The quarterly question: is ISO 31000 fit for purpose?

Many risk professionals are citing the International Standard Organisation's (ISO) 31000:2009 as the risk management standard, but some believe it never was fit for purpose. Why has the standard got so many supporters and detractors, how was it put together, and what does the future hold?

In order to explore this in more detail, we've invited two heavyweights in the world of risk. In one corner we have John Adams FIRM, emeritus professor at University College London, UK, who blogs regularly about risk. His contribution below is a condensed version of his website (john-adams.co.uk) essay entitled "*ISO 31000: Dr Rorschach meets Humpty Dumpty*".

In the other corner we have Grant Purdy, an associate director at Australia-based Broadleaf Capital International, and a 35-year risk management veteran. Grant represented Australia on the group that wrote the international standard and has chaired the committee in Australia that wrote the AS/NZS 4360 standards and associated guidelines. Let's hear what they have to say:

Complex, confusing and clannish, says John Adams

I'm sure others, as I do, frequently reach the end of risk management guidance without a clue as to what it expects the risk manager to actually do.

That is my problem with *ISO 31000 – Risk management – principles and guidelines*. Published in 2009 it aspires to global leadership, if not domination, of the risk management industry. Kevin Knight, leader of the group that produced the document, claims the guide is comprehensive and global, and is "applicable to all organisations, regardless of type, size, activities and location, and should apply to all types of risk".

But having read it several times I still don't know what it expects of me. And here's why: it repeatedly tells me to do what is "appropriate", with 34 references to do the "appropriate" thing – such as "allocate appropriate resources for risk management" – in 26 pages.

What is appropriate? Those deploying the word appear to assume that all readers will share its meaning. But anyone plugged into discussions about risk's disparate cultural perceptions will appreciate that this is a facile assumption. These "appropriates" are Rorschach inkblots – the ambiguous stimuli typically shown to patients by therapists. While psychologists may battle to reach a consensus on the interpretation of the variety of meanings assigned to inkblots, it is clear that different people project very different meanings onto ambiguous stimuli.

And "appropriate" is just one of many

ISO 31000 inkblots, sitting alongside numerous "effectives", "culture/culturals", "relevants", "comprehensives", "acceptables" and "tolerables". If I take the total number of these words and divide them by the page count, ISO 31000 gets an inkblot average of 4.03 per page. It's a fun way of quantifying the sense of vague dissatisfaction generated by so much current risk management literature.

One word that is definitely not an inkblot is "risk", defined by ISO as "the effect of uncertainty on objectives – positive and/or negative". Section two contains 29 terms and definitions elaborating the meaning of "risk", supplemented by 44 explanatory notes and further definitions.

But this is deemed insufficient. To be absolutely confident that one is on the ISO 31000 wavelength one must also master *Risk management – vocabulary* (ISO Guide 73:2009), a 15-page dictionary further elaborating the ISO 31000 terms and conditions. Like Humpty Dumpty, when ISO uses a word it is determined that it should mean just what it chooses it to mean — neither more nor less.

This ISO definition of risk is described as "pivotal" by Knight. Certainly it is the pivot around which its authors believe all discussion of risk management should rotate. But they have a couple of problems.

First, their definition is shared by no standard dictionary. The rest of the world understands "risk" as something negative – a threat, hazard, loss or injury. Dictionaries have the merit of defining words as most people use them. With its idiosyncratic definition ISO appears to aspire to establish itself as a priestly caste with a private vocabulary inaccessible to the vulgar horde.

It is claimed on networking sites such as LinkedIn that ISO's approach has been adopted by several thousand "experts". Possibly. But they are vastly outnumbered by hundreds of millions of other lay and expert risk managers who share the

dictionary meaning – who understand risk to be something negative

Second, a major part of a risk manager's job involves communication with non-experts. Not only is the ISO "risk" definition unlikely to appear in the dictionaries that most of the non-experts are likely to consult, but it can only be found in ISO 31000 and the supplementary vocabulary guide, together currently costing over £200 – a rather expensive textbook for would-be students.

In attempting to assert its mastery over the word "risk" - a word requiring an expensive dictionary before those deploying it can be confident that they know what they mean by it - the ISO experts face can expect to be frustrated by the blank incomprehension of those whose access to their private language is blocked by this daunting paywall.

Purdy has described ISO 31000 as "a new globally accepted standard for risk management". Accepted by whom? Most people interested in risk management have never been asked about it, never read it, and probably never heard of it. The academic world is comprehensively ignorant of it because it can be found in no libraries. I have only been able to join this discussion because a friend sent me bootleg copies.

In a world where the vast majority use standards that are free, and communicate in the language of the standard dictionaries, the unique approach and language of the ISO "new standard" appear unlikely catch on.

