QRMC RISK, SAFETY AND BUSINESS ADVISORY CONSULTANCY

insight

QRMC NEWSLETTER

Issue 123 March 2022

Insight aims to provide useful information, links and tips in the areas of Risk Management, Work Health and Safety, Business Continuity Management, and other areas relating to management systems and corporate governance.

Risk Appetite or Risk Tolerance or Both?

The terms *risk appetite* and *risk tolerance* are commonly used interchangeably in the risk management world. The Australian Government (Dept of Finance Comcover Statement, 2016) attempts to differentiate between the two terms by stating that risk appetite is a "*qualitative description of an organisation's attitude to risk which describes the willingness of organisations to accept a certain amount of risk to achieve objectives*" whereas risk tolerance is described as a "*quantitative measure to support the risk appetite which measures the levels of risk taking acceptable to achieve a specific objective or manage a category of risk*".

Technically, there is a difference between the two definitions, and in simpler terms, risk tolerance can be represented as the practical application of an organisation's risk appetite. This is typically aligned to categories of risk such as Safety, Governance/Legal, Financial, Reputational, and Environmental. Things get a little greyer with the fact that the International Standard for Risk Management (ISO31000) doesn't actually refer to either term! In fact, the Standard seeks to take a less prescriptive approach by simply stating that the organisation "*establish the amount and type of risk that may or may not be taken to guide the development of risk criteria*".

Regardless of which definition you go with, organisations have recognised that there are significant benefits, and potential restrictions in establishing a Risk Appetite/Risk Tolerance Statement. Let's explore the benefits firstly:

- Top management, with the endorsement of the organisation's board, publicly state the willingness of their organisation to accept a certain amount of risk to achieve their objectives. So long as this position has been effectively communicated, all risk owners throughout the organisation are guided in their decision-making for managing risks within their areas of accountability.
- Following on from the above point, this will support conscious and informed risk taking such as introducing new programs, or implementing efficiency measures. A clear risk appetite provides structure to the process of considering changes in the workplace.
- Promotes more consistent risk management across the organisation, including by top management, when monitoring and reviewing any Extreme or High risks to the organisation.
- Allows the organisation to clearly state their position on unacceptable areas of risk taking (this can also be a potential restriction – see below).
- Allows investors, regulators, other stakeholders and the public to know the organisation's risk position on areas of corporate social responsibility and the environment – what the organisation *values*.

So, what are the potential restrictions or disadvantages to promoting a Risk Appetite/Risk Tolerance Statement?

The biggest issue we have seen in a number of organisations is in relation to the inclusion of generalised statements such as "*the organisation has zero appetite for undertaking activities of high risk*". Whilst of good outward intention, internally these statements can paint the organisation into a corner by potentially preventing it from undertaking some of its operational activities. No more work at height, no exploration of revenue opportunities from high risk/high reward streams, no investment or research into potentially game-changing technologies, etc.

This can also send mixed messages to lower-level Managers and employees, and potentially create artificially lower risk assessments as workers attempt to align their activities with the corporate position. Consequently, visibility of genuine Extreme or High risks to top management could be obscured, with the possible realisation of these risks coming as a major surprise and impacting on the organisation's ability to effectively manage risk and meet objectives.

While risk appetite will often mean different things to different people, a properly communicated, non-contradictory Risk Appetite/Risk Tolerance Statement can actively help organisations make the appropriate decisions to achieve their goals whilst providing their Managers, employees, investors and the public with its position on what is acceptable and what its values are when it comes to managing its strategic and operational risks.

Please contact QRMC for more information.

Disease, flood, famine (well, supply shortages) ... when is pestilence coming?

Did your organisation's Business Continuity Plan provide meaningful guidance during COVID and the recent flooding events?

Was it even referred to? If it was, has it been reviewed since then?

Most BCPs include a lot of theory but are often too bulky to provide any meaningful guidance during a disruption event. In many instances they are developed with external assistance and whilst including useful background information, they generally aren't developed in such a way as to assist in managing the actual continuity of business operations immediately following a disruption event.

A BCP should be developed as part of a process and not as a stand-alone document. This includes the following:

- Consideration of the organisation's Critical Services / Functions. This is generally facilitated via a workshop with key stakeholders to commence the Business Impact Analysis process and includes a review of key processes whilst identifying the Critical Functions and current and required controls.
- Determination of the Maximum Acceptable Outage times for Critical Functions, being the maximum period of time that the organisation (and more importantly, its customers) can tolerate the loss of capability of a critical function, asset or IT application.
- Once critical functions have been identified, a threat risk assessment workshop needs to be undertaken on the Critical Functions to identify, in view of the controls the organisation currently has in place (e.g. work arounds, redundant plant etc.), which of these presents the greatest risk to delivering its services within Maximum Acceptable Outage times.
- The output of this threat assessment workshop is generally a Critical Functions Risk Register that establishes priorities for all future actions in regard to the development of the BCP.
- BCP documentation must then be designed to be user-friendly, incorporating response, continuity and recovery activities, related roles and responsibilities, resourcing requirements and organisational interdependencies that are specific to the organisation's needs.

It is always advisable to review a BCP after a business disruption event whilst the event is still fresh in stakeholders' minds. This ensures that learnings are captured and knowledge is retained within the organisation. It is also a good opportunity to review BCP documentation to critically assess what did not add value and is thus not required.

The most useful BCP is one that is current and actually provides guidance to end users both before and during an event.

Please contact QRMC for more information.