# Embedding Risk Management

## Audience

This information sheet is intended to assist Commonwealth officials at the Specialist and Executive levels to understand:

- how to test how effectively risk management is embedded in your entity,
- practical strategies for recognising and successfully embedding risk management in an entity's day-to-day operations, and
- how to embed risk management within typical public sector processes and programs using practical examples.

## At a glance

Managing risk is a core responsibility of Commonwealth officials at all levels. However, the way in which individuals assess risk and their personal appetite for risk vary considerably. An entity's risk management framework that is effectively embedded is an essential tool to encourage consistency in risk decision making.

## Testing how well risk management is embedded in an entity

The greatest test of how well risk management is embedded in an entity is the extent to which it influences decision making and behaviours. Some practical questions to test how well this is being achieved include:

- Is a risk assessment an essential part of key business processes and planning activities?
- Is there a culture of speaking openly about risks?
- Are risks routinely communicated and their management broadly discussed or are risks identified and managed in silos?
- How diligently do officials appointed ownership or stewardship of individual risks monitor and manage those risks?
- Is there a senior champion for risk management in the entity?

- Are risk governance arrangements such as a risk committee of the board, risk committee of management, or the discussion of risk as an agenda item of the board appropriately informed and influential?
- Do officials refer routinely to the entity's risk appetite and ensure their decision making and risk judgements reflect the articulated risk appetite of the senior executive?
- When risks are realised, are they used to improve the management of similar risks, or are narrow solutions implemented?

# Practical strategies for embedding risk management

It is important that risk management within a process or activity is not seen as a burden that adds effort but littlevalue. Accordingly, the effort expended in considering risk needs to be commensurate with the level of risk itself.

The following are some practical strategies which encourage the successful embedding of risk management.

## Begin with objectives in mind

Each activity or process in an entity will ideally have objectives which link to the objectives of the entity. These objectives are the starting point for embedding risk management, as they define the critical measures of success against which risk must be most carefully managed.

For example, when planning for the delivery of critical and essential public services in a post natural disaster environment, the requirement for the rapid deployment of capability in affected areas may be more important than broad, sustained coverage. Hence, the initial focus of risk management in the activity might be identifying the risks to achieve this.

## Develop risk processes that are fit-for-purpose and easy to implement

Where possible, weave the consideration of risk into existing activities or requirements. For example, in assessing risk during a major procurement project, add the consideration of risk into existing project reviews and gateway processes. Where possible, align project risk reporting into established project health status reports or dashboards. This encourages a culture where managing risk in a structured manner is an integral part of day-to-day management.

## Identify where risk needs to be managed in an activity

The nature of risk in different business processes or activities varies, therefore risk management needs to be tailored. Some examples of risk management objectives or priorities in a typical process include:

- Understanding the relevant accountable authority's appetite for risk in that process, and under what circumstances and against which outcomes they are prepared to accept it.

- Ensuring the process is not unacceptably affected by risks to which it is exposed from stakeholders and its supply chain. Sometimes these exposures will not be immediately apparent, however by identifying the risk up-front further information can be sought to ensure they are sufficiently understood.
- Managing and communicating where the process may expose others to risk (shared risk). For example, thinking about whether the burden of responsibility between different entities for delivery of a public service expose another entity to risk they are not well placed to manage
- Understanding where risks are shared and may require several entities or partners to work collaboratively to manage the risk. This may require understanding the potential for cascading failures where a common cause or event can cause multiple risks to be realised.

## Build staff awareness and encourage a positive risk culture

Embedding risk management is ultimately about influencing the manner in which decisions are made. However,officials can only embed risk management in their work if they understand and value it. As each entity applies risk management in different ways, it is important that staff understand the entity's own unique requirements and expectations in addition to the basic theory or risk management.

Equipping staff to embed risk management requires:

- Risk management training relevant to an official's role and responsibilities.
- Providing easy access to generic and agency specific risk management guidance materials.
- Establishing collaborative forums where staff can share how they have been able to successfully embed risk management in their activities. This may include encouraging 'risk champions' who can lead by example and mentor their colleagues.
- Ensure the management of risk, and the application of the entity's risk management framework is an explicit component of performance management.

## Engage the senior executive

How senior executives question and challenge the management of risk will be influential in determining the value staff perceive in it. Often referred to as 'tone from the top', the most senior executive can support the uptake and embedding of risk management by:

- Setting a personal example through the visible consideration of risk in their own personal decision making and ensuring that the entity's strategic risks are managed consciously and communicated well.
- Treating issues and undesirable events as the realisation of risks. When things go wrong, asking whether the relevant risk had been identified, assessed and whether the treatment strategy was documented.

- Rewarding or recognising those who manage risk well. This includes supporting officials who took informed sensible risks but may not have achieved the outcome they had hoped for.

## Embed risk management across the 'three lines of defence'

A common model for applying risk management within an organisation is referred to as the 'three lines of defencemodel'. In this model, the day-to-day decisions of officials at all levels is the first line of defence, supporting functions such as the entity risk management team are the second line of defence, and impartial review such as through audit is the third line of defence. Working together, these three lines protect entities from excessive or undesirable risk.

