Demystifying Risk Appetite

Grant Purdy, Broadleaf Capital International

We have been using the term risk appetite for many years. It is used regularly in the media and all the major consultancy groups and many professional associations with an interest in risk management discuss the term and describe its interpretation and application. Now regulators are asking companies to prepare statements of their risk appetite as part of their governance processes and auditors are being asked to verify these.

The concept of risk appetite seems deceptively simple: it is often described as how much risk we might wish to 'take' to achieve a desired return. In practice, however, an organisation's risk appetite can be exceedingly difficult to tie down or define.

Although many authors discuss risk appetite, most of the current definitions are vague, ambiguous and contradictory, and the gap between theory and practice is often wide. Efforts to quantify risk appetite can sometimes produce an illusion of precision while, in practice, the resulting statements are of little practical use.

Just to add to the confusion, the equally rubbery phrase 'risk tolerance' is also often used at the same time as risk appetite. The two terms are often used interchangeably and sometimes appear to have overlapping definitions.

Clearly organisations and their stakeholders need to gain assurance that they are not exposing themselves to too much or too little risk. However, as with all other performance outcomes, the most useful way to appreciate whether levels of risk are acceptable is to set and use criteria. Auditors then have a straightforward role to see that risk criteria are correctly derived and are being properly used.

1 Definitions

There are many definitions for risk appetite the companion term of risk tolerance. COSO[i] defines risk appetite as:

> *the degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals*

and also as:

> *the amount of risk an entity is willing to accept in pursuit of value.*

However it is not at all clear why these definitions are different or even what they mean in practice: COSO does not tell us what a 'degree of risk' is and how this is different to an 'amount of risk'; it also does not explain why one term is concerned with the pursuit of goals and the other the pursuit of value and what that value is.

The third revision of the South African King Report on Corporate Governance[ii] contains many requirements for risk management. Clause 4.2 specifies that the Board should determine the levels of risk tolerance and the code says under a subordinate clause (4.2.2) that this can involve the board "setting limits for the risk appetite". This suggests that the authors of King III see risk appetite as some subordinate property of risk tolerance – something that seems contra-intuitive.

The UK based Institute for Risk Management has recently produced fairly complex guidance[iii] that aims to assist companies determine their risk appetite so that they can satisfy the recent UK Corporate Governance Code[iv]. However, the code does not explicitly require the establishment of 'risk appetite'. It only says that:

> *The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives.*

Recent requirements for the financial sector are contained in the report from the Basel Committee on Banking Supervision that is euphemistically called "Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches"[v]. This defines risk appetite as:

> *a high level determination of how much risk a firm is willing to accept taking into account the risk/return attributes; it is often taken as a forward looking view of risk acceptance.*

However, this does not seem at all clear because 'high level determination' and 'forward looking view of risk acceptance' are not further explained.

The Basel Committee document then goes on to define risk tolerance as:

> *a more specific determination of the level of variation a bank is willing to accept around business objectives that is often considered to be the amount of risk a bank is prepared to accept.*

Again, this definition is not clear and both definitions are further compromised when the report says, in relation to risk appetite and risk tolerance, that:

> *In this document the terms are used synonymously.*

It is noteworthy that all the codes mentioned so far view risk as only involving negative and detrimental consequences, that has to be shed or at least put up with in the pursuit of good returns and the achievement of objectives. These definitions do not seem to accommodate the natural concept of taking on more risk to provide more opportunities for benefit.

The Institute of Internal Auditors[vi] has adopted a more succinct definition for risk appetite of:

> *The level of risk that an organization is willing to accept.*

This is one of the simpler and more useful definitions in common use.

One of the duties of the Working Group created to prepare ISO 31000:2009, Risk Management[vii] was to update and align ISO Guide 73[viii], the vocabulary for risk management. Guides are ISO documents whose purpose is to achieve standardisation across all ISO standards. While many of the terms defined in Guide 73 are broadly consistent with the intent and approach to risk management in ISO 31000, the Guide includes some that are not used in the Standard.

