Business Horizons (2016) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

The challenges of and solutions for implementing enterprise risk management

John R.S. Fraser [a], Betty J. Simkins [b,*]

[a] Former Chief Risk Officer Hydro One Networks Inc., Toronto, Canada
[b] Spears School of Business, Oklahoma State University, Stillwater, OK 74078, USA

KEYWORDS
Enterprise risk management;
Corporate governance;
Risk;
Corporate culture;
ISO 31000

Abstract Enterprise risk management (ERM) began to take root in the late 1990s and has since become generally recognized as an expectation of good management and corporate governance. However, as evidenced by surveys and research, many companies still struggle with ERM implementation. This article explores the challenges companies face when implementing ERM and offers solutions for firms struggling with the concepts and execution. We draw upon Hydro One's experience in achieving ERM maturity as a best practice case study. The company's ERM methods have been researched and documented extensively. With over 15 years of ERM success, Hydro One is an excellent organization to benchmark for ERM best practices.

1. The importance of enterprise risk management

Historically, risk management was viewed very narrowly and handled separately in silos. Under this fragmented view of risk, businesses focused on specific potential events that could be insured against (e.g., property, safety, health). In financial areas, the focus was on interest rate risk, currency risk, or commodity risk (Kloman, 2010). In the mid-1990s a number of publications began advocating to businesses that risk management should include all risks, not just specific ones that are easier to quantify, and that risks should be managed as a portfolio across the enterprise. Leading the way were the Australian/New Zealand Risk Management Standard 4360, Tillinghast-Towers Perrin, and the Conference Board of Canada. The Australian/New Zealand Risk Management Standard was first published in 1995 and the Canadian Standards Association (1997) soon followed with its version that added 'communication' and 'consultation' to the framework (CAN/CSA-Q850-97). The Australian/New Zealand Standard was then re-issued (Standards Australia/Standards New Zealand, 1999) with updates, including the Canadian additions.

The 1990s saw an increased emphasis on governance, risk, and control, with several important publications moving forward the concepts of governance and risk management. These included the Group of Thirty report (USA), CoCo (the criteria of control model developed by the Canadian

* Corresponding author
E-mail address: simkins@okstate.edu (B.J. Simkins)

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.06.007

Institute of Chartered Accountants), the Toronto Stock Exchange Dey report (Canada), and the Cadbury report (UK). During this period, many thought of enterprise risk management (ERM) as just another flavor-of-the-month management technique, especially since it was often consultants who pushed for it—with their guidance, of course.

ERM has come a long way since we began researching the topic at the beginning of this century. Much has been written about it and the concepts are now well enough entrenched that ERM is likely here to stay. Many misconceptions exist about ERM, however, such that someone starting on the implementation journey is likely to be confused. Furthermore, a number of additional drivers for ERM have emerged: rating agencies (particularly Standard and Poor's and Moody's, which include assessments of ERM in their methodologies); regulators; and, in the United States, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which in 2004 developed its own ERM framework, lending credibility to the concept of ERM among U.S. management and boards.

The credit crisis of 2008/2009 demonstrated that risk management was weak in many companies. As a result, financial regulators now promote ERM to help manage risks and to demonstrate that they are taking action. Given this momentum, one would expect that ERM would now be widely adopted, practiced, and entrenched. Unfortunately, however, the lack of progress has been disappointing. Recent surveys demonstrate that only about 25% of large organizations claim to have ERM in place (Beasley, Branson, & Hancock, 2015). Some organizations have tried and failed; some are still trying to get started; and many of those who start are struggling and doing only a partial job.

We use Hydro One's ERM practices from 2000 to 2013 as a case study throughout this article to draw on the company's experiences in achieving ERM maturity, and illustrate the process using various aspects of ISO 31000 (see International Standards Organization, 2009). With over 15 years of ERM success, Hydro One is an excellent organization to benchmark for ERM best practices. ERM methods at Hydro One have been investigated and documented in numerous academic and other publications (e.g., Aabo, Fraser, & Simkins, 2005; Mikes, 2010). We also draw on the experiences documented in our second book on ERM, *Implementing Enterprise Risk Management: Case Studies and Best Practices* (Fraser, Simkins, & Narvaez, 2014), and numerous interviews with active risk managers/executives. This article explores the struggles organizations face and offers some solutions. We proceed by explaining the challenges many organizations experience in attempting to implement ERM, as well as why this leads to frustration and failure or ineffective results. We then provide highlights of proven solutions and suggestions, referencing additional guidance materials to assist implementers of ERM.

