Defining Risk Appetite and Tolerance

**At a glance**

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 effectively in decision making.

While a risk assessment enables an entity to understand its risk exposure, it is risk appetite and tolerance that defines 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
- understanding the concepts of risk appetite and tolerance and the difference between them
- examples of how risk appetite can be expressed in practice.

**Defining risk appetite and tolerance**

**Risk appetite** - The amount of risk an entity is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describes the entity’s attitude towards risk taking. Determining an entity’s risk appetite occurs through the development of risk appetite statements which clearly set out what the executive consider to be acceptable risk-taking.

Risk appetite statements are usually aligned to categories of risk e.g. financial, people and reputation risks. Risk appetite statements will look and feel different according to an entity’s internal and external context. to be followed. If these 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.

**Risk tolerance** - The levels of risk taking acceptable to achieve a specific objective or manage a category of risk. Risk tolerance represents the practical application of risk appetite and is typically aligned to categories of risk such as strategy, financial, people or reputation.
What are the benefits of defining risk appetite and tolerance?

Supporting conscious and informed risk taking

By defining how much risk the entity is willing to accept, officials can make informed choices about taking on new programs, improve efficiency, and reduce delays in decision making. Risk appetite provides structure to this conversation and communicates explicitly what is acceptable.

Promoting 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 articulating risk appetite facilitates this process and encourages useful debate on what constitutes desirable, acceptable and 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 the risk or define the treatment approach to be followed. If these 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.

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

Together, risk appetite and tolerance form the key components of a risk appetite statement. Although the specific content and format 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 of 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 below in the table below:

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Relative Level of Risk Tolerance</th>
<th>Risk Tolerance Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lowest</td>
<td>Highest</td>
</tr>
<tr>
<td>Health &amp; Safety</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Entity is committed to providing a safe workplace for all employees, visitors and contractors and there is <strong>very low appetite</strong> for death, permanent disability or time lost because of inadequate safety protocols.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>There is <strong>low appetite</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>Systems &amp; Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td>There is a <strong>moderate appetite</strong> 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>We have the <strong>lowest level</strong> of tolerance for the deliberate misuse of our systems for inappropriate, illegal or fraudulent purposes.</td>
<td></td>
</tr>
<tr>
<td>Financial</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td>There is <strong>low appetite</strong> for non-compliance with accounting standards, government financial management orders and relevant regulatory requirements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>There is <strong>very low appetite</strong> 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.</td>
<td></td>
</tr>
</tbody>
</table>

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 level 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 the entity has been established, officials can confirm what the entity’s appetite is for particular risks.

² Rittenberg L, Martens F. Understanding and Communicating Risk Appetite, Committee of Sponsoring Organisations of the Treadway Commission, January 2012, Pg 11
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 by 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 for consulting key stakeholders. Below is a simple process:

- **Initiation**
  
  2.1
  
  - Establish a core team to draft, refine, workshop, test and deliver the work.
  
  TIP: A Senior Executive who can act as a champion for the activity will assist in gaining other stakeholder’s support and managing change.

- **Setting Context**
  
  2.2
  
  - Validate the current risk categories to ensure that are right for the current context and strategic objectives
  
  - Review the risk profile to ensure currency and identify key risk issues. The themes will serve as valuable input into the forthcoming discussion on risk appetite and tolerance statements.

- **Define, Consult, Refine**
  
  2.3
  
  - Discuss and agree an overarching risk appetite statement and definition of risk tolerance statements for each risk category, with Senior Executives. This process may be completed over a number of iterations in which Subject matter Experts are also consulted in relation to specific risk categories.

- **Approve**
  
  2.4
  
  - Engage in approval processes as appropriate for your organization. This will likely include the presentation of the risk appetite and tolerance statement to:
    
    » A committee or board or for endorsement
    » Department Secretary or CEO for final approval.

- **Implement**
  
  2.5
  
  - Update the risk management framework to align with the new risk appetite statement
  
  - Operationalise the statement through updating the risk consequence and likelihood descriptors and re-calibrate the risk matrix accordingly
  
  - Communicate these changes across the organization.
Step 3: Monitor and report

Once risk appetite 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 actual exposure sits against the different tolerance zones described above. A simple example of some KRIs, and associated tolerance limits is provided below:

<table>
<thead>
<tr>
<th>Specific Risk Area</th>
<th>Key Risk Indicator</th>
<th>Tolerance</th>
<th>Metric Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Metric</td>
<td>Timeframe</td>
<td>Range</td>
</tr>
<tr>
<td>Employee Safety</td>
<td>OH&amp;S compliance training completion</td>
<td>Annual</td>
<td>Not more than 10% not completed</td>
</tr>
<tr>
<td>Systems &amp; Infrastructure</td>
<td>Number of outages for System A</td>
<td>Annual</td>
<td>Not more than 5% allowance</td>
</tr>
<tr>
<td>Financial</td>
<td>% of material external audit findings &gt;2</td>
<td>Quarterly</td>
<td>No findings greater than 2</td>
</tr>
</tbody>
</table>

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 that time that the required data is available.
- timeframes for each risk reflect those of the corporate plan. Differing timeframes could result in excessive or insufficient risk taking, ultimately undermining the achievement of the entity’s objectives.

The figure opposite, 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.

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

- If the risk profile is less than the lower limit, consider whether there is an opportunity to take additional risks
- If the risk profile is above the upper trigger, corrective action needs to be considered and additional risk controls explored
- If the risk profile exceeds the upper limit, then corrective action needs to be undertaken
- 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 where it can relax controls and promote considered risk taking and innovation or, conversely, it can identify if the organisation is taking 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 tolerance levels.

<table>
<thead>
<tr>
<th>Extent of risk appetite</th>
<th>Risk tolerance level</th>
<th>Risk management approach</th>
<th>Management action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No appetite</td>
<td>Zero tolerance</td>
<td>Highly cautious</td>
<td>Crisis management</td>
</tr>
<tr>
<td>Low appetite</td>
<td>Low tolerance</td>
<td>Cautious</td>
<td>DG approval</td>
</tr>
<tr>
<td>Moderate appetite</td>
<td>Moderate tolerance</td>
<td>Conservative</td>
<td>ED / GM approval</td>
</tr>
<tr>
<td>High appetite</td>
<td>High tolerance</td>
<td>Confident</td>
<td>Business case</td>
</tr>
</tbody>
</table>

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.