Defining Risk Appetite and Tolerance

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.

Summary

Risk appetite is the amount of risk that an entity is willing to accept, or retain in order to achieve its objectives. Determining and articulating an entity's risk appetite assists entities to make better choices by considering risk more robustly in decision making. **Risk tolerance** uses risk appetite on a more micro level to set the acceptable levels of variation around risk appetite.

While a risk assessment enables an entity to understand its risk exposure, it is risk appetite and tolerance that define how much risk the entity will accept. Determining and defining risk appetite or risk attitude assists entities to make better choices. The risk assessment process enables an entity to understand how much risk it is exposed to, and defining risk appetite and tolerance allows them to articulate how much risk the entity is willing to accept. Only when both risk appetite and tolerance are clearly understood can the entity understand if its risk exposure is acceptable.

It is important for entities to recognise that risk appetite and risk tolerances change over time in response to events such as changes in priorities, strategy, or government and stakeholder expectations.

This information sheet provides high level guidance to support element one the *Commonwealth Risk Management Policy*. Topics covered include:

- the purpose of defining an entity's risk appetite and its benefits
- the concepts of risk appetite and tolerance and the difference between them
- examples of how risk appetite can be expressed in practice
- steps to embed risk appetite and tolerance in an entity.

Defining risk appetite and tolerance

Risk Capacity. Risk capacity is an objective measure of the maximum amount of risk an organisation can sustain that will not disrupt the achievement of objectives. It is usually expressed as a measure against each agency risk category. Risk capacity is used to inform the risk appetite.

Risk Appetite. Risk appetite is qualitative description of an organisation's attitude to risk. Appetite describes the willingness of organisations to accept risk a certain amount of risk to achieve objectives. It describes a 'comfort zone' for agency risk taking and is usually expressed as a measure against each agency risk category. Risk appetite is used to inform risk tolerances.

Risk Tolerance. Risk tolerance is a quantitative measure to support the risk appetite. Risk tolerance measures the levels of risk taking acceptable to achieve a specific objective or manage a category of risk. Tolerance thresholds are set to inform risk mangers when a risk profile is moving towards the edge of a risk appetite. Risk tolerance triggers

and limits are designed to keep the organisation within the risk appetite and to provide a safety margin to prevent a program from reaching or exceeding its risk capacity.

Distinguishing between risk appetite and risk tolerance

Both risk appetite and risk tolerance set boundaries to define how much risk an entity is prepared to accept. However, it can be difficult to distinguish between the two; a risk appetite statement is a higher level measure that broadly considers the levels of risk management deemed acceptable, to contrast risk tolerances are narrower and set the acceptable levels of variation around objectives.

An example of a risk appetite statement would be an entity saying that that it will not accept risks that would cause significant injury to employees. In extending this to a risk tolerance statement, an entity may declare that it will only allow employees to engage in high risk physical activity for one hour a day.

Risk tolerance represents the practical application of risk appetite and is typically aligned to categories of risk such as strategy, financial, people or reputation. While risk appetite usually involves qualitative statements, risk tolerance operationalises the statements by using quantitative measures where possible, to better enable monitoring and review of the risk.

What are the benefits of defining risk appetite and tolerance?

- Support conscious and informed risk taking - By defining how much risk an entity is willing to accept, officials can make informed choices when talking about new programs, efficiency, and decision making. Risk appetite provides structure to this conversation and explicitly communicates what is acceptable.
- Promote more consistent risk management - An entity's risk appetite communicates broadly how much risk is acceptable, or indeed desirable, enabling more consistent risk taking throughout the entity.
- Guiding risk decision making and seizing opportunities - Risk appetite statements can increase the transparency of the decision making process by enabling officials to
better understand the entity's position on risk. It allows officials to better identify opportunities for further risk taking or identify areas where unacceptable risk taking is occurring.
- Structuring the executive conversation on risk taking - Senior executives can often find it challenging to articulate appropriate levels of risk taking. A structured approach to articulate risk appetite facilitates this process and encourages useful debate on what constitutes as a desirable, acceptable or unacceptable risk.
- Calibrating the entity risk assessment process - Most entities use likelihood and consequence tables and 'heatmap' matrices to assess the severity of individual risks. In turn, these risk severity ratings typically determine the acceptability of a risk or define the treatment approach to be followed. If these risks are not calibrated, the resultant actions may be skewed either too lightly (e.g. no action required) or result in an over-controlled risk response.
- Narrative statements - A carefully developed risk appetite can support the development of these narrative statements often used to describe different levels of risk. Indeed, for entities with otherwise mature existing risk frameworks, these can form a starting point for developing risk appetite.

