Understanding and Managing Shared Risk

Audience

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

- **Foundation level:** All officials, regardless of level or role, who are required to understand basic risk management concepts and how risk is managed in the Commonwealth.
- **Generalist level:** Officials, regardless of level, whose role requires them to engage with and apply their entity's risk management framework to successfully deliver outcomes.
- **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

This information sheet is designed to assist entities in implementing element seven of the Commonwealth Risk Management policy.

It includes guidance on:

- understanding shared risk and why it can be challenging to manage
- recognising where shared risks may be encountered and who may be involved
- practical strategies for the identification, assessment and management of shared risk.

What is shared risk?

A shared risk is a risk with no single owner, where more than one entity is exposed to or can significantly influence the risk.

Shared risk includes risks that extend across entities and potentially the community, industry, international partners and other jurisdictions. In large, complex entities, shared risk can exist within the entity as well as between them.

Although they will differ in scale and nature, shared risks have a number of distinguishing characteristics.

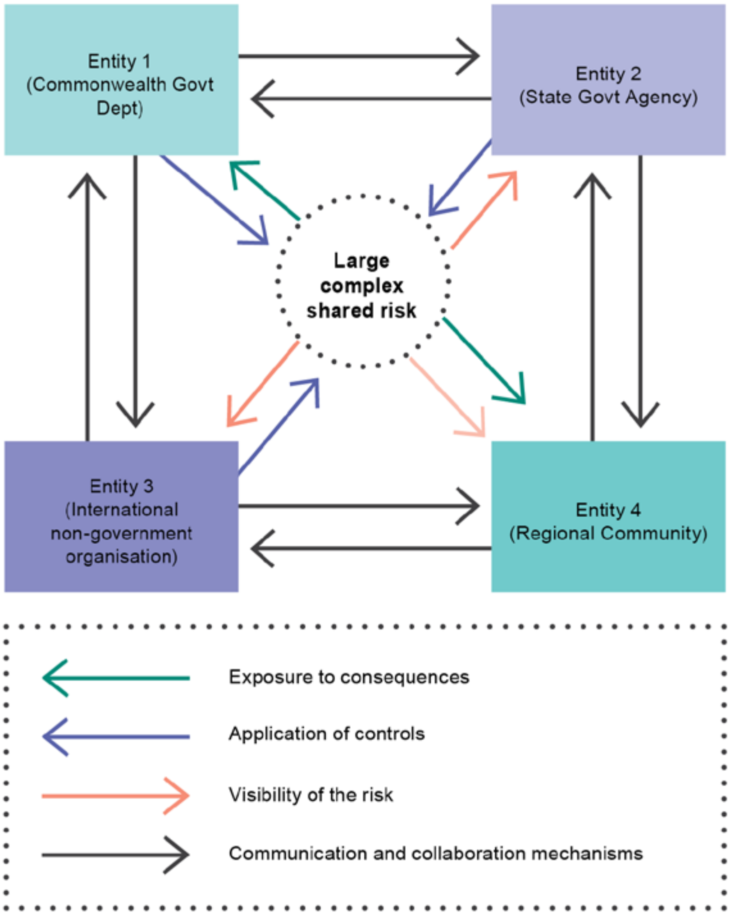
- A shared risk may have no naturally apparent owner. Unlike simpler risks, no one entity may be able to manage the risk on their own. Shared risks often require a network of distributed responsibilities and relationships.
- Shared risks can have complex causes, and can be influenced by the actions (or inaction) of a range of participants in different ways.
- Should a shared risk be realised, they can affect different organisations in different ways, and can have complex and widespread impacts.

The growing use of collaborative approaches by government such as through shared services public-private partnerships and inter-agency task forces means that shared risk is becoming more prevalent.

How can entities contribute to managing shared risk?

Entities and other contributors to shared risk may have different relationships with that risk including:

- **Visibility of the risk.** Often, no single entity will have complete visibility or understanding of a shared risk. Proactive, complete and honest information exchange is essential to build a complete picture of the nature and severity of the risk, monitor its status, and warn others of its potential realisation.
- **Controls and treatments.** No single entity may be able to satisfactorily control or manage a shared risk. Collaborative approaches to designing, deploying and assuring controls are required.
- **Exposure to consequences and effects.** Should it be realised, a shared risk may impact the objectives of many entities. Where practicable, entities may consider establishing mechanisms to appropriately share the burden of the risk exposure.



The diagram to the left illustrates a hypothetical situation where a Commonwealth entity (Entity 1), a state government agency (Entity 2) and an international non-government organisation (Entity 3) are working together to manage a risk in a regional community (Entity 4).

