation through the entity's internal network, publications such as newsletters, displays in corridors and lifts and making it available externally via the internet.

Practical tips

- Undertake regular reviews to ensure the entity's risk management policy and risk appetite remain aligned with risk processes.
- Link the entity's risk management policy to other elements of the risk management framework such as more detailed procedures and guidance material.
- Include a visionary statement in the risk management policy that includes what the entity is seeking to achieve through good risk management and key goals for the risk management program in the future.

[2] Standards Australia, SA/SNZ HB 436:2013 Risk Management Guidelines – Companion to AS/NZS ISO 31000:2009, p31

Element two - Establishing a risk management framework

Commonwealth Risk Management Policy

An entity *must* establish a risk management framework which includes:

a. the overarching risk management policy
b. an overview of the entity's approach to managing risk
c. how the entity will report risks to both internal and external stakeholders
d. the attributes of the risk management culture that the entity seeks to develop, and the mechanisms employed to encourage this
e. an overview of the entity's approach to embedding risk management into its existing business processes
f. how the entity contributes to managing any shared or cross jurisdictional risks
g. the approach for measuring risk management performance
h. how the risk management framework and entity risk profile will be periodically reviewed and improved.
i. The risk management framework *must* be endorsed by the entity's accountable authority.

Designing a risk management framework

A risk management framework is a set of components that support the consistent and systematic management of risk in an entity. Each entity needs to determine its own risk management framework that is the best fit for the entity's purpose, structure and size.

An entity's risk management framework is most effective when it is aligned with other business processes. Key amongst these include the entity's:

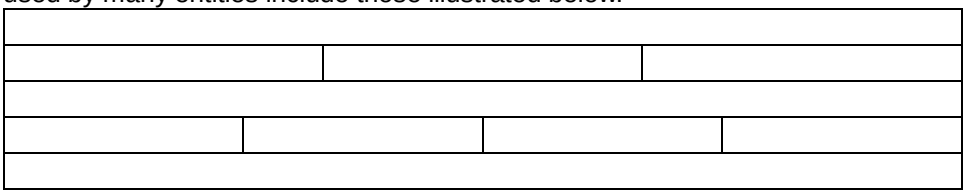
- corporate plan
- management and decision making
- governance and assurance arrangements
- change and business improvement programs
- operational program planning, management, and reporting requirements.

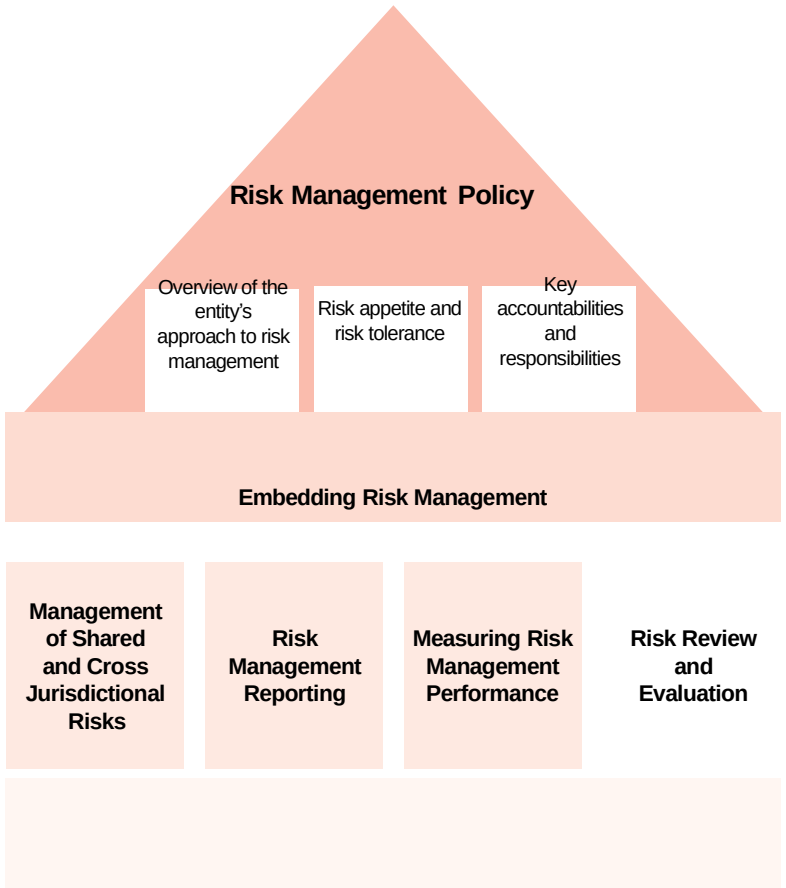
While a risk management framework sets the foundation for risk management, it is the entity's risk culture that will ultimately determine how effective it is in changing the behaviour of officials.

The key attributes of a good risk management framework

- It is fit-for-purpose and tailored to the needs of the entity.
- It is well understood, consistently applied, integrated and centralised across the entity.
- It details the required actions for designing, implementing, monitoring, and reviewing risk management in the entity.
- It is used by officials as part of their day-to-day decision making.

