Enterprise Risk Management

How do we govern it?

Canadian Institute of Actuaries
Institut canadien des actuaires

Essays on Risk Governance: ERM – How do we govern it?

Effective risk management requires an unwavering dedication to one thing—everything. Holistic management of risk is not fulsome when it ignores what is difficult to identify and assess. As such, the goals of risk management to manage and mitigate the risks faced by an organization will fall short without active, engaged, and meaningful governance.

In risk management, there are often more questions than answers. Picking up on that theme, the idea behind this publication is to ask a series of questions on the topic of risk governance, and then ask knowledgeable practitioners why contemplating such questions is relevant.

In the pages that follow, you will read from a series of authors who represent a wide swath of perspectives and experiences. The topics presented span from assessing an entity's governance structure to identifying the right risks; from the importance of cultivating a positive risk culture to understanding an organization's risk capacity. Topics address the importance of establishing a risk policy, linking risk management and strategic direction, the art and science of risk measurement, and the guidance provided by a well-articulated risk appetite.

Resilience does not just occur, it is crafted, and the governance of risk plays a significant role in the development of that resiliency. The design of an organization's enterprise risk management (ERM) program should consider the questions presented within these essays with the ultimate goals being to establish a clear sense of the risks faced, construct a meaningful approach to managing and measuring these risks, and foster ongoing dialogue in addressing any identified gaps.

The Canadian Institute of Actuaries' Enterprise Risk Management Applications Committee (ERMAC) would like to recognize the contributions of our committed volunteers, the many valued authors, and the efforts of the staff at the CIA Head Office. This initiative would not have seen the light of day if not for their involvement.

What is our Governance Structure?

Good governance can be viewed as the lifeblood of an organization and the governance structure as the heart of its operations. Reviewing the governance structure can and should be an ongoing process by organizations at many levels: individual, sectorial, national, and international.

Globally, the principles of governance are being reviewed by the Organization for Economic Co-operation and Development (OECD).

Given the increasing challenges to economic stability and global competitive pressures, the relevance of the current governance structure in facing the current and future reality is not only timely, but essential. It relates to the importance of long-term thinking and ERM to ensure business sustainability in all sectors: public and private, financial and non-financial.

The term governance structure refers generally to the procedures and processes according to which an organization is directed and controlled. This definition could apply to both the public and private sectors.

In the private sector, "the corporate governance structure specifies the distribution of rights and responsibilities among the different participants in [an organization]—such as the board, managers, shareholders, and other stakeholders—and lays down the rules and procedures for decision-making."[1]

Most organizations will disclose the governance structure publicly as it is key to achieving their missions and strategic plans. However, there is a wide variance in how comprehensive the description is. For example, the role of risk management at the enterprise level may not be mentioned. However, this may be changing following the financial crisis of 2008. Also, rating agencies are now incorporating ERM in their rating assessments.

Most financial institutions are committed to ERM as part of the governance structure. As an example, the TD Bank Financial Group outlines the key responsibilities of its Board Risk Committee:

Supervising the management of risk of TD:

- Approve Enterprise Risk Framework (ERF) and related risk category frameworks and policies that establish the appropriate approval levels for decisions and other measures to manage risk to which TD is exposed.
- Review and recommend TD's Risk Appetite Statement and related metrics for approval by the Board and monitor TD's major risks as set out in the ERF.

- Review TD's risk profile against Risk Appetite metrics.
- Provide a forum for big-picture analysis of an enterprise view of risk, including considering trends and emerging risks.[2]

At the global level, the OECD corporate governance principles peer review process is ongoing and open to OECD and non-OECD jurisdictions. An exchange of experiences and expertise "provides participants with an overview of existing practices and approaches and an opportunity to identify good practices that can stimulate and guide improvements. The reviews are also forward looking, so as to help identify key market practices and policy developments that may undermine the quality of corporate governance."[3]

In addition to corporations, effective risk management is critical at the national level. At a meeting in Paris of the OECD Council at Ministerial Level in May 2014, the OECD recommended that "(m)embers establish and promote a comprehensive all-hazards and transboundary approach to country risk governance to serve as a foundation for enhancing national resilience and responsiveness."[4]

Perhaps the question should be rephrased to ask: Does our current governance structure include ERM and ensure the long-term sustainability of our mission, be it private or public? The actuarial profession has been asking the deeper questions about enterprise risk, including long-term sustainability and the application of actuarial skills to innovative and systemic solutions for decision-makers at the board level.