2. The challenges

This section discusses challenges we have observed in companies trying to implement ERM. We have identified these challenges—including misconceptions, implementation challenges, corporate governance, and external challenges—through our own experience, research, analysis, and conversations with risk executives. The challenges represent obstacles to success.

2.1. Misconceptions

In our article *Ten Common Misconceptions about Enterprise Risk Management* (Fraser & Simkins, 2007), we described many of the misconceptions about ERM that were then limiting organizations' abilities to implement ERM. Based on our research to date, we do not believe that—in the last decade—much progress has been made in overcoming these issues.

2.2. Internal challenges

We next discuss eight internal challenges we have observed in implementing ERM. These are: (1) corporate culture, (2) boards of directors' knowledge, (3) not applying a KISS mindset, (4) training without having risk workshops, (5) identifying too many risks, (6) no timeframes, (7) not making ERM enjoyable or meaningful, and (8) not recognizing ERM as change management.

2.2.1. Corporate culture

Unfortunately, ERM will not work in all corporate cultures. Successful implementation of ERM depends on organizational willingness to be open, to share, and to develop teamwork among the board of directors, senior management, and staff. Much of Hydro One's ERM success was due to the firm's openness and desire for transparency on the part of various chairs, CEOs, and senior management over the years. More research is needed regarding how corporate culture affects ERM. We would postulate that a firm's chances of success with ERM are directly proportional to its cultural capacity for openness, transparency, and teamwork.

2.2.2. Boards of directors' knowledge

While boards of directors' knowledge about ERM is increasing, it is still far from adequate. Various surveys (e.g., Deloitte, 2007; Deloitte/Economist Intelligence Unit, 2004) reveal a lack of knowledge about the information on risks, as well as the purpose and value of ERM. Many director organizations (i.e., those that train directors and provide networking opportunities) offer risk training to board members, but older directors especially may feel they do not need the education. Without an understanding of ERM as a methodology, board members will not be able to evaluate the adequacy of an organization's ERM processes and the credibility of risk reporting to the board. The role of the board in risk oversight is still not well understood (see Fraser, 2016). In brief, the board needs to review and be satisfied with the ERM process and then review and be satisfied with the risk reporting.

2.2.3. Not applying a KISS mindset

On starting the ERM journey, there is a temptation to implement too many features at once, leading to complexity. This can present an added bureaucratic burden on line management (e.g., maintaining cumbersome risk/loss registers with too much detail). Interestingly, however, many of the organizations we have researched have enjoyed great success with only two or three ERM staff facilitating the methodology (see Fraser et al., 2014). The more-successful implementations seem to come from those organizations that do pilots first and then later add additional features (e.g., resource allocation based on risk criteria, the use of key risk indicators). In the beginning, it is important to remember the KISS principle: keep it simple, silly.

2.2.4. Training without having risk workshops

We have observed organizations that decide to implement ERM by first launching into a series of training sessions. One major multinational had a team traveling globally, presenting and teaching ERM to managers; only several years later did the firm stage its first risk workshop. There is much evidence that presenting and teaching ERM first without conducting workshops is of limited value, and little is retained by attendees. A far more practical and engaging method of training staff entails holding workshops in which ERM methods can be applied to practical business realities; here, attendees learn the methods, language, and risk criteria being used, and then relate them to solving their own real-life business problems.

2.2.5. Identifying too many risks

Some organizations—especially those influenced by well-meaning but conflicted consultants—create extensive lists of risks. Indeed, one author of this article has heard of up to 700 risks being listed. If these risks are then recorded in a risk register and updated, this becomes an administrative burden that may impress regulators or boards, but is not seen as helpful or relevant by line management. Shorter can often be better, with the top 10 to 20 risks being monitored by each part of the organization and then reported upward, based on predetermined criteria.

2.2.6. No timeframes

To identify risks and the related probabilities, it is essential to define the time period being discussed. Amazingly, few organizations think of this. Consider the following example we use when teaching ERM to a class: ''What is the likelihood of you dying?'' This is typically followed by a variety of answers listing various percentages, until someone shouts out ''100%.'' We acknowledge: ''Yes, that is correct. Everyone is going to die.'' But suppose we ask: ''What is the likelihood of you dying in the next five years?'' The percentage will, hopefully, be much less than 100%, say 2% — 5% or less. This exercise illustrates that without defining a timeframe, one cannot meaningfully discuss probabilities.

