CFGR | FCRG

Canadian Foundation for Governance Research
Fondation canadienne de recherche sur la gouvernance

The Robert Bertram Doctoral Research Awards

2012 RESEARCH REPORT

Articulating Acceptable Risk for Organizations: Toward a Better Risk Appetite Framework

Christopher Eaton, PhD candidate in Risk Management
Haskayne School of Business, University of Calgary

Final Research Report
Robert Bertram Doctoral Research Award

Articulating Acceptable Risk for Organizations: Toward a Better Risk Appetite Framework

CHRISTOPHER EATON
PhD Candidate, Risk Management
Haskayne School of Business
University of Calgary

Fall 2012

I thank the Canadian Foundation for Governance Research (CFGR), the Institute of Corporate Directors (ICD), the case study organizations that participated in this research, my mentor for the Award, Mr. Robert Bertram, and my co-supervisors, Dr. Norma Nielson and Dr. Laurie Milton. Although many people contributed to this research project, I am solely responsible for any errors.

INTRODUCTION AND OVERVIEW

The 21st century has witnessed a significant shift in attention toward organizational risk. Boards of directors and senior management teams face increasing pressure to formalize and improve the ways they oversee and manage risk, or their risk governance. Whether driven by organizational performance concerns, broader institutional concerns, or some combination of these factors, the diffusion of risk governance innovations is gaining momentum and patterns are emerging. In this new regime, the board is responsible for risk oversight while senior management and others throughout the organization are responsible for risk management. Such aspects of corporate governance and risk management would seem to enhance organizational performance; however, progress toward "best practices" in risk governance is in the early stages.

One risk governance innovation would have an organization's board and senior management articulate the nature and extent of risk that is acceptable for the organization. Although many policymakers and practitioners acknowledge the need for such an innovation, they often lack the relevant guidance to craft and implement a suitable framework. Despite recent attention from practitioners, policymakers and researchers alike, there is a lack of consensus on concepts and processes and limited progress toward convergence. Many foundational concepts such as risk criteria, risk attitude, risk capacity, risk appetite, and risk tolerance have been developed, but confusion remains. Diffusion has been finance-centric, with higher adoption in the financial services industry and lower adoption—or resistance or rejection—in non-financial industries.

Through this research, I explore how boards and senior management teams should articulate acceptable risk for the organizations they serve. This process and its outcome are critical responsibilities within the emerging organizational risk governance regime. Ideally, the formal expression of an organization's acceptable risk—or its risk appetite framework (RAF)—should guide decisions and actions throughout the organization. The RAF should evolve through meaningful consultation with the organization's stakeholders and should meet their many needs. It should achieve a balance between *stability* to reflect the organization's enduring values and objectives and *dynamism* to enable the organization to adapt to complex and novel situations. This is a tall order—one with which practitioners, policymakers, and researchers are struggling.

To address this problem I conducted research using an engaged scholarship approach, qualitative methods, and theory building from multiple cases. I integrated knowledge from diverse but complementary domains, including corporate governance, risk management, behavioral theory of the firm, and structured decision making. I relied on two detailed case studies for this research project. The present study involved a Canadian organization in the energy/utilities industry; a previous study involved a Canadian organization in the financial services industry. I conducted interviews, reviewed documents, facilitated workshops, and presented preliminary findings at each organization. I also explored the same topic using publicly available material on other organizations at the individual and aggregate levels.

Through this research I found that the articulation of acceptable risk for organizations is still in early stages. Guidance and diffusion varies considerably across jurisdictions and industries, with the United Kingdom and the financial services industry at the vanguard. Motivation for and commitment to the implementation of an RAF also varies across organizations and industries, and not all organizations are ready, willing, and able to move in this direction. RAF initiatives are often intensive and lengthy but may yield benefits through improvements to decision quality. Using an objective-centric approach, boards and senior management teams can evaluate the organization's critical objectives, map its principal risks, and determine risk criteria (e.g., risk tolerances, risk appetite, and risk capacity) to include in its RAF. Risk appetite and risk capacity are organizational concepts, which are derived from risk tolerances using a structured approach. Once implemented, the organization and its stakeholders can use the RAF to inform decisions and actions that involve risk. The board and others can then monitor and sustain the RAF.

This study has implications for practice, policy, research, and teaching. Organizations can use the approach described in this report to understand and implement RAFs. This is particularly important across diverse organizational contexts and risk profiles. If these concepts are proven, then existing rules/guidelines and standards/frameworks should be modified accordingly. Researchers can elaborate and extend the theory through analyses of additional case studies and even broader samples if quantitative data become available. Researchers could convert their case study experience(s) into teaching cases, with the consent of the case study organization(s).

Below I describe research on the articulation of acceptable risk for organizations using RAFs. I start by describing the idea and its importance and my project. Next, I review the "state of the art/science" of board risk oversight and articulation of acceptable risk for organizations, mainly within a Canadian context. Then I describe the key findings of my research. I finish with some conclusions and suggested future directions. I cite accessible references throughout the report.

I. THE IDEA, ITS IMPORTANCE AND THE RESEARCH

The idea and its importance

> *An area of increasing importance for boards and which is closely related to corporate strategy is risk policy* [later linked to risk appetite]. *Such policy will involve specifying the types and degree of risk that a company is willing to accept in pursuit of its goals. It is thus a crucial guideline for management that must manage risks to meet the company's desired risk profile (OECD, 2004: 60).*

All organizations face uncertainty, the effects of which may lead to their success or failure. Boards of directors and senior management teams are under increasing pressure to articulate the acceptable risk for the organizations they serve or, as this concept is often called, "risk appetite." But many boards of directors and senior management teams continue to struggle with practical aspects of determining risk appetite for their organizations and expressing it in meaningful ways. They often struggle with content (the "what"), process (the "how"), or both of these dimensions. Sometimes they question whether risk appetite is appropriate or useful for their organizations. Risk appetite is surrounded by confusion, but it is an important component of risk governance.[1] Through this study, I address how an organization should determine and express its risk appetite. Consistent with—and yet somewhat distinct from—current guidance, I define risk appetite as the "nature and extent of risk(s) an entity is willing to accept in aggregate."

Risk governance has recently emerged as a critical aspect of corporate governance in modern organizations. Risk governance can be described as the system, structures, tone and behaviours by which an organization is directed and controlled and held accountable regarding the nature

[1] In this study I focus on risk governance in organizations. This concept is different from other concepts of risk governance which focus on issues with broad consequences (e.g., climate change, nanotechnology) that are often experienced and addressed at higher levels of analysis (e.g., sector, society). Refer to IRGC (2008) for a discussion.

and extent of risk it accepts, which permit decisions to be made, objectives set, and performance monitored to ensure the efficient and effective use of resources and safeguarding of assets (derived from BSI, 2011: 5). Risk governance encompasses *risk oversight*—primarily a responsibility of the board—and elements of *risk management*—primarily a responsibility of senior management. However, the dividing line between these areas is neither clear nor fixed.

Growing evidence indicates that an organization's board risk oversight affects its performance and can affect the performance of industries and societies in which it is exercised. Experiences from the recent global financial crisis are both illustrative and compelling. One review of financial services organizations found "widespread failure of risk management" in which "boards were in a number of cases ignorant of the risk facing the company" (OECD, 2009: 8). Another review noted a "disparity between the risks that...firms took and those that their boards of directors perceived the firms to be taking" (SSG, 2009: 4). Thus, risk governance and risk oversight are increasingly viewed as important board issues, along with acceptable risk.

Acceptable risk has played a key role, for example through lack of "active board involvement in setting the risk appetite for firms in a way that recognizes the implications of...risk taking" (SSG, 2009: 4). Organizations face pressures to articulate acceptable risk to enhance their performance, address stakeholders' expectations, or a combination of these factors. Ultimately, the value of RAFs derives from enhancements to the quality of decision making and risk taking. Many boards and senior management teams are responding by implementing RAFs that contain policy guidance on acceptable risk for the organization and its stakeholders. However, there is only limited agreement on what RAFs should include and how they should be implemented.

In summary, acceptable risk is emerging as a cornerstone of organizational risk governance and board risk oversight more specifically. It is an important matter for the practitioner and policymaker communities and for communities affected by organizational risk and risk taking. Under the circumstances, it is also a matter that could benefit from increased scholarly attention.

The research project

This research project arose out of two anomalies regarding the articulation of acceptable risk for organizations. The first anomaly centres on the pattern of diffusion, with adoption in the financial services industry and resistance or rejection in other industries. In itself, this anomaly is not particularly surprising because many risk governance innovations have originated and largely remained in the financial services industry. What makes it interesting is the second anomaly, which centres on confusion about what the innovation is, how organizations should proceed if it is desired, and the influence of organizations' confusion on their attitude toward the innovation. At the same time, there is some convergence of concepts across knowledge domains and contemporary practitioner, policymaker, or researcher conversations. These conditions lend themselves to an applied form of inquiry that I and other researchers find rewarding and useful.

Acceptable risk is not only important for risk governance practice and policy, it is also important for research and teaching. The topic presents a complex challenge and a fascinating opportunity. To address this challenge, for the present study and the broader project, I used an engaged scholarship approach (Van de Ven, 2007) and qualitative methods (Corbin & Strauss, 2008) to build theory from multiple case studies (Yin, 2009). This overall research approach and the associated research methods are particularly appropriate and effective for studies which are collaborative efforts among researchers and practitioners designed to understand complex social processes in real-world contexts and to prescribe and implement innovative solutions.

This was the second study in a research project on the articulation of acceptable risk for organizations. In the first study, I worked with a Canadian financial services organization to develop theory from December 2010 to September 2011. In the present study, I worked with a Canadian energy/utilities organization to refine theory from December 2011 to September 2012. I selected these two case study organizations based on their theoretical suitability—particularly differences in their industry contexts and risk profiles—and their commitment to participate in the studies. For each case study organization, I obtained data by interviewing and/or surveying key people, reviewing relevant internal and external documents, participating in meetings and

workshops, and discussing research results and implications. The names of these organizations and other specific details cannot be disclosed to protect their anonymity and confidentiality.