Risk appetite statements

Risk appetite and tolerance form the key components of a risk appetite statement. Although the specific content will vary in line with the needs of individual entities, a risk appetite statement is typically a short document containing:

- a clear statement of endorsement from the senior executive, reinforcing the importance of informed risk taking
- a definition of what the risk appetite statement is and how it is to be used
- a high level statement of the entity's risk appetite, including its overall attitude to risk taking and acceptance
- a series of risk tolerance statements, typically aligned against risk categories and sub categories (where additional detail is desired). These are often presented in a tabular format and describe the relative level of tolerance for that nature of risk (for example ranging from very low tolerance to very high tolerance) and the conditions, caveats and limitations in exercising that risk tolerance.

Some simplified examples of risk tolerance statements are provided in the table below:

Fig.1

Risk Category	Relative Level of Risk Tolerance	Risk Tolerance Statements
	Lowest Highest	
Health & Safety		The Entity is committed to providing a safe workplace for all employees, visitors and contractors and there is ***very low appetite*** for death, permanent disability or time lost because of inadequate safety protocols. There is ***low appetite*** for the potential of minor injuries of staff and contractors undertaking delivery projects, recognising that there is inherent risk in the nature/location of some project work practices and locations.
Systems & Infrastructure		There is a ***moderate appetite*** associated with manual systems and outage of non-critical internal systems, accepting that some inefficiency may exist and non-critical errors may occur, provided they do not result in a breach of regulation, privacy and/or result in litigation. We have the ***lowest level*** of tolerance for the deliberate misuse of our systems for inappropriate, illegal or fraudulent purposes.
Financial		There is ***low appetite*** for non-compliance with accounting standards, government financial management orders and relevant regulatory requirements. There is ***very low appetite*** for internal fraud and the risk may only be accepted where all legislative fraud control requirements are in place and the risk has been reduced to the point where additional controls have negative cost/benefit.

To guide actions and behaviours in entities, risk appetite statements are most useful when they contain tolerance limits and triggers. Risk tolerance limits are the levels of risk which, if breached, would necessitate immediate escalation and corrective action. There can be both upper and lower tolerance limits as risk tolerance (refer table above) effectively set the boundaries of acceptable performance variability.[2]

Once the tolerance limits are established, risk triggers (both upper and lower) are then required. These are defined as the level at which escalation occurs as a result of the risk profile being sufficiently close to the risk appetite limit that corrective action is considered. The upper and lower triggers bound the optimal zone for maintain a particular risk.

The steps to embedding risk appetite and tolerance in an entity

Step 1: Identify risk capacity and determine how risk appetite will be used within the entity

It is critical that risk appetite is aligned with the entity's objectives. To do this, an entity may wish to first consider and identify its risk capacity. Setting risk capacity involves determining the maximum level of risk in which an entity can operate, while remaining within its budgetary constraints and the expectation of stakeholders. Capacity can be expressed in terms of budget limits, regulatory obligations and stakeholder demands. Once the risk capacity of an entity has been established, officials can confirm what the entity's appetite is for particular risks.

Some considerations:

- What size risks or opportunities do we expect management to bring to the attention of the Executive, governing bodies or Ministers attention and are these reporting thresholds reflected in our management reporting structures?
- What priorities or views have been expressed by Ministers or Cabinet?
- How have stakeholders reacted to past risk events?
- What are the entity's performance expectations as set out in its corporate plan?
- How do risk tolerances relate to the risk appetite and to risk categories?
- What scenario-planning or other risk discussion tools are used in setting the risk appetite and tolerances?