There is no standard format or structure for a risk management framework. The nature of the work carried out by each entity will determine the design and sophistication of its risk management framework. However, framework elements used by many entities include those illustrated below.





Positive Risk Culture

Practical tips

- Include a document map in the risk management framework to clarify and differentiate between policy, guidance and process documents. This avoids confusion.
- Structure documents into a logical hierarchy; separated into strategic and operational level guidance.
- Provide training and ongoing support to officials so that they are aware of, and understand, the entity's risk management framework.
- Make it easy for officials to access the framework content, for example, through the entity's intranet and other internal networks.
- Review and update the entity's framework promptly after restructures or changes in operating environment.
- Regularly review the entity's risk management framework to ensure that all classes or categories of risk to which the entity may be exposed are being considered and managed.

Element three - Defining responsibility for managing risk

Commonwealth Risk Management Policy

Within the risk management policy, the accountable authority of an entity *must* define the responsibility for managing risk by:

a. defining who is responsible for determining an entity's appetite and tolerance for risk

b. allocating responsibility for implementing the entity's risk management framework

c. defining entity roles and responsibilities in managing individual risks.

Key responsibilities for managing risk

Responsibility for determining risk appetite and tolerance

This may include:

- the person who is ultimately responsible for determining risk appetite and tolerance (usually the accountable authority working with the senior executive)
- specific responsibilities for developing, approving, monitoring and adjusting an entity's risk appetite and tolerance.

Responsibility or implementing the risk management framework

This may include:

- design
- publication
- review of the entity's risk management framework

These responsibilities will be most effective where they are clearly defined, effectively communicated and assigned to a specific person or team

Responsibility for managing individual risks

Responsibilities that may be defined include:

- **Risk owners.** Accountable for managing a particular risk
- **Control owners.** Responsible for maintaining the effectiveness of measures to modify risk
- **Risk treatment owners.** Responsible for implementing strategies in cases where the risk level is unacceptable after controls are applied

Guidance can be provided on how to discharge these responsibilities and how risk and control owners can best interact so that risks are actively managed within agreed tolerances.

Entities are encouraged to include a statement in their risk management framework that all officials at all levels of the entity are responsible for managing risk. These responsibilities include risks within an individual's area of control and whole-of-entity and shared risks.

Examples of some typical risk management responsibilities can be found at Appendix B.

Practical tips

- Document the entity's risk processes, including guidelines, so that the accountable authority and all other senior officials understand their responsibilities for overseeing the entity's risk management processes and key risks.
- Ensure that officials understand any business risks that they own, how these risks relate to and may impact on the entity's enterprise risks, and their roles in managing risk.
- Develop clear and consistent risk register templates which, when completed, make the risk management responsibilities of each official clear and easily updated as required.
- Make risk management a key competency and responsibility of all officials. Incorporate risk management responsibilities into job descriptions, duty statements and performance agreements.

Element four - Embedding systematic risk management into business processes

Commonwealth Risk Management Policy

Each entity *must* ensure that the systematic management of risk is embedded in key business processes.

Opportunities to embed risk management

Successfully embedding risk management into an entity's business processes is challenging and thought provoking. It requires an approach tailored to the entity's corporate objectives, operating environment and context. A useful approach to embedding risk management can be to establish short and long-term plans for embedding risk management. These can then be communicated to key stakeholders.

Embedding risk management takes time, but there are a number of opportunities to achieve quick wins in the following areas:

- **Governance**. An entity's governance function has a number of key risk management roles. These include helping to integrate risk management into strategy, establishing risk appetite through the entity's risk management policy, defining risk management roles and responsibilities, benchmarking, and reviewing how risk is managed within the entity.
- **Corporate planning**. Assessing and managing an entity's enterprise risks is an integral part of an entity's corporate planning framework. An entity's strategic objectives can be the starting point of any risk identification process.
- **Change management**. Change management policies and instructions may include the requirement for a risk assessment of all significant change activities.
- **Projects and programs**. Project and program implementation involves constantly identifying and managing risk, such as shared risk in complex projects and risk interdependencies between projects. This could allow individual project risks to be aggregated to provide a program and portfolio view.
- **Audit and assurance programs**. Clearly understanding an entity's risk profile enables the prioritisation of an entity's audit and assurance activities. The outcome of internal and external audit activities may influence the design of an entity's control framework.

- **Organisational resilience**. Increasing organisational resilience allows entities to resist being affected by an event or increases their ability to return to an acceptable level of performance in an acceptable period of time after an event has occurred.[3]

Alignment with specialist risk categories

Specialist risk categories often have their own legislation, standards, compliance and reporting obligations. Entities may also have specialist programs and processes including:

- business continuity and disaster recovery
- fraud control
- workplace health and safety
- protective security

While a specialist program may lead to an increased focus and management of these risks, specialist programs may benefit from being connected to the entity's overarching risk management framework to ensure consistency. This can be achieved by adopting common terminology and processes across all programs.

