



RISK DOCTOR BRIEFING

THE DEFINITION DEBATE – CONTINUED



© December 2009, Dr David Hillson PMP HonFAPM

david@risk-doctor.com

Most of us had hoped that the debate about how to define a risk was settled. This was a “hot topic” around the turn of the century, particularly focused on the question of whether the concept of risk should include opportunity as well as threat, or whether risk was exclusively negative. The majority consensus now seems to be agreed that risk is double-sided and covers both upside and downside.

Now the issue of the ISO31000 “Risk management – Principles and guidelines” standard (published in November 2009) looks likely to reignite the definition debate, and this time the issue is equally fundamental. At first sight the definition of risk in ISO31000 appears to be clear and unambiguous, with just five words:

Risk is “effect of uncertainty on objectives”

This contains all three vital words that any definition of risk must include.

1. Risk is about *uncertainty* and it may never happen.
2. Risk matters and must be managed because it has an *effect*.
3. We measure that effect against defined *objectives*.

So far so good. But looking more closely at the ISO31000 definition, a problem appears. The ISO risk standard clearly states that “Risk is effect...” If we follow this approach, we would define the following as negative risks: delay, overspend, accidents, reputation damage, lost market share, inefficiency etc. On the upside we would see time or cost savings as positive risks, or enhanced performance or increased shareholder value. All of these things are effects on objectives that could arise from uncertainty.

By contrast, every other risk standard previously has defined risk in terms similar to the following:

Risk is “an uncertainty that, if it occurs, will have an effect on objectives”

This is completely different from the ISO31000 definition. The other risk standards clearly state that a negative risk is an uncertainty that would cause delay or overspend or reputation damage if it happened. An upside risk is also uncertain and its occurrence would result in time or cost savings, or improved reputation. A risk can be an uncertain event or an uncertain set of circumstances or an uncertain assumption, but the key point according to these standards is that the risk is *uncertain*. Of course because a risk is uncertain then it may never happen, but if it does happen then it will have an effect on objectives. But *the risk is not the effect. The risk is the uncertainty* that would result in an effect.

This matters because it determines the goal of risk management. If “Risk is effect...” then risk management seeks to manage those effects, and the risk process must focus on how to avoid or minimise negative impacts and how to exploit or maximise positive impacts. But if “Risk is uncertainty...” then the aim of the risk process is to address uncertain events or conditions. This means to stop negative risks from happening if possible, or at least to reduce their probability and/or impact. It also means to capture positive risks or maximise their probability and/or impact. Addressing the uncertainty leads to a more proactive approach than trying to tackle the effect.

It is also important to be clear about the definition of risk in order to avoid confusion and disillusionment among teams who are trying to manage their risks. While most risk specialists will be able to cope with the variation introduced by ISO31000, others are likely to find it distracting.

One possibility is that in their search for a simple elegant definition of risk, the authors of ISO31000 have oversimplified and therefore created this confusing change. It seems unlikely that the whole world of established risk management practice will change direction to match this new definition of “Risk is the effect of uncertainty on objectives” instead of “Risk is an uncertainty that, if it occurs, will have an effect on objectives”. Instead we must hope that common sense prevails and perhaps the ISO31000 definition might change.

STANDARD	DEFINITION OF "RISK"	
	"UNCERTAINTY ..."	"... THAT MATTERS"
British Standard BS6079-3:2000 (2000)	"Uncertainty inherent in plans and the possibility of something happening (i.e. a contingency) ..."	"... that can affect the prospects of achieving business or project goals."
British Standard BS IEC 62198:2001 (2001)	"Combination of the probability of an event occurring ..."	"... and its consequences on project objectives."
A Risk Management Standard (Institute of Risk Management et al, 2002)	"The combination of the probability of an event ..."	"... and its consequences."
Australian/New Zealand Standard AS/NZS 4360:2004 (2004)	"The chance of something happening ..."	"... that will have an impact on objectives."
Risk Analysis & Management for Projects [RAMP] (Institution of Civil Engineers et al, 2005)	"A possible occurrence ..."	"... which could affect (positively or negatively) the achievement of the objectives for the investment."
APM Body of Knowledge (Association for Project Management, 2006)	"An uncertain event or set of circumstances ..."	"... that should it or they occur would have an effect on achievement of one or more project objectives."
Management of Risk [M_o_R]: Guidance for Practitioners (Office of Government Commerce, 2007)	"An uncertain event or set of events ..."	"... that should it occur will have an effect on the achievement of objectives."
A Guide to the Project Management Body of Knowledge [PMBok® Guide] (Project Management Institute, 2008)	"An uncertain event or condition ..."	"... that if it occurs has a positive or negative effect on a project's objectives."
British Standard BS31100:2008 (2008)	"Effect of uncertainty ..."	"... on objectives."
ISO31000:2009 (2009)	"Effect of uncertainty ..."	"... on objectives."