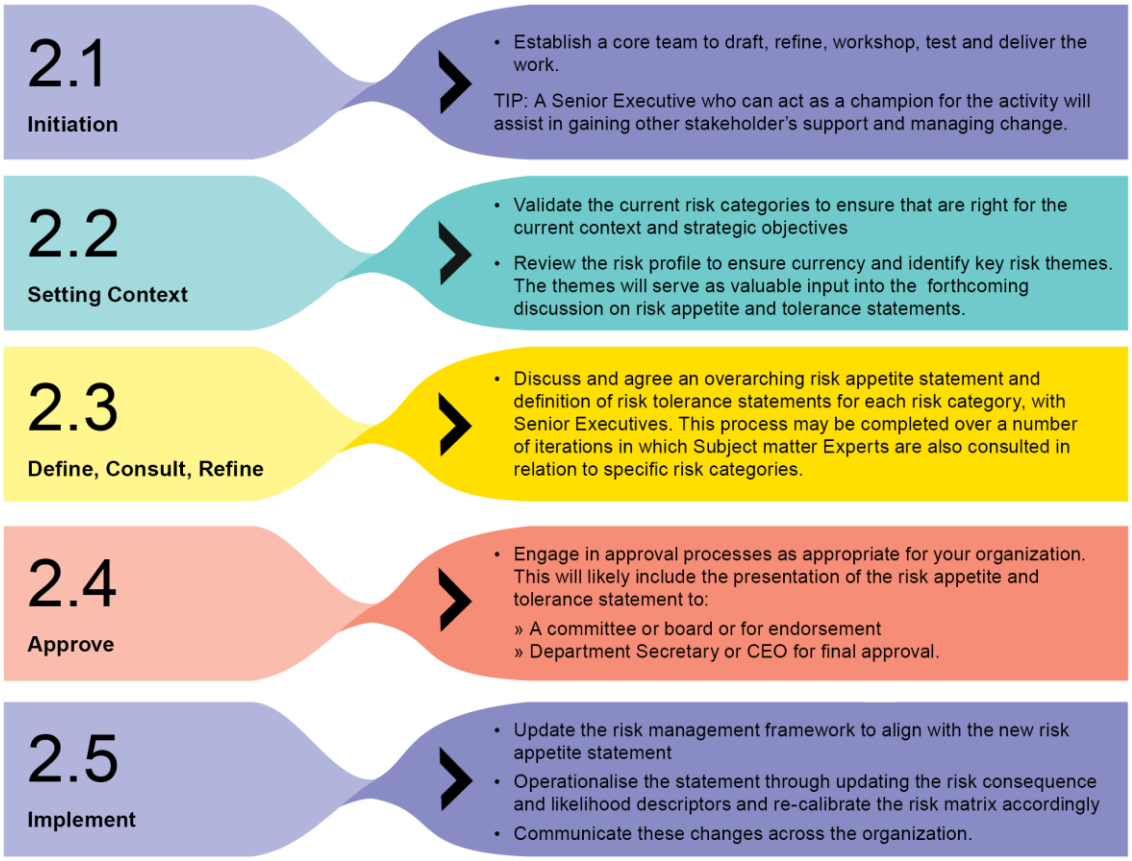
The outcome of this assessment can then be a documented risk strategy which relates the entity's objectives to its risk management priorities and articulates two things very clearly:

- the risks the entity needs to manage to achieve its objectives, and
- the capabilities to manage those risks.

Step 2: Develop risk appetite tolerance statements and limits

The process through which risk appetite and tolerance statements are developed will differ depending on the characteristics of the entity. The complexity of the entity's risk environment will all need to be considered, as well as methods to consult key stakeholders. Below is a simple process:

Fig. 2



[2] Rittenberg L, Martens F. Understanding and Communicating Risk Appetite, Committee of Sponsoring Organisations of the Treadway Commission, January 2012, Pg 11

Step 3: Monitor and report

Once risk appetites has been defined, the next step is to continually monitor how the entity is performing against them. This involves evaluating actual risk exposure levels (as determined by the entity's risk assessment processes) against the stated risk appetite, and adjusting decision making, resourcing or activities to better align actual risk exposure with the defined risk appetite.

In entities with mature risk frameworks, risk exposure can be best compared against risk appetite through the use of Key Risk Indicators (KRIs). Tolerance limits and triggers can then be assigned to each KRI to assist in identifying how the actual exposure sits against the different tolerance zones described above. A simple example of some KRIs, and associated tolerance limits is provided below:

Fig. 3

Specific Risk Area	Key Risk Indicator		Tolerance		Metric Owner
	Metric	Timeframe	Range	Comparator	
Employee Safety	OH&S compliance training completion	Annual	Not more than 10% not completed	Commonwealth Government average	XXXX
Systems & Infrastructure	Number of outages for System A	Annual	Not more than 5% allowance	Commonwealth Government average	XXXX
Financial	% of material external audit findings >2	Quarterly	No findings greater than 2	Commonwealth Government average	XXXX