In addition to the primary data from these two case study organizations, I also collected and analyzed secondary data from other organizational contexts based on individual and aggregated case studies, surveys, and examples. Other individual cases included the Royal Bank of Canada, Scotiabank, National Bank of Australia, and Commonwealth Bank of Australia (IIF, 2011); TD Bank Group (Gandz, 2012); Canada Mortgage and Housing Corporation (Ebsary, 2011); Hydro One (Mikes, 2008); University of Alberta (UofA, 2005); Royal Bank of Scotland (FSA, 2011b); Lloyd's (Lucas, 2012); Lehman Brothers (Valukas, 2010); and LEGO (Læssøe, 2011). I also drew on publicly reported material from aggregated case analyses (e.g., SSG, 2010; IIF, 2011), surveys (e.g., CBOC, 2005, 2011), and examples (e.g., COSO, 2004, 2012; CCRO, 2006).

To develop and refine theory on the articulation of acceptable risk for organizations, I integrated concepts from four knowledge domains: corporate governance, risk management, behavioral theory of the firm, and structured decision making. Corporate governance and risk management knowledge domains were particularly useful to frame the idea because of their grounding in real-world interests, perceptions, and experiences (i.e., the "why", "who", "when", and "where"). However, concepts from these practice- and policy-oriented domains sometimes lacked grounding in management theory related to complex organizations and social processes.

To address "what", I drew on modern *behavioral theory of the firm (BTF)*, including aspects of organizational decision theory, managerial risk taking, and behavioral strategy (e.g., Cyert & March, 1992; March, 1988, 1994, 1999; March & Shapira, 1982, 1987; Shapira, 1995, 1997; Greve, 2003; Bromiley, 2005). To address "how", I drew on *structured decision making (SDM)*, including aspects of multi-attribute utility theory, decision analysis/risk analysis, and behavioral decision theory (e.g., Keeney, 1992; Keeney & Raiffa, 1993; Clemen, 1996; Hammond, Keeney & Raiffa, 1999; Slovic, 2000; Pidgeon, Kasperson & Slovic, 2003; Lichtenstein & Slovic, 2006; Gregory et al., 2012; Fischhoff et al., 1981; Fischhoff, 2012; Kahneman, 2011).

Through this research project, I developed and refined theory on the articulation of acceptable risk for organizations. I continuously analyzed the data that I collected to identify patterns

("constant comparison") and sought new and disconfirming data to clarify preliminary findings ("theoretical sampling") until the incremental value of collecting and analyzing such data seemed minimal ("theoretical saturation"). I confirmed that the new theory can generalize to a degree ("external validity") by cross-checking preliminary findings across diverse organizations and environments ("replication logic") and a wide range of data sources, theoretical perspectives, and analytical methods ("triangulation"). In terms of my contribution, I shed light on a critical aspect of risk governance practice and policy and built a solid foundation for research and teaching.

II. THE CURRENT STATE OF THE ART/SCIENCE

In this section, I review the state of the art/science for board risk oversight and the articulation of acceptable risk. Refer to Appendix B for illustrative sources of information on this topic across Canada, the United Kingdom, the United States, and multilateral/other jurisdictions.

A review of the corporate governance and risk management knowledge domains provides evidence of convergence on board risk oversight responsibilities, many of which involve risk appetite or similar concepts. However, the extent of convergence is influenced by jurisdiction, industry, and organization—it is not "one size fits all." Emerging board responsibilities include:

1. review, understand, and approve the organization's risk management policy(ies);
2. articulate the nature and extent of risk the organization is willing and able to accept;
3. guide identification of the organization's risk, especially its key or principal risks;
4. review and understand analyses of the organization's risk, especially its principal risks;
5. evaluate the organization's risk to determine whether it is acceptable or unacceptable;
6. evaluate the organization's strategies, practices and decisions that involve material risk;
7. guide treatment of the organization's risk, especially for any risks deemed unacceptable;
8. review, understand, and approve selected risk-related communications and disclosures;
9. instill a culture of informed and prudent risk taking throughout the organization; and
10. ensure appropriate and effective risk management and risk oversight systems are in place.

Many of these responsibilities are typically addressed by the full board while some aspects may be delegated to one or more of its committee(s), such as the audit committee or a risk committee. Importantly, each responsibility typically involves a degree of coordination between the board and the senior management team, internal units of the organization, and/or external entities.

Responsibilities of boards in Canada regarding risk oversight and acceptable risk are generally less demanding than those of similar organizations in some other jurisdictions. With a few exceptions, prevailing rules and guidelines in Canada do not require boards to articulate acceptable risk for their organizations. For example, boards of publicly traded companies in Canada are responsible for considering opportunities and risks through strategic planning, identifying principal risks, ensuring appropriate systems are implemented to manage such risks, and disclosing basic risk oversight practices (CSA, 2005a, 2005b). Boards are also encouraged but are not required to make additional voluntary disclosures on principal risks (TSX, 2006).

Many organizations in the financial industry and some in the public sector in Canada are subject to more specific responsibilities regarding the articulation of acceptable risk. For example, boards of federally regulated, private sector financial institutions are required to "review and approve the overall risk philosophy and risk tolerance of the institution" and monitor material changes and/or exceptions to such risk tolerances and limits (OSFI, 2003: 9). Boards of federal crown corporations in Canada have a very similar responsibility regarding the articulation of acceptable financial risk for their organizations (FC, 2009).

Rules and guidelines regarding board responsibility for the articulation of acceptable risk in many multilateral and other national jurisdictions are generally more demanding. Multilateral corporate governance guidelines outline articulation of acceptable risk as a board responsibility (e.g., OECD, 2004, 2009; FRC, 2012a; BCBS, 2010a); for example, "determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives" (FRC, 2012a: 18). The United States is moving tentatively in this direction, driven by the global financial crisis, particularly for financial services organizations and specific risk types (e.g., liquidity risk) (FRS, 2012). Other U.S. requirements, such as audit committee discussion of risk policies (NYSE, 2012) and disclosures of board risk oversight practices (SEC, 2009), are only indirectly related to acceptable risk. Trends distilled from legal proceedings provide limited or conflicting guidance on these requirements (e.g., Bainbridge, 2009; Pan, 2010; Valukas, 2010).

This aspect of board risk oversight has had greatest acceptance in the financial services industry, followed by the energy/utilities industry and parts of the public sector such as crown

corporations (e.g., CBOC, 2005, 2011). Boards and other stakeholders from non-financial organizations in other jurisdictions have resisted such board responsibilities based on perceived differences between the nature and extent of risk facing the organization and relevance of quantitative versus qualitative risk analysis and evaluation techniques (ICAEW, 2009). Recent standards/frameworks (e.g., SA/SNZ, 2004a, 2004b; COSO, 2004, 2009a, 2012; ISO, 2009a, 2009b, 2009c; CSA, 2010; BSI, 2009, 2011; IRM, 2011) provide useful risk appetite concepts but often lack detail and consistency, particularly regarding board risk oversight responsibilities.

Evaluations of Canadian corporate governance rules and guidelines and associated proposals for reform hinted at expanded risk oversight responsibilities for boards. A recent example did not explicitly address acceptable risk but did mention "setting the overall vision and long-term direction...including risk and return expectations and non-financial goals" (CSA, 2008: part 3, principle 1). However, these proposed governance reforms were deferred indefinitely. With respect to federally regulated, private sector financial institutions in Canada, a recent proposal by the regulator would require affected boards to approve an RAF for their organizations and would provide some detailed guidance on components of a suitable RAF (OSFI, 2012).

Risk attitude is sometimes preferred to risk appetite, particularly outside the financial services industry (ICAEW, 2009). Risk appetite and risk tolerance are often used interchangeably, even in the financial services industry (e.g., BCBS, 2010a). There is some agreement that risk appetite and risk capacity are more abstract, higher level concepts that reflect the overall nature and extent of risk the organization is willing and able to accept, respectively. There is some agreement that risk tolerance is a less abstract, lower level concept that reflects the nature and extent of risk the organization is willing or able to accept regarding specific objectives or risks, often expressed as variability around reference points. Risk criteria is an umbrella concept that includes these and possibly other concepts. There are notable differences between these and similar concepts such as risk preference and risk propensity (e.g., Weber, 2010; IRM, 2011).

Articulations of acceptable risk for organizations typically take the form of RAFs, which may include risk appetite statement (RASs), risk tolerances, and risk evaluation guidelines. In a review of financial services organizations, RAFs ranged from "high-level, brief, and qualitative"

to "complex, lengthy, and quantitative" (SSG, 2010: 4). Organizations were at "different development stages" and "no single firm was observed to have developed a fully comprehensive framework containing all the better practice elements" and, as a group, organizations were "not particularly mature in their development" (SSG, 2010: 4). There was "no clear agreement about the scope and reach" for RAFs, but they were thought to "not simply be a set of loss tolerances or limits" and to "include a wide array of measures to monitor the firm's risk profile...from the dynamic and forward looking to the static and point-in-time" (SSG, 2010: 9). RAFs may also include "rules that go beyond risk criteria" by "using measures that are not risk measures (e.g. level of investment), requiring a wider range of actions (e.g. escalation of decisions) and applying to decisions outside instances of the risk management process" (BSI, 2011: 28).

To add the most value, RAFs should: enhance the quality of decisions and actions throughout organization; fulfill board and senior management risk governance responsibilities; facilitate meaningful risk communication; reflect a broad range of the organization's values and objectives and its uncertainties and events, regardless of difficulty in quantification; facilitate reconciliation of diverse perspectives on values, objectives, uncertainties, and events; support the use of quantitative and qualitative indicators; support the incorporation of "upside risk" and "downside risk"; support risk aggregation and risk integration (e.g., BCBS, 2003); strike a good balance between stability and flexibility; apply across organizational contexts (e.g., financial/non-financial) and time horizons (e.g., short/long term); and leverage applicable "best practices."