Practical tips

- Use the entity's risk management policy and its accountable authority instructions to link the risk management framework to other corporate frameworks and processes.
- Reflect the entity's risk appetite and tolerances in the entity's internal control framework and delegation arrangements in areas such as finance, procurement, business continuity and human resources.
- Assist business unit owners to embed risk management into their activities by providing common risk tools and templates that can be incorporated into their documents and processes.
- Use changes or restructures in the entity as an opportunity to embed risk management in business processes or functions.
- Include easy-to-use risk management tools and templates into corporate and business planning documentation and processes.
- Communicate quick wins as soon as they occur. Highlight how embedding risk management into business processes resulted in innovative outcomes or other benefits to the organisation through identifying and treating risks.

[3] ASIS SPC.1-2009 American National Standard, Organisational Resilience: Security, Preparedness and

Element five - Developing a positive risk culture

Commonwealth Risk Management Policy

An entity's risk management framework *must* support the development of a positive risk culture.

Characteristics of a positive risk culture

A positive risk culture exists in an entity when officials understand the risks facing their entity and consistently make appropriate risk-based decisions. A poor risk culture is often evidenced by officials being ignorant of the entity's risks, being excessively risk averse or overconfident.

A positive risk culture generally includes the following attributes:

- leaders, managers and supervisors consistently and positively demonstrate and discuss the importance of managing risk appropriately
- the entity's risk management framework is integral to its operating model
- officials are comfortable talking openly and honestly about risk, using commonly understood risk terms and language
- officials understand and agree the need and value of effective risk management
- officials own and manage risk and proactively seek to involve others as appropriate
- officials own and manage complex and shared risks with others
- incentives reinforce appropriate risk-related behaviour
- officials are comfortable raising concerns with authority figures and those being challenged respond positively
- the entity has a supportive environment for escalating risk issues with the senior executive.

Why is a positive risk culture important?

Culture is more than just complying with your entity's risk management framework. The behaviours and attitudes to risk are just as important as the framework.

Decisions are often made, and risks managed, without complete information, with inadequate resources and against competing priorities. In these circumstances a strong risk culture will support the proper management of risk.

How to influence risk culture

A brief description of the influencers of risk culture, and some examples of desirable and detrimental risk behaviours are provided below.

Risk competence The collective risk management competence of the entity	
Desirable behaviours	• Proactive sharing of best practice • Consulting with others often
Detrimental behaviours	• Reluctance to learn from past mistakes • Following the herd
Organisation's risk environment How the organisational environment is structured and what is valued	
Desirable behaviours	• Adhering to risk management policies, processes and procedures • Listening to others • Involving risk professionals in important risk decisions
Detrimental behaviours	• Reluctance to escalate risks • Minimising risks, optimism bias • Cutting corners
Motivation The reasons why people manage risk the way that they do	
Desirable behaviours	• Innovating and changing poor practices • Taking personal accountability for managing risks • Admitting to making mistakes
Detrimental behaviours	• Shooting the messenger • Avoiding responsibility • Rewarding excessive risk taking
Relationships How people in the entity interact with others	
Desirable behaviours	• Open and honest dialogue regarding risks • Constructive response to challenge
Detrimental behaviours	• Inadequate challenge of excessive risk taking • Yielding to inappropriate pressure from others

In determining the risk behaviours they will display, officials are often guided by the accountable authority and the entity's executives. Key elements include:

- **Role models**. Influential individuals who lead by example. The risk management behaviours they display guide others. It can be useful to assign accountability of the entity's risk culture to a visible senior executive sponsor.
- **Explicit messages**. During recruitment and induction, and throughout their careers, officials are provided with many instructions and guidelines that will influence how they view and manage risk.
- **Incentives**. The manner in which officials are rewarded and recognised. How these incentives take into account risk management behaviours will indicate how risk management is valued.
- **Symbols and actions**. The daily actions of leaders will be noted by officials and mirrored.

Measuring risk culture

It may take years for an entity to develop and maintain a positive risk culture. An entity's risk culture can be monitored and formally assessed through staff surveys or consultations.

Practical tips

- Identify and prioritise key behaviours to influence and shape a positive risk culture.
- Encourage all officials in management roles to communicate regularly with their teams about the value of good risk management.
- Identify and connect a network of risk champions across the entity that can encourage positive risk behaviours through their role, personal experience or reputation.
- Reward and recognise positive risk management behaviour both publicly and through the entity's performance management processes. Positive reinforcement of successful risk management approaches and outcomes maintains momentum and promotes good risk management practices.
- Where an entity accepts an optimal level of risk, this may result in that risk being realised. Treat these events as opportunities to review, learn and improve the management of similar risks.
- In establishing a more positive risk culture, focus on changing attitudes and behaviours rather than just implementing new policies and procedures.
- A positive risk culture is not a single activity. Prioritise the key risk management behaviours you wish to change and implement practical measures to influence and shape these first.

Element six - Communicating and consulting about risk

Commonwealth Risk Management Policy

Each entity *must* implement arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders.

How to communicate risk

Communicating risk information with stakeholders is important, as it maintains confidence and trust and develops a common understanding of the entity's risks. External stakeholders such as ministers, other government entities, suppliers and the wider community may need an opportunity to communicate their views and feel involved in decision making where appropriate.

Develop a risk communication plan

A risk communication plan can be an effective way of documenting an entity's approach to communicating risk. When developing a risk communication plan, consider both external and internal reporting requirements. To minimise duplication, risk information provided in corporate reporting may be used to inform senior executives when completing annual reporting tasks.