2.2.7. Not making ERM enjoyable or meaningful

Staff members are not always enthusiastic about the advent of ERM in the organization; many view it as an additional bureaucratic burden, with surveys or useless paperwork to be filled out. However, proponents of risk workshops have found that participants actually look forward to these sessions, both as a learning experience and in helping to solve real business problems. The key to meaningful workshops involves having the right people in the room (i.e., those with relevant knowledge of the subjects being discussed), employing a skilled facilitator, and designing the class/presentation to touch on important issues. The use of voting methods (e.g., software) provides elements of surprise, excitement, and reality that participants enjoy. Workshop attendees typically report they feel the time was well spent and that they better understand organizational risks and what is needed in light of those risks. As noted in section 2.2.1., though, some organizational cultures will not permit open and transparent discussions.

2.2.8. Not recognizing ERM as change management

ERM is a change management initiative. It requires a change in the way information is shared and how many critical activities are conducted. ERM is not about having a separate group at headquarters manage risk while others in the organization continue as before, with little attention paid to this initiative. ERM will re-enforce business objectives by constantly referencing them during risk workshops, risk interviews, and business planning. Risk will need to be factored into all capital projects, both as part of the proposals and during the project phases. All requests for funding and resources will need to be supported by explanations as to the risks being addressed and the related strategic objectives. By using consistent risk criteria throughout these activities, there will be a common understanding of agreed risk tolerances. For example, on an impact scale of 1 to 5, a rating of 3, 4, or 5 was considered intolerable at Hydro One. Managers were expected to take action to reduce any such-scored risks to level 1 or level 2 (i.e., tolerable). After several years of having it in place, Hydro One management confirmed that they could not confidently operate the business without ERM; too many unknowns and a lack of clarity about risks would exist, they said via executive interviews (Mikes, 2010).

In summary, there are many challenges in implementing ERM. But these are not insurmountable. Next, we offer solutions.

3. The solutions

To overcome many of the ERM implementation challenges discussed in the previous section, we present the following solutions.

3.1. The basics of ERM

Much has been written about how to implement ERM. Our recent book, *Implementing Enterprise Risk Management: Case Studies and Best Practices* (Fraser et al., 2014), contains case studies of how major organizations (e.g., Lego, GM, TD Bank) have implemented ERM. The best practices for successful implementation of ERM may be summarized as two critical concepts: conversations and prioritization.

Conversations are essential in establishing understanding and engaging staff. They are best conducted via risk workshops, risk interviews, and—ultimately—executive team/board talks regarding objectives and risks. *Prioritization* is achieved through the use of risk criteria, such as pre-determined risk significance scales and what is/is not considered tolerable. Risk criteria may also include impact, probability and control scales, prioritization of objectives relative to each other, and prioritization of resources as part of business planning.

These techniques provide the basis for entrenching ERM into the organizational culture. Conversations and prioritization are explained more fully in Fraser (2014). The concepts captured by Fraser are as follows.

ERM, with its simple, focused approach, gives every organization—from small not-for-profits to the largest organizations and even countries—a method to come back to the basics of good management:

- What are you trying to achieve, and in what time frame(s)?
- What are the sources of risk that could impact these objectives?
- How impactful could these be, and how probable?
- What can and should be done to optimize the opportunities and to reduce the potential downsides?
- Are resources being allocated to those areas of risk that most need them?
- How well are these objectives, risks, and treatments understood by staff, and how committed and engaged are they to executing the plans?

3.2. Basic techniques for implementing ERM

In this section we summarize 26 basic techniques that we believe need to be considered and, as appropriate, used to build an ERM methodology. Not every feature is required for all organizations. For example, 'champions' (see section 3.2.6.) are only necessary in large, geographically dispersed organizations; here, the Chief Risk Officer (CRO) or corporate risk group cannot visit frequently, so a local presence is needed.

3.2.1. ERM policy

It is recommended that firms have an overarching ERM policy. This should be approved at the board level, either by the full board or a delegated committee such as the audit or risk committee. At a minimum, the policy should contain the general principles (e.g., that risks will be managed

holistically) and define the accountabilities of key persons such as the CEO, the CRO, and the board. Definitions of major concepts such as 'risk' should also be included so that the same definitions may be used company-wide (see section 3.2.4.). Some organizations will also include additional information, although much of this may be better placed in the framework (see section 3.2.2.). Two to four pages of description should suffice for an ERM policy.

3.2.2. ERM framework

The framework is the procedure manual for how ERM will be conducted. A firm can base its ERM framework on an extant framework such as ISO 31000 and then customize the language to suit the organization. For small and medium-sized enterprises (SMEs), the International Standards Organization (2015), or ISO, has just issued the publication *ISO 31000 Risk Management: A Practical Guide for SMEs*. The length recommended for the framework document is about 10 to 15 pages.

