Australian Government
Department of Finance

Establishing a Risk Management Framework

Audience

This information sheet is intended to assist Commonwealth officials at the following level:

- **Specialist level:** Job role specialists who are required to design, implement and embed an entity's risk management framework. Specialists facilitate generalists and executives to fulfil their risk management responsibilities.

At a glance

A risk management framework is a set of components that set out the organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout an entity.

Aside from the requirements of the Commonwealth Risk Management Policy, there is no standard format for a risk management framework as each entity will tailor their framework to meet their specific requirements.

This information sheet provides guidance in relation to element two of the Commonwealth Risk Management Policy. It includes an explanation of the core elements of a risk management framework and some suggested priorities for implementing them.

The core elements of a risk management framework

An overarching risk management policy

An entity's risk management policy is a document that communicates to all stakeholders why and how it manages risk and refers to other components of the risk management framework to provide additional detail.

An entity's risk management policy must meet the requirements of element one of the Commonwealth Risk Management Policy which states that:

> 13.1 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; and
>
> d. is endorsed by the entity's accountable authority.

An overview of the entity’s approach to managing risk

Effective risk management frameworks generally describe the risk management processes to be used in the entity. This may include a common process for the assessment and management of individual risks including:

- risk identification - how and when risks are identified
- risk assessment - how risks are assessed (likelihood, consequence, vulnerability, speed of onset etc)
- risk treatment - the entity’s approach for treating risks (mitigate, share, transfer, accept etc)

How the entity will report risks to both internal and external stakeholders

Risk reporting is important to provide information on the monitoring of risk against the objectives of the entity. It allows for risks to be escalated if they are realised or can be used to proactively report risks before they are realised in cases when tolerance limits and triggers are breached.

Risk reporting is most effective when it is embedded into decision making and business processes. Information that is reported can include what the risk is, what it means, who needs to know and what actions can be taken.

For specific guidance on reporting risk, see the information sheet *Communicating Risk*.

The attributes of the risk management culture that the entity seeks to develop

Risk culture is the set of shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities. The risk management framework has an important role to play in defining the characteristics of a positive risk culture in an entity and the practical measures which will be implemented to encourage it.

For specific guidance on fostering risk culture, see the information sheet *Developing a Positive Risk Culture.*

An overview of the entity’s approach to embedding risk management into its existing business processes

Risk management is of greatest benefit when aligned and integrated with other business processes. The framework can assist in this regard by describing how the entity’s risk management program supports the achievement of its objectives and is integrated into the entity’s business processes.

To support the understanding and embedding of risk management, the framework can be used to define the risk management concepts and categories of risk applicable to the entity. Categories enable risks to be aggregated and reported upon so that material risks can be shared with senior management to support decision making.

The framework has an important role to play in ensuring risk management within the entity is as consistent as possible, particularly where specialist categories of risk (such as business continuity and work health and safety) may have their own requirements and processes.

For further guidance on embedding risk management, see the information sheet *Embedding Risk Management*.

How the entity contributes to managing any shared or cross jurisdictional risks

A shared risk is where more than one entity is exposed to or can significantly influence the risk.
The Commonwealth Risk Management Policy requires entities to implement arrangements to understand and contribute to the management of shared risk.

Examples of such arrangements that can be documented in an entity’s risk management framework can include:

- definitions and examples of shared risk that will be relevant to the entity
- responsibilities for managing shared risk
- mechanisms for identifying, monitoring and reporting on the management of shared risk.

For further guidance on shared risk, see the information sheet *Managing Shared Risk*.

The approach for measuring risk management performance

Like any business process, risk management is most effective when it is efficient and aligned against the requirements and objectives of the entity. To assist with assessing risk management performance, the risk management framework can describe relevant measures of success and how these are to be assessed.

How the risk management framework and entity risk profile will be periodically reviewed and improved

An entity's risk appetite and risk exposure changes over time. Accordingly, it is important that an entity's risk management framework is reviewed and continuously improved. Entities may wish to consider including the following four review activities as part of their risk management framework:

- reviewing the entity's risk management framework for its fitness for purpose and compliance with external requirement
- mechanisms to measure and encourage compliance with the framework
- review of the entity's risk profile and its overall exposure
- review of individual risks being managed and their relevant controls and treatments.

For further guidance on reviewing a risk management framework, see the information sheet Reviewing a *Risk Management Framework*.

For further guidance on reviewing an entity risk profile, see the information sheet *Maintaining an Entity's Risk Profile*.

Developing and embedding a risk management framework

As entities requirements differ significantly, it is not possible to prescribe a single approach to designing a risk management framework. However, it is often best to build the framework progressively over time, embedding each element in turn.

The highest priority elements are typically to:

- draft and publish the risk management policy, establishing the importance of structured risk management and assigning key responsibilities
- publish a common language for risk and a core risk management process
- define key organisational responsibilities for assessing, managing and reporting risk.

The *Commonwealth Risk Management Policy* requires the risk management framework be endorsed by the entity's accountable authority. Often, a message of personal commitment by the accountable authority can be a useful addition to a risk management framework and help convey its importance and relevance to all staff.

Successful implementation will also require a well-planned education and awareness program including specific training on how to use the risk framework. Intranet portals can provide convenient access points for the risk management framework and any supporting tools, templates or guides.

Contact

If you have any questions or feedback in relation to this information sheet please contact Comcover Member Services at comcover@comcover.com.au.

Use of this information sheet

Comcover's series of Risk Management Information Sheets are designed to be used as learning resources and are not mandatory

It is important that entities develop risk management frameworks and systems that are tailored to the needs of their organisation. Entities may choose to adapt some or all of the concepts contained in this information sheet to suit their specific needs or use alternative methodologies.