The Conference Board of Canada
Insights You Can Count On

Review May 2012

Risk Watch

Thought Leadership in Risk and Governance

Table of Contents

ACKNOWLEDGEMENTS

The Conference Board of Canada would like to thank the authors for contributing their articles and for the teamwork involved in ensuring a seamless delivery of this publication.

The opinions expressed in these articles are solely those of the authors.

By John Lark and Grant Purdy

Enhance Your Risk Management and Create Value

THE BASIC CONTENTION

We all manage risk, every day and all the time. We may not do it very systematically and, unless we are particularly well informed or inspired, it is likely that we will fail to properly understand and fully appreciate the risks that matter and therefore fail to take the most appropriate action to treat them.[1]

Organizations are no different. Organizations of all kinds face internal and external factors and influences that make it uncertain whether, when, and to what extent they will achieve or exceed their objectives. The effect this uncertainty has on the organization's objectives is "risk."[2]

Like individuals, organizations and the people who lead them do not naturally understand the risks that arise as a consequence of the decisions they make. Often their approach to assessing and responding to risk can be haphazard, informal, and ad hoc. And this means that the organizations suffer losses and detrimental consequences at a higher rate than is acceptable and fail to identify, appreciate, and respond to all opportunities that might lead to gains.

Clearly, shareholders and stakeholders reward and respect organizations that achieve their objectives. If organizations want to improve their level of success, they must understand the uncertainties they face and how to tackle these when they make decisions and take actions. This is, after all, the reason why so many corporate governance codes around the world now require boards to gain assurance on how well their organizations manage risk.

GUIDANCE ON MANAGING RISK

The practice of risk management has arisen from this need to optimize decision-making. While there are various models as to how this should take place, that contained in the International Standard ISO 31000:2009[3] is now achieving a wide degree of acceptance as reflecting world best practice.

The risk management process described in the International Standard came from the Australian and New Zealand Standard, AS/NZS 4360, which, since 1995 and through two revisions and updates, had become the most widely used standard for risk management in organizations. ISO 31000 also draws from best practice in many other countries. For example, Clause 4 on implementation through integration was based on an elegant approach using the organizational improvement cycle of "Plan Do Check Act" (PDCA) in Part 2 of the Austrian risk management standard.[4]

The final version of ISO 31000 contains very little of the original text from other standards; it was rewritten, reviewed, and revised many times, by thousands of contributors, so that it became quite homogeneous and now reflects the global consensus on how best to manage risk within organizations.

Two of the most important qualities of the International Standard are its brevity and its advice on integration as a means

1 International Organization for Standardization, *ISO Guide 73:2009, Risk Management—Vocabulary*, "Process to Modify Risk," 9.

2 International Organization for Standardization, *ISO Guide 73:2009: Risk Management—Vocabulary*, "Effect of Uncertainty on Objectives," 1.

3 International Organization for Standardization, *ISO 31000:2009: Risk Management—Principles and Guidelines.*

4 Austrian Standards Institute, *ONR 49002-2.* The motto was made famous by Dr. W.E. Deming in 1950 during his work with Japanese industrialists and was provided as a way to ensure quality.

of ensuring that the management of risk is both systematic and meaningful to managers and decision-makers.

Other standards do exist and of those, probably that produced by the U.S.-based Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2004 is best known.[5] However, the approach given there now looks dated and, compared with the International Standard, seems narrow and confused.

A recent review of the COSO ERM code found the following:[6]