3.2.3. Executive risk committee

It is a good idea to have a management committee to focus on risk. This function can be handled by an existing executive committee. This committee should consist of the most senior executives, preferably including the CEO.

3.2.4. Common language

ERM is a change management initiative; as such, there will be changes in how the business is managed. Separate departments will now need to be on the same page and this will require a shared understanding of how the organization views and treats risks. An extensive dictionary is not needed, but common ERM terms such as risk, residual risk, greatest credible risk, treatment/mitigants/control, etc. should be understood and used in the same way by all departments.

3.2.5. Dedicated corporate risk group

It is a good idea to have a centralized group, perhaps even including the CRO, that will facilitate and guide ERM. Whether additional risk-related functions are added to this group is up to each organization. Based on our research, most such groups require two to three individuals; however, additional functions—such as insurance, security, whistleblower hotlines, etc.—can increase this number. The various types of roles that a CRO may play are explained by Mikes (2010).

3.2.6. Champions

Champions are individuals that help promote and engage employees with ERM at the local level. This is especially critical in large, diverse organizations. Champions should be trained in ERM techniques and conduct workshops, perform risk interviews, prepare risk profiles, and liaise with the central risk group.

3.2.7. Integration with loss control

Most companies keep track of their losses, however defined (e.g., fines, lawsuits, product returns). This is useful information for ERM, especially as key risk indicators of future trends, and should be available to the CRO. Hopefully, these losses are already being tracked and monitored by management.

3.2.8. Integration with strategic planning

Each company's definition of risk derives from that firm's business objectives. Thus, risk is variable from corporation to corporation. However, identifying and discussing risks as they relate to strategy is an iterative process. The best ways to integrate ERM and strategy are explained by Beasley and Frigo (2010).

3.2.9. Integration with business planning

ERM best practice dictates allocation of resources based on risks. As part of business planning, all business units should prepare risk assessments to support the need for resources. Also, enterprise-wide risk prioritization needs to be implemented to ensure that resources are used where the risks are most critical. Toneguzzo (2010) and Grose (1986) explain ways of prioritizing resources based on risks.

3.2.10. Risk criteria and approved risk tolerances

In order to identify, evaluate, and prioritize risks, firms must have predetermined risk criteria.[1] These are best articulated as scales to facilitate prioritization (e.g., with ranges from 1—5). The ranges that are deemed tolerable versus intolerable should also be agreed on to assist in implementing ERM. As described, this concept is sometimes thought of or referred to as 'risk appetite,' but specific criteria provide a practical application compared to the vague wording in most risk appetite statements seen to date. For a more complete discussion on risk criteria, see Purdy (2011).

3.2.11. Risk workshops for line staff

Successful ERM entails having a common understanding of objectives, risks, and treatments in place (or to be implemented). This is best achieved through conversations and prioritization among the staff responsible. The most efficient and effective way of doing this is via risk workshops; obviously, this

[1] Refer to ISO 31000 for examples.

can prove more difficult in large, multinational or geographically dispersed organizations. How to design and facilitate risk workshops is described in detail by Quail (2010).

3.2.12. Risk workshops for the leadership team

Risk workshops among the leadership team are also essential toward a common understanding and prioritization of risks and actions to be taken. In addition, such workshops build essential team spirit. Leadership team members will, in turn, take the acquired risk knowledge into risk workshops with their own staff, thereby embedding the concepts, knowledge, and risk tolerances throughout the organization.

3.2.13. Voting software

We recommend the use of voting software for the immediate and iterative feedback of workshop participants. While voting can be conducted via pens and slips of paper, voting software adds a sense of excitement that has been found to make workshops more enjoyable and efficient. Without the use of voting technology, discussions can become dominated by the loudest voices or most-senior persons present. These may not be the most knowledgeable, leading to biased or politically motivated decisions.

3.2.14. Risk interviews

One-on-one risk interviews can be a key source of conversations to gather and disseminate information related to risks. These can elicit information that some staff may not feel comfortable sharing in a group setting. They also offer an opportunity to reinforce corporate business objectives and risk-related issues outside of the interviewee's purview. See Fraser (2010) for how to conduct risk interviews.

3.2.15. Measurement: Broad ranges

The measurement of risks in quantitative terms is relatively easy as regards certain domains (e.g., investment portfolios). This is not the case, however, in other areas (e.g., regulatory risk, government risk, safety); here, in order to understand and prioritize risks it is necessary to utilize broad ranges. This is the most popular method at present among organizations practicing ERM. The use of ranges to measure risks is explained by Hargreaves (2010).

