Good Governance Guide

Risk appetite statement

Governance Institute of Australia

Recognise and manage risk

It is **good governance** for organisations to articulate and communicate their appetite for risk with a formal risk appetite statement.

Regulators may require the board to set a risk appetite statement.

What is risk?

The International Standard for risk management, *ISO 31000:2009 Risk management – Principles and guidelines*, defines risk as the 'effect of uncertainty on objectives'.

An organisation's appetite for risk is central to the way it does business. The amount of risk accepted in pursuit of strategic goals will vary widely from business to business, depending on individual circumstances. Some factors that may affect risk appetite include:

- industry
- external environment
- shareholders
- ownership structure
- organisational maturity.

Setting appropriate boundaries for risk-taking is the core function of risk appetite and risk tolerance.

What is risk appetite and risk tolerance?

The International Organisation for Standardization (ISO) produced Guide 73 which provides definitions of generic terms in relation to risk management. The ISO's definitions are explicit yet lack detail:

- Risk appetite is 'the amount and type of risk that an organisation is willing to pursue or retain'.
- Risk tolerance is 'an organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives'. It is important to note that risk tolerance can be limited by legal or regulatory requirements.

The Committee of Sponsoring Organisations of the Treadway Commission (COSO):

- defines risk appetite as 'the amount of risk, on a broad level, an organisation is willing to accept in pursuit of value'. It reflects an organisation's risk management philosophy, and in turn influences its culture and operating style.
- suggests risk tolerance relates to risk appetite, but differs in one fundamental way — risk tolerance represents an application of risk appetite to specific objectives.

Considered, clearly articulated risk appetite and risk tolerance provide a sound foundation for risk management. Setting the risk appetite explicitly articulates the attitudes to and boundaries of risk that the board expects senior management to take. Without this, risk management will be carried out with unclear boundaries and expectations, resulting in an organisational culture where decisions are made without consideration of risk.

What is the risk appetite statement?

The risk appetite statement is commonly the document that articulates the organisation's approach to risk, and would include both the risk appetite and risk tolerances. It can be both quantitative and qualitative. The risk appetite may consist of high-level statements in only one or two paragraphs that in turn drive a more detailed listing of risk tolerances. The two parts work together and in their entirety constitute the risk appetite statement.

In documenting the risk appetite statement, organisations should consider that:

- risk appetite is:
  - strategic, aspirational and directly related to the achievement of business objectives
  - part of whole-of-organisation governance
  - the broad pursuit of risk
- while risk tolerance is:
  - tactical and operational

- enables an organisation to control its appetite for risk in line with organisational, strategic objectives
- the level of risk that can be borne in the context of specific transactions or activities.

Role of governing body

The board or governing body is ultimately responsible for deciding the nature and extent of the risks it is prepared to take to meet objectives.

It is the role of the board to set the risk appetite for the entity, and the role of management to ensure that the organisation operates within the risk appetite set by the board.

Management may recommend changes to the risk appetite. However, only the board or governing body should approve changes to the risk appetite.

Risk appetite is a function of the maturity of the organisation and its levels of controls. Importantly, a board or governing body should not increase the risk appetite simply in order to take a more aggressive strategy unless it has satisfied itself that the organisation's risk framework is capable of supporting the higher risk appetite. A board or governing body can take a more aggressive strategy because the organisation is capable of taking higher levels of risk.

The board or governing body should evaluate risk appetite annually.

Risk tolerances

An organisation's appetite for risk may be different over time, during a crisis, in different geographies, for different business units or for different categories of risk. Tolerance is typically presented in different ways for different risk categories. For example, financial risk tolerance may be expressed in dollars or percentage of capital, whereas people risk tolerance may be expressed in terms of severity of injury.

Risk tolerances may also be considered in terms of major types of risk:

- strategic risk — the risk of not identifying optimum strategies or of failing to execute those strategies
- credit risk — the risk of financial loss where a customer fails to meet their financial obligations
- market risk — the risk to profits from changes in market factors, such as foreign exchange rates, interest rates, commodity prices and equity prices
- operational risk — the risk that arises from inadequate or failed internal processes, people and systems or from external events
- liquidity risk — the risk of not meeting payment obligations.

Alternatively, risks tolerances may be aligned with balanced scorecard perspectives of:

- customer
- financial
- internal business processes
- learning and growth.

Risk tolerances across all risk categories should be aligned with strategic objectives and performance management systems operating within an organisation.

Link to the risk register

A well-articulated risk appetite statement provides a baseline for comparing risk ratings calculated on a risk register, with the tolerance for risk in that category, to determine what controls or actions are required to bring individual risks within the organisation's risk appetite.

See *Continual maintenance of risk register*

References

APRA *Prudential Standard CPS 220 Risk Management*, January 2015

Principle 7 of the ASX *Corporate Governance Council's Corporate Governance Principles and Recommendations*, 3rd ed, 2014

Commonwealth Department of Finance, *Commonwealth Risk Management Policy*, July 2014

NSW Treasury, TPP 15-03, *Internal Audit and Risk Management Policy for the NSW Public Sector*, Version 1.0, July 2015