Risk appetite is a case in point. ISO Guide 73 defines this as:

> *The amount and type of risk that an organisation is willing to pursue or retain;*

Risk tolerance is defined as:

> *Organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.*

Although these definitions seem much clearer and less likely to be misinterpreted, the ISO Working Group decided not to use them in ISO 31000 because it wanted to explain the risk management process as simply as possible, avoiding jargon and unnecessary complications. The Standard therefore adopts a more pragmatic approach that requires an organisation to derive and set or adopt risk criteria as the basis for its decisions. These are derived as part of the vital step of 'Establishing the Context' and are to be based on the objectives of the organisation and those of its important stakeholders. Risk criteria are defined as the:

> *terms of reference against which the significance of a risk is evaluated.*

They are used as part of risk evaluation, to determine the priority for considering risks and to help decide if they need treatment.

Risk criteria are also mentioned in the annex to the standard where it suggests that to demonstrate effective risk management organisations should be able to satisfy the outcome tests that:

> *The organisation has a current, correct and comprehensive understanding of its risks;*
>
> *The organisation's risks are within its risk criteria*

These are clearly exacting tests that could form the basis for questions that a Board might ask of an organisation's management.

2 Why Risk Appetite is Difficult to Define

Even if the prevailing definitions for risk appetite were not confused and contradictory, a rational analysis of the concept demonstrates why it is not easy to prepare a simple

statement that describes this for an organisation. Most of the challenges faced in defining risk appetite arise out of commonplace mis-understandings about risk and are complicated by personal and group perceptions arising out of experience.

If people do not understand risk and how it arises, discussions about risk appetite can be confused and mis-directed. For example, risk is often seen to be independent of an organisation, its actions and intentions and is confused with impacts and consequences: people talk about "when risk eventuates" or when it "occurs". The definition of risk in ISO 31000:2009, that risk is the effect of uncertainty on objectives, makes it clear that risk is only 'caused' by the decisions of the organisation and through the setting of objectives. It arises solely because these objectives are pursued against a background of external and internal factors and circumstances that create uncertainty.

There are three broad areas that make defining a statement of risk appetite difficult and unreliable.

2.1 Conceptual Problems

Some of the conceptual problems faced are:

- People define 'risk' in different ways in their day-to-day communication, using the term variously to describe events, impacts, likelihoods or worst-case outcomes. This may make it very hard to reach agreement on what is being described as 'risk', without even getting into the further complications of how it might be measured.
- It is not always clear whether the appetite refers to individual risks (presumably those that are either high or have significant consequences) or some aggregate measure of 'risk' that applies to the organisation. This affects how the appetite is defined and measured.
- There seems to be little credit given to existing controls when defining risk appetite. In fact the discredited measure of 'inherent risk' is normally used when discussing it. However, Boards need information about the current levels of risk and the effectiveness of key controls so that they can fulfil their governance obligations. A statement about risks at hypothetical and unrealistic levels will not provide directors, shareholders or stakeholders with much useful information from which to draw conclusions on capability of the organisation to manage risk.
- An organisation's appetite may vary according to its current activities and the decisions that must be made. For example, a Board may have little tolerance for material threats to the organisation's balance sheet, but it may be prepared to accept high risks where there is a significant business opportunity.

2.2 Measurement Problems

Risk needs careful measurement to be meaningful. Some of the problems in this area are:

- The risks an organisation faces may have many different kinds of consequences, not all of which can be measured on a common scale (for example, in dollars). This makes it very difficult in practice to develop a single aggregated measure of 'risk' for the portfolio of risks the Board must address.

- Defining risk appetite only using financial measures does not recognise the importance of other, less tangible outcomes such as staff morale, brand value and reputation and the social licence to operate. Ignoring these will lead to poorly founded decisions, which in turn can significantly reduce value to stakeholders and shareholders.
- Even in sectors where financial measures of outcomes are used and standardised, the way in which risk is defined across a portfolio can vary considerably.
- The way 'reward' is measured is often subject to the same difficulties, and so the risk/reward trade-offs to which many commentators refer may in practice be more notional than real in terms of their use for practical decision-making.