A risk communication plan can be tailored for each individual entity and may include information on:

- the attitude and approach to managing risk
- the risk profile
- individual risks
- specific control responsibilities.

An entity's risk profile is a key tool for informing senior executives and stakeholders on the priorities and management of risk and may be developed at a corporate level as well as at business unit and branch levels. Clear communication of the entity's risks relies on developing quality risk profiles that provide a complete view of key risks.

Build a culture of open risk communication

All officials are responsible for communicating risk and sharing risk information within the entity and with external stakeholders as appropriate.
Open communication requires time to develop and relies on officials acknowledging that good risk communication provides an opportunity to innovate and improve performance.

As part of effective communication, entities are encouraged to provide regular, candid briefings on key risks, threats and opportunities. Where appropriate, significant issues can then be escalated to the accountable authority and/or minister.

Consider communication requirements

Entities are encouraged to use risk communication to identify, assess and provide information on the monitoring of risks against the corporate objectives of the entity. This may be aligned with other reporting frameworks.

When communicating about risk, ask yourself the following questions:

- What needs to be communicated?
- Who needs to know?
- What is the time frame?
- Will terminology be an issue?
- What is the most acceptable format when presenting information?
- What analysis has been performed to provide robustness to the data?
- What follow-up action is needed?

Risk communication is critical to ensure that the entity's risk management processes are consistently implemented at all levels. Operational risk reporting to senior executives is most effective when it occurs at regular intervals throughout the year.

Practical tips

- Tailor the structure and content of risk reports for the audience, the nature of the risks being reported and the circumstances.
- Develop templates for risk assessments that capture enough information to support the risk assessment process.
- Work with key stakeholders to share risk processes and terminology and standardise these as much as possible.
- Be flexible in adopting strategies to communicate risk information to officials.
- Examples include internal entity news, policy awareness programs, internal risk forums and newsletters, a risk management intranet page, questionnaires and surveys, participation in webinars, facilitated workshops, focus groups, external working groups and forums.[4]
- 'Dashboards' which highlight areas of concern or opportunity can quickly and effectively convey information to senior executives to enable them to focus on key issues.

[4] AS/NZS Handbook 327-2010, Communicating and Consulting about Risk, provides further information about matters that need to be considered when planning communication and consultation.

Element seven - Understanding and managing shared risk

Commonwealth Risk Management Policy

Each entity *must* implement arrangements to understand and contribute to the management of shared risks.

Characteristics of shared risk

Shared risks are those risks that extend beyond a single entity, requiring high levels of cooperation between stakeholders to effectively understand and manage those risks. Stakeholders often go beyond government to include other partners, such as industry, the wider community and across jurisdictions.

Shared risk is a crucial element of program/policy delivery and failing to identify and manage these risks often impacts a broad range of stakeholders.
It is therefore important that entities, in collaboration with their stakeholders, cooperate to identify and manage risks, develop clear roles and responsibilities for managing these risks and agree to outcomes.

Aspects to consider in managing shared risk

Visibility of the risk. Proactive and comprehensive information exchange is essential to fully identify the nature and severity of risks, monitor their status and manage the potential realisation of risks.

Controls and treatments. Responsibility for implementing and managing specific controls and treatment programs may be allocated or dispersed across separate entities. This involves collaborative approaches to designing, deploying, monitoring and reporting the effectiveness of controls and treatments.

Exposure to consequences and effects. When a risk is realised, a shared risk may impact a number of entities and the wider community. Where practicable, entities are encouraged to establish mechanisms to appropriately share the burden of the risk exposure. This can be achieved through pooled or collaborative response capabilities, defining financial exposures explicitly in governance arrangements, or through agreeing integrated treatment plans.

Documenting the management of shared risks

Documenting shared risks is good governance, improves understanding of complex relationships and clarifies the extent of knowledge of shared risks at a point in time.

When defining how an entity manages shared risk, guidance to officials may include:

- a meaningful definition of shared risk in the entity's risk management policy the concept of shared risk, and the arrangements for managing it, into project or program management frameworks and processes
- examples of shared risks that are relevant to the entity
- a list of those in the entity likely to be responsible for managing shared risk
- protocols for establishing mechanisms to collaboratively manage shared risks
- an identification of the mechanisms and protocols to be used for recording, monitoring and reporting on managing shared risk, both internally and externally.

Collaborative resilience

Common shared risks within the Commonwealth include risks which threaten the safety and security of entities and the services they provide. These may include natural disasters, acts of terrorism, and infrastructure or market failures. Significant opportunities exist for Commonwealth entities to collaborate in order to enhance their individual and collective resilience to such risks.

Entities are encouraged to work with stakeholders to better understand common threats, shared vulnerabilities and to optimise their collective ability to prevent, manage and recover from disruptive events. Communities of practice, peer entities or those in close proximity to one another can be formed to encourage this.