1. In discussing the preparation of a risk assessment, the code mentions external factors, but focuses the majority of the discussion on internal factors, systems, culture, etc. This can easily lead to organizations focusing inwardly and not actively identifying risks that reflect external factors and circumstances.
2. Stakeholders, particularly external ones, are not mentioned and stakeholders' objectives and their influence on decisions about the significance of levels and types of risk are omitted.
3. Risks are described as events, and events are described and illustrated by examples of sudden, acute occurrences. There is no appreciation of the slow changes in circumstance and situation (for example, a deterioration in internal culture or market sentiment) that gives rise to some of the most critical risks.
4. The code advises that the level of risk is estimated in terms of the probability of an event and its "typical" consequences. However, we will not always get "typical" consequences every time an event occurs. In practice, people who follow the COSO ERM approach to estimating the level of risk will omit the conditional probabilities that should be applied to the event probability, which means that they will always overestimate the level of risk. This prevents individual risks from being properly assessed and compromises any realistic modelling of the effectiveness of controls.
5. The term "risk likelihood" is used, but risk does not, per se, have a likelihood. Likelihood is one of the attributes used to measure the level of risk.
6. While there are some concessions to what are called "opportunities," in the COSO ERM code risks are mostly about losses and risk treatment (response) is about reducing the likelihood and severity of losses. The thinking in the code is not mature enough to appreciate and explain that risk is just the effect of uncertainty in what you set out to achieve and that outcomes can be beneficial, detrimental, or both.
7. The discussion about "risk responses," "control activities," and "monitoring" is confusing and confused. In places the terms are used interchangeably and it is unclear if "control" is being used as a noun or a verb.
8. While the problems with the concept of inherent risk are well known, the COSO ERM code continues to advocate this artificial, theoretical state where no controls exist—which is contrary to best practice and the advice of the Institute of Internal Auditors.[7]
9. The whole area of risk appetite and what COSO ERM calls "risk tolerance" is handled in a mechanistic and naive way. The material on risk appetite has led to greater confusion and more wasted consultancy dollars than any other part of the code.
10. The COSO ERM code confuses the *framework* (the organizational structures, policies, and arrangements put in place to promote, integrate, and improve the management of risk) with the *process* used for risk management, particularly that used for risk assessment, risk treatment, and monitor and review.

Hydro One in Ontario is recognized as having one of the best implementations of risk management. Its Chief Risk Officer, John Fraser, has commented, "ISO 31000 is a simple, workable and proven concept. COSO is complex, unworkable and demonstrably can never work effectively."[8]

CREATING VALUE

The first principle of effective risk management given in ISO 31000:2009 is that risk management should create and protect value. This principle emphasizes that the underlying purpose of risk management is to assist an organization to create and protect value—i.e., to achieve those ambitions that are expressed by its objectives. This requires that risks be detected, understood, and modified as necessary. The linkage between success (i.e., creating and protecting value) and the effectiveness of risk management is unavoidable and thus can be exploited to create value.

5 Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management.*

6 Marks, *10 Reasons.*

7 Institute of Internal Auditors—Australia and Standards Australia/Standards New Zealand Joint Technical Committee, *HB 158: Delivering Assurance.*

8 Fraser, John. Personal communication to John Lark. March 22, 2012.

This principle also implicitly promotes the idea that risk should be managed in the most efficient way possible—for example, in a way that does not waste resources. The corollary is, of course, that if we do not manage risk effectively, value is destroyed or not created.

John Fraser and his co-authors have identified the tangible benefits of effective risk management to his company, as shown in Table 1.[9]

HOW TO ENHANCE YOUR ORGANIZATION'S APPROACH TO MANAGING RISK

ISO has started the development of a new standard, ISO 31004, which is intended to provide advice on how ISO 31000 should be implemented. The two authors of this article are both members of the working group that is developing that implementation guide.

One of the challenges all organizations face is how they move their approach to risk management forward to enhance the organization and make it more responsive to the organization's needs. ISO 31004 will contain advice on how organizations can:

- move from an approach in which different types of risk are managed in distinctive ways, each with their own techniques and defined terms, to one using a common approach fully integrated into the organization's system of management;
- move from an approach concerned primarily with a narrow range of outcomes, such as financial reporting, to the full range of valued outcomes;
- achieve better alignment with the principles of ISO 31000; and
- ensure that uncertainty and its effect on all objectives are consistently considered as part of decision-making.

Regardless of the motive for making this transition, the expected outcome from doing so will be to ensure that the organization makes its decisions with a correct understanding of the associated risks and that the decisions ensure that the risk is within its risk criteria.[10]

To be successful, the strategy for transition should recognize that the organization is already managing risk to some extent and that it is always a good change management approach to adapt and modify existing arrangements rather than simply eliminating the arrangements and starting from the beginning.

Whatever the detail of the process adopted for the transition, it must be led by top management to ensure that the purpose is clear and that the necessary resources that are needed to make the transition as quickly as possible are made available.

