Steve Leybourne's reflections on David Hillson's Risk Doctor briefing

Over the past year or so, a debate has been reopened relating to how many of us perceive risk within the project domain. In late 2009, David Hillson, an expert on risk within projects, circulated a Briefing Note to his colleagues and contacts within the sector, highlighting the way in which the new ISO standard defined risk, and the effect that may have on how risk could be perceived within the management of projects.

The ISO31000 — 'Risk Management' standard has now been published by the International Standards Organization (ISO). The description of the standard at http://www.iso.org/iso/iso_catalogue/management_standards/specific_applications/specific-applications_risk.htm states that the intention is to set out: *"principles, a framework and a process for the management of risk that are applicable to any type of organization in public or private sector. It does not mandate a 'one size fits all' approach, but rather emphasizes the fact that the management of risk must be tailored to the specific needs and structure of the particular organization."*

This laudable intention does, however, indicate that 'defining' risk is becoming more of a challenge, with some significant tension arising.

Historically, risk has been defined in terms of uncertainty, or an uncertain event, that results in changes that could be either positive or negative, but which have to be managed. The uncertainty aspect means that the event may or may not occur, but if it does, then it will have an effect.

However, ISO3100 defines risk as *'the effect of uncertainty on objectives'* (my emphasis). This suggests that ISO is offering a new definition of risk; moving away from the uncertainty of an event occurring, and focusing on the 'effect' that will ensue if and when it does.

Traditionally, risk planning in projects has focused on two elements: the likelihood of something happening that could impinge on the project; and the likely impact if it did occur. Likelihood is more concerned with uncertainty, and impact is more concerned with effect. So arguably, we have always considered the two elements, but the IS31000 standard is — intentionally or unintentionally — causing a change in the focus of risk planning and risk management, through its adoption of an alternative definition of risk.

It could be argued that this is an exercise in semantics, in that risk management in the project domain has always considered both effect and uncertainty. One thing is apparent, however; those organisations that are going to adopt and implement the ISO31000 standard will also have to adopt the definition of risk that the ISO has chosen to incorporate into its standard.

So, is this apparent shift in defining risk, driven by an established and respected standards organisation, going to make any difference to the way that we consider and prioritize risks on projects?

In order to carry this discussion forward, perhaps it is important to consider the purpose of the ISO standard, which is to standardize vocabulary, performance criteria and process, and to offer guidance on integration into the organisation (Purdy, 2010). The standard explains that risk is the consequence of an organisation setting and pursuing objectives against an uncertain environment. Is a consequence the same as an effect? I suspect that in most instances it is.

However, it appears that what ISO31000 is attempting to do is to shift the management of risk from the assessment of uncertain occurrences to a process that optimizes, so that the achievement of objectives is more likely. There are some problems here, in that 'effect' is explained in the standard as a deviation from the expected, but the type and context of a 'deviation' could be based on an original baseline best guess, personal viewpoint or opinion, or a statistically modelled expectation (Leitch, 2010). In trying to be more explicit about risk, maybe the ISO31000 standard is actually introducing more ambiguity, or more avenues of interpretation.

I doubt that this is what was intended, but the fact of the matter is that ISO31000 has been adopted as the *de facto* standard by at least 25 countries, with more adopting as it gains global traction. The standard is being driven forward by the leading international organisation for standard setting, which is an organisation with significant global presence and prestige.

Do we have any option but to adopt its terminology and definitions? Realistically, I do not think so.

References

Leitch M. 2010, ISO31000:2009 — The new international standard on risk management, *Risk Analysis*, vol. 30, no. 6, 887-892.

Purdy G. 2010, ISO31000:2009 — Setting a new standard for risk management, *Risk Analysis*, vol. 30, no. 6, 881-886.

Dr Steve Leybourne
Boston University