– by Shannon Patershuk

What's Our Risk Culture?

This may be the single most important question to ask of the risk management function and the organization as a whole. Unfortunately, it may also be the topic discussed least often.

An entity's risk culture describes the values and behaviours that affect risk-related decision making. An unsupportive risk culture can lead to a chasm between the anticipated and realized benefits of risk management. This gap occurs not because of unskilled people or a lack of resources, but because the risk culture does not promote the right values and behaviours, such as accountability and an effective challenge of the company's initiatives and strategies.

Understanding an organization's risk culture, and in particular what elements it lacks, is a fundamental first step to cultivating a culture that is supportive of the types of behaviours that produce strong risk management practices. Look in any publication on the topic of risk culture and you will find principles that may resemble the following:

- Establish an appropriate tone at the top regarding the accepted level of risk-taking;

- Demand accountability in the management of the key risks faced;
- Create an effective challenge process rooted in improving the enterprise;
- Establish a strong ethical compass that articulates behavioural expectations; and
- Incentivize decision-making that accounts for risk.

The above list reads like an annual report to shareholders; it says all the right things, but leaves the reader wondering if the theory truly matches the practice. Right there is where the difficulty lies. Taking the ideologies and knowing what steps are needed in order to make the theory a reality has never been a trivial matter.

An observable process that can add value to everyday decision-making,

generate movement from theory to practice, and improve an enterprise's risk culture is to treat the decision-making process as an experiment. In part, risk culture pertains to the knowledge and understanding about risk that is shared by a group of people with a common purpose. When structured and executed correctly, experiments can generate critical findings and advance an organization's understanding of risk—regardless of the experiments' outcome.

For some, engaging in this type of activity will prove difficult as it asks the decision maker to acknowledge that they may not know the optimal decision. For others, admitting that the enterprise is vulnerable to a shifting landscape of risk will come naturally, as their experience has shown them that change is inevitable.

A well-designed experiment will include a clearly articulated potential outcome or goal, an observable measure that allows for the determination of success or failure, and a mechanism for providing feedback for continuous learning. This approach promotes accountability, challenges the assumptions made during the experiment, seeks to actively learn from mistakes, and acts as a source of further understanding of the risks.

– by Mark Struck

Do We Have an Effective Risk Policy?

The compelling question you should be asking as a board member is whether your organization is really pursuing ERM. Most organizations respond with a resounding yes. However, a significant number of them pursue risk management, but do not pursue ERM systematically across the enterprise. If you are pursuing ERM, or planning to implement it, the critical item is to ensure that there is a risk policy.

A risk policy encapsulates the risk management guidelines of your organization. It clearly articulates the risk appetite (the level of risk that an organization is prepared to accept to support its business strategy and objectives). The risk appetite is then cascaded to the business unit or department level, and the risk tolerance (the specific maximum risk that the organization is willing to take for specific categories of risk such as strategic, financial, operational, and regulatory) is clearly articulated. Specifically, risk targets—the maximum level of risk acceptable for each risk factor within a risk category—should be set. For example, for the financial risk category, specific risk factors such as interest rate, cash flow, currency, and commodity must be defined at the business unit or department level.

The implementation of risk policy is effective only if there is a robust risk culture and risk governance within your organization.

An enterprise's risk culture can be defined as the system of values and behaviours that shape risk decisions. An organization with a strong risk culture can influence the decisions of the board, management, and employees even if they are not consciously weighing risks and benefits. An element of a risk culture is having a well-defined risk taxonomy standard, or risk speak. This allows for easy communication, discussion, and monitoring of risk among everyone in the organization.

Risk governance provides for effective delegation, coordination, and facilitation of ERM by clearly laying out procedures, trigger points, and escalation processes at the designated authority levels as defined in the risk policy. The risk sponsor has the overall accountability for management of a specific risk, the risk owner has the responsibility of managing and coordinating all aspects of that risk, and the controller is responsible for management and execution of controls and actions for it.