In this situation, none of the parties, operating in isolation, have full visibility of the risk, and alone, none are able to appropriately control it. For example, in this case the Commonwealth department has no representatives 'on the ground' and relies upon the other stakeholders to be kept up to date on the risk. It is only through effective communication and collaboration that the four entities can effectively manage this shared risk. In this example, there could also be roles for industry, local government, and other contributors.

Why managing shared risk can be challenging

Risk is the effect of uncertainty on objectives. As entities have different individual objectives, they may view the same risk very differently. In complex examples, the objectives or measures of success for a joint activity may not be the same as any of the contributing entities.

Risk is managed through controls, and where several entities are involved in controls to the same risk they may be uncoordinated or even at cross-purposes. This is especially true in rapidly changing situations, it can be difficult to coordinate action and understand how different controls can work together as opposed to operating in potential conflict. Sometimes it can be difficult to understand how effectively the various controls are working in aggregate.

Managing shared risk requires the effective sharing of information. However, this can be subject to a number of constraints, both real and perceived. For example, national security classifications and privacy constraints can be real impediments to the exchange of risk information. However, mechanisms can often be established to support the appropriate exchange of information where there is a legitimate reason to do so. For example, inter-entity memoranda of understanding can be established to formalise information sharing and establish appropriate mechanisms to protect it from misuse or mishandling.

Practical strategies for managing shared risk

Identifying the potential for shared risk when setting the context[1]

Setting the context it is an important step for understanding the internal and external context in which risk is managed, but one often given inadequate attention. Carefully completing this step can help identify the potential for shared risk.

Three elements of setting the context are particularly valuable:

- Understanding the organisational context, strategies and objectives of all the potential parties to the risk.
- Developing a stakeholder map to ensure that the interdependencies often featuring in shared risk are understood[2].
- Seeking the assistance of subject matter experts can help clarify where shared risk may exist.

The role of the executive

The senior executive have an important role in setting expectations for the collaborative management and identification of risk.

This is primarily achieved through the following mechanisms:

- Championing good shared risk behaviours and setting a personal example in leading collaborative approaches to risk management.
- Directing the establishment of an entity risk framework which provide clear guidance on how to identify, assess, communicate and contribute to the management of shared risk.
- Encouraging a culture where managing shared risk is viewed as important, by ensuring that individual and collective performance management mechanisms recognise the management of shared risk.
- Establishing a monitoring mechanism to ensure that the process of managing shared risk is operating to expectations.

Recognising and building on existing mechanisms that manage shared risk

Many existing mechanisms already contribute to the management of shared risk. Inter-agency committees, task forces, working groups, and policies are often already working to address shared risks. These activities may already have established terms of reference and operating models which can be adapted to cater for different shared risk challenges.

It is important for entities to take a step back from the exiting arrangements that manage shared risks to ensure that they are able to build a complete picture of shared risks. It's also possible that existing shared risks may have evolved. There may be new risk partners, changes to the nature of the risk, or the flow-on impact of a risk may need to be considered.

Establishing foundational mechanisms

Differing risk management approaches and language amongst the entities involved can be an impediment to the effective management of shared risk. Where shared risk is commonplace or likely, a number of foundational mechanisms can be established to facilitate effective communication between those involved.

Examples of areas where aligned approaches can be adopted include common risk terminology, established mechanisms for information exchange (MoUs etc), and joint risk training.

---

[1] Setting the context is the first step in the ISO AS/NZS 31000:2009 Risk Management Standard process.
[2] For further guidance on identifying stakeholders see Comcover's information sheet *Communicating Risk available at www.finance.gov.au/comcover/risk-management/.*

Establishing foundational mechanisms

Differing risk management approaches and language amongst the entities involved can be an impediment to the effective management of shared risk. Where shared risk is commonplace or likely, a number of foundational mechanisms can be established to facilitate effective communication between those involved.

Examples of areas where aligned approaches can be adopted include common risk terminology, established mechanisms for information exchange (MoUs etc), and joint risk training.

How to manage differing appetites for the same risk

An entity's appetite for risk establishes how much risk it is prepared to tolerate or seek. Entities with different risk appetites may view the same risk as being of very different tolerability. In some cases, the manner in which the risk is assessed will affect how it is viewed by different parties. For example, how consequence is measured, how likelihood is defined, and how the severity of the risk is determined can influence how it is perceived.

To overcome this in practice, the first step is to understand and explicitly acknowledge why contributing entities have differing tolerances for the same risk. Understanding the specific consequences of concern to all parties may reveal the mismatch is not as bad as it first appeared and that a few additional controls might address the concern.