The key steps of the transition process are:

- the clear expression of the intent of top management for the change to occur and their support in terms of the allocation of the resources required to achieve a desired level of capability;
- the development of a clear understanding of the organization's characteristics and its internal and external context, including the objectives of its key stakeholders;
- the setting of some performance-based "standards" that specify the desired behaviours of managers and decision-makers in the organization. In particular, these should lead to the integration of the risk management process into the organization's system of management and, in particular, decision-making;
- an evaluation of the existing practices and processes. This evaluation can involve both a gap analysis and a maturity assessment—and ISO 31000 provides an ideal basis for this;
- the development of a transition plan that specifies, in practical terms, what needs to be done to bring about the desired changes so that the organization complies with its own performance-based standards;
- the implementation of that plan—with appropriate tracking and monitoring of progress; and
- a periodic and formal review of both progress with the transition plan and of the suitability, effectiveness, and relevance of the company standards. This should, if necessary, lead to a realignment of the standards and a revision and update of the plan.

CONCLUSION

While managing risk is a natural part of life and business, we can all benefit from advice on how this can be achieved better and with more beneficial outcomes.

9 Aabo, Fraser, and Simkins, "The Rise and Evolution of the Chief Risk Officer."

10 *Risk criteria* are terms of reference against which the significance of a risk is evaluated.

Table 1
Benefits of ERM and Outcomes at Hydro One

EXAMPLES OF ERM BENEFITS	HYDRO ONE EXPERIENCES
Achieve lower cost of debt	Realized higher debt rating and lower interest costs than expected on $1 billion debt issue, which was the first issue as a new company. Issue was heavily oversubscribed. Ratings analysts stated ERM was a significant factor in the ratings process for Hydro One.
Capital expenditures process focused on managing/allocating capital based on greatest mitigation of risk per $ spent	Capital expenditures are allocated and prioritized based on a risk-based structural approach. An "optimal portfolio" of capital investments is achieved providing the greatest risk reduction per $ spent. Also, ERM has been used in the management of major projects such as the 88 corporate utility acquisitions during 2000 and the potential building of an underground cable to the USA.
Avoid "land mines" and other surprises	Since starting ERM, there have been many unusual occurrences at the company. Two significant ones were spelled out in the Corporate Risk Tolerances ahead of time: the dismissal of the Board of Directors and the reaction to a large oil spill.
Reassure stakeholders that the business is well managed—with stakeholders defined to include investors, analysts, rating agencies, regulators, and the press	During the IPO road shows, the Corporate Risk Management Group was told that the ERM workshops had greatly assisted the executive team in articulating the risks they faced and what was being done about them. There are many other examples.
Improve corporate governance via best practices guidelines	Hydro One has moved from the Board Committees asking why these risk summaries were being brought to them to a point at which they now routinely expect this information. Directors recognize that Hydro One is ahead of other companies on whose boards they sit.
Implement a formalized system of risk management that includes an ERM system (a required component of the 1995/1999/2004 Australian Standard for Risk Management)	Hydro One has a formalized system that drives periodic assessment, documentation, and reporting of all risks.
Identifying which risks the company can pursue better than its peers	Although not necessarily attributable solely to ERM: ◆ A subsidiary marketing electricity was sold due to high commodity risks. ◆ Several processing and administrative functions were outsourced to transfer labour union and labour costs risks.

Source: Aabo, Fraser, and Simkins, "The Rise and Evolution of the Chief Risk Officer," 551.

The publication of ISO 31000 in 2009 represented a very significant milestone in our journey to understand and harness uncertainty as part of decision-making.

New standards, by their nature, reset goals and ways of thinking. Undoubtedly, the publication of ISO 31000, and its adoption as their national standard by countries such as Canada,[11] is stimulating organizations to examine their current ways of working, so that those who are faced with making decisions obtain simple, consistent, useful, and unambiguous information that will help them reduce uncertainty in the achievement of objectives. This can only lead to greater confidence in decision-making and, ultimately, to better decisions and the creation of more value.

11 Canadian Standards Association, *CAN/CSA ISO 31000-10*.

John Lark
Managing Principal
Coherent Advice Inc.

John Lark has over 12 years' experience in risk management. He designed and implemented the department-wide risk management system used in the Department of Fisheries and Oceans, developing new tools and innovative approaches and creating a risk management governance system that remains self-sustaining. In 2007 Mr. Lark began working as an independent risk management expert, assisting organizations ranging in size from 30 to over 20,000 employees. He has worked with municipal, provincial, and territorial governments as well as with large and small federal departments. Mr. Lark was on the team that developed the new Canadian risk management standard CAN/CSA Q31001. A Canadian delegate to ISO, he is working on the next global risk management standard, ISO 31004. He has earned the prestigious CPRM certification in risk management from the Risk Management Institution of Australasia.

