

Risk management

New work reinforces a solid toolbox

by Kevin W. Knight AM¹⁾

One could argue that the global financial crisis was caused by a failure of management rather than a failure of risk management. Those organizations whose boards promoted an effective risk management culture passed through the crisis relatively unscathed – the banking and finance industry in Australia and Canada being two examples.

That both of these countries had developed national standards on risk management was a major contributor to their survival. Top level commitment had sent a clear message within the organizations that uncertainty must be effectively managed so as to maximize opportunity while minimizing threats to the achievement of their objectives.

Cornerstone of confidence

Certainty – relying on a product or person without doubt – is the cornerstone of confidence. Already a difficult goal at a national level, it is even harder to attain at a global one. ISO, together with its national standards bodies (NSBs), develops International Standards that aim to build global confidence and bring down barriers to trade. One notable standard in this regard is ISO 31000:2009, *Risk management – Principles and guidelines* – which directly focuses on managing risk and uncertainty.

Taking on the challenge

Indeed, the greatest challenge to confidence is uncertainty – a challenge that the ISO Technical Management Board (TMB) took, when it established in 2005 a working



group (WG) to develop a standard for the management of risk.

The WG was mandated to produce a document outlining principles and practical guidance on a risk management process applicable to all organizations, regardless of type, size, activities, location, and risk. Most importantly, the new standard was to be a guideline document, and not for certification purposes.

As a result, in 2009, the WG published:

- ISO 31000:2009, *Risk management – Principles and guidelines*
- ISO Guide 73:2009, *Risk management – Vocabulary*.

ISO 31000 is the first international document dealing with risk management.

These two documents were complemented by a joint document developed by ISO and the International Electrotechnical Commission (IEC) – ISO/IEC 31010:2009, *Risk management – Risk assessment techniques*.

As a result of this work, it was agreed that risk would be defined as “the effect of uncertainty on objectives”.

A big success

ISO 31000 is a significant milestone because it is the first international document dealing with the management of risk that has been developed by consensus and been widely adopted by a majority of G8 and G20 groups of major global economies, as well as the BRIC (Brazil, Russia, India and China) group of emerging economies. The key to the success of ISO 31000 lies in that it was developed by a broad group of technical experts, backed by input from national mirror committees (NMCs) – national committees that “mirror” international work – with wide representation.

The standard has thus been positively received, and is already a bestselling ISO document. It has also been adopted as a national standard by a wide range of NSBs.

ISO 31000 has prompted the development of sister standards such as the Austrian ONR 49000, Canadian Q 31001, Irish NWA 31000, UK BSI 31100, and the draft Australia and New Zealand AS/NZS HB 436:201X companion documents to assist stakeholders in the application of the standard.

An interesting result of the development of ISO 31000 has been its enthusiastic reception by those charged with auditing organizations after the global financial crisis.

Michael Parkinson, a director of KPMG in Australia, member of AS/NZS JTC OB/7

1) Member of the General Division of the Order of Australia.

– *Risk management*, and Vice Chair of professional services at the Institute of Internal Audit, is a strong advocate of ISO 31000 because, he says, “It provides an objective way of assessing how important the control systems of any process are to the organization.”

Mr. Parkinson does not consider it problematic that ISO 31000 is not a certification standard since it “nevertheless provides a basis for internal auditors to build a normative model, and the principles against which an auditor can test the performance of the risk management process.”

Mr. Parkinson also values the fact that ISO 31000, “can be expanded to assist with control design and the assessment of organizational risk management practices... The processes are simple and scalable — that is, they can be explained quickly to a client and they can be used at any level and in any part of an organization. They are completely independent of the subject matter,” he concludes.

Its greatest strength

ISO 31000 can be used to address risk at any level and on any subject, which in my view is its greatest strength. It explains why it has been adopted widely by many

public and private organizations around the globe.

The greatest challenge to confidence is the effect of uncertainty.

The standard also provides the risk management world with an internationally agreed vocabulary. This means that not only is it possible for risk management practitioners to speak a common language, but also allows safety, security, quality and internal auditors to join in the conversation, in turn promoting cooperation and better outcomes.

New developments in sight

Global interest in ISO 31000 has spurred a growing demand for guidance on its implementation, and for specific applications such as managing disruption-related risk, particularly since the spate of earthquakes in New Zealand and Japan.

In February 2011, the ISO/TMB established a project committee ISO/PC 262, *Risk management*, to develop guidance on the implementation of ISO 31000. The work programme of the committee may be

expanded in the future to include the development of other risk management documents, in which case its status may then change to that of a technical committee (TC).

Its tasks could include:

- Ensure full harmonization of the guidance standard under development with ISO 31000, ISO Guide 73 and ISO/IEC 31010
- Carry out ongoing maintenance of the three existing documents
- Develop new work items proposed by members
- Provide a liaison point for other TCs and WGs relating to the management of risk in other standards.

The PC currently has 33 participating and 3 observer members covering the majority of the G8, G20 and BRIC economies, and has received a number of requests for liaison status from other bodies, including UN agencies. It held its first meeting in September 2011.

The PC will begin work quickly on a guidance standard based on the best elements of the national documents mentioned above. This will ensure the speedy development of a draft that can be sent for comment to the NMCs. If they in turn seek comments from a broad stakeholder base from their constituent bodies, we can ensure that the future document will meet the needs of the widest community. ■

About the author



Kevin W. Knight AM is Chair of ISO project committee ISO/PC 262, *Risk management*. He was Chair of the ISO working group that developed

ISO 31000:2009, 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 30 years.