Practical tips

- Establish memoranda of understanding with partners to formalise an agreed understanding of responsibilities and expectations for managing shared risk.
- Develop shared risk registers and profiles with key partners and hold regular collaborative risk assessment workshops with representatives of these partners to encourage participants to look beyond their own entity's view of the risk.
- Educate officials on their responsibility to identify and contribute to managing shared risks.
- The entity's risk register and risk profile templates can be enhanced by documenting the controls and control owners for monitoring shared risk. For example, ensure that risk controls managed from outside the entity are noted and monitored.
- Ensure shared risks are linked to governance arrangements such as interdepartmental committees or established joint arrangements.
- Provide guidance to officials on opportunities to consider shared risk as part of contractual arrangements or the administration of grants.

Element eight - Maintaining risk management capability

Commonwealth Risk Management Policy

Each entity *must* maintain an appropriate level of capability to both implement the entity's risk management framework and manage its risks.

Determining the appropriate level of risk management capability

When determining an appropriate level of risk management capability, consider the severity of the risks being managed and the importance or profile of the objectives they may affect. The level of risk management capability in an entity may be measured against the potential cost of the risks, should they be realised, and the entity's risk appetite and tolerance for those risks.

Maintaining an appropriate level of risk management capability does not necessarily mean owning it exclusively in an entity. Many Commonwealth entities face common risk challenges and can therefore share the specialist capabilities needed to manage them. For example, the specialist expertise required to analyse particular natures of risk can be shared by peer entities as can the lessons learned.

Capabilities that can help an entity manage risk

Risk systems and tools

The risk management frameworks and risk profiles of entities will vary greatly in complexity and scale. Risk processes and tools can be tailored accordingly and may range in complexity from simple spreadsheets to dedicated enterprise risk management software.

Some of the functions provided by risk systems and tools include:

- integrated storage of risk information and risk profiles
- analysis of risk information, including analytics such as 'causal factor' analysis and key risk indicator monitoring
- risk information dissemination and sharing, including risk status reports and risk and compliance dashboards
- automation of risk processes workflows.

Risk systems and tools will be most effective when they are appropriate to the entity's needs, well maintained and complemented by training and workplace support. If they are overly complex they will be underutilised. If they are inadequate, they will not provide the functionality desired or support efficient work processes.

People capability

Building the capability of an entity's officials is critical as it ensures a consistent approach to managing risk across the entity. Equipping officials to effectively manage risk may include:

- clearly defined risk responsibilities and accountabilities
- risk competency acquired through learning and development, mentoring and experience
- access to relevant communications and information access
- peer support and collaboration mechanisms
- risk management as part of the staff induction program
- ongoing risk management training
- recognition and reward
- risk management being integrated into officials' performance agreements.

Learning and development opportunities will be most effective where they are tailored to the current competency level of officials and the risk management requirements of their role. The appropriate level of risk competence among officials will vary significantly between different roles and levels.

To identify the entity's risk management training needs, entities can:

1. determine and compile the risk management competency requirements of their workforce
2. undertake a skills analysis to determine their current level of capability. Comparing these will provide a clear understanding of competency needs in order to develop a prioritised learning and development program.

Managing risk information

The quality and availability of information on risk needs to be accurate and readily available to ensure that risks are successfully assessed, monitored and treated across the entity. Access to reliable risk information allows risk to be measured and communicated to both internal and external stakeholders.

Risk information will be most reliable where it is:

- based on established data sets or benchmarks
- consistent across the organisation
- unambiguous and provides a balanced view of the risk
- sufficiently enduring to allow comparison of risks over time
- generated and processed efficiently.

Building effective risk management processes

An entity's risk manager, or risk management team, can support the development of good risk processes through:

- developing a fit-for-purpose risk management policy and processes in the entity
- supporting senior executives by coordinating, compiling and presenting clear and concise risk information able to be used in planning and decision making
- ensuring there are easily accessible systems and processes in place to enable all officials to systematically manage risk in their day-to-day work
- supporting business units to implement the risk management process
- ensuring risk management processes are applied consistently across the entity
- developing and implementing an appropriate risk communication strategy
- identifying the needs for skills development and specific training in risk management across the entity
- developing and maintaining a risk reporting framework to enable regular reporting of key risks, and the management of those risks, to senior management.

Practical tips

- Think holistically about the capabilities the entity needs to effectively manage risk including people, processes, systems, and information. Conduct a capability needs analysis to determine and prioritise risk management capability gaps.
- Provide appropriate risk and risk management awareness training to officials both initially and on a regular basis as a refresher. Include an overview of the entity's risk management framework in the induction program and highlight the capabilities officials can draw on to help them manage risk.
- Identify, train and connect risk champions drawn from diverse parts of the entity. These champions can help spread risk management good practice and influence behaviours.
- Identify opportunities to develop skills through more informal learning methods such as regular lunchtime discussion sessions or opportunities for people to learn through practical experience.
- When considering the acquisition or development of risk tools or systems, ensure the entity identifies a fit-for-purpose solution.
- Share case studies and lessons learnt based on previous experiences in the entity wherever possible.

Element nine - Reviewing and continuously improving the management of risk

Commonwealth Risk Management Policy

Each entity *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.

Reviewing the management of risk

As an entity's environment, objectives and capabilities change over time, so do its risks, its risk appetite and its exposure to existing risks. To ensure new risks are identified, and existing risks remain appropriately managed, entities need to continuously review their risk management framework and the risks being managed.