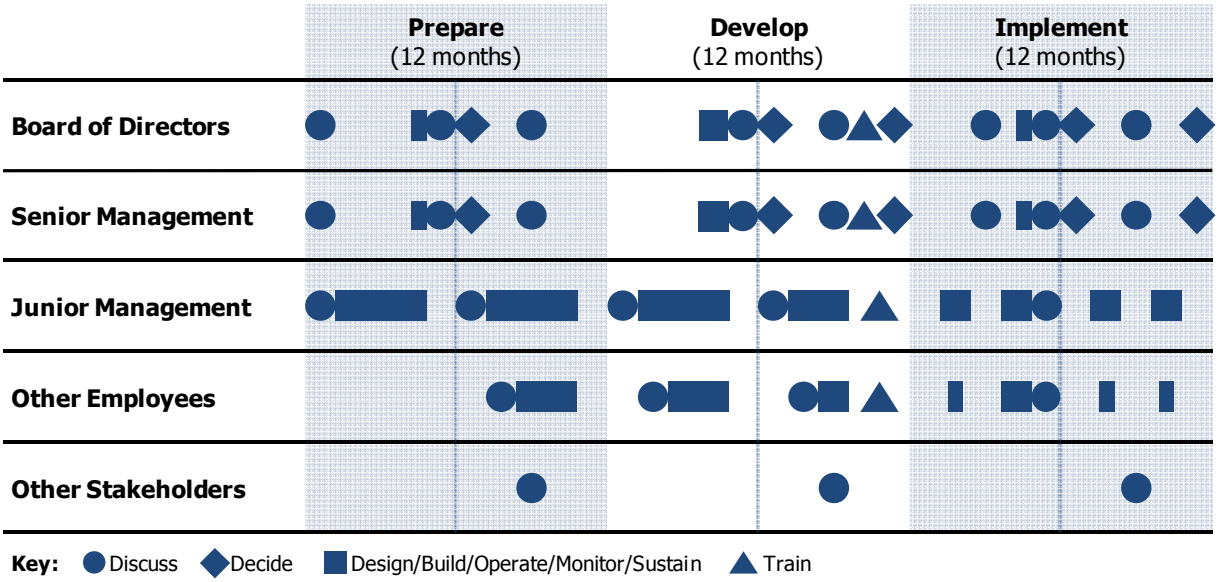
III. KEY FINDINGS OF THE RESEARCH

The primary focus of this research project and the present study is how organizations should articulate acceptable risk. However, given the lack of agreement on key terms, in both studies I focused significant attention on the "what" of acceptable risk. Both topics are addressed below.

The process of articulating acceptable risk should involve three phases: prepare, develop, and implement. The timeframe for such an initiative could span 24 to 36 months, depending on the organization's initial readiness and ongoing commitment. The prepare and develop phases typically follow a project approach similar to that used to develop new strategy, while the

implement phase typically becomes an integral part of the organization's ongoing management and oversight processes. The RAF initiative should be tightly integrated with the organization's governance, strategic, and performance management cycles and processes (e.g., planning, budgeting, reporting) and associated decision-making activities (e.g., dedicated time at senior management and board or committee meetings). The approach should also take advantage of related work, such as scenario analyses for strategic planning, and should be highly iterative within and between activities. Figure 1 provides an illustrative RAF implementation roadmap.

Figure 1—Illustrative Roadmap for RAF Implementation



Prepare phase

Not every organization is ready, willing, and able to implement an RAF. Organizations that are ready, willing, and able often differ in their motivations and commitment. At some organizations, interest is stimulated by regulatory or other stakeholder pressures and is driven by the board to meet its emerging governance responsibilities. At other organizations, interest is stimulated by the desire to enhance the quality of decisions and actions in the pursuit of value and is driven by senior management to meet or exceed its established performance expectations. Organizations also differ in terms of the attention and resources available for such an initiative.

Whatever the particular context, it is useful to assess and, if necessary, enhance the readiness of any organization that is interested in implementing an RAF.

Some preparedness indicators include: pressure from influential external stakeholders; active support of the board and senior management; commitment of potentially affected internal groups and individuals; availability of resources, particularly board and senior management attention; maturity of the related governance, strategic, performance and risk management frameworks; and fluency with basic RAF concepts. For an RAF initiative to be successful, several of these indicators will likely need to be favorable. The occurrence of a governance failure or adverse event can stimulate interest but may not translate into sustainable commitment or may take the initiative in a direction that dwells on the past rather than one that looks toward the future.

RAFs still seem to be in early adoption stage, particularly outside the financial services industry, despite recent anecdotal evidence and survey results (mainly from self-reported data) suggesting that significant progress has been made on the articulation of acceptable risk. Many organizations are reluctant to even seriously consider exploring an RAF initiative, much less assess their preparedness and develop and implement an RAF. Experiences attempting to recruit multiple case study organizations for this research project and related inquiries are cases in point. This phenomenon may be partly explained by confusion around some basic RAF concepts.

Although an RAF initiative should be structured into phases, the line separating each phase is generally not very distinct because of the iterative nature of this work. The initiative should be sponsored by the chief executive officer (CEO), led by the chief risk officer (CRO) or equivalent executive, and overseen by the board of directors. It should also actively involve leaders from the organization's business units and functional areas. Concepts from organization theory such as the dominant coalition (Cyert & March, 1992) and top management team (TMT) (Finkelstein, Hambrick & Cannella, 2009) can be useful for identifying critical participants and the underlying rationales for them, such as expectations regarding who will decide, act, monitor, and/or enforce.

Ongoing support by the organization's leaders is critical because implementing an RAF could have the potential to significantly change "business as usual" and threaten the discretion of senior management and the board. RAFs are most relevant for guiding the exercise of judgment

and discretion; they can be perceived as enabling or constraining senior management's and the board's latitude for decisions and actions. These factors need to be addressed throughout the RAF initiative, in both the RAF's process and content. In the prepare phase, senior management and the board must decide whether to proceed with the RAF initiative. If they decide to proceed, they should agree on the basic RAF concepts, RAF scope, and the overall approach to develop and implement (and subsequently operate, monitor, and sustain) the RAF. A preliminary or sample "sketch" of what the organization's RAF might look like is often useful for this purpose.

Through the present study and the previous study, I worked with a primary contact at each case study organization to select key people from the board, senior management, and other areas of the organization to interview and survey. Interviewees and survey respondents were selected for their diverse perspectives on each organization's risk, risk capacity, risk appetite, and risk tolerances, their influence within the organization, and their commitment to contribute. I interviewed 15 people in the present study and 25 people in the previous study. All interviews were semi-structured and 30-90 minutes in length; proceedings of most were audio recorded. I also surveyed nine people in the present study to explore a subset of the organization's risk tolerances that applied most directly to one of its business units in a more structured way.

In addition, I collected and reviewed internal and external documents from each case study organization. Most of these documents were directly related to their governance, risk management, strategic management, and/or performance management frameworks. Review of these documents provided insights into each case study organization's values/objectives, uncertainties/events, decisions/actions, performance, and existing risk criteria over multiple time horizons. At each case study organization, I presented results from the relevant study to the senior management team and discussed potential implications and future directions with them. These activities provided insights into each organization's preparedness for an RAF initiative, input into the decision on whether to proceed, and ultimately development of the RAF itself.

Key RAF concepts

The decision whether to proceed with an RAF initiative and the approach taken are influenced by the underlying concepts and scope of the RAF. There has been convergence on some basic

concepts, including risk, risk criteria, risk attitude, risk capacity, risk appetite, risk tolerance, and risk profile. Box 1 contains definitions of key terms. Appendix A contains additional details.

Box 1—Key Acceptable Risk Terms
(Refer to Appendix A for additional details)

risk	effect of uncertainty on one or more value(s)
effect	positive and/or negative deviation from the desired
uncertainty	state, even partial, of deficiency of information related to, understanding or knowledge of, or confidence in event(s) or value(s) and/or any relevant underlying characteristic(s)
value	aspiration or goal and associated outcome(s) considered desirable
risk criteria	terms of reference for evaluating the significance and acceptability of risk(s)
risk attitude	disposition toward risk(s) and any associated decisions and/or actions
risk capacity	nature and extent of risk(s) an entity is able to accept in aggregate
risk appetite	nature and extent of risk(s) an entity is willing to accept in aggregate
risk tolerance	nature and extent of risk(s) an entity, or a part thereof, is willing to accept with respect to any relevant underlying characteristic(s) and/or set(s) thereof
risk profile	set of risks related to an entity or a part thereof

Sources: Derived from ISO (2009a), FRC (2012a), COSO (2012), Keeney (1992), March (1994, 1999), Shapira (1995).

RAF scope

Risk appetite statement (RAS). A risk appetite statement (RAS) serves as the foundation of an organization's RAF by describing a few critical boundaries or constraints for the organization. An RAS should be relatively straightforward and unambiguous to facilitate its acceptance and use. Sometimes described as a "mission statement for risk" (SSG, 2010: 5), an RAS should be closely aligned with strategic and performance management frameworks. An RAS should also contain a few common elements that express the organization's risk policy (e.g., the scope of its business, generic preferences for objectives and risks, relevant trade-offs, some risk indicators). These key elements can be expressed in positive terms (i.e., "We will do X"), negative terms (i.e., "We will not do Y"), or a combination of these. For example, TD's high-level RAS is:

> *We take risks required to build TD's business, but only if those risks: 1) fit TD's business strategy and can be understood and managed; 2) do not expose TD to any significant single-loss events; and 3) do not risk harming the TD brand (TD, 2011).*

In this case and many others, additional details that clarify the organization's RAS are provided internally to facilitate interpretation but are only selectively shared outside the organization.

Risk tolerances. Risk tolerances represent the most challenging part of RAFs and also the greatest potential opportunity for improvement and contribution to "best practices." To date, most financial services organizations have included their existing loss, risk and other limits in their RAFs through a "bottom up" approach. As a result, their RAFs may not be comprehensive, coherent, nor integrated with their related frameworks. For example, they may be biased toward indicators that are more easily quantified, they may contain gaps and overlaps among indicators, and they may make it difficult for leaders to see the "big picture" while also providing clear guidance for employees. More importantly, many organizations' RAFs do not appear to be well integrated with governance, strategy and performance through their respective frameworks (e.g., SSG, 2010). Grounding risk tolerances in the organization's values and objectives is a potential way to address these problems, as described in the next section on the develop phase below.

Risk evaluation guidelines. Risk evaluation is the process of comparing the results of an organization's risk analysis with its risk criteria to determine whether the organization's risk is acceptable (ISO, 2009b, 2009c) and guiding risk treatment if its risk is unacceptable. This process depends on three earlier processes: establishing the context, risk identification, and risk analysis (ISO, 2009b). If the organization's risk is deemed to fall outside its risk criteria, then the organization's senior management and/or board likely need(s) to make decisions and take actions consistent with these guidelines to modify the relevant risk exposure (ISO, 2009b). Such guidelines typically contain rules for applying the RAF, including exceptions, conditions, and escalations to assist with interpretation and related decisions and actions (e.g., BSI, 2011).