2.3 Perceptual Problems

Dealing with personal and group perceptions create perhaps the greatest problems:

- The experience and knowledge of individuals affects their perceptions of outcomes, likelihoods and what is acceptable. This may make consensus very difficult to attain. This is a particular challenge for Boards whose members come from diverse backgrounds with a wide range of different types of experience.
- What is perceived to be important varies with time, and is often influenced by recent high-profile events within the organisation or the sector or as reported in the media. These variations can occur within the timespan of days.
- Risks are seen by many people as events (incorrectly) and therefore frequent events and their cumulative impacts greatly influence what is perceived to be unacceptable risk.
- Executives are 'closer to the action' and so may have different perceptions of risks from Board members. This may arise from a genuinely better understanding of operational controls within the organisation, or it may be related to an optimistic bias associated with 'ownership' of proposals and projects.
- There is rarely a simple correlation between the level of risk and the returns that can be earned. Many authors and institutions continue to use the phrase 'risk vs. reward' or 'risk reward ratio' which reinforce the view the risk appetite is somehow linked to the level of return or reward. In fact, while identifying and creating opportunities for gain may lead to improved returns, just increasing exposure to risk does not necessarily ensure a greater return. Reducing the level of risk does not automatically work either. It seems that this is a false paradigm that many people just repeat without critical consideration.

3 Establishing Risk Criteria

ISO 31000:2009 adopts a practical and pragmatic way of dealing with the matters for which some would have us use the concept of risk appetite: it requires the levels of risk that are linked to certain outcomes to be set before risk assessment takes place. These are called risk criteria and risks are compared with them to determine their relative significance and to help justify the need for further risk treatment.

Risk criteria comprise two components:

1. The method to be used for determining the 'level of risk' for each objective (i.e. how consequences and their likelihoods are to be combined and presented);
2. The rules that are to be applied when making decisions that relate to the level of risk once it has been determined as part of the risk assessment.

Figure 1 shows the general, six-step process that should be followed when risk criteria are established for an organisation.

Risk criteria should be set by the organization as a whole to reflect its objectives and overall attitude to risk. More detailed or specific expression of these criteria may be required for a particular application of the process (for example, for assessing the risk related to a project). However, any such amplification must be consistent with the overarching criteria.

Risk criteria should be documented and communicated to relevant stakeholders to facilitate understanding and consistent application. They should also be reviewed periodically and updated to ensure that they continue to reflect the organization's and its key stakeholders' values and objectives.

Risk criteria can be quantitative or qualitative and they can apply to consequences, likelihoods or levels of risk. They can be single limits or decision-making schemes such as the 'As Low As Is Reasonably Practicable' (ALARP) approach often used in health and safety.

Because risk criteria frame the way in which risks should be assessed, they should relate to an organisation's objectives and, in particular, its critical success factors (CSFs). These are areas in which an organisation must succeed and they are derived from its strategic intent, mission and vision statements.

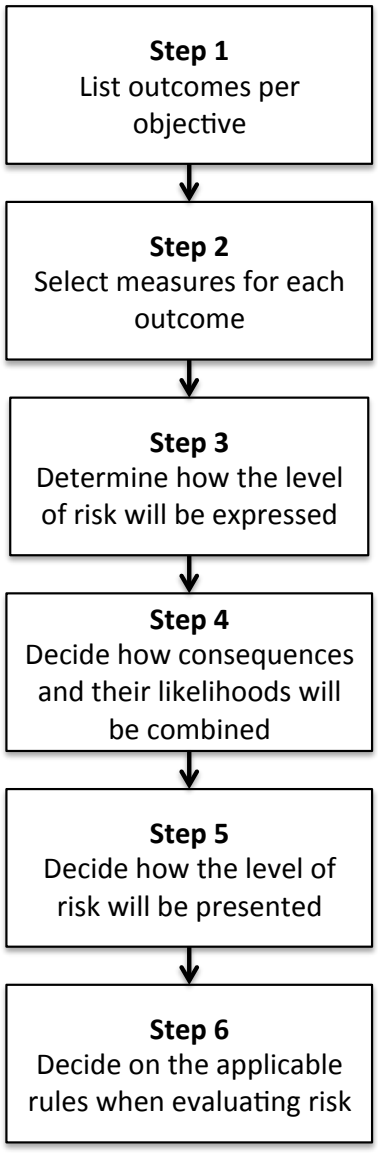

Figure 1: Steps to defining risk criteria

Much advice is already available on how quantitative, financial risk criteria can be developed. However there is considerably less advice available on how organisations can develop risk criteria for non-financial consequences that can be used as part of qualitative risk analysis. Despite the principle of ISO 31000:2009 that risk management should be tailored, in practice many organisations just copy their criteria from others that have different objectives and different CSFs. This means that the basis on which these organisations make risk-based decisions may be invalid.