This briefing has been reprinted in the *Journal of Project Program and Portfolio Management* with the permission of Dr. David Hillson to seek reflections on his briefing to be published in the Viewpoint section of the journal. The editors would like to thank Dr. Hillson for allowing us to reprint it.

Summary of reflections on David Hillson's Risk Doctor briefing

Steve Leybourne, Section Editor, Viewpoint

Risk and the ISO31000 Standard

A number of scholars, including myself, have been considering the implications that the relatively recent ISO31000 Standard may have on project management, using a December 2009 briefing by David Hillson, an acknowledged expert on project risk, as the baseline. Specifically, the Hillson (2009) offering was concerned about the way that the ISO had arbitrarily challenged and replaced one of the key definitions in risk management; the definition of risk itself, shifting the emphasis from the 'uncertainty' attached to risk, to the 'effect' of that risk.

This is an important change, in that almost all the previous standards and bodies of knowledge have looked at risk more in terms of the likelihood of it occurring, rather than the effect that it has if and/or when it does occur. Hillson (2009) tabulates these definitions across the various standards, providing a degree of clarity and ease of comparison that brings these issues to the fore in an effective way.

At the journal, we see this as an important issue for project managers, and we were therefore keen to get a number of different perspectives from academics with an interest in the evolution of the literature relating to the project domain. Hopefully, these differing perspectives will be evident as the three contributions —from Roger Atkinson of Bournemouth University in the UK, Anbang Qi of Nankai University in China and myself— will show.

My own reflections, to some extent, consider the inevitability of the new definition from ISO being adopted. I think many of us feel that when a large and influential global standards organisation enters the fray and starts to document process in any area, the likelihood of change being forced upon those who, for one reason or another, need to adopt those standards is high. The ISO is of course keen to 'standardise' the concept of risk (as, indeed, it is attempting to standardise many other areas), although it is evident from the project management literature that the 'one size fits all' approach is untenable. Notwithstanding this, the advantages to an organisation of publishing the accepted standard in an area cannot be underestimated, and we have a perfect example of that in the PM domain with the dominance of the PMI *Body of Knowledge*.

Atkinson touches on the commercial implications of 'owning' an accepted definition, suggesting that this definition can then be franchised to others. He also takes another viewpoint, and applies an element of systems thinking to the consideration of changing definitions, linking in addition to issues of complexity. Atkinson looks at the motivations of ISO's attempt to vary the previously accepted understanding of risk in the project domain, and his view is that the constant

challenging of definitions keeps them relevant and, indeed, that these challenges keep the debate current and fresh.

Qi brings a different perspective, one that is culturally dramatically different from the 'Westernized' ideals of both Atkinson and myself. He considers risk from a different philosophical angle, suggesting that risk and change are interlinked, and that change is inevitable. This leads to, and includes, change in the way that we consider key elements of practice. Traditional Chinese management practices see change as a constant, and tend to be focused on the opportunity that arises from that change, and the ability to manage or govern events around such change for advantage.

Interestingly, all three contributions in this section on Risk focus on change, and the benefits that may accrue or emerge through the effective interaction between change and outcomes. In this respect, maybe organisations like the ISO are creating opportunities for reflection on, and improvement in, PM practice.

We all agree that can only be a good thing.