RAF approach

An organization's risk appetite framework (RAF) is an integral part of its risk management framework, which may be based on enterprise risk management (ERM) principles (e.g., COSO, 2004; ISO, 2009b). To be integrated, the RAF should be aligned with the organization's strategic management framework (e.g., planning, budgeting) and its performance management framework (e.g., monitoring, compensation). The RAF should also be an integral part of an

organization's governance framework (e.g., board risk oversight). Like much of the policy guidance implemented in modern organizations, the RAF may be developed and implemented mainly by management, albeit with active participation and oversight by the board and frequent and meaningful consultation with other internal and external stakeholders. An RAF may thus be developed and proposed by management; reviewed and, if acceptable, approved by the board; implemented by management, the board, and others; monitored and enforced by senior management and the board; and periodically reviewed by internal auditors or other parties.

The nature of uncertainty facing an organization—in terms of complexity and dynamism—and the perceived difficulty of aggregating the organization's risk are critical factors affecting an organization's decision to develop and implement an RAF, particularly in the absence of strong regulatory drivers. Highly complex organizations in highly complex environments may face a wide range of uncertainty that is "unknown" or even "unknowable" and that does not lend itself to quantitative risk analysis. Many financial services organizations are now struggling with this challenge formally to incorporate operational risk, strategic risk, and reputation risk. Many non-financial organizations have faced this challenge for some time and likely resisted developing and implementing traditional RAFs as a result. A solution to the "incommensurability problem" to enable risk aggregation across domains is needed to facilitate adoption (e.g., BCBS, 2010b).

Develop phase

Most of the work occurs during the develop phase, in which the RAF is developed, reviewed, and approved. No widely accepted approach has emerged, but this phase typically includes a combination of interviews, surveys, and workshops. Such an approach should involve evaluating the organization's values and objectives, mapping its uncertainties and events, and determining its RAF components based on its risk tolerances, risk appetite, and risk capacity. These steps are described below and are followed by a few general points for the develop phase.

<u>Evaluate values and objectives</u>

Organizations should follow an objective-centric approach, which starts with their values and objectives, because these are the common link between governance, strategic management,

performance management, and risk management. Organizations may need to re-consider and refine their existing objectives, indicators, and targets to more consistently and accurately reflect their values and to prepare objectives for use in later steps (e.g., Hammond et al., 1999; Gregory et al., 2012). Common issues include gaps and overlaps, sacrifices in accuracy to gain precision, and over-specification (e.g., Meyer, 2002). The organization's objectives and associated indicator(s) help clarify its relevant domains of consequences (e.g., financial, health/safety).

Organizations may use multiple reference sources when setting objectives, indicators, and targets, including their own values, performance, and expectations as well as those of reference organizations or groups (Cyert & March, 1992). It is important to differentiate between expectation and aspiration in this context. A target should be considered the desired or aspiration level rather than the likely or expectation level. These two levels are the same as a special case, rather than a general case. It is useful to acknowledge that an organization may have established objectives and executed on them well, but the objectives simply turned out to be "wrong" given the circumstances; even strong operational performance could result in "failure" (March, 1994).

Senior management and the board should prioritize the organization's objectives according to their relative importance to the organization in most situations. This activity should be done in light of the associated indicator(s) and target(s) and the organization's broader strategies, alternatives, and constraints. It does not need to entail a forced ranking but it should result in meaningful differentiation among objectives (e.g., Hammond et al., 1999; Gregory et al., 2012). Prioritizing objectives can be difficult and emotionally charged, particularly when the exercise involves objectives, events, or tradeoffs that are considered taboo; however, techniques do exist to help facilitate such discussions (e.g., Gregory et al., 2012; Schoemaker & Tetlock, 2012).

Map uncertainties and events (or risks)

Risk identification is the process of finding, recognizing, and describing the organization's risk(s). Finding and recognizing individual risks should involve broad and iterative searches and draw on internal and external sources. Individual risks should be described at an appropriate level of detail for later stages (e.g., risk analysis, risk evaluation, risk treatment) and should follow the mutually exclusive and collectively exhaustive ("MECE") principle. Individual risks

should be categorized first according to common or similar "cause" (i.e., uncertainty and event) and next according to common or similar "consequence" (i.e., value and objective). Risk analysis is the process of estimating the nature and extent (or type and amount) of the organization's risk using a combination of qualitative and quantitative techniques (ISO, 2009b, 2009c). The steps below require the use of results from both risk identification and risk analysis.

Rather than trying to convert all of the organization's risks to a common unit of measure (e.g., dollars), senior management and the board should map the organization's uncertainties and events to its values and objectives based on domains of consequences (e.g., Gregory et al., 2012). Any given uncertainty and event may affect one or more domain(s) of consequence. Senior management and the board should prioritize the organization's risks according to their likely impact on objectives in most situations. This activity should be done in light of indicator(s) and target(s) and the organization's broader strategies, alternatives, and constraints. It does not need to entail a forced ranking but it should result in meaningful differentiation among risks.

Determine risk criteria

Risk taking in organizations depends somewhat on context and situation and tends to vary across domains of consequences (e.g., Shapira, 1995; Weber, 2010). To determine risk criteria, senior management and the board should use consequence tables that contain comparable ranges of consequences (e.g., Hammond et al., 1999; Gregory et al., 2012). It is important to specify consequences on both sides of the target or aspiration level for each objective and indicator; most organizations to date have only specified for negative or "downside risk" (e.g., Mikes, 2008). Although "downside risk" is clearly most relevant in a variety of situations (e.g., loss, damage) (Shapira, 1995), "upside risk" is often relevant, particularly in exceptionally strong performance situations, if real or perceived "spillovers" could adversely affect other organizational values and objectives or breach some legal, regulatory, or public threshold(s) for appropriate outcomes.

Many organizations initially struggle with the concept of "upside risk" thresholds. However, my study and others show there are likely multiple reference points for organizational risk taking which could be useful for determining risk criteria (e.g., Lewin et al., 1944; Cyert & March,

1992; March, 1988, 1994, 1999; March & Shapira, 1982, 1987; Shapira, 1995, 1997; Greve, 2003; Bromiley, 2005). Table 1 contains a few reference points that appear to be relevant.

Table 1—Illustrative Reference Points for Risk Criteria

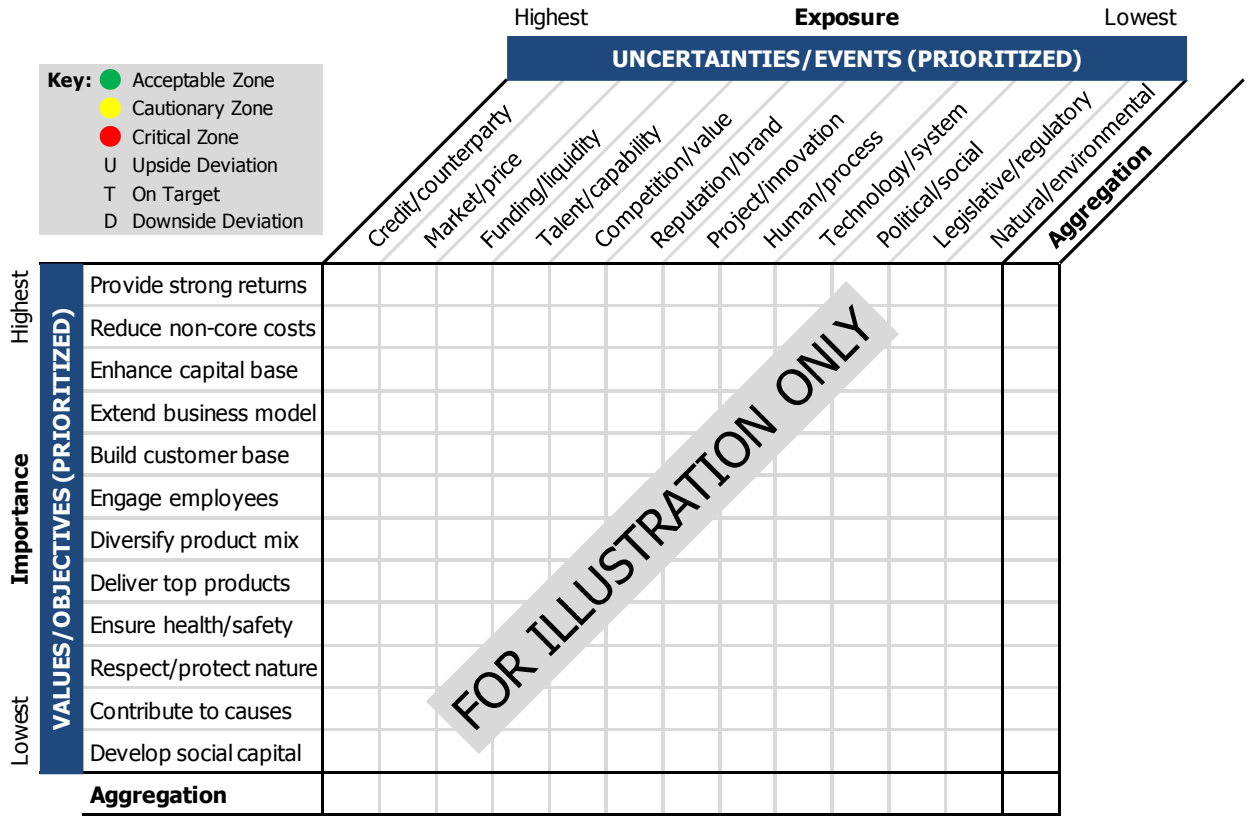
Reference	Description
Antagonization	exceptionally strong performance; multiple/broad adverse "spillovers" across domains
Exasperation	straining for performance; some adverse "spillovers" and increased risk taking potential
Aspiration	desired performance; typically different from expectation; can set others' expectations
Expectation	likely or reasonable performance; typically lower than aspiration; same in special case
Desperation	straining for performance; some adverse "spillovers" and increased risk taking potential
Devastation	exceptionally poor performance; multiple/broad adverse "spillovers" across domains

Senior management and the board should next determine the range of acceptable outcomes around the target for each objective and indicator, in light of the associated indicator(s) and target(s) and the organization's broader strategies, alternatives, and constraints. A range of methods are promising, but interviews, surveys, and scenario analyses in workshops are often used. Scenarios should focus separately on an extreme but plausible "positive" situations (i.e., mainly "upside risk" outcomes) and an extreme but plausible "negative" situations (i.e., mainly "downside risk" outcomes) to explore the upside and downside thresholds of the organization's individual risk tolerances and, ultimately, provide insights into its risk appetite and risk capacity.