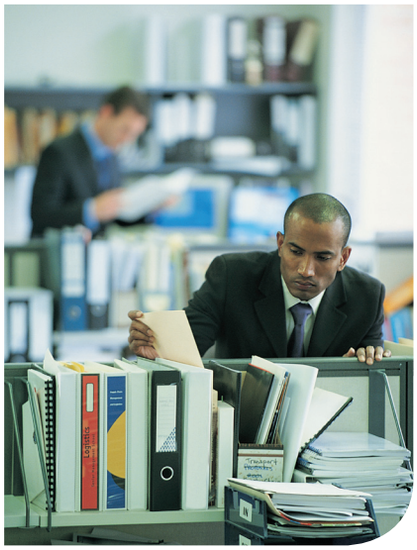
Never perfect, but inclusionary, practical and widely accepted, says Grant Purdy

Organisations and their stakeholders are increasingly using published standards to draw conclusions on whether they are being properly run. They provide the basis for benchmarking, give specific and prescriptive technical specifications and methods, and provide general and generic guidance. ISO 31000 falls into the last of those categories, but is sometimes confused with standards in the first two.

Standards are created because society wishes to treat risk, but standards bring their own risks. Notwithstanding the standardisation of standards and the fact they are periodically reviewed and revised, standards may not always reflect the 'best available' practices and leading thinking; sometimes because nominated representatives are restricted in what they can say, not expert at all, or because their views no longer reflect current needs.

Standards can be biased, have compromises, or have their clarity and precision clouded by ensuring words are translatable into other languages. The language of a standard and the terms it uses can be ambiguous because it has to accommodate many points of view, interpretations and beliefs.

It would be naïve to think that ISO 31000 is immune from the above. But having worked on other national standards, like that from Australian and New Zealand (AS/NZS 4360:2004), developed and improved over 15 years and two revisions, ISO 31000 is based on the ways that many thousands of international organisations have managed risk over a long time period. Thousands of people had their say during the public consultation, and it was voted for by 23



of 26 nations, with Germany and Uruguay abstaining and Italy voting against.

ISO 31000 cannot be 'perfect'. Compromises to accommodate different points of view and interests inevitably led to some 'fudging' and the introduction of some unnecessary complexity. While the standard is a remarkably good and succinct set of guidelines, further simplification would enable it to be even more realistic and pertinent for those who need to make decisions and manage risk.

But to paraphrase Winston Churchill, the current approach to standards-making is the worst way of doing it except all the others that have been tried.

Next year a formal review of ISO 31000 will give us an opportunity to improve the basic standard, but I know from recent experience that vested interests and commercially motivated stances have increased significantly over the last three years and that therefore any revision is going to be subjected to many pressures. Generally there seems to be a strong motivation to add rather than reduce complexity in risk management. Often this seems to be by adopting and endorsing various three-letter acronyms (GRC, ERM, BCM, SRM etc) or by creating a new 'risk-something' term to describe some property, action or outcome that was previously not considered important.

While it would be nice if all standards were free, I think the idea is unrealistic. After all, in the UK you even have to pay for copies of statutes! I'm less concerned about academics than I am about managers and decision makers - the primary audience. Given the benefits that come from effective risk management, I would have thought that the sum involved was a pretty good investment and hardly a barrier.

Changes in definitions inevitably offend some practitioners with different views and long histories of propounding other theories or approaches. The definition of "risk", in particular, has polarised views of the standard.

But I'm not sure why a dictionary definition of a concept as complex as "risk" is to be preferred over that produced by many people who have been thinking about this and working on it for years, and which has been tested out on many more of those who actually have to manage it daily. The ways that words are defined in dictionaries probably does not involve as many stakeholders as are involved in standards making and while dictionaries tend to look backwards, its is the purpose of standards to set future norms and to change the ways that people think and act.

Whether they accept the definition of risk in ISO 31000 or not, most people agree that to make good decisions they need to have reliable answers to four questions:

- what are we trying to achieve?
- who should be involved?
- what creates uncertainty and how significant is it?
- what can we do to ensure success?

These are, of course, the elements of ISO 31000 that concern the process for risk management and the framework that ensures that the process becomes integrated with an organisation's system of management.

While not all practitioners agree with the definition of risk given in the standard, this is being understood and appreciated by managers who have to employ the risk management process to help them make better decisions. The core process for managing risk and the need for a framework that achieves its integration into a system of management are widely accepted. ■

ISO favoured in standards survey

Three times as many risk professionals prefer the ISO 31000 risk management standard to the COSO ERM Framework, according to an online survey carried out by a Fellow of IRM.

The survey (not associated with IRM) of 180 risk practioners, carried out on networking site LinkedIn by Norman Marks FIRM, found that 52 per cent of respondents prefer ISO to COSO, with 14 per cent opting for COSO, 25 per cent saying they have no preference as both can be used effectively, and the remainder (eight per cent) saying both are ineffective.

Seventy-five per cent of those surveyed said they had read both documents, with 12 per cent saying they have only read COSO, seven per cent saying they have only read ISO, and the remainder (six per cent) unfamiliar with either.

Respondents who favoured COSO praised its comprehensiveness, longevity, better discussion of risk appetite, "strong" focus on corporate governance and linkage to strategies and objectives. ISO advocates complimented its user-friendliness, flexibility, top-down approach to risk management and that it represented "the collective wisdom of global risk leaders".

Marks admits that the results are "meaningful but not authorative", while adding that those ambivalent about both documents said that there is little evidence that either actually works. Others suggested that the two should be combined. He concluded that all risk practitioners should read both sets of guidance.