3.2.16. Measurement: Detailed metrics

To better gauge the potential effects of risks among a multiplicity of scenarios, statistical analysis is a useful tool. For example, Monte Carlo simulations can be run to analyze the interrelationship of impacts across multiple events. The use of statistical analysis to measure risks quantitatively for ERM is explained by Hargreaves (2010).

3.2.17. Risk register

A risk register, which lists all identified risks and information pertinent to the same, is often considered essential for risk management. There is a danger, however, that upkeep and maintenance of the risk register will prove an administrative burden unrelated to managing the business. This, in turn, can lead to irrelevance of the process and frustration on the part of management. Some records are helpful, but risk management is a living, real-time activity, not an outdated record. This must be understood by all.

3.2.18. Business plan templates

As part of risk-based business planning, it is recommended that line management be provided with templates as to what information should be supplied on risks, and thereby support the need for resources. Risk-based resource allocation is described by Toneguzzo (2010) and Grose (1986).

3.2.19. Key risk indicators

Key risk indicators (KRIs) are statistical data that provide potential insights to future situations. Unlike key performance indicators, which record past accomplishments, KRIs can warn management of evolving issues that may increase or reduce risks, and should be developed and factored into risk discussions and analyses. For further reading on key risk indicators, see Hwang (2010).

3.2.20. Scenario analysis

Scenario analysis, especially in a brainstorming setting, is a useful technique for identifying and planning for possible sources of risk. In the financial industry, there are often regulatory requirements for stress testing the impact on an institution's financial position under various scenarios. This technique is also useful when discussing black swans (see section 3.3.3.).

3.2.21. Sign-off by line management

Some organizations have adopted the practice of having line managers sign off as to the adequacy of risk disclosure in their reports, business planning, etc. This can be helpful in the early days of ERM to ensure that line managers fully understand their accountability regarding risk evaluation and disclosure.

3.2.22. ERM in executives' personal contracts

Directly referencing the risk responsibilities listed in executives' personal annual contracts—which are

used to evaluate their performance and determine bonuses—can support the attention paid to risks and risk management by executives.

3.2.23. Corporate risk profile

A corporate risk profile should periodically be prepared for executive management and the board. At a minimum, this should be done semi-annually, with updates for important changes in the interim. The profile should reflect the key risk information of residual risks in excess of predefined tolerances for a given future time period (e.g., five years). Corporate risk profiles typically take the form of risk maps, lists of top ten risks, and heat maps, all supplemented with accompanying narratives explaining the sources of risks, objectives impacted, and actions in place/proposed. These profiles are usually prepared by the corporate risk group under the direction of the CRO or equivalent, and based on the various databases of risk information. Such databases may include risk registers, results of workshops and risk interviews, key risk indicators, recent events analysis, and relevant records. How to design and conduct risk profiles is described in detail by Fraser (2010).

3.2.24. Reporting to leadership

Many firms implement ERM to ensure that members of the leadership team share an understanding of the risks that may affect company objectives. The first step in reporting to leadership entails composition of an initial risk profile. In smaller organizations, ERM may be launched with risk workshops where executive team members brainstorm the risks and subsequently prioritize them for any additional actions required.

3.2.25. Reporting to the audit (or other board) committee

When accountability for risk oversight has been delegated by the board to a committee, that committee periodically should ask for risk profiles from management. These profiles typically contain the aforementioned risk maps, lists of top ten risks, and heat maps, all supplemented with accompanying narratives explaining the sources of risks, objectives impacted, and actions in place/proposed. Frequent updates may also be required upon major changes in circumstances that could affect the accomplishment of business objectives.

3.2.26. Reporting to the board

As previously described, there is debate as to what level of detail and effort the full board should focus on regarding risk. If no board committee performs more detailed oversight, the full board must do this review.

3.3. Additional practical techniques for ERM

This section contains more-complex concepts and additional techniques for employment in ERM. First, we offer explanations about the confusion over risk appetite as a concept, and provide a suggestion for addressing this concept and employing a practical method of prioritizing strategic objectives. Second, we present guidance on the use of risk criteria, in line with ISO 31000 guidelines. Third, we proffer practical guidance on dealing with 'black swans' (high-impact, low-probability events). Fourth, we supply a practical example of using risk criteria to solve a major business problem. Fifth, and finally, we introduce a new technique: creating a 'risk calendar' to track upcoming events that could create risk for the organization in the future.