The expected outcomes for the CSFs form the basis for the types of impact or consequence that can be used to characterise risks. Scales are then normally formed for each consequence type to allow the level of consequence to be graded. Typically there are five to seven levels in the scales.

Most risks do not involve only negative or positive consequences but can be normally described in terms of both beneficial and detrimental outcomes. For this reason it is useful if the descriptions of the consequence criteria contain both positive and negative outcomes or are worded in such a way that they can mean either type. Figure 2 gives an example for a state transport agency that was used for the high-level risk assessment of a strategic plan.

Similarly, using overly negative labels for levels such as 'catastrophic' or 'extreme' does not facilitate the application of the table to beneficial outcomes.

Some organisations use different sets of consequence tables to represent beneficial and detrimental outcomes, but often these are cumbersome in practice.

Figure 2: Neutral worded consequence scales

Rating	Safety	Legal & compliance	Capacity	Equity	Community reaction	Sustainability	Financial
Massive	Multiple Fatalities and/or severe irreversible disability to many persons	Profound and enduring implications and onerous obligations for the organisation and its officers	The social and economic environment of ??? or one of the regions would be altered dramatically	The relative provision of services to separate groups or regions would be affected dramatically	The community's perception of public transport would be completely transformed and this could lead to changes in transport administration	The sustainability of transport in??? would be significantly transformed from its current level	Financial resources available to public transport would be affected to the extent that large elements of service provision would be markedly revised
Major	Fatality and/or severe irreversible disability to one or more persons	Serious implications and onerous obligations for the organisation and its officers that would persist for several years	The social and economic environment of ??? or one of the regions would be affected significantly	The relative provision of services to separate groups or regions would change significantly	The community would feel there had been a marked change in public transport and this would have significant flow on effects	The sustainability of transport in ??? would be markedly different from its current level	Financial resources available to public transport would be affected to the extent that some elements of service delivery would change
Moderate	Moderate irreversible injury or impairment to one or more persons	Significant implications and obligations for the organisation and its officers	Isolated groups or regions would see a significant effect but the remainder would be not be affected	The relative provision of services to separate groups or regions would change enough to be clearly visible	The community would feel there had been an appreciable change in public transport and this might have some flow on effects	The sustainability of transport in ??? would be altered slightly from its current level	Financial resources available to public transport would be affected but the changes would be limited in extent or duration
Minor	Hospitalisation required. Largely reversible injury to one or more persons	Modest implications and obligations for the organisation and its officers	There would be occasional changes in capacity affecting small groups or areas but it would not be sustained	There would be minor changes in the distribution of services but they would not have widespread implications	The community would acknowledge minor or isolated changes in public transport	Elements of the sustainability of transport in ??? would be altered a little from current levels	Financial resources available to public transport would be affected but the changes would be accommodated within the portfolio budget
Insignificant	Reversible injury requiring hospital treatment	There would be no appreciable effect	Capacity would be affected in principle but it would pass without comment	Minor variations in provision would not attract special attention	Community sentiment about public transport would not change appreciably	There would be no appreciable or persistent change	Minor financial changes would be absorbed without formal reallocation of funds

Deriving risk criteria in this way captures the organisation's attitude towards risk in terms of the consequences types chosen and the alignment of the levels for different consequences. It can also be reflected in likelihood criteria scales and in the manner in which the levels of consequence and their likelihoods are combined to produce a level of risk.

In most cases, ordinal consequence scales are used for qualitative risk analysis, as opposed to ratio scales, and this means that even if the labels for levels are numerals, an

arithmetic expression should not be used to combine a level of consequence with a level of likelihood to obtain a level of risk. Arithmetic expressions that combine other factors, such as one that might represent control effectiveness, are also generally invalid.