In the **first line**, officials manage their risks day-to-day. Risk management in the first line depends upon these staff being competent, having a clear focus on objectives, and being appropriately resourced. It also relies upon them being able to make informed and appropriate risk judgements in each decision they make. Officials will be best able to do this where they are supported by quality risk frameworks and risk guidance relevant to their activity.

The **second line** provides the mechanisms to support the first line and to enable its effective operation. The second line includes the entity's control frameworks and risk management function. In part, the second line has a key responsibility to design and build risk management into the day-to-day processes of an entity.

The **third line** has an important role to play assessing how well the entity is identifying and managing its risks. In some entities this is overseen by an audit committee, others have risk committees to fulfil this role. They provide a degree of independent oversight, alerting management to excessive, imbalanced or poorly understood risk taking.

# Developing a plan to embed risk management

The first step in successfully embedding risk management into an organisation is to develop and implement a high quality fit-for-purpose risk management framework. This will be most effective where it provides clear guidance on how risk should be managed through:

- a risk appetite statement articulating what level of risk the entity should be taking,
- clearly defined risk management accountabilities and responsibilities, and
- a common risk management vocabulary and process.

Building on this foundation and the strategies described above, the key steps to embedding risk management include:

1. Establish a staged plan with target maturity states at achievable intervals. Communicate success stories quickly to build momentum and encourage adoption.

2. Prioritise and focus on those processes where the positive outcome will be greatest. Commonly, governance and corporate planning processes provide significant benefit as they are often highly influential on senior decision making. Use these as models for further implementation.
3. Work with stakeholder and peer entities to share good practice and encourage consistency wherever sensible to do so.
4. Ensure that the entity's change management guidelines and processes require risk management be an integral element and outcome of any change program.
5. Some specialist categories of risk may require their own risk assessment and management approaches. Ensure that these are as consistent as possible with the entity risk management framework.
6. Recognise that embedding risk management requires time to achieve, in part because it is as much about changing behaviours as it is about changing processes.

## Examples of embedded risk management in common processes

| Business Area | Good | Better | Best |
|---|---|---|---|
| **Program Delivery** | A formal project risk assessment is conducted and a risk register maintained to monitor and report on key risks. | Project reporting incorporates near real time assessments of project keyrisk indicators. Decision making delegations at the project and program level are linked to the levelof risk exposure in each decision. | Project dashboard reporting incorporates risk adjusted performance metrics such as risk-adjusted budget forecasts. Program managers actively allocate resources between projects based on assessments of risk against agreed tolerances. |
| **Policy Formulation** | A formal risk assessment is conducted at policy conception stage and a riskregister maintained to monitor and report on key risks to the successful implementation of the policyin practice. | Policy developers and implementerswork together to assess key risks toboth the successful developmentand implementation of the policy. | All policy stakeholders work together tosystematically understand and managerisks to and from the policy throughoutits life cycle. Arrangements to manage these risks are an integral element of thepolicy itself. |
| **Corporate Functions** | Risk registers are maintained by corporate areas to monitor and report on key risks to the successful delivery of corporate services. | Collaborative workshops are conducted between corporate functions and business units/ clients to identify shared risks to the achievement of the entity'sobjectives. The risk exposures and effectiveness of corporate functions as controls is monitoredat a whole of entity level. | Delivery of corporate functions is prioritised in part by the significance ofthe risks being managed in different business units. |
| **Strategic Planning** | The entity develops and maintains a strategic risk profile which assesses keyrisks to the achievement of its strategic objectives. | An integrated corporate planning framework links strategic risks to corporate objectives and businessplans. Strategic risks are reviewedin cycle with planning activities. | An entity's strategic risks are an integralcomponent of corporate planning. Initiatives and priorities stemming fromboth corporate planning and strategic risk management activities are integrated seamlessly. |

| | | | |
|---|---|---|---|
| **Entity Resilience** | Key resilience risks are identified, documented andtreated, however this often occurs in siloes. | Resilience risks are identified and communicated in a common language with the entity framework.<br>Any customised risk assessment processes or outcomes are translatedinto the entity risk framework. | Resilience risks are assessed and managed as part of an integrated cycleof activity which links seamlessly with the entity enterprise risk framework.<br>Resilience treatments are consolidatedand prioritised in competition with otherstrategic priorities and risk treatment requirements. |
| **Performance Management** | Performance management agreements include an assessment of an individual's ability to manage risk. | Assessing an individual's risk management performance includes their ability to manage risk, and theirimplementation of the entity risk management framework. | An official's or business unit's risk management performance is a significantpart of their remuneration or funding consideration. Individuals are assessedon the extent to which they model desirable risk management behaviours. |

## 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 entity. Entities may choose to adapt some or all of the concepts contained in this information sheet to suittheir specific needs or use alternative methodologies.