About the author:

Dr Steve Leybourne is a full-time member of the faculty at Boston University. He has a PhD from Cardiff Business School in the UK, has published papers on project management, change management, and improvised working practices, and has presented at many national and international peer-reviewed conferences, including the US Academy of Management conferences and the PMI Research conferences. He is a recognised thought leader in the area of improvisation, complexity and ambiguity in the project domain. His research interests include organisational improvisation, innovation and the implementation of change using projects. He is a member of the Editorial Board of the *Project Management Journal* and of the *Journal of Project, Program and Portfolio Management*, and was a member of the UK-based and EPSRC-funded Rethinking Project Management network. He is a member of numerous professional and academic associations, including PMI, and was an invited keynote speaker at the 5th Brazil National PM Conference in 2010.

Roger Atkinson's reflections on David Hillson's Risk Doctor briefing

Organisations and individuals are living with constant change, and the environment within which we live and work has to, naturally, keep pace with those changes. One example of a framework that impinges on organisational change is the new ISO31000 standard for Risk Management. An early discussion about where that new standard fits in with other definitions and standards has been written by David Hillson, who raised the question about the new ISO definition and how it was attempting to differentiate from other definitions of risk.

The fact that there are several other definitions of risk indicates that, as with standards, the issue with definitions is that there are so many from which to choose. The fact that we have several definitions for risk indicates that there is no single agreed definition. My guess as to why that will continue is also the reason why I would consider these issues as they relate to Project Management. As soon as any one organisation has a standard or definition for concepts such as risk or project management and seeks to achieve global acceptance of that definition, it usually attempts to franchise its version to others who want to use it. Thus, the opportunity for financial gain, is the reason why there will be no a global agreement for such definitions.

The fact that there is a continual move to at least try and refine and update a definition of risk is understandable and necessary. It can also be seen to fit comfortably within systems thinking as suggested by Beer (1995), who suggested that managing systems was essentially about managing complexity (something project management now includes), and that could be measured by a '... loose portmanteau variable' that he termed 'variety'. The Beer (1985) axiom was that the "variety" of the environment would always be greater than the 'operators' that serve it and, in turn, the 'operators' will exceed the 'management' that tries to regulate or control. The variety and complexity of risk, as with project management, will remain one step ahead of those trying to control and manage it, which provides one reason for trying to achieve a definition.

So it would appear reasonable that a search for a definition of risk will continue. If Beer's axiom is proven correct, that search will be never ending. The origin of risk from the Latin *Risco*, meaning danger, indicates how the definition of risk, or at least the meaning currently attached to the word, has emerged over time. The early attempts from the 18th century, with the development of both the normal distribution and standard deviation, some measures of risk, indicate how young the methods of measuring and managing risk are.

However, while a continual search for a definition of risk can be understood, what would be interesting to know is, What were the drivers to create ISO31000, given that there is limited time to undertake all the things we would like to achieve. Why change, and why now?

Using — as we are informed in Hillson's paper — the three vital words that any definition of risk should have as a framework, let us now consider why the ISO31000 standard was created.

First, uncertainty. What uncertainty existed that required the ISO to be written? Was it, for example, to solve a known problem with, or answer a question about, some existing ISO, or the ten other definitions? Is it possible to know what drove the need for the ISO?

Second, effect. What effect did writing the new definition hope to achieve, and is that reason known? Were those changes to the effect research driven? If so, what research, or was it just thought that it was perhaps time to create a new ISO? That last question as a rhythm to ISO development work rather than reaction to problem would be valid.

Third, objectives. Against what measures will the effects of the new ISO be judged? Do these include short-term objectives, as that is all that will be known at this time, or are there medium- and long-term objectives as well?

If we don't continue to challenge existing definitions, then potential benefits might be lost. However, at the same time, it would be interesting to know the logic and reason for the ISO31000 definition wording. The new definition has reduced any vagueness under which risk could be considered. This has both positive and negative issues. A positive is that we have a clear focus; a negative point is that risk as agreed involves uncertainty, and if Beer's axiom is true, it also includes complexity. This begs the question of how the effect would be measured if the risk is possibly unknown. Hillson provides some additional challenges to the new definition.

A benefit of having a change in the definition of risk is that it keeps the debate alive, and that has to be a good thing.

Reference

Beer, S. 1985, *Diagnosing the System for Organisations*, Chichester, Wiley.