Through the present study and the previous study, I collaborated with the primary contacts at each case study organization to plan, prepare, and participate in meetings and workshops with groups of key people, many of whom were also interviewees and survey respondents. As part of a workshop for the previous study, the senior management team—initially in many small groups and then in a single large group—considered two separate extreme but plausible "upside" and "downside" scenarios over one and a half days to explore the organization's risk tolerances, risk appetite, and risk capacity. As part of a workshop for the present study, the management team from a business unit reviewed aggregated results from their individual members' surveys and engaged in a facilitated discussion to better understand the business unit's risk tolerances.

An organization's risk appetite and risk capacity can be derived from an aggregation of its risk tolerances, as long as the aggregation is accomplished using a structured and objective-centric approach like the one advocated here. Senior management and the board should use the organization's objective-centric risk tolerances to determine its risk appetite and risk capacity. For example, significant breaches of multiple risk tolerances associated with one or more of the organization's critical objective(s) could constitute a breach of its risk appetite or risk capacity. An acceptable risk dashboard such as the one provided in Figure 2 could facilitate scenario analyses and stress tests for senior management and the board to explore what types of breaches of risk tolerances might constitute a breach of the organization's risk appetite or risk capacity.

Figure 2—Illustrative Dashboard for Acceptable Risk



Agreement among senior management and the board on the intersection of the most important values and objectives and highest exposure uncertainties and events could be used to express the organization's risk appetite and risk capacity in its RAS (e.g., COSO, 2012). This could also

provide the basis for identifying the organization's principal risks based on important exposures. In more sophisticated applications, the organization's risk profile, risk appetite, and risk capacity could be further quantified using composite measures or indices (e.g., Gregory et al., 2012).

General points

Organizational risk is socially constructed, as are risk criteria such as risk tolerances, risk appetite, and risk capacity. Preferences and perceptions regarding risk vary throughout most organizations and across stakeholders. It is important for senior management and the board to be actively involved in this process from the outset. Some amount of the board's early involvement could be delegated, possibly through a dedicated risk committee. To be rigorous and ultimately useful, the RAF process needs to result in widespread agreement among the organization's critical decision makers and influencers (e.g., Cyert & March, 1992; Finkelstein et al., 2009).

Individuals, groups, and organization are susceptible to cognitive biases regarding risk (e.g., Slovic, 2000; Kahneman, 2011; Gregory et al., 2012). Senior management and the board should familiarize themselves with these biases and take steps to de-bias their discussions and decisions to the extent practicable. The RAF development process should be both interactive and iterative, with multiple opportunities for individual participants to consider and update their perspectives. There is value in individual reflection before, during, and after group discussions and workshops. There is also value in reviewing anonymous, aggregated survey results in group discussions and workshops and monitoring changes in individual perspectives during and after such activities.

Interrelationships and tradeoffs among the organization's objectives and events should be explicitly addressed throughout the develop phase. Activities in this phase should involve evaluating each potential relationship (i.e., objective-objective, objective-risk, and risk-risk) in terms of directness (e.g., direct, indirect, n/a), strength (e.g., strong, weak, n/a), and direction (e.g., positive, negative, curvilinear, n/a). The relevant time horizon for consideration of an organization's risk criteria should be consistent with the time horizons for its related governance and management processes (e.g., planning, budgeting). However, in some cases senior management and the board may actually need to consider a longer time horizon when developing risk criteria to provide a sufficient timeframe for extreme and plausible scenarios to unfold.

Many organizations should be more disciplined when specifying their objectives and risks. For example, many need to extend their thinking on risk criteria to include "upside risk" as well as "downside risk", resist the tendency to focus solely on risk that can be easily quantified, and move beyond RASs based on simple "rolling up" of loss or risk limits. Similarly, organizations should avoid using a simple line drawn across a likelihood-consequence matrix to express risk appetite and risk capacity because such an approach tends to mask interrelationships and fails to place sufficient emphasis on the relevant consequences, within and across domains. Finally, organizations should take advantage of existing tools and techniques to facilitate completion of the develop phase (e.g., ISO, 2009c; BSI, 2011; IRM, 2011; COSO, 2012; Gregory et al., 2012).

Implement phase

In the implement phase, the board and senior management establishes the RAF as policy by actively communicating, following, monitoring, and enforcing it. After risk identification and risk analysis, senior management and the board evaluate the organization's risk by comparing its risk profile with its risk criteria to determine whether the nature and extent of its risk is acceptable. This phase reflects the organization's commitment to widespread, consistent, and ongoing use of the RAF. Unequivocal support by senior management and the board is particularly important during this phase to ensure that commitment to the RAF remains strong and is sufficiently robust to ensure adherence in the context of strategic decisions and actions that could involve extreme risk/reward tradeoffs and volatile performance (e.g., Valukas, 2010).

In this phase, senior management, the board, and possibly other stakeholders (e.g., internal auditors, external auditors, regulators, credit rating agencies) may also evaluate whether the RAF is "in place" and "operating effectively." Senior management and the board should review the RAF at least annually, ideally through the organization's strategic planning processes. Monitoring should focus on any breaches of risk criteria, decisions and actions to remedy such situations, any noted deficiencies in the RAF, and any critical changes to its major components. Effective risk communication is critical in this phase to ensure that the board and senior management can fulfill their respective risk governance responsibilities. A dashboard such as the one in Figure 2, along with underlying information, could be a useful for internal reporting.

IV. CONCLUSIONS AND FUTURE DIRECTIONS

Risk governance, risk oversight, and acceptable risk are emerging as critical issues for boards and senior management teams. The articulation of acceptable risk for organizations is still in early stages, rising in prominence as a result of failures from the recent global financial crisis. Organizations are implementing this innovation in response to a combination of performance and legitimacy drivers. Implementation of RAFs is progressing rapidly in the financial services industry but is lagging or being actively resisted in other contexts. Significant differences in risk profiles and risk analysis among organizations are contributing to this diffusion pattern. However, such frameworks are increasingly expected as part of good board risk oversight.

Despite these trends, not all organizations are ready, willing, and able to implement an RAF. If an organization is favorably inclined, implementing an RAF could span from 24 to 36 months and require significant effort by the board, management, and others. RAF initiatives should be structured into prepare, develop, and implement phases and should be followed with operate, monitor, and sustain elements after implementation. Sound techniques are available and typically include interviews, scanning, workshops, and consultations, over multiple iterations.

An organization's RAF typically includes a high-level risk appetite statement (RAS) and more detailed risk tolerances and risk evaluation guidelines to provide clarification. A structured approach that focuses first on the organization's values and objectives should help deliver a sound and useful RAF. Senior management and the board should determine risk tolerances at the individual objective level, aggregate these risk tolerances to determine risk appetite and risk capacity, and then use these risk criteria to evaluate the acceptability of the organization's risk.

It is important to have the right people involved throughout the RAF initiative, particularly from senior management and the board. The CEO should sponsor the initiative, the CRO or equivalent executive should lead it, and the senior management team and the board should actively contribute to it. The process should result in agreement and commitment among people who will be responsible for deciding and acting in accordance with the RAF and monitoring and enforcing it. It is also important to consult frequently with internal and external stakeholders.

Implementing RAFs in diverse organizations based on the approach outlined in this report can advance practice and policy. Such innovations can be used by boards and senior management teams to improve the effectiveness of risk management and risk oversight in organizations across diverse contexts. Although benefits may be difficult to quantify, improvements to decision quality could be significant. Future effort should be directed toward linking RAFs with emerging practice and policy related to risk culture, converting existing RAFs to the approach outlined in this report, and enhancing efforts to analyze aggregate risk through quantification. Rules, guidelines, standards, and frameworks may have to be modified to facilitate adoption.

From a research and teaching perspective, this study could be extended to explore whether this RAF approach generalizes across diverse organizational contexts, including: government-owned, publicly traded, privately held; for-profit, not-for-profit; financial and non-financial industries; early or advanced maturity; and across Canada or in other jurisdictions. Engaged scholarship approaches to elaborate theory from multiple case studies seem like a natural fit. After some time, data should be available to support quantitative empirical studies, notably to advance research on organizational risk taking. Ultimately, researchers could convert the case study experiences into teaching cases, if the case study organizations are willing to consent.

REFERENCES AND SUGGESTED READING

Adams, J. 1995. *Risk*. London: Routledge.

American Bar Association (ABA). 2011. *Corporate Director's Guidebook, 6th Ed.*

AON. 2010. *Global Enterprise Risk Management Survey*.

Ashby, S., & Diacon, S. 2010. *Risk Appetite in Theory and Practice*.

Association of Insurance and Risk Managers (AIRMIC). 2009. *Research into the Definition and Application of the Concept of Risk Appetite*.

Association of Insurance and Risk Managers (AIRMIC), Public Risk Management Association (Alarm), & Institute of Risk Management (IRM). 2010. *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000*.

Association of Investment Companies (AIC). 2010. *Code of Corporate Governance*.

Australian Securities Exchange (ASX). 2010. *Corporate Governance Principles and Recommendations with 2010 Amendments, 2nd Ed.*

Bainbridge, S. 2009. Caremark *and Enterprise Risk Management*. Journal of Corporation Law, 34(4): 967-990.

Baird, I., & Thomas, T. 1990. What is risk anyway? Using and measuring risk in strategic management. In R. Bettis & H. Thomas (Eds.), *Risk, Strategy and Management*, 21-52: Greenwich: JAI Press.

Basel Committee for Banking Supervision (BCBS). 2003. *Trends in Risk Integration and Aggregation*.

——. 2009. *Range of Practices and Issues in Economic Capital Frameworks*.

——. 2010a. *Principles for Enhancing Corporate Governance*.

——. 2010b. *Developments in Modelling Risk Aggregation*.

——. 2011. *Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems*.

Bernstein, P. 1996. *Against the Gods: The Remarkable Story of Risk*. New York: John Wiley & Sons.