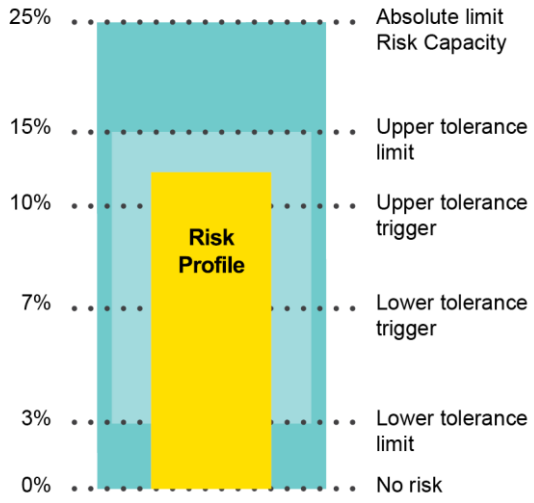
When developing a monitoring and reporting protocol, it is important for the entity to ensure that:

- responsible persons are clearly identified as risk owners. By involving relevant personnel this will help to create and/or strengthen a positive risk culture across the entity.
- there is sufficient data available to reliably report on the defined measure. Where data is not available, an alternate measure can be used until the required data is available.
- timeframes for each risk reflect those in the corporate plan. Differing timeframes could result in excessive or insufficient risk taking, ultimately undermining the achievement of the entity's objectives.

Fig. 4

Figure 4, conceptually illustrates how risk capacity, risk appetite, tolerance limits and tolerance triggers operate in practice. The example concerns a project timeline where there is an inbuilt project delay of 15%.

In this example, the risk of project delay is sitting between the upper trigger (10%) and upper limit (15%). The risk therefore needs to be escalated as it exceeds the entity's desired range in between the upper and lower triggers.

