Future ISO 31000 standard on risk management

and ISO standards

Organizations with a commitment to managing risk know that implementing standards can enable them to do so more effectively and therefore maximize opportunities and minimize losses in the course of achieving corporate objectives. This article examines the future ISO 31000 standard which will be a strategic-level document covering all forms of risk, including safety and the environment.

by **Kevin W. Knight**

Many organizations prefer to spend time debating whether to introduce "holistic risk management" or "enterprise risk management" or even "enterprise-wide risk management", while others are content to settle for a "tick and flick" compliance programme that will hopefully keep the regulators happy. The successful organization however works on identifying the risks involved in achieving their objectives and managing them to ensure a successful outcome.

Organizations with a commitment to managing risk are generally more open to the adoption of standards such as ISO 9001:2000 (quality management), ISO 14001:2004 (environmental management) and ISO 15489:2001 (records management). Organizations know that adopting International Standards, in full or in part, can enable them to manage risk more effectively and therefore maximize opportunities and minimise losses in the course of achieving corporate objectives.

Management of risk is an integral part of good management. It is an iterative process that is best embedded into existing practices or business processes.

RISK and ISO standards

An effective risk management regime is a combination of an organization's culture (beliefs, values and behaviours), processes and structures that are directed toward realizing potential gains whilst avoiding or limiting losses

An organization's culture is the sum of its people, symbols, stories, business experiences, power structures, control systems, organizational structures, rituals and routines that, when combined, make it unique.

The structure adopted must ensure that all risks have owners who have accountability for their management and who also have the authority to make decisions with respect to the management of the risk.

Cultural change

Risk management practitioners are often their own worst enemy when it comes to championing the cultural change required in an organization if it is to effectively manage its risks.

Sadly, this is not a recent phenomenon as the following quote from Felix Kloman, a long-time commentator, prophet and philosopher on risk management and the management of risk illustrates. His comment in "The Revolt of the Risk Manager", published in *Bests Review*, October 1971, is as fresh and applicable today as when first made 36 years ago:

"Until the Risk Manager can be completely free of his real and psychological ties to insurance and the insurance industry, he will not be able to perform the risk management function."

Organizations know that adopting International Standards can enable them **to manage risk more effectively**

The challenge facing today's risk manager is not just breaking free of the mantra that "risk management is all about insurance, and if we have insurance, then we have managed our risks", but rather being accepted as a provider of professional advice and service to the risk makers and the risk takers at all levels within an organization.

It is the risk makers and the risk takers who must be the owners of risk and accountable for its effective management.

A consequence of the uncertainty as to the place of the management of risk in an organization, and the role of the risk practitioner, has seen a plethora of persons and professional

The author

Kevin W. Knight *is Chairman of the ISO Working Group on Risk Management Terminology, a member of the Standards Australia Management and Business Standards Sector Board, and member of the Standards Australia/Standards New Zealand Joint Technical Committee OB/7* – Risk Management.

He has been very active in furthering the risk management profession and the professional development of its practitioners, both worldwide and throughout the Asia-Pacific Region in particular, over the past 25 years.

E-mail kknight@bigpond.net.au

bodies presenting themselves as the true "risk managers".

The accounting and audit bodies are the latest to set themselves up as the arbiters of the management of risk through their active involvement in the development and promulgation of the latest framework document from the United States' Committee of Sponsoring Organizations of the Treadway Commission (COSO), with its heavy accounting, financial management and audit bias.

Those seeking to find the most useful processes and guidance on the management of risk are continually faced with the difficult task of deciding what to recommend to their Boards and executive management.

The standards community has not been idle in the face of this dilemma.

Standards and risk

It all started when the Standards Australia/Standards New Zealand Joint Technical Committee developed AS/NZS 4360 – *Risk Management,* which was first published in November 1995, revised in 1999 and most recently revised in 2004. Standards organizations in Canada (1997) and Japan (2001) followed with their own versions and then in 2002, ISO and the International Electrotechnical Commission (IEC) published ISO/IEC Guide 73, *Risk management – Vocabulary – Guidelines for use in standards*.

Felix Kloman in his monthly publication *Risk Management Reports*, Volume 31, Number 11 of November 2004, described AS/NZS 4360:2004 as follows:

> Management of risk is an integral part of **good management**

"The Aussies and Kiwis have just finished their latest modification and they've done a superb job again! AS/NZS 4360:2004 was and still remains the clearest and most concise guideline yet published. Its text, only 28 pages, is a model of brevity.

