

News Analysis

ISO 31000: The devil in the detail

David Hillson follows up the feature in our December issue by examining the fine print of the new risk management standard

Most of us had hoped that the debate over defining a risk had been settled. It 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 seems to be that risk is double-sided, covering both upside and downside.

But publication last November of the *ISO 31000 Risk management - Principles and guidelines* standard looks likely to refuel the debate on a different front, and this time the issue is equally fundamental. At first sight the definition of risk in ISO 31000 appears clear and unambiguous with just five words: risk is "effect of uncertainty on objectives". This has three vital words that any definition of risk must include.

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

So far so good. But looking more closely at the ISO 31000 definition, a problem appears. The ISO risk standard clearly states that "Risk is effect..." Following this approach, we

would define the following as negative risks: delay, overspend, accidents, reputation damage, lost market share and inefficiency. On the upside we would see time or cost savings as positive risks, or enhanced performance or increased shareholder value. All of these are effects that could arise from uncertainty. By contrast, most other risk standards have defined risk as some variation of "uncertainty that matters" (see table below). These definitions might be summarised in the phrase: Risk is "an uncertainty that, if it occurs, will have an effect on objectives".

This is completely different from what ISO 31000 says. Other risk standards clearly state that a negative risk is an uncertainty that would lead to 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

STANDARD	DEFINITION OF "RISK"	
	"UNCERTAINTY ..."	"... THAT MATTERS"
A Risk Management Standard (Institute of Risk Management et al, 2002)	"The combination of the probability of an event ..."	"... and its consequences."
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."
British Standard BS31100:2008 (2008) ISO31000:2009 (2009)	"Effect of uncertainty ..."	"... on objectives."

have an effect on objectives. But the risk is not the effect. The risk is the uncertainty that would result in an effect.

This is important 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 the uncertainty. 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, to avoid confusion and disillusionment among teams trying to manage their risks. While most risk specialists will be able to cope with the variation introduced by ISO 31000, others are likely to find it distracting.

One possibility is that in searching for a simple elegant definition of risk, the authors oversimplified and 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 that the ISO 31000 definition is changed in the near future. The alternative is that organisations will continue to understand and manage risk in the same way as before, ignoring this subtle but important change of focus introduced by ISO 31000.

IRM publishes ISO31000 Guide

The Institute of Risk Management has teamed up with AIRMIC and Alarm to produce a practical guide to the successful implementation of the international standard ISO 31000 Risk Management – Principles and Guidelines, released at the end of 2009.

The new guide, entitled A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000 is available for free download from the IRM's website at <http://www.theirm.org/publications/PUpublications.html>

The guide provides a helpful commentary on ISO 31000 as well as further guidance on successful implementation. In particular, it recognises that risk has both an upside and a downside, and offers additional advice on various concepts including risk appetite.



Dr David Hillson FIRM FRSA FCFI HonFAPM, known globally as The Risk Doctor, is director of Risk Doctor & Partners (www.risk-doctor.com).



School of Social Sciences Safety, Health and Environment courses

Do you want to further your career?

Nottingham Trent University has an enviable record of achievement in safety, health and environmental education. Our courses are designed to meet the needs of practitioners who want to enhance their subject knowledge, and meet personal and professional development requirements.

MSc Health and Safety Risk Management

- Professionally accredited/endorsed by IOSH and the CIEH
- Incorporates an international perspective enabling practitioners to operate effectively at a strategic level
- Modules can be studied as stand-alone elements for Continuing Professional Development (CPD)

Professional Diploma in Safety, Health and Environmental Management

- Professionally accredited/certified by IOSH and IEMA
- Assessments allow you to utilise your own workplace or experience
- Completion within 12 months via day release

Postgraduate Certificate in Corporate Responsibility

- Certified by IEMA at Associate level and modules count for Continuing Professional Development (CPD)
- Engages wider view of business risk and responsibilities and considers and evaluates approaches to their management in practice
- Delivered primarily via distance learning, assessment methods focused on practice

For further details please contact the Admissions Team on 0115 848 4200

www.ntu.ac.uk/rm

NOTTINGHAM
TRENT UNIVERSITY