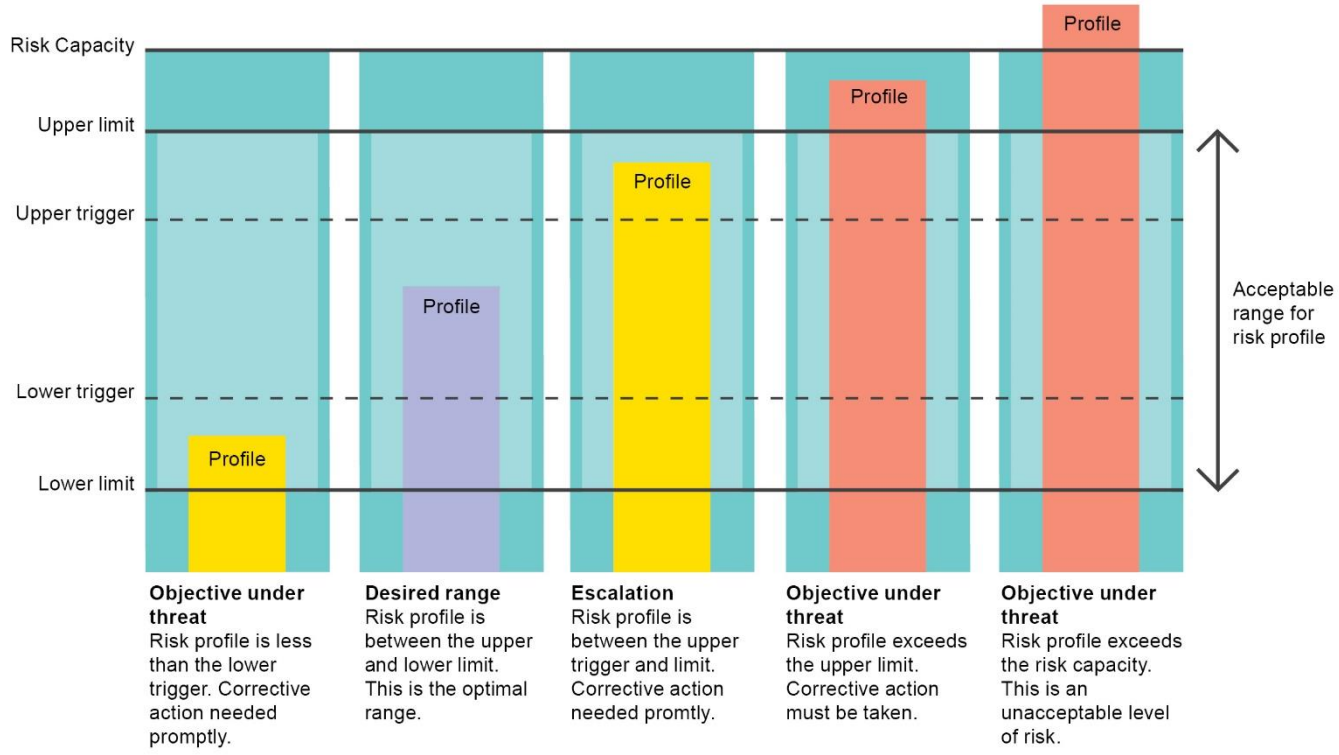


Step 4: Control and correct

Using the knowledge obtained from the monitoring and reporting activities outlined in Step 3, an entity then needs to determine whether corrective action needs to be taken. This might mean either increasing or decreasing the amount of risk the entity is exposed to. Alternatively, rather than increasing or decreasing the risk, the entity may actually need to reassess its risk appetite. Whatever the circumstances and resulting action, the objective is that unacceptable risk positions are identified and acted upon in a timely and informed manner.

The figure below, is a visual representation of five states where the risk profile of the entity is displayed relative to its risk capacity, appetite and limits. For each state, the corrective actions required to be undertaken will differ depending on where the risk profile sits within the risk appetite range. When defining escalation levels for each scenario, be careful to ensure that each category aligns with the risk appetite and tolerance defined by the entity.

Fig. 5



In particular, the following actions are typical of those an entity may define:

- less than the lower limit - If the risk profile is less than the lower limit, consider whether there is an opportunity to take additional risks
- is above the upper trigger - If the risk profile is above the upper trigger, corrective action needs to be considered and additional risk controls explored
- exceeds the upper limit - If the risk profile exceeds the upper limit, then corrective action needs to be undertaken
- exceeds risk capacity - If the risk profile exceeds risk capacity, a recovery and resolution plan needs to be enacted to prevent the entity from an impending crisis.

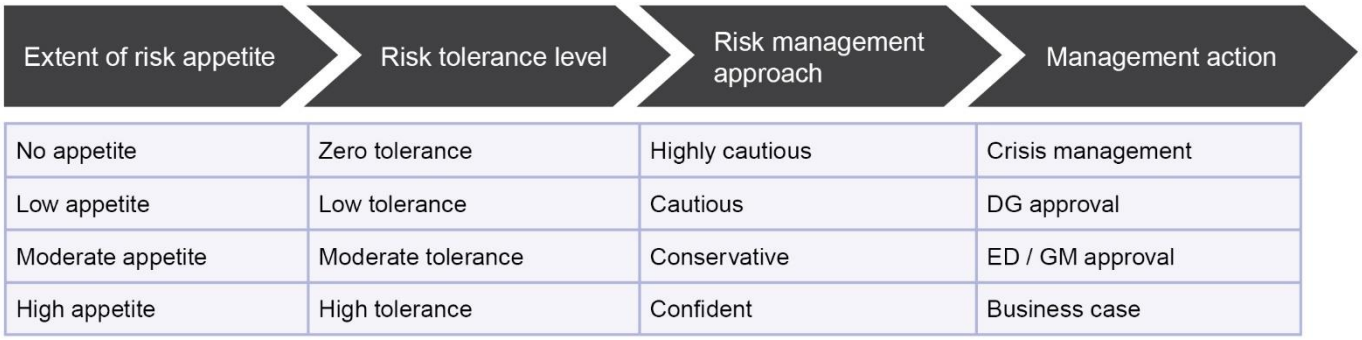
Using the project delay example from step 3 where the risk profile was assessed as being above the upper trigger, corrective action needs to be undertaken to reduce the risk of project delay. Examples of appropriate risk treatments may include reducing project scope or assigning additional resources to the project team to move the risk back into the desired range.

Implementing risk appetite in practice

An effective approach to implementing a risk appetite goes beyond process compliance. It supports the communication of those risks that matter the most. It can increase the transparency of the risk management process, and enables stakeholders to better understand the entity's position on risk. This will enable officials to identify opportunities that can relax controls and promote considered risk taking and innovation or, conversely, it can identify if the organisation is shouldering an undesirable level of risk. Ultimately, the entity is better-placed to anticipate and plan for future risks.

The below table provides high level examples of different management responses that may be defined in at different risk appetite and risk appetite and risk tolerance levels.

Fig. 6



No appetite	Zero tolerance	Highly cautious	Crisis management
Low appetite	Low tolerance	Cautious	DG approval
Moderate appetite	Moderate tolerance	Conservative	ED / GM approval
High appetite	High tolerance	Confident	Business case

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.