Booz & Company (Booz). 2009a. *What is Your Risk Appetite? A Disciplined Approach to Risk Taking*.

——. 2009b. *A Comprehensive Risk Appetite Framework for Banks*.

Bowden, A., Lane, M., & Martin, J. 2001. *Triple Bottom Line Risk Management*. New York: John Wiley & Sons.

British Standards Institution (BSI). 2009. *BS-ISO 31000: Risk Management—Principles and Guidelines*.

——. 2011. *BS 31100: Risk Management—Code of Practice and Guidance for the Implementation of BS-ISO 31000*.

Bromiley, P. 2005. *The Behavioral Foundations of Strategic Management*. Malden: Blackwell.

Bromiley, P., Miller, K., & Rau, D. 2001. Risk in strategic management research. In M. Hitt, R. Freeman & J. Harrison (Eds.), *Blackwell Handbook of Strategic Management*: 259-288. Malden: Blackwell.

Bromiley, P., & Rau, D. 2010. Risk taking and strategic decision making. In P. Nutt & D. Wilson (Eds.), *Handbook of Decision Making*: 307-325. Sussex: John Wiley & Sons.

Buehler, K., Freeman, A., & Hulme, R. 2008. Owning the right risks. *Harvard Business Review*, September: 102-110.

Business Roundtable (BRT). 2010. *Principles of Corporate Governance*.

California Public Employees' Retirement System (CalPERS). 2011. *Global Principles of Accountable Corporate Governance*.

Canadian Coalition for Good Governance (CCGG). 2010. *Building High Performance Boards*.

Canadian Institute of Chartered Accountants (CICA). 2006. *20 Questions Directors Should Ask about Risk, 2nd Ed.*

——. 2008. *Building a Better MD&A Risk Disclosure*.

——. 2012. *A Framework for Board Oversight of Enterprise Risk*.

Canadian Securities Administrators (CSA). 2005a. *NP 58-201: Corporate Governance Guidelines*.

——. 2005b. *NI 58-101: Disclosure of Corporate Governance Practices*.

——. 2008. *Proposed Repeal and Replacement of NP 58-201: Corporate Governance Guidelines, NI 58-101: Disclosure of Corporate Governance Practices, and NI 52-110 Audit Committees and Companion Policy 52-110CP Audit Committees*.
——. 2009. *Staff Notice 58-305: Status Report on the Proposed Changes to the Corporate Governance Regime*.
——. 2010. *Staff Notice 58-306: 2010 Corporate Governance Disclosure Compliance Review.*
Canadian Standards Association (CSA). 1997. *CAN/CSA-Q850-97: Risk Management—Guideline for Decision-Makers*.
——. 2010. *CSA-ISO 31000-10: Risk Management—Principles and Guidelines*.
Clemen, R. 1996. *Making Hard Decisions: An Introduction to Decision Analysis, 2nd Ed*. Pacific Grove: Duxbury Press.
Committee of Chief Risk Officers (CCRO). 2002. *Governance and Controls (Volume 2 of 6).*
——. 2006. *Enterprise Risk Management and Supporting Metrics*.
Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise Risk Management: Integrated Framework*.
——. 2009a. *Effective Enterprise Risk Oversight: The Role of the Board of Directors*.
——. 2009b. *Strengthening Enterprise Risk Management for Strategic Advantage*.
——. 2010. *Board Risk Oversight: A Progress Report*.
——. 2012. *Understanding and Communicating Risk Appetite*.
Committee on Corporate Governance (CCG). 1998. *Final Report ("Hampel Report").*
Conference Board (CB). 2005. *From Risk Management to Risk Strategy*.
——. 2006. *The Role of U.S. Corporate Boards in Enterprise Risk Management*.
——. 2009. *Corporate Governance Handbook: Legal Standards and Board Practices, 3rd Ed.*
——. 2010. *The Role of the Board in Risk Oversight*.
Conference Board of Canada (CBOC). 2005. *Enterprise Risk Management: Inside and Out*.
——. 2008. *Risk, Governance, and Corporate Performance: A Board's-Eye View*.
——. 2011. *Enterprise Risk Management: A Review of Prevalent Practices*.
Corbin, J., & Strauss, A. 2008. *Basics of Qualitative Research, 3rd Ed*. Thousand Oaks: Sage.
Corporate Governance Council (CGC). 2012. *Risk Governance Guidance for Listed Boards [Singapore]*.
Council of Institutional Investors (CII). 2011. *Corporate Governance Policies*.
Counterparty Risk Management Policy Group (CRMPG). 2008. *Containing Systemic Risk: The Road to Reform*.
Cronin, P., & Murphy, F. (Eds.). 2012. *Corporate Governance for Main Market and AIM Companies*. London: London Stock Exchange.
Cyert, R., & March, J. 1992. *A Behavioral Theory of the Firm, 2nd Ed*. Malden: Blackwell.
Deloitte & Touche (D&T). 2009a. *Getting Bank Governance Right*.
——. 2009b. *Risk Intelligent Governance*.
——. 2011a. *Global Risk Management Survey [Financial Services], 7th Ed.*
——. 2011b. *Risk Intelligent Proxy Disclosures*.
——. 2012. *Risk Committee Resource Guide for Boards*.
Department of Trade and Industry (DTI). 2003. *Review of the Role and Effectiveness of Non-Executive Directors ("Higgs Report").*
Diebold, F., Doherty, N., & Herring, R. (Eds.). 2010. *The Known, the Unknown, and the Unknowable in Financial Risk Management*. Princeton: Princeton University Press.
Donaldson, L. 1999. *Performance-Driven Organizational Change: The Organizational Portfolio*. Thousand Oaks: Sage.
Drucker, P. 1954. *The Practice of Management*. New York: Harper & Row.
Eaton, C. 2010. What does risk integration look like, really? *Risk Watch*, September: 2-4.

——. 2011. *The Adoption and Diffusion of Risk Governance Structures and Practices*. Ottawa: Conference Board of Canada.
Ebsary, J. 2011. *ERM and the Canada Mortgage and Housing Corporation (CMHC): Developing and Applying a Risk Appetite Framework*.
Economist Intelligence Unit (EIU). 2009. *Beyond Box-Ticking: A New Era for Risk Governance*.
Edwards, W., Miles, R., & Von Winterfeldt, D. (Eds.). 2007. *Advances in Decision Analysis: From Foundations to Applications*. Cambridge: Cambridge University Press.
Elkington, J. 1998. *Cannibals with Forks: The Triple Bottom Line of 21st Century Business*. Gabriola Island: New Society.
Enterprise Risk Management Initiative (ERMI). 2009. *Current State of Enterprise Risk Oversight, 1st Ed.*
——. 2010. *Current State of Enterprise Risk Oversight, 2nd Ed.*
——. 2011. *Current State of Enterprise Risk Oversight, 3rd Ed.*
——. 2012. *Current State of Enterprise Risk Oversight, 4th Ed.*
Ernst & Young (E&Y). 2010. *Risk Appetite: The Strategic Balancing Act*.
European Banking Authority (EBA). 2011. *Guidelines on Internal Governance*.
Federal Reserve System (FRS). 2011. *Trading and Capital Markets Activities Manual*.
——. 2012. Proposed rules—Enhanced prudential standards and early remediation requirements for covered companies. *Federal Register*, 77(3): 594-663.
Finance Canada (FC). 2009. *Minister of Finance Financial Risk Management Guidelines for Crown Corporations*.
Financial Reporting Council (FRC). 2005. *Internal Control: Revised Guidance for Directors on the Combined Code*.
——. 2009. *Going Concern and Liquidity Risk: Guidance for Directors of UK Companies*.
——. 2011a. *Guidance on Board Effectiveness*.
——. 2011b. *Boards and Risk: A Summary of Discussions with Companies, Investors and Advisers*.
——. 2011c. *Developments in Corporate Governance: The Impact and Implementation of the UK Corporate Governance and Stewardship Codes*.
——. 2012a. *The UK Corporate Governance Code*.
——. 2012b. *The UK Approach to Corporate Governance*.
——. 2012c. *Guidance on Audit Committees*.
Financial Reporting Review Panel (FRRP). 2011a. *Press Notice 130*.
——. 2011b. *Annual Report*.
Financial Services Authority (FSA). 2010. *Effective Corporate Governance*.
——. 2011a. *SYSC 21: Risk Control—Additional Guidance*. In FSA Handbook.
——. 2011b. *The Failure of the Royal Bank of Scotland*.
Finkelstein, S., Hambrick, D., & Cannella, A. 2009. *Strategic Leadership: Theory and Research on Executives, Top Management Teams, and Boards*. Oxford: Oxford University Press.
Fischhoff, B. (Ed.). 2012. *Risk Analysis and Human Behavior*. New York: Earthscan.
Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S., & Keeney, R. 1981. *Acceptable Risk*. Cambridge: Cambridge University Press.
Fox, C., Bugalla, J., & Narvaez, K. 2011. *An Evolving Model for Board Risk Governance*. Risk and Insurance Management Society (RIMS).
Fraser, J., & Simkins, B. (Eds.). 2010. *Enterprise Risk Management*. Hoboken: John Wiley & Sons.
Funston, R., & Wagner, S. 2010. *Surviving and Thriving in Uncertainty: Creating the Risk Intelligent Enterprise*. Hoboken: John Wiley & Sons.
Gandz, J. 2012. *Risk Leadership at TD Bank Group*. Ivey Case 9B12C001.
Gomory, R. 1995. The known, the unknown and the unknowable. *Scientific American*, 272(6): 120.
Govindarajan, D. 2011. *Corporate Risk Appetite: Ensuring Board and Senior Management Accountability for Risk*. ICMA Centre Discussion Papers in Finance DP2011-22.

