Future ISO 31000 standard on risk management

by Kevin W. Knight AM, Chair, ISO working group developing ISO 31000

Some would suggest that the global financial crisis was caused by a failure of risk management rather than the failure of boards and top management to effectively manage risk. The future ISO 31000, *Risk management – Principles and guidelines*, is expected to help industry and commerce, public and private, to confidently emerge from the crisis. This much-awaited International Standard is expected to be published in the third quarter of 2009.

Without risk, there is no reward or progress. Unless risk is managed effectively, organizations cannot maximize opportunities and minimize threats. Risk is all about uncertainty, or more importantly, the effect of uncertainty on the achievement of objectives. This is where ISO 31000 is clearly different from existing guidelines in that the emphasis is shifted from something happening – the event – to the effect on objectives. Every organization has objectives to achieve, and in order to achieve them, any uncertainty that could interfere with their realization must be effectively managed.

Applicable and adaptable to all

ISO 31000 sets out principles, a framework, and a process for the management of all forms of risk, including safety and environment, in all organizations, regardless of size. It does not mandate a one-size-fits-all approach, but emphasizes tailoring the principles and guidelines to the specific needs and structure of the organization.

Following a list of terms and definitions, the standard sets out 11 principles to be addressed in order to effectively manage risks and achieve objectives. The principles need to be reviewed by the

board and top management so they may reflect the organization's policy.

The next section looks at the framework needed to provide the foundations and arrangements that will embed the management of risk at all levels of the organization. It calls for risk management components to be adapted into the existing management system in order to ensure ownership of the policy and process by management and staff.

About the author

Kevin W. Knight AM is Chair of the ISO working group developing the new ISO 31000 risk management standard and the revision of ISO/IEC Guide 73, and a founding member of the Standards Australia/Standards New Zealand Joint Technical Committee OB/7– *Risk management*.

He is well known through his very active work in the development of Risk Management Standards and has been 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.

He can be contacted at:

P.O. Box 226,
Nundah Qld 4012,
Australia.

E-mail kknight@bigpond.net.au

Commitment of top management

The overarching component of the framework is the mandate and commitment of the organization's board and top management to the implementation, review and continual improvement of how risk is managed. The end goal: to ensure risk is fully focused on the achievement of objectives. This focus on objectives is imperative if enterprise risk management (ERM) is to be achieved by a common language and process throughout the organization.

"Risk needs to become an integral part of how things are managed."

The framework calls for a clear understanding of the context in which the organization operates. The risk management policy must clearly state the organization's commitment to the management of risk. More importantly, the standard requires organizations to identify risk owners to ensure accountability and authority. For example, the standard seeks to differentiate between those who are "accountable" for managing risk (those persons with a liability, either corporate or legal, for their decisions or lack of decision) and those who are "responsible" for specific tasks (those persons with an obligation to carry out an instruction from a competent authority).

The framework also sets out how the management of risk is to be woven into the organizational fabric. Risk needs to become an integral part of how things are managed; it should not be an add-on, or a separate activity divorced from the mainstream management of the business.

A strategic process

The risk management process contained in ISO 31000 follows the well worn lead set by the Australian and New Zealand standard AS/NZS 4360, which consists of:

- Communication and consultation
- Establishing the context
- Risk assessment consisting of the three steps of identification, analysis and evaluation
- Risk treatment
- Monitoring and review.

The process set out needs to become an integral part of how business is managed at all levels. It must be tailored to the business processes and woven into the culture and practices of the organization that make it uniquely different from its competitors.

All activities should be traceable by way of records that provide the foundation for improvement in methods and tools, as well as in the overall process.

Finally, an informative annex sets out the attributes of enhanced risk management for those organizations that have been working on managing their risks for some time and may wish to strive for a higher level of achievement.

Representing the very best

The working group that produced ISO 31000 contained experts from some 28 countries representing all continents (except Antarctica). All meetings of the working group had strong attendance, ranging from 40 to 60 delegates depending on the meeting location, with a significant core group who participated in all meetings. It is precisely because of this core group, ably supported by the other expert delegates and backed up by the national mirror committees, that has ensured ISO 31000 represents the very best of contemporary risk management thought.