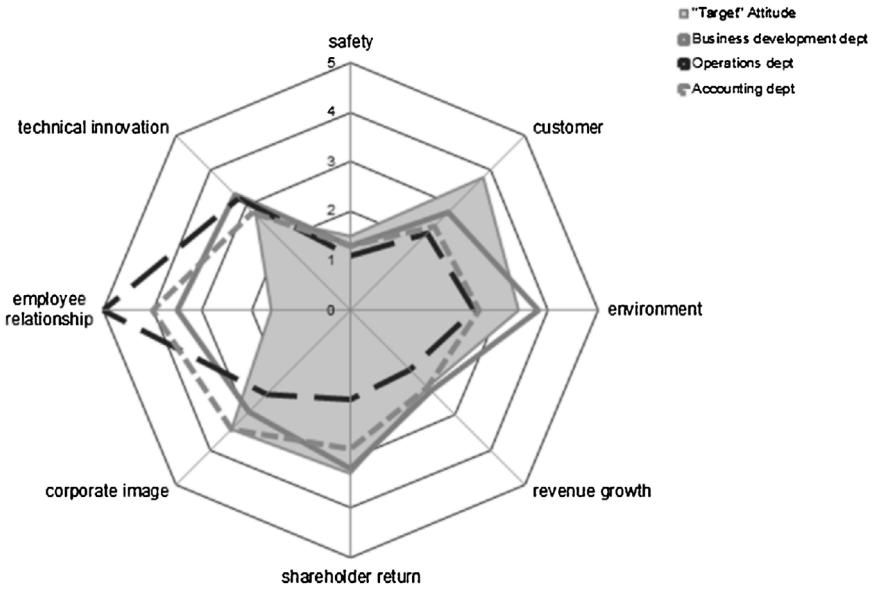
3.3.1. Risk attitude/risk appetite

As mentioned, the mass confusion generated by COSO in its definitions of risk appetite and risk tolerance has been one of the great inhibitors of successful implementation of ERM. This confusion was recognized by ISO, which decided not to use either term in the ISO 31000 (Purdy, 2011). Instead, it used the term 'risk attitude,' which we illustrate in this section.

ISO 31000 only mentions risk attitude twice, once being in its definition. Hydro One has explored this concept in order to gauge and provide feedback on whether its employees' views of risk attitude are those intended by executive management and the board. As shown in Figure 1, Hydro One uses a spider diagram graphic and associated ranking criteria, first to establish the executive team's attitude toward each major strategic objective (i.e., the target attitude). Then, at the beginning of every risk workshop, staff members are surveyed to gauge their perception of the organization's attitude and behaviors toward the strategic objectives. Rob Quail (2012), Vice President — Customer Service at Hydro One, describes this process in more detail.

In testing this methodology, Hydro One discovered somewhat diverse views to risk attitude throughout the company. This is important feedback regarding communication in the organization and whether the attitude needs to change or the communications efforts need to be enhanced. As with all its initiatives, Hydro One seeks here to create structured conversations so that optimal prioritizations can be made. This feedback will also influence the impact and tolerance criteria.

Figure 1. Risk attitude*



*This diagram shows a comparison of opinions by staff across work units. This input is obtained by use of voting technology during risk workshops throughout the company. This is a model only.

3.3.2. Risk criteria: The essence of prioritization

ISO 31000 defines risk criteria as the "terms of reference against which the significance of a risk···is evaluated" (International Standards Organization, 2009). Some examples provided include: "the nature and types of causes and consequences that can occur and how they will be measured; how likelihood will be defined; the timeframe(s) of the likelihood and/or consequence(s); the level at which risk becomes acceptable or tolerable" (International Standards Organization, 2009).

Risk criteria drive much of the ERM process. For example, risk criteria include the use of scales for impact, probability, control, etc. The benefit comes from (1) the conversations and agreement as to appropriate scales and (2) the ability to prioritize risks and treatments. Risk workshops should be facilitated for all major projects; for major types of risks; by business units through business planning; and for the executive team and—where appropriate—the board of directors, both to obtain their input and to demonstrate how management identifies and assesses risks. Given that they all use the same criteria and methodology, this also educates and embeds the understanding of risks and risk attitude. Risk workshops and how to design and facilitate them are described in hard-hitting detail by Quail (2010).

