## Is ISO 31000 fit for purpose?

**The debate**

"Is ISO 31 000 fit for purpose" is the headline above a debate published in the June edition of *Risk Management Professional* – for online version click here. The "debate" consisted of an abbreviated version of my blog – "*ISO 31 000: Dr Rorschach meets Humpty Dumpty*" - and a "rebuttal" by Grant Purdy, one of the principal authors of the ISO Standard.

"Debate" and "rebuttal" have been enclosed in quotation marks because a serious debate did not take place. The rebuttal is entitled "*Never perfect, but inclusionary, practical and* ***widely accepted*****",** and consists mostly of an explanation of (and excuse for) any imperfections that it might have.

It observes that:

- "standards may not reflect the 'best available' practices and leading thinking."
- "a standard can be biased because of prevailing influences in the committee that prepared it.
- "significant compromises are often required to obtain consensus in a committee."

and concedes that

- "it would be naïve to think that ISO 31000 could not suffer from any of the problems described above."

The rebuttal further acknowledges "some fudging" and "some unnecessary complexity". None of these admissions of possible imperfection are related to any specific parts of ISO 31000; readers are left to work out for themselves where within the document they might be found.

**Is it fit?**

But let's move on to the *purpose* of ISO 31000. Is it fit for it? Here is what it proclaims in its introduction: "this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context." The most appropriate response to this is "Wow!!"

At this point we must remind ourselves just what it is that the ISO is offering to help the world to manage: *risk* is defined by the ISO as "the effect of uncertainty on objectives - positive and/or negative". The ISO is clear that uncertainty (i.e. risk) must be dealt with *comprehensively*. Uncertainty must be put "within a comprehensive framework"; there must be a "comprehensive list" of uncertainties); and the managing organization must have a "comprehensive understanding" of the uncertainties that it is managing. And finally there must be a "comprehensive, fully defined and fully accepted accountability for risks (i.e. uncertainties)". The task that the ISO has set itself can be fairly described as oxymoronic; uncertainty cannot be captured comprehensively.

**Widely accepted?**
Let us next consider Purdy's contention that the ISO oxymoron is "widely accepted". I have recently been invited to participate in two risk conferences - one in Bilbao and one in Zurich. At these conferences I availed myself of the opportunity to investigate how far ISO 31000 had penetrated constituencies not consisting of internal auditors or members of the C-suite.

The Bilbao conference was large – over 1200 registrations – and had a title, the *10th International Conference on Occupational Risk Prevention* - that suggests that those attending were unlikely to be signed up to the ISO definition of risk. I conducted a small survey during receptions and coffee breaks in which I asked 25 fellow presenters if they had heard of ISO 31000. Only one had heard of if, but confessed he had not read it.

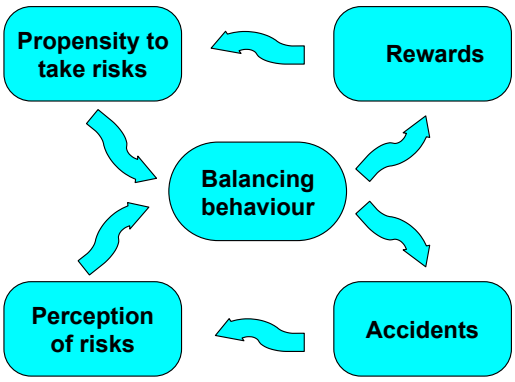
In one presentation I had hopes of finding someone better informed about ISO 31000. Enrico Occhipinti is a professor at Milan University and author of a foreword to an ISO Technical Report – *Ergonomics — Manual handling of people in the healthcare sector.* But he had not heard of ISO 31000.

The second conference was the annual conference of the European Society for Risk Analysis. It had over 200 registrations. I took advantage of my position as an opening keynote speaker to ask the plenary a different question: "How many of you have read ISO 31000?" Ten hands went up. One was an editor who told me later that he had read it for the purpose of judging (and rejecting) an article on the subject. Another told me he had only read it because his curiosity had been piqued by what I had said about it in one of my blogs.

In pursuit of wide acceptance ISO 31000's champions have a further problem – the paywall. As previously noted the cost of the ISO risk management standard and its supporting documents is likely to rule out participation in their project by most academics with an interest in risk. And the paywall is getting higher. Last May a conference was held in Paris to promote ISO 31000. The Conference Pack is offered online for a mere €499.00.

**Risk: positive and/or negative?**
In my presentation to the Zurich conference I introduced the Society for Risk Analysis to the ISO definition of risk, highlighting the definition's contention that risk could be positive. I speculated about how this definition might have been arrived at. I described an encounter that I had had with the SHE (Safety, Health and Environment) managers of a large pharmaceutical firm. I showed the SRA conference my simple model of risk management (Figure 1) that I had used in my workshop with the SHE managers.

