January 6, 2010

ISO 31000 — The New, Streamlined Risk Management Standard

by Chris McClean
with Robert Whiteley and Nicholas M. Hayes

EXECUTIVE SUMMARY

In November 2009, the International Organization of Standardization released the ISO 31000:2009 Risk management — Principles and guidelines standard, a well-crafted and straightforward framework explaining the elements of an effective risk management program. The standard will help risk professionals clearly define terminology, establish formal processes, explain the context of their efforts, and consider the opportunity inherent in risks. But this is just a start. The current version will not help risk professionals determine how to measure risk, make sure their risk taxonomy is complete, develop practical risk management tools, or make the business case for risk management investments. Regardless, we expect widespread adoption and recommend using the standard to bring your risk management program up to speed.

THE TIMING IS RIGHT FOR GREATER RISK MANAGEMENT STANDARDIZATION

Just as buildings and bridges are retrofitted after an earthquake in anticipation of potential shocks to come, the risk management discipline is due for some additional fortification. Successes are hard to quantify — we don't know how many financial meltdowns, bankruptcies, product safety failures, or worker casualties have been prevented by good risk management. The recent disasters, however, leave lasting impressions.

The Pressure Is On For Risk Professionals

In the wake of massive risk management failures, regulators, rating agencies, executives, partners, and investors are expecting more from corporate risk managers. They will be asked to broaden the scope of their programs and to provide more detailed data and analysis to support better decision-making. This includes those concentrating on core niches of risk, such as IT risk professionals, who tell Forrester they are being asked to take on more formal risk management responsibilities. Keeping up with these growing demands while the pace of business accelerates is beyond difficult — and industry guidance to help organize risk management efforts is a welcome development.

ISO 31000 PROVIDES A SIMPLIFIED REFERENCE GUIDE

November 2009 saw the release of the long-awaited ISO 31000:2009 Risk management — Principles and guidelines standard.[1] With fewer than 25 pages of content, the standard is extremely accessible, even to those with little experience in risk management. Unlike some other ISO standards, the 31000 standard is not designed for certification. Its stated role is to establish "a number of principles that need to be satisfied to make risk management effective."

This new standard is worthy of its early praise, but risk professionals must temper any expectations that it will dramatically change their discipline. Previous risk management frameworks, including the Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM) framework and the Australia/New Zealand 4360:2004 Risk Management Standard (AS/NZS 4360), gave similar guidance on risk management principles and processes; the primary difference with ISO 31000 is that it delivers its content more succinctly. The success of ISO 31000 will depend on the level of endorsement it receives from industry associations, regulators, and government bodies, as well as the level of its adoption by corporations worldwide. It is therefore important to understand what the framework will and will not provide for risk managers who adopt it.

It Will Help You Formalize And Discuss Risk Management Practices

Forrester's clients in risk management roles often discuss difficulties stemming from a poorly defined risk vocabulary and a lack of formal, end-to-end risk management processes. Sharing best practices among industry peers is becoming more important as well, but this is difficult unless risk professionals have a common context in which to frame the conversation. The ISO 31000 standard will provide substantial help in solving these and other problems. Specifically, it will help you:

- **Achieve agreement on definitions for a set of risk management terms.** A full six of the standard's substantive pages are dedicated to defining terms such as risk, control, risk attitude, and consequence. Additional guidance on risk management terminology is also provided by the ISO Guide 73:2009 Risk management — Vocabulary.[2] This information should help remove the cumbersome language barriers that exist between compliance, audit, and other business functions, as well as between various risk management teams.

- **Double-check your risk processes.** It's possible that many of the processes described in ISO 31000 are already part of your risk management program, but it will give you good pointers on things you may be missing. For example, do your risk assessments include separate steps for identification, analysis, and evaluation? Do the process owners and decision-makers involved understand the different requirements of each step?

- **Put risk management practices into proper context.** Understanding where risk management fits in the organization is hard for risk managers and often nearly impossible for everyone else. ISO 31000 guides readers to define risk management in the context of the organization's internal and external environment — from strategy and governance down to information systems and culture.