Graham, J., & Wiener, J. (Eds.). 1995. *Risk vs. Risk: Tradeoffs in Protecting Health and the Environment*. Cambridge, MA: Harvard University Press.
Gregory, R., Failing, L., Harstone, M., Long, G., McDaniels, T., & Ohlson, D. 2012. *Structured Decision Making: A Practical Guide to Environmental Management Choices*. Chichester: Wiley-Blackwell.
Greve, H. 2003. *Organizational Learning from Performance Feedback: A Behavioral Perspective on Innovation and Change*. Cambridge: Cambridge University Press.
Group of Thirty (G30). 2012. *Toward Effective Governance of Financial Institutions*.
Hammond, J., Keeney, R., & Raiffa, H. 1999. *Smart Choices: A Practical Guide to Making Better Life Decisions*. New York: Broadway Books.
Harner, M. 2010. Ignoring the writing on the wall: The role of enterprise risk management in the economic crisis. *Journal of Business & Technology Law*, 5(1): 45-58.
Harvard Business Review Analytic Services (HBRAS). 2011. *Risk Management in a Time of Global Uncertainty*.
Her Majesty's Treasury (HMT). 2004. *Management of Risk—Principles and Concepts ("Orange Book")*.
——. 2006. *Managing Your Risk Appetite: A Practitioner's Guide*.
——. 2011. *Corporate Governance in Central Government Departments: Code of Good Practice*.
Hillson, D., & Murray-Webster, R. 2007. *Understanding and Managing Risk Attitude, 2nd Ed*. Aldershot: Gower.
——. 2012. *A Short Guide to Risk Appetite*. Aldershot: Gower.
Hu, S., Blettner, D., & Bettis, R. 2011. Adaptive aspirations: Performance consequences of risk preferences at extremes and alternative reference groups. *Strategic Management Journal*, 32: 1426-1436.
Hutter, B., & Power, M. (Eds.). 2005. *Organizational Encounters with Risk*. Cambridge: Cambridge University Press.
IBM. 2008. *Risk Appetite: A Multifaceted Approach to Risk Management*.
Information Technology Governance Institute (ITGI). 2003. *Board Briefing on IT Governance, 2nd Ed.*
Institute of Chartered Accountants of England and Wales (ICAEW). 1999. *Internal Control: Guidance for Directors on the Combined Code ("Turnbull Report")*.
——. 2009. *Getting it Right: Risk Governance in Non-Financial Services Companies*.
Institute of Corporate Directors/Toronto Stock Exchange (ICD/TSX). 1999. *Report on Corporate Governance: Five Years to the Dey*.
Institute of Directors (IOD). 2012. *Business Risk: A Practical Guide for Board Members*.
Institute of Directors in Southern Africa (IODSA). 2009. *King Code of Governance for South Africa*.
Institute of International Finance (IIF). 2008. *Final Report of the IIF Committee on Market Best Practices: Principles of Conduct and Best Practice Recommendations*.
——. 2009. *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System*.
——. 2011. *Implementing Robust Risk Appetite Frameworks to Enhance Financial Institutions*.
Institute of Risk Management (IRM). 2011. *Risk Appetite & Tolerance Guidance Paper*.
——. 2012. *Risk Culture Guidance Paper (Working Draft)*.
Institutional Shareholder Services (ISS). 2012a. *Canadian Proxy Voting Guidelines: TSX-Listed Companies*.
——. 2012b. *U.S. Proxy Voting Summary Guidelines*.
International Corporate Governance Network (ICGN). 2009. *Global Corporate Governance Principles (Revised)*.
——. 2010. *Corporate Risk Oversight Guidelines*.
International Finance Corporation (IFC). 2012. *Risk Taking: A Corporate Governance Perspective*.
International Organization for Standardization (ISO). 2009a. *ISO Guide 73: Risk Management—Vocabulary*.

——. 2009b. *ISO 31000: Risk Management—Principles and Guidelines*.
——. 2009c. *IEC/ISO 31010: Risk Management—Risk Assessment Techniques*.
International Risk Governance Council (IRC). 2008. *An Introduction to the IRGC Risk Governance Framework*.
Joint Committee on Corporate Governance (JCCG). 2001. *Beyond Compliance: Building a Governance Culture*.
Kahneman, D. 2011. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.
Kaplan, R., & Norton, D. 1996. *The Balanced Scorecard: Translating Strategy into Action*. Boston: Harvard Business School Press.
Keeney, R. 1992. *Value-Focused Thinking: A Path to Creative Decision Making*. Cambridge: Harvard University Press.
Keeney, R., & Raiffa, H. 1993. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. Cambridge: Cambridge University Press.
Kluckhohn, C. 1951. Values and value-orientations in the theory of action: An exploration in definition and classification. In T. Parsons & E. Shils (Eds.), *Toward a General Theory of Action*: 388-433. Cambridge: Harvard University Press.
Koenig, D. 2012. *Governance Reimagined: Organizational Design, Risk, and Value Creation*. Hoboken: John Wiley & Sons.
Kolb, R., & Schwartz, D. (Eds.). 2010. *Corporate Boards: Managers of Risk, Sources of Risk*. Chichester: Wiley-Blackwell.
KPMG. 2009. *Understanding and Articulating Risk Appetite*.
——. 2011a. *Risk Management: A Driver of Enterprise Value in the Emerging Environment*.
——. 2011b. *Using Risk Appetite to Drive Value*.
Læssøe, H. 2011. A practical approach to risk appetite. *Risk Watch*, September: 12-16.
Lant, T. 1992. Aspiration level adaptation: An empirical exploration. *Management Science*, 38: 623-644.
Lant, T., & Shapira, Z. 2008. Managerial reasoning about aspirations and expectations. *Journal of Economic Behavior & Organization*, 66: 60-73.
Lewin, K., Dembo, T., Festinger, L., & Sears, P. 1944. Level of aspiration. In J. Hunt (Ed.), *Personality and the Behavior Disorders*: 333-378. New York: Ronald Press.
Lichtenstein, S., & Slovic, P. (Eds.). 2006. *The Construction of Preference*. Cambridge: Cambridge University Press.
Lloyd's. 2012. *Risk Management Toolkit*.
Locke, E., & Latham, G. 1990. *A Theory of Goal Setting and Task Performance*. Englewood Cliffs: Prentice-Hall.
London Stock Exchange. 2004. *Corporate Governance: A Practical Guide*.
Lopes, L. 1987. Between hope and fear: The psychology of risk. *Advances in Experimental Social Psychology*, 20: 255-295.
Lucas, A. 2012. *Lloyd's Approach to Risk Appetite*.
MacCrimmon, K., & Wehrung, D. 1986. *Taking Risks: The Management of Uncertainty*. New York: Free Press.
March, J. (Ed.). 1988. *Decisions and Organizations*. Oxford: Basil Blackwell.
——. 1994. *A Primer on Decision Making: How Decisions Happen*. New York: Free Press.
——. (Ed.). 1999. *The Pursuit of Organizational Intelligence*. Malden: Blackwell.
March, J., & Shapira, Z. 1982. Behavioral decision theory and organizational decision theory. In G. Ungson & D. Braunstein (Eds.), *Decision Making: An Interdisciplinary Inquiry*: 92-115. Boston: Kent.
——. 1987. Managerial perspectives on risk and risk-taking. *Management Science*, 33: 1404-1418.
March, J., & Simon, H. 1958. *Organizations*. New York: Wiley.
McKinsey. 2010. *A Board Perspective on Enterprise Risk Management*. Working Papers on Risk, 18.

Meyer, M. 2002. *Rethinking Performance Measurement: Beyond the Balanced Scorecard*. Cambridge: Cambridge University Press.
Mikes, A. 2008. *Enterprise Risk Management at Hydro One*. Harvard Business School Case 9-109-001.
Miller, K. 2009. Organizational risk after modernism. *Organization Studies*, 30: 157-180.
Murray-Webster, R., & Hillson, D. 2008. *Managing Group Risk Attitude*. Aldershot: Gower.
National Association of Corporate Directors (NACD). 2002. *Risk Oversight: Board Lessons for Turbulent Times*.
——. 2009a. *Risk Governance: Balancing Risk and Reward*.
——. 2009b. *Public Company Governance Survey*.
——. 2011. *Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly Traded Companies*.
National Research Council (NRC). 1996. *Understanding Risk: Informing Decisions in a Democratic Society*. Washington: National Academy Press.
New York Stock Exchange (NYSE). 2010. *Report of the NYSE Commission on Corporate Governance*.
——. 2012. *Listed Company Manual*.
Niven, P. 2002. *Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results*. New York: John Wiley & Sons.
Office of Government Commerce (OGC). 2010. *Management of Risk: Guidance for Practitioners, 3rd Ed*.
Office of the Superintendent of Financial Institutions (OSFI). 2003. *Corporate Governance Guideline*.
——. 2012. *Corporate Governance of Federally Regulated Financial Institutions (Draft)*.
Oliver Wyman. 2007. *What's Your Risk Appetite?*
——. 2008. *Risk Governance: Seeing the Forest for the Trees*.
——. 2009. *Risk Governance: Post-Crisis Priorities*.
Ontario Teachers' Pension Plan (OTPP). 2012. *Good Governance is Good Business: Corporate Governance Principles and Proxy Voting Guidelines*.
Open Compliance & Ethics Group (OCEG). 2009. *GRC Capability Model "Red Book" 2.0*.
Organisation for Economic Co-operation and Development (OECD). 2004. *Principles of Corporate Governance*.
——. 2005. *Guidelines on Corporate Governance of State-Owned Enterprises*.
——. 2006. *Methodology for Assessing the Implementation of the Principles of Corporate Governance*.
——. 2008. *The Corporate Governance Lessons from the Financial Crisis*.
——. 2009. *Corporate Governance and the Financial Crisis: Key Findings and Main Messages*.
——. 2010. *Corporate Governance and the Financial Crisis: Conclusions and Emerging Good Practices to Enhance Implementation of the Principles*.
——. 2011. *Board Practices: Incentives and Governing Risks*.
Pan, E. 2010. *The Duty to Monitor under Delaware Law: from* Caremark *to* Citigroup. New York: Conference Board.
Pidgeon, N., Kasperson, R., & Slovic, P. (Eds.). 2003. *The Social Amplification of Risk*. Cambridge: Cambridge University Press.
PricewaterhouseCoopers (PwC). 2004. *Risk Appetite: How Hungry are You?*
——. 2012. *Annual Corporate Directors Survey*.
Professional Risk Managers' International Association (PRMIA). 2009. *Principles of Good Governance*.
Protiviti. 2010. The current state of board risk oversight. *The Bulletin*, 4(4): 1-4.
——. 2011. *Formulating an Initial Risk Appetite Statement*.
Risk and Insurance Management Society (RIMS). 2012. *Exploring Risk Appetite and Risk Tolerance*.
Rokeach, M. 1973. *The Nature of Human Values*. New York: Free Press
Rosa, E. 1998. Meta-theoretical foundations for post-normal risk. *Journal of Risk Research*, 1: 15-44.