Grant Purdy
Associate Director
Broadleaf Capital International

Grant Purdy has worked in the practical application of risk management for over 35 years and in over 25 countries. He is an Associate Director of Broadleaf Capital International and was previously Group Manager of Risk Management at BHP Billiton, the world's largest resource company.

Mr. Purdy has been a member of the Standards Australia and Standards New Zealand Joint Technical Committee on Risk Management for over 10 years and served as chair for the last 7. He co-authored the 2004 version of AS/NZS 4360 and has written many other risk management handbooks and guides. He was the nominated expert for Australia on the working group that prepared ISO 31000 and is now Head of Delegation for Australia on ISO PC 262, which is preparing the implementation guide ISO 31004.

BIBLIOGRAPHY

Aabo, Tom, John R.S. Fraser, and Betty J. Simkins. "The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One." In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, by John Fraser and Betty Simkins, 531–56. Hoboken, NJ: John Wiley & Sons, Inc., 2009.

Austrian Standards Institute. *ONR 49002-2: Risk Management for Organisations and Systems, Part 2: Guidelines for the Integration of Risk Management Into the General Management System*. Vienna: Austrian Standards Institute, 2004. www.as-institute.at/en/. (Note that this document has now been withdrawn and replaced by *Risk Management for Organizations and Systems, Part 2: Guidelines for Methodologies in Risk Assessment—Implementation of ISO 31000*, published in 2010.)

Canadian Standards Association. *CAN/CSA-ISO 31000-10: Risk Management—Principles and Guidelines* (adopted ISO 31000:2009, first edition, 2009-11-15). Mississauga, Ont: CSA, 2009.

Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management: Integrated Framework*. Executive Summary, September 2004. www.coso.org/documents/coso_erm_executivesummary.pdf.

International Organization for Standardization. *ISO 31000:2009: Risk Management—Principles and Guidelines*. Geneva: ISO, 2009.

—. *ISO Guide 73:2009: Risk Management—Vocabulary*. Geneva: ISO, 2009.

Institute of Internal Auditors—Australia, and Standards Australia/Standards New Zealand Joint Technical Committee OB 007. *HB 158: Delivering Assurance—Based on ISO 31000:2009*. Sydney: Standards Australia, 2010.

Marks, Norman. *10 Reasons Not to Like the COSO ERM Framework: A Discussion With Grant Purdy*. February 21, 2011. http://normanmarks.wordpress.com/2011/02/21/10-reasons-not-to-like-the-coso-erm-framework-—-a-discussion-with-grant-purdy (accessed April 5, 2012).

About The Conference Board of Canada

We are:

- The foremost independent, not-for-profit, applied research organization in Canada.
- Objective and non-partisan. We do not lobby for specific interests.
- Funded exclusively through the fees we charge for services to the private and public sectors.
- Experts in running conferences but also at conducting, publishing, and disseminating research; helping people network; developing individual leadership skills; and building organizational capacity.
- Specialists in economic trends, as well as organizational performance and public policy issues.
- Not a government department or agency, although we are often hired to provide services for all levels of government.
- Independent from, but affiliated with, The Conference Board, Inc. of New York, which serves nearly 2,000 companies in 60 nations and has offices in Brussels and Hong Kong.

Publication 12-288
E-copy: $175

The Conference Board of Canada
Insights You Can Count On

255 Smyth Road, Ottawa ON K1H 8M7 Canada
Tel. 613-526-3280 • *Fax* 613-526-4857 • *Inquiries* 1-866-711-2262

The Conference Board, Inc. 845 Third Avenue, New York NY 10022-6679 USA *Tel.* 212-759-0900 • *Fax* 212-980-7014 • www.conference-board.org
The Conference Board Europe Chaussée de La Hulpe 130, Box 11, B-1000 Brussels, Belgium *Tel.* +32 2 675 54 05 • *Fax* +32 2 675 03 95
The Conference Board Asia-Pacific 2802 Admiralty Centre, Tower 1, 18 Harcourt Road, Admiralty Hong Kong SAR *Tel.* +852 2511 1630 • *Fax* +852 2869 1403