Effective risk management programs require regular review and evaluation mechanisms, both formal and informal. This guides whether the entity's approach to risk management is consistent with its objectives, ensures that the risk management framework is continuously improved and that good risk management practice is recognised and rewarded. These mechanisms also provide assurance to the accountable authority on the efficiency, effectiveness and relevance of the entity's approach to risk management.

To assess the performance of an entity's risk management framework, three key aspects can be considered:

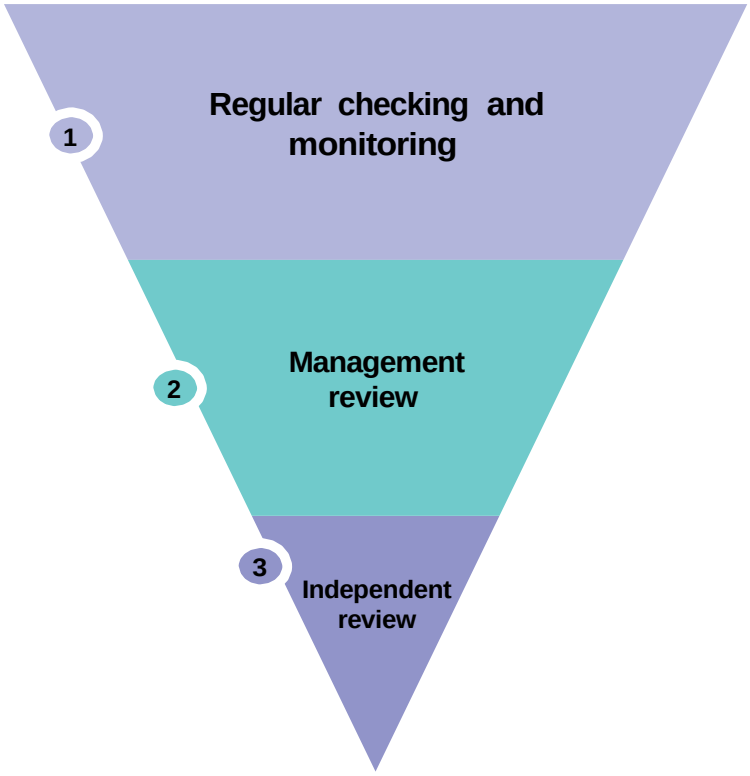
- **Value add.** The degree to which risk management is contributing to the achievement of the entity's objectives and its effectiveness in identifying and managing risk.
- **Maturity.** Whether the risk management framework is fit for purpose for the entity and represents the appropriate application of better practice.
- **Compliance.** The extent and the consistency of the application of the risk management framework in practice across the entity.

Reviewing an entity's approach to managing risk, and the performance of its risk management framework, has four key steps:

1. review the entity's risk management framework
2. review compliance with and the application of the framework
3. review the entity's risk profile
4. review individual risks and the controls that are in place to manage them.

How to review the risk management program

Ongoing review and evaluation of an entity's risk management framework, program and practice occurs at three levels.



Level one – Regular checking and monitoring

The first line of responsibility for managing risk is the day-to-day decisions of officials in all roles and at all levels. Accordingly, this is where the first line of review also lies. Individuals will choose to accept or reject risks on a given day for a variety of reasons – some appropriate and informed, and some not.
A process of ongoing discussion about risk, and work group and peer moderation is important to ensure a consistent approach.

Relevant issues for consideration include the accuracy and effectiveness of the risk register, whether the consequences and impact levels of individual risks are still relevant and the effectiveness of controls and treatments.

Level two – Management review

Reinforcing the Level One review, management review of both risk assessment and controls forms the next level of review. Management review of these decisions, behaviours and actions fulfils two roles simultaneously:

- monitoring, correcting errors or misjudgments
- building risk management capability, competence and confidence.

To fulfil this role effectively, managers are encouraged to understand the context, objectives and business of the entity, its risk management framework, and its risk appetite and tolerances.

These reviews will be most effective when they are regular and seen as routine, and undertaken on a programed basis. Reviews may be planned to target high risk processes, but also sample broadly across the entity and its service providers. Where issues are identified, determine if they are specific to an individual risk or risk decision maker, or systemic in the entity.

Once determined, the issue is addressed with findings and corrective actions documented.

Level three – Independent review

Independent reviews, such as audits, can provide a level of assurance that a comprehensive risk management framework and process is in place and implemented effectively.[6]

Independent review also brings a fresh perspective, and can identify where an entity's framework lacks alignment with its organisational objectives, opportunities for improvement in processes, and instances of non-compliance.

Independent reviews can be useful in identifying opportunities to enhance consistency across the entity including more effective ways of managing similar risks, or categories of risk, from an entity-wide perspective.

[6] Advice on the scope and planning of audits and other forms of assurance is given in the HB 158-2010 Delivering Assurance Based on ISO 31000: 2009, Risk Management Principles and Guidelines.