Savitz, A., & Weber, K. 2006. *The Triple Bottom Line: How Today's Best-Run Companies are Achieving Economic, Social, and Environmental Success*. San Francisco: Jossey-Bass.
Schoemaker, P., & Tetlock, P. 2012. Taboo scenarios: How to think about the unthinkable. *California Management Review*, 54(2): 5-24.
Securities and Exchange Commission (SEC). 2009. *Final Rule—Proxy Disclosure Enhancements*.
Securities Commission Malaysia (SCM). 2012. *Malaysian Code on Corporate Governance*.
Senior Supervisors Group (SSG). 2008. *Observations on Risk Management Practices During the Recent Market Turbulence*.
——. 2009. *Risk Management Lessons from the Global Banking Crisis of 2008 and Self-Assessment Template*.
——. 2010. *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure*.
Shapira, Z. 1995. *Risk Taking: A Managerial Perspective*. New York: Russell Sage Foundation.
——. (Ed.). 1997. *Organizational Decision Making*. Cambridge: Cambridge University Press.
Simkins, B., & Ramirez, S. 2008. Enterprise-wide risk management and corporate governance. *Loyola University Chicago Law Journal*, 39: 571-594.
Sitkin, S., & Pablo, A. 1992. Reconceptualizing the determinants of risk behavior. *Academy of Management Review*, 17: 9-38.
Slovic, P. (Ed.). 2000. *The Perception of Risk*. London: Earthscan.
Slovic, P., Finucane, M., Peters, E., & MacGregor, D. 2004. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis*, 24: 311-322.
Standard & Poor's (S&P). 2006a. *ERM: The New Standard and Practice in Good Corporate Governance*.
——. 2006b. *Evaluating Risk Appetite: A Fundamental Process of Enterprise Risk Management*.
Standards Australia & Standards New Zealand (SA/NZS). 2004a. *AS/NZS 4360: Risk Management—Standard*.
——. 2004b. *AS/NZS 4360: Risk Management—Guidelines*.
Strategy Unit (SU). 2002. *Risk: Improving Government's Capability to Handle Risk and Uncertainty*. London: United Kingdom Cabinet Office.
TD Bank Group (TD). 2011. *Annual Report*.
Thompson, J. 1967. *Organizations in Action*. New York: McGraw-Hill.
Toronto Stock Exchange (TSX). 1994. *Where Were the Directors? ("Dey Report")*.
——. 2006. *Guide to Good Disclosure for NI 58-101 and MI 52-110*.
Towers Perrin. 2010. *Risk Appetite: The Foundation of Enterprise Risk Management*.
Treasury Board Secretariat (TBS). 2005. *Meeting the Expectations of Canadians: Review of the Governance Framework for Canada's Crown Corporations*.
——. 2010. *Framework for the Management of Risk*.
United Nations Conference on Trade and Development (UNCTAD). 2006. *Guidance on Good Practices in Corporate Governance Disclosure*.
University of Alberta (UofA). 2005. *Risk Management Policy: Appendix A—Risk Appetite Statement*.
Valukas, A. 2010. *Report of the Bankruptcy Examiner for Lehman Brothers Holdings Inc*.
Van de Ven, A. 2007. *Engaged Scholarship: A Guide for Organizational and Social Research*. Oxford: Oxford University Press.
Walker Review Secretariat (Walker). 2009. *A Review of Corporate Governance in UK Banks and Other Financial Industry Entities: Final Recommendations ("Walker Report")*.
Weber, E. 2010. Risk attitude and preference. *WIREs Cognitive Science*, 1: 79-88.
Weber, E., Baron, J., & Loomes, G. (Eds.). 2001. *Conflict and Tradeoffs in Decision Making*. Cambridge: Cambridge University Press.
Yates, J. (Ed.). *Risk-Taking Behavior*. Chichester: John Wiley & Sons.
Yin, R. 2009. *Case Study Research: Design and Methods, 4th Ed*. Thousand Oaks: Sage.

APPENDIX A—KEY ACCEPTABLE RISK TERMS (WITH DETAILS)

risk	effect of uncertainty on one or more value(s) 1. *often characterized by reference to potential event(s) and associated consequence(s) with respect to value(s), or a combination thereof;* 2. *often expressed in terms of a combination of the consequences of event(s) with respect to value(s) and the associated likelihood of occurrence of the event(s);* 3. *may also be characterized by reference to and/or expressed in terms of one or more other underlying characteristic(s) (e.g., velocity, controllability, voluntariness).*
effect	positive and/or negative deviation from the desired 1. *often characterized by reference to differences between past, present, and/or future (e.g., expected or forecasted) results(s) and target(s) over time or at a point in time;* 2. *often expressed in terms of appropriateness or preference, where past, present, and/or future (e.g., expected or forecasted) outcome(s) are compared with target(s);* 3. *often expressed in terms of achievement or performance, where past, present, and/or future (e.g., expected or forecasted) outcome(s) are compared with target(s).*
uncertainty	state, even partial, of deficiency of information related to, understanding or knowledge of, or confidence in event(s) or value(s) and/or any relevant underlying characteristic(s)
value	aspiration or goal and associated outcome(s) considered desirable 1. *often expressed in general terms as vision, mission, mandate, and/or principle(s);* 2. *often expressed in specific terms as objective(s), along with associated indicator(s), target(s), and one or more other reference point(s);* 3. *often influenced by past, present, and/or future (e.g., expected or forecasted) effect(s) of a focal entity and/or one or more reference entity(ies);* 4. *can apply in different domains (e.g., strategic, financial, operational, social), at different stages in a causal chain (e.g., means, ends), and/or at different units and/or levels of analysis (e.g., organization, subunit, group, program, project, product, process).*
risk criteria	terms of reference for evaluating the significance and acceptability of risk(s) 1. *can be influenced, determined, adjusted, monitored, and/or enforced by external entities (e.g., through resources, laws, regulations, orders, reviews, audits, fines, penalties);* 2. *often includes risk capacity, risk appetite, and/or risk tolerance(s).*
risk attitude	disposition toward risk(s) and any associated decisions and/or actions
risk capacity	nature and extent of risk(s) an entity is able to accept in aggregate 1. *often characterized by reference to value(s), event(s), and their associated effect(s);* 2. *often expressed in terms of one or more threshold(s) a focal entity must not breach;* 3. *should be at least as broad and extensive as risk appetite.*
risk appetite	nature and extent of risk(s) an entity is willing to accept in aggregate 1. *often characterized by reference to value(s), event(s), and their associated effect(s);* 2. *often characterized by reference to the aggregation of applicable risk tolerances;* 3. *often expressed in terms of one or more threshold(s) a focal entity should not breach;* 4. *should be consistent with and no broader nor extensive than risk capacity.*
risk tolerance	nature and extent of risk(s) an entity, or a part thereof, is willing to accept with respect to any relevant underlying characteristic(s) and/or set(s) thereof 1. *often characterized by reference to value(s), event(s), and their associated effect(s);* 2. *also characterized by reference to entity(ies), location(s), asset(s), liability(ies), etc.;* 3. *often expressed in terms of acceptable variation around one or more target(s);* 4. *should be consistent with and no broader nor extensive than risk appetite.*
risk profile	set of risks related to an entity or a part thereof

Sources: Derived from ISO (2009a), FRC (2012a), COSO (2012), Keeney (1992), March (1994, 1999), Shapira (1995).

APPENDIX B—ILLUSTRATIVE RISK GOVERNANCE REFERENCES

Jurisdiction	Rules/Guidelines	Standards/Frameworks	Evaluations/Proposals	Studies/Perspectives
Canada	CSA (2005a, 2005b) OSFI (2003, 2012) TBS (2005, 2010) FC (2009)	CSA (1997, 2010) TSX (2006) CICA (2006, 2008, 2012)	TSX (1994) ICD/TSX (1999) JCCG (2001) CCGG (2010) OTPP (2012) ISS (2012a)	CBOC (2005, 2008, 2011) Eaton (2010, 2011)
United Kingdom	FRC (2005, 2012a) FSA (2010, 2011a) SU (2002) HMT (2004, 2011)	FRC (2009, 2011a, 2012c) BSI (2009, 2011) HMT (2006) OGC (2010) IRM (2011, 2012)	CCG (1998) ICAEW (1999) DTI (2003) FRC (2011b, c, 2012b) Walker (2009) AIC (2010) IOD (2012)	Murray-Webster & Hillson (2008) Hillson & Murray-Webster (2012) ICAEW (2009) AIRMIC (2009, 2010) Ashby & Diacon (2010) Govindarajan (2011) Cronin & Murphy (2012) Lloyd's (2012)
United States	NYSE (2012) SEC (2009) FRS (2011, 2012)	NYSE (2010) COSO (2004, 2009a, 2012) CCRO (2002, 2006) PRMIA (2009) BRT (2010) NACD (2011) ABA (2011)	NRC (1996) NACD (2002, 2009a) S&P (2006a, b) CalPERS (2011) CII (2011) ISS (2012b) RIMS (2012)	CB (2005, 2006, 2009, 2010) ERMI (2009, 2010, 2011, 2012) Buehler et al. (2008) Bainbridge (2009), Harner (2010) Pan (2010) NACD (2009b), COSO (2010) Kolb & Schwartz (2010) Diebold et al. (2010) Fox et al. (2011), Koenig (2012)
Multilateral/other	OECD (2004, 2005) IODSA (2009) ASX (2010) ICGN (2009, 2010) EBA (2011) BCBS (2011) CGC (2012) SCM (2012)	OECD (2006, 2011) SA/SNZ (2004a, b) ISO (2009a, b, c) UNCTAD (2006)	OECD (2008, 2009, 2010) SSG (2008, 2009, 2010) BCBS (2010a) CRMPG (2008) IIF (2008, 2009, 2011) G30 (2012)	D&T (2009a, b, 2011a, b, 2012) E&Y (2010), PwC (2004, 2012) KPMG (2009, 2011a, b) OW (2007, 2008, 2009) Booz (2009a, b), McKinsey (2010) IBM (2008), Protiviti (2010, 2011) AON (2010), TP (2010) Fraser & Simkins (2010) EIU (2009), HBRAS (2011)