Figure 1. The Risk Thermostat




The thermostat is set in the upper right-hand corner. Everyone has some propensity to take risks – some call it their "risk appetite". A propensity to take risk leads to risk taking behaviour that leads, by definition to a probability/possibility of an adverse outcome – an "accident". It is through surviving accidents and learning from them, or seeing them on television, or being warned by mother or, if you are an actuary, studying accident data, that people acquire their perception of risk. The model proposes that when propensity and perception get out of balance there is a behavioural response that seeks to restore the balance. Why do we take risks? There are rewards. And the magnitude of the reward influences propensity.

Before the workshop I had been sent the SHE managers' in-house risk management manual and been asked to comment on it. The manual contained a wiring diagram much more complicated than Figure 1, with lots of arrows and feedback loops and boxes with labels such as "risk identification", "analysis", "evaluation", "treatment", "monitor" and "implement". I persuaded the SHE managers that their model reduced, in essence, to the bottom loop of my model. Their job, as specified by their model, was risk reduction.

At that point I asked the SHE managers who in the company was responsible for the top loop, the rewards loop. After muttering amongst themselves they thought it was probably the marketing department. And who, I then inquired, was in charge of the balancing act. After much more muttering they concluded that it had to be the CEO. And where I asked is the wiring diagram that describes how he performs this act. So far as I am aware, many years later, they are still looking for it.

I am afraid that my workshop was considered demoralizing. One of the SHE managers commented rather morosely: "so that's why they call us the sales prevention department." On reflection I felt guilty. They worked in an industry, and for a company, that had large and numerous hazards that required managing, and their risk management manual, so far as I could judge, set out the job in a sensible manner. It wasn't their fault that, in the division of labour, responsibility for the top loop, the rewards loop, had been assigned to another department.

The solution to the morale problem of the sales prevention department does not lie in the redefinition of risk. It would clearly be impractical, if not counterproductive, to

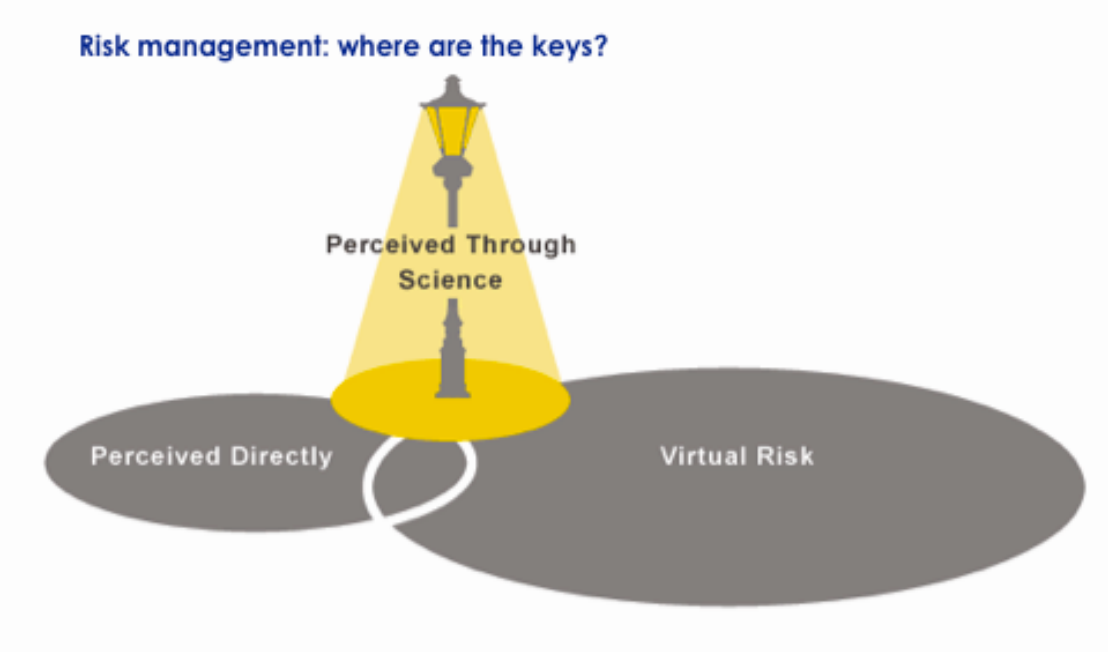
add sales targets to the responsibilities of those responsible for everything from trip hazards to dangerous chemical releases.