Measurement of risk impact and risk tolerance as applied by Hydro One was designed such that a rating of 1 or 2 (minor or moderate, respectively) is considered a tolerable impact. A rating of 3, 4, or 5 (major, severe, or worst-case, respectively) is considered an intolerable impact, and the sources of these risks must be addressed and prioritized for treatment.[2]

Table 1. Velocity*

5	Instantaneous	Less than one day
4	Immediate	One day to one month
3	Rapid	One month to one year
2	Gradual	One to five years
1	Slow	More than five years

* Velocity is the interval between the initiating event and its peak impact on the organization's business objectives.

3.3.3. Risk criteria: Black swans

Popularized by Nassim Taleb (2007), the term 'black swan' describes an event that comes as a surprise, has a major impact, and—after the fact—is recognized as something that should have been foreseen. Nowadays, the term is often used to describe a high-impact but low-probability potential event. Several years ago, Hydro One realized that it did not always create explicit conversations around these types of risks. As a result, the firm re-evaluated its approach and recognized that different criteria would be required for assessing and prioritizing these risks. It determined that the key consideration factors for these types of risks were speed/velocity of impact (see Table 1) and preparedness of the firm

[2] See page 539 of Fraser and Simkins (2010) for an example.

Table 2. Resilience*

5	Immediate	Appropriate resources and plans accessible or in place; are regularly tested and could be deployed immediately.
4	Full	Resources accessible or in place; could be deployed with some effort. Responsibility for development of plans is clear.
3	Substantial	Resources are accessible for large aspects of the risk and its impact, but there are significant gaps; would require organization, procurement of resources, and development and deployment 'on-the-fly'.
2	Partial	No resources exist for significant aspects of the risk or its impact; coping with the risk would take years of planning and resource redeployment.
1	Minimal	Plans and resources unavailable.

* Resilience is the ability to detect and deploy (plans, organizations, and structures), and the availability of resources (people, knowledge, liquidity, equipment, etc.).

Table 3. Risk calendar*

Strategic Objectives	2016	2017	2018	2019	2020
Customers	Major new computer system		Government elections		
Regulatory				New regulations take effect	
Human Resources		Union agreements to renew	CEO has announced retirement for June 2018		
Other		Lease on warehouse due to expire	Major competitor announced opening here		Patents for major product due to expire in 2020

* The risk calendar keeps track of important future risk events that could affect the organization in a material way. In discussing these, each should be evaluated as to the possible benefits, opportunities, and impacts that might occur and how these can best be addressed.

(see Table 2). As a result, Hydro One structured scales to allow the company to have meaningful discussions about such risks (e.g., computer failures in which the back-up also fails; massive, but unlikely, regulatory or government decisions). Hydro One now maps results onto a velocity x resilience chart to help ensure that its contingency plans and resource allocations for resilience match the potential speed of the impacts (e.g., having a 'hot' back-up site for an event that will not provide the firm with adequate warning).

3.3.4. Making decisions and solving problems

First and foremost, ERM must be viewed as providing important information that aids in decision making, thereby helping to solve managers' problems. This does not mean that ERM team members will themselves possess the requisite expertise in particular areas, but it *does* mean using methodologies that facilitate sound decision making and optimal outcomes for managers. Hydro One's ERM team members earned their stripes early in the implementation phase by helping managers make decisions and solve problems. For example, as part of a planned initiative, 20% of Hydro One's workforce took early retirement in 2000. This changed staffing scenario left the company with a dramatically different risk profile. Hydro One applied the aforementioned techniques using risk criteria, workshops, etc. to show how areas of greatest residual risk could be identified and treatments prioritized (Aabo et al., 2005). Hydro One's ERM team was thereafter constantly requested to facilitate risk workshops and advise on risk issues.

3.3.5. The risk calendar

While not all events will necessarily experience difficulties, future events can create risks due to the uncertainty of whether or not they will actually occur and what the impacts—good or bad—may be. Accordingly, it is a good idea that someone (e.g., the CRO or his/her staff) maintain a calendar recording major upcoming events (e.g., government elections, union negotiations, lease renewals) several years into the future so that these can be monitored, planned for, and leveraged whenever

possible (see Table 3). In discussing these events, each should be evaluated regarding the possible benefits, opportunities, and impacts that might occur and how these can best be addressed.

4. Conclusion

In this article, we presented explanations from our research as to the challenges faced by implementers of ERM. We provided a summary of the basic techniques for implementing ERM and included some additional techniques that may be used when appropriate. Numerous surveys (Beasley et al., 2015) show that the successful implementation of ERM trails the expectations of senior management, boards, and regulators. This article provided specific practical explanations of the reasons for frequent failures, as well as simple, effective techniques and guidance on how to improve the chances of success in implementing ERM. References to additional guidance materials on each critical aspect were proffered.