"It is expressed in simple and basic English, free from business jargon. Because its approach is generic, it applies to all forms of organizations. AS/NZS 4360:2004 will become a handy, notated and dog-eared reference on the desk of anyone who practices this discipline.

"Furthermore, as the standard is generic and requires adaptation to a specific organization, it avoids the complaint that standards are 'dangerous' because they can stimulate unneeded legislation and regulations. True, risk management is still evolving, but these guidelines, already in their third evolution, help any organization to begin and modify the process.

"… These are but minor caveats for a superb statement of the nature and process of our discipline. As I stated before, this document belongs as a working guide for all practicing risk managers: don't even think of stuffing it into a bookcase."

AS/NZS 4360 met a global need for a generic guide to the application of a risk management process to organizations of all sizes both private and public.

Following on from the publication of ISO/IEC Guide 73:2002, a proposal was put to the ISO Technical Management Board (TMB) in 2004 that there was a need for an ISO standard on risk management.

The proposal was discussed at a number of TMB meetings until in September 2004 the TMB invited the Japanese Industrial Standards Committee (JISC) to submit a new work item proposal (NWIP) for the establishment of a Working Group (WG) to develop the standard.

At its meeting in February 2005 the TMB approved the circulation of the NWIP on risk management submitted by JISC (Japan) to all ISO member bodies.

The result of the NWIP ballot saw 26 member bodies vote in favour, two against and two abstain. The TMB at its meeting in June 2005 confirmed the establishment of a WG under the TMB to address risk man-

RISK and ISO standards

agement, to be chaired by Australia and the secretariat to be provided by Japan.

The inaugural meeting was held in Tokyo in September 2005 with subsequent meetings in Sydney and Vienna in 2006 and Ottawa in April 2007. A consequence of the work undertaken by the WG was a recommendation to the TMB that the WG also be tasked with revising ISO/IEC Guide 73:2002 to ensure that both the ISO standard – to be designated ISO 31000 – and the guide were harmonized and subject to conjoint review every five years

Risk management and safety

Like the WG that produced ISO/IEC Guide 73:2002, this WG has extensively debated the relationship between risk management and safety. While a large majority agreed that it would be inappropriate to exclude safety aspects from the standard's scope of application, a significant number called for care to be taken to formulate the document's provisions in such a way as to respect and address the serious concerns of safety and other communities.

It was argued that addressing such concerns need not compromise the generic, top-level character of the standard. Indeed, it was argued, its generic nature would be proven and enhanced by its capacity to bring together diverse communities around a common understanding of how risk should be managed in all fields.

Arguments questioning the merit of exceptional efforts to accommodate the concerns of safety experts, or of experts in any other field, were also advanced. Safety, it was argued, is not "special", though a person or organization might legitimately place a high priority on it. Therefore, there is no reason to assign it special weight or special treatment of any sort in the formulation of ISO 31000, which, after all, promises to alter the conception of risk held by many experts in many fields.

ISO 31000 is required to be a top-level document addressing all forms of risk, including safety and the environment, and the Introduction and Scope would make clear the standard's character as a generic top-level document respecting the diversity of needs of its intended users.

Obviously, where an organization is in an industry subject to specific safety and/or environmental legislation, its risk management programme will be more of a compliance programme and they will be looking to specific safety and environmental standards to manage their risks.

ISO 31000 is the starting point in the journey and it is expected that many national and regional standards bodies will develop a range of handbooks to complement and explain the implementation of this new standard.

Harmonization

It has never been the intent of the Risk Management Working Group to produce a document that would override existing standards, but rather to provide a generic document that will assist in achieving greater harmonization in how standards address the management of risk over the coming years.

Once ISO 31000 and the revised ISO/IEC Guide 73 are published, the WG will be wound up until the five-year review of both documents is due when the ISO TMB would need to re-establish a WG or similar body to undertake the review.

My reason for this view is that once we have ISO 31000 and Guide 73 published, I would expect either regional or national standards bodies to produce a range of explanatory and specific handbooks like those produced in Australia and New Zealand.

ISO 31000 is required to be a top-level generic document addressing all forms of risk

Certainly the view of the AS/NZS Joint Technical Committee OB/7 – *Risk Management* is that once the vote is finalised on ISO 31000 and Guide 73, they will immediately commence a full review of all risk management related handbooks (HB), especially HB 436:2004, to ensure they are in conformity with these international documents as they apply to the Australian and New Zealand communities.

Whilst one day there might be a range of ISO handbooks, the first step must be through regional groups like the European Committee for Standardization (CEN). Perhaps after ISO 31000 and Guide 73 are next revised in 2013, there may be sufficient global consensus to produce other documents addressing the management of risk. •