For some decades I have been pointing out that people take risks in pursuit of rewards and, with help of Figure 1, I have managed to complain about risk management practices that ignore the opportunity costs of excessive risk aversion without redefining the word.

**What is risk?**

My presentation to the SRA was entitled "What is risk?" and concluded with a Venn diagram that I have been using for some years (Figure 2). I used it to point out that people frequently use the same word "risk" to mean quite different things and talk (or shout) past each other. Here the diagram has been embellished to illustrate the metaphor of the drunk who lost his keys in the dark, but searches for them under the street light because that is where there is light to see.

Figure 2




The first circle, "perceived directly" contains the sorts of risk we all manage directly using *judgment:* some unformalized and unquantified combination of instinct, intuition and experience. We do not undertake a formal probabilistic risk assessment before crossing the road. ISO 31000 has nothing to say about the management of such risks.

The second circle, "perceived through science" contains the sorts of phenomena considered in most of the discussions on the ISO 31000 Linkedin website, most of the presentations to both conferences referred to above, and most articles published in journals such as *Risk Analysis.* In this circle "risk" is reduced to numbers – frequencies, probabilities and magnitudes of consequence. ISO 31000 is insistent that in order for risk to be managed it must be measured: "in order to ensure that

risk management is effective … the organization should measure risk management performance" (4.5)

But are the numbers produced and published in this circle measures of risk as defined by ISO 31000? The people who produce them often insist that that they are measures of "real" or "objective" risk, as distinct from the "perceived" risk that lies in the mind of the non-expert general public. But outside the casino that plays with honest dice, decks and roulette wheels, all risk is perceived. It is a word that refers to a future that exists only in the imagination.

One can collect information about past accidents and project discernible patterns and trends into the future – and call them risks. But such projections can serve as useful estimates of risk only to the extent to which one can safely assume that the future will replicate the past. But with risks involving human behavior, outside a few specialist actuarial areas such as motor or house contents insurance, one can't make this assumption. Risk as defined by the ISO – "the effect of uncertainty" – is confined to the third circle of Figure 2 – *virtual risk.* Here science can provide no clear guidance. As in the first circle we must rely on judgment, and again ISO 31000 has no helpful advice to offer.

Lord Kelvin famously said, "Anything that exists, exists in some quantity and can therefore be measured"[1] This dictum sits challengingly alongside that of another famous scientist, Peter Medewar who observed, 'If politics is the art of the possible, research is the art of the soluble. Both are immensely practical minded affairs. Good scientists study the most important *problems they think they can solve* [my emphasis]. It is, after all, their professional business to solve problems, not merely to grapple with them.'[2]

There are some risks for which science can provide useful guidance to the imagination. The risk that the sun will not rise tomorrow can (I hope) be assigned a very low probability by science. And actuarial science can estimate with a high degree of confidence that the number of people killed in road accidents in Britain next year will be 2000, plus or minus a hundred or so. But these are predictions, not facts. Such predictions rest on assumptions; that tomorrow will be like yesterday; that next year will be like last year; that future events can be foretold by reading the runes of the past. Sadly, the history of prediction contains many failures – from those of stock market tipsters to those of vulcanologists seeking to predict eruptions, earthquakes and tsunamis.

In the area lit by the lamp of science one finds risk management problems that are potentially soluble by science. Such problems are capable of clear definition relating cause to effect and characterized by identifiable statistical regularities. On the margins of this circle one finds problems framed as hypotheses, and methods of reasoning, such as Bayesian statistics, which guide the collection and analysis of

---

[1] quoted in Beer S 1967. *Management Science*, London: Aldus.
[2] Art of the Soluble: Creativity and Originality in Science - (Feb 1967) by P.B. Medawar

further evidence. As the light grows dimmer the ratio of speculation to evidence increases. In the outer darkness lurk unknown unknowns. Here lie problems with which, to use Medawar's word, we are destined to ‘grapple’.

The ISO having proclaimed that ISO 31000 “provides the principles and guidelines for managing any form of risk” now appears to concede that its guidance is less clear or comprehensive than it might be. It has established an international committee to produce guidance for the guidance: *ISO 31004 : Risk management -- Guidance for the implementation of ISO 31000* is due to be released in 2014. Despite having issued exhaustive guidance about the meaning of the words that it has been using - including *risk* itself – it accepts that further guidance is needed. But as yet it evinces no doubt about the validity of ISO 31000 itself; it only concedes that further guidance in implementing it is required.

How this further guidance will assist with the quantification of uncertainty is awaited with interest. Will ISO 31004 render ISO 31000 fit for purpose? The jury has yet to see the evidence. This juror doubts that it will.