Reviewing a Risk Management Framework

Audience

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

- **Specialist level:** Job role specialists who are required to design, implement and embed an entity's risk management framework.
- **Executive level:** Senior executive service officials (SES) whose role requires them to identify and determine the acceptable levels of risk that are appropriate to their agency's profile, allocate resources and lead the adoption of risk management policies, strategies and best practices.

At a glance

A risk management framework sets the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management capability. Undertaking a periodic review to assess the effectiveness of an entity's risk management framework is necessary to ensure that the framework continues to evolve and meet the needs of the entity.

This information sheet provides guidance in relation to element two and element nine of the *Commonwealth Risk Management Policy*, including:

- determining when to review a risk management framework
- deciding who is responsible for the review
- selecting the scope and method for a review
- examples of how to conduct a review
- practical tips and questions to ask when undertaking a review

Determine the timing for the review

Element nine of the *Commonwealth Risk Management Policy* states that:

> 22.1 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.

The exact timing and frequency of this review will be dependent on the nature of the organisation's operations. For instance, if an entity has experienced significant change, or its exposure to risk has increased, the framework may need to be reviewed more frequently.

Conversely, if an entity's risk management framework has been in place for a number of years, and its operations are relatively stable, the review cycle could be conducted less frequently (for example once every two years).

The identification of an increasing number of 'near misses' and incidents can, over time, indicate that not only is an entity's management of individual risks unsatisfactory, but that the framework itself may require review.

Assign responsibility for conducting the review

An entity's risk function, or the role that is tasked with risk management in an entity, is well placed to complete a review of the risk management function. However, broad consultation may be undertaken across the entity to ensure the risk management framework, and the risk function are meeting expectations. An effective risk management framework supports decision making and key processes, and should not be a seen as an outcome in its own right.

An independent review of the risk management framework can also be useful. This provides the risk function or designated risk role with a fresh perspective, including challenging current norms and practices.

Select the scope and method for the review

Establish the scope

When undertaking a review of the risk management framework, it is important to determine if it has been appropriately communicated and tailored to the entity allowing risks to be:

- efficiently and effectively identified and appropriately assessed
- considered in the context of the entity's objectives and other business processes
- adequately treated and controlled where relevant, with residual exposures understood
- effectively and regularly monitored and reviewed by management, executives and the board.

Select the type of review

- There are several approaches to reviewing a risk management framework, some of which include:
- conducting a high level review of the key components of the risk management framework.
- conducting a risk management maturity assessment against the *Commonwealth Risk Management Policy*, ISO31000, COSO principles, and peer entities
- requesting that the risk management framework be reviewed by internal audit
- benchmarking performance against other entities.

Determine the approach

The review approach is dependent on the entity's specific circumstances including:

- the amount of change in an entity's operations or operating conditions
- current maturity of the risk management program
- complexity of the entity's operations
- number of near misses
- whether risk events have materialised over a 12 month period

These are the factors that ultimately determine whether a high level or detailed review of the risk management framework is conducted. For example, an entity which has previously been told it has a mature risk management framework but has had a significant organisational restructure, would most likely need a detailed review of its risk management framework to ensure it meets its new needs.

Conduct the review

The following planning activities have been outlined below as a guide to completing a review of an entity's risk management framework. An entity may decide that it does not need to complete all activities based on the nature of their entity's operations (e.g. an entity which is relatively small and has staff members assuming multiple roles, may not require a detailed project plan).

1 - Plan

- Identify an executive sponsor for the review. Typically this would be the audit and risk committee and the accountable authority of the entity.
- Appoint a team to complete the review.
- Develop a scope which includes:

  terms of reference

  approach, including interviews, surveys, documentation to be examined

  the review team and relevant accountabilities

  timelines and milestones.
- Issue a communications brief to be disseminated throughout the areas of the entity impacted by the review.

2 - Execute

- Mobilise the review team and complete the review.
- Document results and findings.

3 - Report and Communicate

- Draft findings and recommendations in a report.
- Socialise the findings with key stakeholders to obtain buy-in and seek guidance in relation to the appropriateness of recommendations.
- Finalise report.
- Issue report to the senior executive, accountable authority and the audit and risk committee.

You can also use a review of your risk management framework as an opportunity to engage your senior executives on risk and to encourage them to think how changes can be more fully leveraged to achieve better business outcomes.

Practical tips on testing the alignment of your risk management framework to the Commonwealth Risk Management Policy

- The elements of the *Commonwealth Risk Management Policy* (RM Policy) are tested in the Comcover Benchmarking Survey. Consider using your survey results to determine where effort may be required to better align your risk management framework with the RM Policy.
- Map your entity's existing risk framework to the elements of the RM Policy to understand where your entity currently stands.
- Systematically review your existing documentation and systems against the requirements of the RM policy.
- If areas of your risk framework need to be further developed to align with the RM Policy, develop an action plan and seek senior executive and audit and risk committee commitment to oversee the review.

Sample questions to ask when reviewing a risk management framework

The following questions have been included to guide entities in reviewing their risk management framework. This is not an exhaustive list and the questions may differ depending on the nature of the entity's operations.

- Is a common definition of risk, which addresses both threats and opportunities, used consistently throughout the entity?
- Are the key roles, responsibilities and authorities relating to risk management clearly articulated and followed within the entity?
- Do the governing bodies (e.g., Boards, Audit Committees, Risk Committees, Management Committees) have appropriate transparency and visibility into the entity's risk management practices in order to discharge their responsibilities for oversight?
- Does the risk function's position in the entity enable direct access to the executive management team?
- Has your entity defined relevant risk categories which enable risks to be aggregated, analysed and reported upon?
- Do your entity's risks align to its organisational objectives?
- Does your entity have a clear approach for analysing and evaluating risk?
- Has your entity defined its risk appetite? Does its risk appetite enable decisions to be made that reflect the entity's attitude towards risk, that is, what is acceptable and unacceptable?
- Does your entity have a regular reporting cycle where risk information is incorporated for management review and attention?
- Is there a process which identifies, assesses and treats risks for all key activities (e.g. projects, programs, policy development and business processes)?

Contact

If you have any questions or feedback in relation to this information sheet please contact Comcover 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.