Practical tips

- Establish a rigorous process of 'near miss' or incident reporting, analysis and review. This allows an entity to share lessons learnt dealing with issues, crises, problems and successes.
- Review the entity's approach to managing risk and its risk management framework at regular intervals. Entities are encouraged to conduct a comprehensive annual review as a sensible benchmark.
- Ensure that the senior executive schedule time to discuss and debate the entity's risk profile. This may include the rolling review of individual risks in detail, a complete review of the entity risk profile, and occasional opportunities to consider the entity's risks from a fresh 'clean sheet of paper' perspective.
- Constantly monitor the ongoing effectiveness of controls. Develop performance measures for each significant control to support consistent and reliable monitoring and reporting.
- Include risk issues in the entity's annual audit plan, commissioning independent reviews, or through peer review programs with other entities.
- Align the review and oversight of risk management with similar business processes and governance arrangements. In particular, review the relevance of the risk management framework each time the entity's corporate planning processes are revised.
- Consider a range of information sources when reviewing the entity's risks and the effectiveness of its risk management framework. These can include insurance data, benchmarking data, internal audit outcomes, internal reviews, financial performance data, loss event information or anecdotal feedback.
- Benchmark the entity's risk management performance against its peers and meet regularly with counterparts in other entities to exchange good practice.
- Ensure that risk management activities are traceable. In the risk management review process, records provide the foundation for improvements in methods and tools, as well as the overall process.[7]

[7] SA/NZS HB 436:2013 Risk Management Guidelines – Companion to AS/NZS ISO31000:2009, p87.

Appendix

Appendix A - Glossary of terms

Term	Definition
Accountable authority	The person or group of persons who has responsibility for, and control over, a Commonwealth entity's operations. See also: Finance's glossary of resource management terms
Audit and risk committee	An independent committee that provides assurance and advice on the entity's operations including the effectiveness of the entity's risk management framework. Commonwealth entities may have a separate audit and risk committee.
Australian/New Zealand Risk Management Standard (AS/NZS ISO 31000)	AS/NZS ISO 31000 has been developed as a generic and flexible standard that is not specific to any government or industry sector. The Standard identifies elements or steps in the risk management process that can be applied to a wide range of activities at any stage of implementation. It replaced AS/NZS 4360 on 6 November 2009.
Commonwealth entity	A Commonwealth entity is a: a. Department of State; or b. Parliamentary Department; or c. listed entity; or d. body corporate established by a law of the Commonwealth See also: Finance's glossary of resource management terms
Consequence	Outcome or impact of an event that may be expressed qualitatively or quantitatively. There can be more than one consequence from one event. Consequence can be positive or negative. Consequences are considered in relation to the achievement of objectives.
Control	A measure to modify risk. Controls are the result of risk treatment. Controls include any policy, process, device, practice or other actions designed to modify risk.
Corporate Commonwealth entity	A Commonwealth entity that is a body corporate and legally separate from the Commonwealth. See also: Finance's glossary of resource management terms
Enterprise-wide risk management (ERM)	Also known as entity-wide or integrated risk management. An integrated approach to assessing and addressing all risks that threaten achievement of the entity's strategic objectives. The purpose of ERM is to understand, prioritise, and develop action plans to maximise benefits and mitigate top risks.

Term	Definition
Entity risk management policy	A document containing the overall intentions and direction of an entity related to risk management.
Event	The occurrence or change of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences.
Exposure	Extent to which an entity is subject to an event.
External context	External environment in which the entity seeks to achieve its objectives. External context can include: cultural, political, legal, regulatory, financial, technological, economic, natural and commercial environment whether international, national, regional or local, as well as the perception of external stakeholders and key drivers and trends having an impact on the objectives of the entity.
Hazard	A source of potential harm or a situation with a potential to cause loss.
Internal audit	Independent, objective assurance and consulting activity designed to add value and improve an entity's operations and accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
Internal context	Internal environment in which the entity seeks to achieve its objectives. Internal context can include: capabilities understood in terms of knowledge; information systems, decision making processes; policies; perceptions, values and culture; governance structures.
Internal control	Any process, policy, device, practice or other actions within the internal environment of an organisation which modifies the likelihood or consequences of a risk.
Key Risk Indicators (KRI)	Measures and metrics that relate to a specific risk and demonstrate a change in the likelihood or consequence of the risk occurring.
Non-corporate Commonwealth entity	A Commonwealth entity that is not a body corporate and is legally part of the Commonwealth. See also: Finance's glossary of resource management terms
Resilience	Adaptive capacity of an entity to resist being affected by a risk event.

Term	Definition
Risk	The effect of uncertainty on objectives. An effect is a deviation from the expected — positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence.
Risk acceptance	The informed decision to take a particular risk. Risk acceptance can occur without risk treatment or during the process of risk treatment. Risks accepted are subject to monitoring and review.
Risk aggregation	The consideration of risks in combination.
Risk analysis	The process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment.
Risk appetite	The amount of risk an entity is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describes the entity's attitude toward risk taking.
Risk assessment	The process of risk identification, risk analysis and risk evaluation.
Risk capacity	The amount and type of risk an organisation is able to support in pursuit of its objectives.
Risk evaluation	The process of comparing the level of risk against risk criteria. Risk evaluation assists in decisions about risk treatment.
Risk event	A risk event occurs when the conditions for the existence of the risk come together with a triggering action which leads to the creation of an event (can be either a positive or negative event). Risk events lead to measurable effects which may lead to other effects and eventually lead to an undesirable consequence.
Risk identification	The process of finding, recognising and describing risks. Risk identification involves the identification of risk sources, risk events, their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions and stakeholder's needs.
Risk management	Coordinated activities to direct and control an organisation with regard to risk.