- **Consider risk as potentially positive or negative uncertainty.** This is a difficult concept, especially in areas of operational risk, but the processes and definitions in ISO 31000 can be used to evaluate uncertain events or circumstances that might positively affect business objectives. It's going to take most organizations a long time to fully bring this into practice, but it's ultimately the best way for risk management to become a valuable tool for decision-making, beyond one simply for loss mitigation or avoidance.

It Will Not Help You Implement Risk Management Tools And Practices

The biggest hurdles in risk management don't usually come from a misunderstanding of concepts but from a difficulty in translating those concepts into practical tools and processes. Additional guidance on risk assessment practices, including the recently released ISO/IEC 31010:2009 Risk management — Risk assessment techniques standard, offers more practical advice; however, it's important to set expectations by understanding what ISO 31000 does not offer.[3] Specifically, ISO 31000 will not help you:

- **Determine how your organization measures risk.** Many organizations struggle with how to quantify the impact of risks, especially when it comes to analyzing a combination of qualitative and quantitative data. While ISO 31000 recommends using such data in the risk analysis, risk managers will still have to work out ways to properly mine data and expertise that create reliable risk information.

- **Ensure that all important risk areas are considered.** The risk identification process can be overwhelming, especially when you consider every issue or condition (in your control or otherwise) that might either positively or negatively affect the organization's ability to achieve objectives. This step should be to foster creativity and collaboration so that all reasonable ideas are considered for future analysis, but the method for determining what falls into the "reasonable" category is not clearly defined.

- **Develop risk documentation and reports.** Organizations often ask for examples of risk taxonomies, heat maps, or other risk management tools to use as templates when designing their own. In many cases, ISO 31000 explains the elements that should be included in such tools, but risk managers requiring a specific example or template to work from will for now need to rely on consultants, product vendors, or industry peers for help.

- **Make the business case for a comprehensive risk management program.** Describing the elements of risk management and its context within the business will help frame what a risk management program should include. But this does not in itself help justify what will likely become a significant investment in time and resources. Some top executives have been exposed to risk management successes and failures enough to appreciate the importance of a formal program, but others will need a lot of convincing.

RECOMMENDATIONS

MODEL YOUR RISK MANAGEMENT PROGRAM USING ISO 31000 PRINCIPLES

The International Organization for Standardization has the global reach and strong reputation to drive widespread adoption of its standards, and the risk management framework's flexibility makes it applicable to a wide range of programs and situations. Those who choose not to review

ISO 31000 and align their practices with it should expect to face the question "Why not?" from colleagues, business partners, auditors, and industry peers. To take full advantage of the standard, we recommend you:

- **Focus on short-term wins and incremental improvement.** Knowing what ISO 31000 can and cannot help you with, it's worth reviewing the framework with your risk management team and adjusting your internal processes accordingly. Full adoption — especially incorporation of opportunity management — will not be an immediate priority for most organizations. Incremental process improvements and greater ability to communicate goals and expectations, however, will be quick wins.
- **Work to quickly translate ISO 31000 into tangible business benefits.** Adoption will only raise the level of expectations from these stakeholders, who may confuse more formal risk management processes with more effective risk management. That is, they will assume it decreases the risk profile. Risk professionals will have to work hard to make sure that adoption of ISO 31000 translates into tangible benefits — such as more timely identification of risks, improved risk insight, justification of controls, and ultimately, better business performance.
- **Make the business case using focused examples.** Starting with a specific project, product line, or business unit will offer a helpful proof of concept to justify investments and changes to the risk management process. Demonstrating value in terms of performance (e.g., a more lucrative sales pipeline, better customer satisfaction scores, fewer safety violations) will provide strong evidence to support your case.
- **After adopting ISO 31000 principles, turn to ISO 31010 for practical guidance.** ISO/IEC 31010:2009 Risk management — Risk assessment is a supporting standard for ISO 31000. It provides helpful details on the elements of risk analysis and presents a wide range of risk assessment techniques and examples. Use this document to help identify and develop practices that fit your specific needs and available resources.

ENDNOTES

[1] Source: ISO 31000:2009 Risk management — Principles and guidelines (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170).

[2] Source: ISO Guide 73:2009 Risk management — Vocabulary (http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651).

[3] Source: ISO/IEC 31010:2009 Risk management — Risk assessment (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51073).