I. Risk philosophy

A risk management philosophy is the set of shared beliefs and attitudes that characterise how risk is considered in any organizational activities. It affects how risk management components are applied, including how risks are identified, the kinds of risks accepted, and how they are managed.

When the risk management philosophy is not developed, understood, or fully embraced by the staff, an uneven application of risk management across business units, functions, or departments is likely. Even when the philosophy is well developed, cultural differences among units resulting in variation in enterprise risk management application may still be found.

Therefore, risk philosophy, risk appetite and risk strategy should always be kept aligned, as one reflects the other. To this purpose it’s necessary to “measure” risk perception by the management staff – as some managers may be prepared to take more risk, while others are more conservative – as well as the risk maturity of organizational context, since this latter could be more or less resilient in facing risk.

II. Mandate

A mandate in risk management expresses itself through an official statement/document, that clearly indicates the risk management strategy and objectives, the people accountable for them at all levels, and authorizes such people to use proper resources for achieving their assigned objectives.

Defining and communicating this statement testifies an organization’s commitment to implement a risk management system.

Box 1 - An example of mandate among NSIs

“Minimizing any significant risks arising during activities and services, through the application of effective risk management principles and practices. The organization will bear an acceptable level of risk, but only after weighing up the likelihood, consequences and cost of an adverse event occurring against the availability of resources to eliminate or manage the risk”.

Source: Australian Bureau of Statistics – Accountable Authority Instructions

III. Risk management scope

Defining the scope of a risk management strategy means that all staff are made aware of the relevance of risk in achieving their objectives, as well as specific training for such staff is envisaged. It also means that a common approach to risk management is shared across the organization, including a common risk language.

IV. Risk plan

To implement a risk management system, a risk plan is needed that includes:

- Risk management objectives (strategic as well as operational ones);
- Risk management activities, to be undertaken within a proper timeframe, to help the organization achieve its strategic objectives;
- Resources required, including people, knowledge and budget;
- Decisions regarding risk communications, internal and external.

It describes how the risk management strategy progress will be monitored, reviewed and reported.

Regarding the activities to be undertaken, several of them are crucial, whether resulting from an extended program or from a “quick” one through a “prototypal release” of the risk management system. The resources that an organization will invest in implementing such a system are also crucial, to determine the quality and progress of results.