A common strategy in this circumstance is to establish different monitoring and reporting mechanisms to meet the needs of each entity. An entity with a lower tolerance for a given risk might seek more frequent and rigorous reporting to provide a higher level of assurance that the risk remains acceptable.

Establishing governance mechanisms for complex shared risks

In simple situations, it may be possible to assign a single owner to a shared risk. This entity leads the management of the risk and monitors and coordinates the actions and accountabilities of other contributors.

With more complex shared risks, more flexible governance arrangements may need to be agreed. This could involve several entities and stakeholders agreeing a set of mutual and possibly distributed responsibilities. Agreeing and documenting these responsibilities is key, so they are fully understood, resourced and assurance mechanisms put in place. The content and structure of the agreement will generally be commensurate with the significance of the risk and be clear and transparent to all parties.

Governance arrangements may be based on an assessment of risk, the significance, duration, and size of the program or task, and the resources available. Where committees are established, these can have agreed terms of reference and defined frequency of meetings. All agreements will be most effective where they specify agency contacts and/or an agreement manager[3]

In the most complex circumstances, governance mechanisms may need to be agreed that consider the shared risk as a virtual entity in its own right with its own objectives and measures of success. Contributing entities might consider establishing independent mechanisms to assist in managing the risk, similar to how a body corporate manages a building on behalf of tenants.

Documentation of shared risks

A key factor in the management of shared risks is the approach taken to document shared risks. Clear documentation of shared risks is essential for all parties concerned and will aid the communication of shared risks. It is also important to document the control process and each entity's area of responsibility. This may include shared risk registers and other formalised arrangements

[3] The Auditor - General, Audit Report No.41 2009–10, Effective Cross-Agency Agreements, 2010.

Appendix A provides a checklist of examples of shared risk considerations in each step of the Risk Management process.

Examples of shared risk

Public-private partnerships	Failure to deliver a major public infrastructure project on time and budget.	The efficient or optimal allocation of risk, that is the allocation of risks to the party that is able to manage the risk at the least cost is critical to the success of a PPP and relies upon the effective analysis of shared risk and who is best able to contribute to its management.
Commonwealth entities physically clustered together in the same building, precinct or area	Shared resilience risks such as fire, power outage or road closures.	The collaboration of several entities, and sharing of capabilities and plans to build their individual and collective resilience, including their ability to withstand supply chain disruption.
National security and law enforcement	Managing risk in circumstances where no one entity has or is permitted to hold all the relevant information on a particular threat.	Establish an independent information broker to analyse and evaluate risk information from a number of sources who would not normally be prepared to share with each other.
Policy setting and implementation entities	The risk that a new policy will fail in implementation or have unintended negative consequences.	Undertake a formal risk assessment of the new policy in collaboration with the likely implementer/s. Design a shared risk control plan early in the policy development stage.

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.

Appendix A – A shared risk checklist

Risk Management Step	Shared Risk Considerations
Establishing the context	• Develop a stakeholder map to understand with who you may share risk. Include government, industry, community and international organisations where relevant. • Consider the objectives of all contributing entities, how are they different to yours and may result in shared risk. • Consider joint objectives, which may not be critically important to a single party, but are very important to the collective. • Identify existing mechanisms, such as inter-departmental committees which may already be managing shared risk.
Identify the risk	• Conduct joint workshops with key stakeholders to identify shared risk. • Engage subject matter experts and external facilitators to bring an impartial and holistic view. • Look ahead and consider current, emerging and future shared risks.
Risk analysis	• Consider how the same risk can affect entities with different objectives and measures of success in different ways. • Consider risk severity from the perspective of each party, and also to the community as a whole. • Consider cascading impacts between entities, where, for example, realising the risk may affect the ability of a stakeholder to contribute to its management, further increasing its affects.
Risk evaluation	• Consider the risk appetite of each contributing stakeholder when evaluating the tolerability of a risk. • Document the risk assessment, in particular any residual risk exposures.
Risk treatment	• Determine and document stakeholder responsibilities for risk controls and treatments. Ensure all contributors clearly understand their treatment responsibilities, even if they've not been involved in the risk assessment. • Establish inter-entity arrangements to coordinate the application of various controls and treatments. • Determine and document responsibilities for monitoring, reporting and assuring the implementation of controls and treatments.
Communication and Consultation	• Escalate risks to and within entities based on their individual risk appetite and tolerance. • Ensure all parties clearly understand their exposure to the risk. This may require informing government and briefing ministers.
Monitoring and Reporting	• Establish structured reporting frameworks to ensure assurance mechanisms and risk indicators are not forgotten over time. • Incorporate shared risk reporting into the existing governance reporting arrangements of key stakeholders.