Term	Definition
Risk management framework	A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk management plan	A document within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Management components typically include: procedures, practices, assignment of responsibilities and sequence of activities.
Risk management process	The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluation, treating, monitoring and reviewing risk.
Risk oversight	The supervision of the risk management framework and risk management process.
Risk owner	A person with the accountability and authority to manage a risk and any associated risk treatments. Sometimes referred to as a Risk Steward.
Risk profile	A description of any set of risks. The set of risks can contain those that relate to the whole organisation, part of the organisation or as otherwise defined.
Risk reporting	A form of communication intended to address particular internal or external stakeholders to provide information regarding the current state of risk and its management.
Risk tolerance	The levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk. Risk tolerance defines the limits (quantifiable where practicable) that support the entity's risk appetite.
Shared risk	A risk where more than one entity is exposed to or can significantly influence the risk.
Treatment	A treatment is a proposed control, yet to be implemented. The term can also be used to refer to the process of selection and implementation of measures to modify risk.

Appendix B - Examples of typical risk management roles and responsibilities

The table below identifies some common accountabilities and responsibilities for managing risk in an entity. These are examples and may not apply to all entities.

Group	Typical risk management responsibilities
Accountable authority	• Determine and articulate the entity's risk appetite and tolerance. • Establish and maintain an appropriate system of internal controls for the entity. • Champion the entity's risk management framework, ensuring it is appropriate, implemented and continuously evolving to reflect the changing environment. • Approve the entity's enterprise risk profile. • Endorse the approach to managing significant and critical risk areas. • Discuss the entity's key risks with the responsible minister. • Understand the impact of the entity's evolving risk profile on its ability to achieve its objectives.
Executive management committees	• Review recommendations from the entity's audit and risk committee(s) and other assurance and review activities and implement improvements as required. • Support the accountable authority in determining the entity's risk appetite and tolerance. • Review the performance of the risk management framework. • Understand and champion the entity's risk management framework, ensuring it is appropriate and continually evolving to reflect the changing environment. • Review and maintain oversight of the entity's enterprise risk profile.

Group	Typical risk management responsibilities
Audit and risk committees	• Provide independent assurance of the effectiveness of the entity's risk management framework. • Monitor the implementation of the risk management program against the endorsed implementation strategy or plan. • Review an entity's internal control structures and advise whether key controls are appropriate and are operating effectively. • Review compliance with an entity's risk management policy and programs. • Provide advice to the accountable authority to assist them in meeting their external accountability obligations, including statutory and fiduciary duties. • Review the content of reports of internal and external audits to identify material that is relevant to the entity, and advise the accountable authority about good practices. • Monitor and understand the potential implications of emerging risks on the entity's risk profile and its ability to achieve its objectives.
Senior executives	• Model good risk management behaviours. • Contribute to the development of the entity's enterprise risk profile. • Review business unit risk profiles. • Review and assess the current and planned approach to managing significant and critical risk areas. • Ensure the risk management framework is implemented in individual business units/branches. • Support officials who engage with risk in an appropriate and informed manner, regardless of the outcome. • Contribute to the development of the entity's risk profile and understand the effect of emerging risks on the entity's ability to achieve its objectives.
Managers and supervisors	• Identify, review and manage the risks and risk profiles for their business units. • Identify and monitor emerging risks and understand the impact they may have on the risk profile of their business unit. • Ensure officials are aware of the entity's risk management framework in their decision making. • Recognise risk management behaviours (positive or negative) within their teams. • Communicate risk information with both internal and external stakeholders.

Group	Typical risk management responsibilities
Risk manager/ adviser/team	• Coordinate the implementation of the risk management framework. • Promote consistent and accurate risk management practice through effective risk management planning. • Facilitate, challenge and drive risk management capability within the entity. • Report to the senior management group, executive management team and audit committee or board at regular intervals.
Risk owners	• Maintain responsibility for monitoring a specific risk. • Understand the risks they are charged with and be sufficiently senior to influence their management. • Understand and interpret the entity's risk appetite and tolerance as it applies to their risks. • Record and document the risk in appropriate risk registers. • Actively monitor the risk context to understand and respond to any changes. • Challenge the effectiveness of controls. • Communicate and report on the risk at regular intervals.
Risk champions	• Officials who lead their colleagues by modelling good risk behaviours. • Lead risk activities, initiatives and assessments and encourage effective risk management in their area. • Network with other risk champions to share good practice and build skills and capability.
Control owners	• Responsible for maintaining controls and contributing to treatment programs. • Actively monitor the continued viability, relevance and effectiveness of the control or treatment program. • Inform the relevant risk owner when the effectiveness of the control or treatment is at risk.
All officials	• Recognise, communicate and respond to expected, emerging or changing risks. • Contribute to the process of developing risk profiles for their branch/business unit.