Dr Roger Atkinson
Bournemouth University

Anbang Qi's reflections on David Hillson's Risk Doctor briefing

According to David Hillson, 'Now the issue of the ISO31000 "Risk management — principles and guidelines" standard looks likely to reignite the definition debate, and this time the issue is equally fundamental' (Hillson 2009). Yes, he is right. Especially, for the Chinese people, they have their own definitions for risk and risk management from their traditional management philosophy and their definition for these are different to that of Westerners.

According to traditional Chinese management philosophy, everything in the world is changing, either rapidly or slowly. Change makes the world full of risks and human beings need to continually manage risks. They think risk is not an 'effect', or an 'uncertainty', but the result of changes. All of the traditional management philosophy of Confucian, Taoist, and Mohist schools of ancient China originated from the three versions of the *Book of Change* (a book of risk and risk management) and these three traditional Chinese management schools all believed that management means to manage the changes of all things in the world.

In Chinese characters, risk is not one word (like in English) but two characters written as '风险'. The Chinese character of '风 (wind)' means the 'reason for the change' since the wind can blow (or stop to blow) in any direction, and that can cause rain, snow or storms, or even floods and disasters. The Chinese character of '险 (danger)' means the 'the result of the change' because changes can result in a opportunity or some kind of loss.

At Nankai University, we have done a lot of research on risk and developed our own definition of risk based on traditional Chinese management philosophy. The research shows that risk can be defined by the following equation. Risk equals the product of 'probability' and 'opportunity/loss'. Here, 'probability' is the likelihood of changes to the environment and conditions of a project or a thing (Qi 2008). And 'opportunity'/'loss' is the result of these changes.

$$R = P \times (O / L) \quad (1)$$

P—Probability, if P=1, then it is known that things are certain, if P<1, then it is known that some of the things are uncertain, if P=?, then it is unknown if there are things that are uncertain.

O—Opportunity, L—Loss

This definition contains two vital parts. First, risk is caused by changes of the conditions and environment that make a thing become uncertain and this uncertainty should be expressed as a probability. Second, risk can cause a negative result that might probably bring about loss for an organisation or a person, or risk can result in a

positive result that might probably bring about some opportunity to an organisation or a person.

According to traditional Chinese management philosophy, risk management is not only to manage the results of the risk, but also to manage the changes that cause the risk. In Chinese writing, risk management is not two words but four Chinese characters written as ‘风险管理’. The Chinese character of ‘管 (govern)’ means to control the changes and their resulting risks. The Chinese character of ‘理 (study)’ means to search and find out the changes and their results, enabling the changes to be controlled or governed. Each of the traditional management philosophies of the three schools of ancient China developed their own risk management methodology and methods that focused on controlling or governing changes.

We have also done lots of research on risk management based on traditional Chinese management philosophy. Our research shows that risk management can be defined using the following equation (Qi 2011).

$$RM = P \uparrow \times (O \uparrow / L \downarrow) \quad (2)$$

RM—risk management, $P \uparrow$ --increasing the probability, $O \uparrow$ -- enlarging the opportunity, $L \downarrow$ -- decreasing the loss

This definition contains three vital parts. First, risk management means to obtain more information for increasing the probability and changing the $P=?$ into $P<1$ or, further, for changing the $P<1$ into $P=1$. Second, risk management must increase the opportunity provided by changes in order to get more benefit from the changes and risks. Third, risk management must decrease the loss caused by changes, or even convert the loss into opportunity. In fact, all management and administration are considered to be a kind of risk management because if everything in the world is certain (cannot be changed), there will be no need for management or administration.

There are some differences between the Chinese and Western perspectives of risk and risk management. Typical Western definitions include ‘Risk is the effect of uncertainty on objectives’ or ‘Risk is an uncertainty that, if it occurs, will have an effect on objectives’. But the Chinese believe ‘Risk is the change that can result in some opportunity/loss’. We think risk management should govern or control the change and the result of the change in order to avoid loss and to increase the benefit from the risk.

Of course, we also hope that the ISO31000 definition can become more exact through these discussions and debates.

References

Hillson, D. 2009, The definition debate — continued, *Risk Doctor*, www.risk-doctor.com.

Qi, A. 2008, *Project Management*, China Science Press, Beijing.

Qi, A. 2011, *Project Risk Management*, Nankai University Press, Tianjin, China.

Dr Anbang Qi

Nankai University, China

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, ISO31000 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 ISO31000 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