Normally, a matrix or lookup table is used to combine the consequence level with its likelihood level to produce a level of risk and these can also be used to represent the organisation's attitude to risk. While it is generally good practice for there to be roughly the same number of cells for each level of risk, it is possible to 'skew' the matrix as shown in Figure 3 to reflect the organisation's aversion to high consequence, low likelihood risks.

Figure 3: Example skewed matrix

LEVEL OF LIKELIHOOD							
	F	Medium	Medium	High	Very High	Very High	Very High
	E	Low	Medium	High	High	Very High	Very High
	D	Low	Medium	Medium	High	Very High	Very High
	C	Low	Low	Medium	High	High	Very High
	B	Low	Low	Medium	Medium	High	Very High
	A	Low	Low	Low	Medium	High	High
		1	2	3	4	5	6
		LEVEL OF CONSEQUENCES					

4 The Role of Assurance Providers

Assurance providers have two major roles to play in connection with measures of risk appetite. They have to use suitable measures for risk appetite when planning audits (IIA International Professional Practices Framework[ix] Principle 2010) and also have to judge whether those used by the organisation are appropriate and have been properly derived (Principle 2120, Risk Management).

The joint handbook published by the IIA Research Foundation, IIA Australia and by Standards Australia explains how risk criteria should be used for audit planning and, in particular how the consequence measure of potential exposure should be used in preference to the now discredited and unreliable measure of 'inherent risk'.

Section 3 of this paper should help assurance providers understand if the risk criteria used by their organisation to express its risk attitude or appetite are soundly based and are being properly applied.

5 Summary

While the concept of risk appetite might seem seductively simple, there are many dissimilar and ambiguous definitions for the term and it is often confused with a different but related concept called risk tolerance. Of all the definitions available, those for risk appetite and risk tolerance given in ISO Guide 73 seem the most clear and usable. These are also consistent with the risk management process in ISO 31000:2009. That used by the IIA is also simple and also consistent with the Australian and International standard.

Risk appetite is a complex issue and producing a statement that describes it for an organisation is difficult and may prove unnecessary and ultimately unhelpful. ISO 31000:2009 gives an alternative, more practical and pragmatic approach to enable risk-based decisions by using risk criteria. These should be based on critical success factors and are therefore specific to a particular organisation and cannot be simply copied and reused. Some care is required in developing risk criteria to ensure that they accurately reflect the relative weightings the organisation applies to risks with different types of consequences. The organisation's aversion to the most significant consequences can also be simulated in the process used to combine the level of consequences with the level of their likelihood to produce a level of risk.

Setting criteria and measuring outcomes against them is a common manner in which organisations manage all forms of performance. The simple approach advocated in ISO 31000:2009 of setting and using risk criteria can therefore be integrated easily into an organisation's normal, day-to-day systems of management. This should help ensure that decisions across the organisation are informed by assessments of risk that have been made on an appropriate and consistent basis.

Auditors have to use suitable risk criteria when planning audits and also have to judge whether those used by their organisations are soundly based and appropriate. This paper should provide a basis for that evaluation.

6 References

[i] Enterprise Risk Management — Integrated Framework: Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission, September 2004.
[ii] King Code of Governance For South Africa 2009. Johannesburg, Institute of Directors Southern Africa, 2009.
[iii] Risk Appetite and Risk Tolerance – a consultation paper. London, Institute of Risk Management, May 2011.
[iv] The UK Corporate Governance Code. London, Financial Reporting Council, June 2010.
[v] Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches. Basel, Basel Committee on Banking Supervision, Bank for International Settlements, June 2011.

[vi] International Standards for the Professional Practice of Internal Auditing, Institute of Internal Auditors, Inc., 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201 U.S.A.
[vii] ISO 31000:2009, Risk management – Principles and guidelines. Geneva, International Standards Organisation, 2009.
[viii] ISO Guide 73, Risk Management – vocabulary. Geneva, International Standards Organisation, 2009.
[ix] International Professional Practices Framework, Institute of Internal Auditors, Inc., 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201 U.S.A.