It is our belief that in any organization that has successfully implemented ERM, the management team will deem it essential for continued good management and governance. This article should be of interest to organizations implementing ERM, to academics teaching ERM, and to risk professionals desiring to learn more on this evolving process.

References

Aabo, T., Fraser, J. R. S., & Simkins, B. J. (2005). The rise and evolution of the chief risk officer: Enterprise risk management at Hydro One. *Journal of Applied Corporate Finance, 17*(3), 18—31.

Beasley, M. S., & Frigo, M. L. (2010). ERM and its role in strategic planning and strategy execution. In J. Fraser & B. Simkins (Eds.), *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (pp. 31—50). Hoboken, NJ: John Wiley & Sons.

Beasley, M. S., Branson, B. C., & Hancock, M. S. (2015). *Report on the current state of enterprise risk oversight: Update on trends and opportunities*. Durham, NC: AICPA.

Canadian Standards Association. (1997). *Risk management: Guideline for decision-makers (CAN/CSA-Q850-97)*. Mississauga, Canada: CSA.

Deloitte. (2007). *In the dark II: What many boards and executives still don't know about the health of their businesses*. New York: Deloitte Touche Tohmatsu.

Deloitte/Economist Intelligence Unit. (2004). *In the dark: What many boards and executives don't know about the health of their businesses*. New York: Deloitte Touche Tohmatsu.

Fraser, J. R. (2010). How to prepare a risk profile. In J. Fraser & B. Simkins (Eds.), *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (pp. 171—188). Hoboken, NJ: John Wiley & Sons.

Fraser, J. R. (2014). Building enterprise risk management into agency processes and culture. In T. Stanton & D. W. Webster (Eds.), *Managing risk and performance: A guide for government decision makers* (pp. 175—196). Hoboken, NJ: John Wiley & Sons.

Fraser, J. R. (2016). The role of the board in risk management oversight. In R. Leblanc (Ed.), *Handbook of corporate governance*. Hoboken, NJ: John Wiley & Sons.

Fraser, J. R., & Simkins, B. J. (2007). Ten common misconceptions about enterprise risk management. *Journal of Applied Corporate Finance, 19*(4), 75—81.

Fraser, J. R., & Simkins, B. J. (Eds.). (2010). *Enterprise risk management: Today's leading research and best practices for tomorrow's executives*. Hoboken, NJ: John Wiley & Sons.

Fraser, J. R., Simkins, B. J., & Narvaez, K. (Eds.). (2014). *Implementing enterprise risk management: Case studies and best practices*. Hoboken, NJ: John Wiley & Sons.

Grose, V. L. (1986). *Managing risk: Systematic loss prevention for executives*. Atlanta: Omega Systems Group.

Hargreaves, J. (2010). Quantitative risk assessment in ERM. In J. Fraser & B. Simkins (Eds.), *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (pp. 219—235). Hoboken, NJ: John Wiley & Sons.

Hwang, S. (2010). Identifying and communication key risk indicators. In J. Fraser & B. Simkins (Eds.), *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (pp. 125—140). Hoboken, NJ: John Wiley & Sons.

International Standards Organization. (2009). *ISO 31000 risk management: Principles and guidelines*. Available at http://www.iso.org/iso/catalogue_detail?csnumber=43170

International Standards Organization. (2015). *ISO 31000 risk management: A practical guide for SMEs*. Available at http://www.iso.org/iso/iso_31000_for_smes.pdf

Kloman, F. (2010). A brief history of risk management. In J. Fraser & B. Simkins (Eds.), *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (pp. 9—29). Hoboken, NJ: John Wiley & Sons.

Mikes, A. (2010). *Enterprise risk management at Hydro One (Case 9-110-707)*. Boston: Harvard Business School Publishing.

Purdy, G. (2011 September). *Risk appetite: Is using this concept worth the risk?* Wellington, New Zealand: NZ Society for Risk Management.

Quail, R. (2010). How to plan and run a risk management workshop. In J. Fraser & B. Simkins (Eds.), *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (pp. 155—170). Hoboken, NJ: John Wiley & Sons.

Quail, R. (2012). Defining your taste for risk. *Corporate Risk Canada, Spring*, 24—30.

Standards Australia/Standards New Zealand. (1999). *Risk management (AS/NSZ 4360)*. Sydney: Standards Australia.

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. New York: Random House.

Toneguzzo, J. (2010). How to allocate resources based on risk. In J. Fraser & B. Simkins (Eds.), *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (pp. 189—216). Hoboken, NJ: John Wiley & Sons.