Effective risk policy management results if there is an efficient flow of risk information and monitoring among the sponsor, owner, and controller across an enterprise on a timely basis, and clear reporting to management and the board of well-defined risk metrics (e.g., risk-adjusted measures) with line of sight to the business strategy and objectives.

– by Minaz Lalani

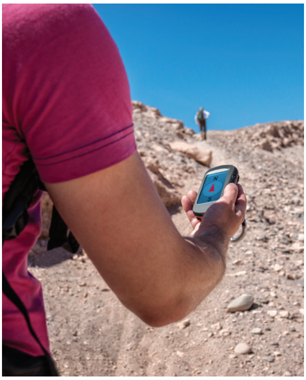
How is Enterprise Risk Management Helping to Inform Our Strategic Direction?

In addressing this question, it is important to consider the link between ERM and a company's strategic direction. Regardless of industry or sector, a structured strategic plan is based on a strong understanding of the level of risk a company will choose to assume in its day-to-day business activities.

An ERM framework can help a company understand its risks and, accordingly, address why it is important in setting a strategic direction. In asking the question, "How is ERM helping to inform our strategic direction?" staff and board members can gain a better idea as to how the company and its management truly understand the risks inherent in their business.

When the aforementioned question is asked of management, board members should be looking for three things:

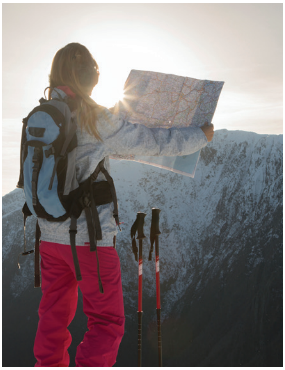
- The identification of risks the company will encounter (whether internal to the company's operation or from external factors, including environmental factors);
- The quantification of those risks (usually in estimated dollar amounts that impact earnings or the balance sheet) and what impact they will have in an economically stressed environment; and
- How these risks can be mitigated, if at all, and what are some of the consequences of the mitigation (e.g., does a partner who agrees to assume these risks have the financial strength to absorb them in times of stress—also known as counterparty risk).



Generally, the ERM plan should show how thoroughly and diligently company management, through its risk management function or its chief risk officer, has thought about risk. As management gives its directors or other stakeholders answers to the questions above, board members should be scratching beneath the surface to feel comfortable with answers to the following:

- Have all risks—including those that appear to be a result of implausible events—been considered in the identification process?
- Would any risk, or any collection of risks that arise together (or in a correlated way), pose undue danger to the company's strategic plan—and its ability to operate within it—or financial health?
- If identified risks are mitigated in some way, what are the consequences if that mitigation strategy failed, and how does this failure impact the company?

As an ERM process is being designed, it should also take account of the various stakeholders who may have an interest in the company's well-being and its



strategic direction. Together with the board members, the plan would also address communications with the management, employees, customers, suppliers, regulators, and financial counterparties (banks, creditors, and investors, including shareholders). Where a company is in the public domain and has a service or product important to the public at large (e.g., an electrical utility), a communication strategy must also be considered. The ERM plan and its link to its strategic plan should also feature an understanding of competitors.

As noted above, specific terms should be addressed in the ERM process and plan, including:

- The identification of risks and risk events;
- The quantification of the risks and common risk events;
- The quantification of the effect of risk mitigation strategies;
- The likelihood of risk events occurring; and
- A list of highly unlikely, highly impactful risk events and their financial effect.

In many instances, certain risk events are difficult to measure and if so, an estimation of the event—such as loss in revenue, loss in earnings, or balance sheet loss (capital)—should be considered.

As an ongoing feedback loop, when the board reviews the company's strategic direction and assesses it, members should ask themselves and management why the managers have chosen to assume such a level of risk and whether that is within the company's financial strength as noted in the ERM plan.

By discussing these questions and regularly updating the ERM plan (for example, a quarterly update of the risks' impact and an annual update of the risk profile), board members and external constituents should gain a thorough understanding of the ERM process, how it is integrated to the organization's strategy, and what plans can be invoked in case of an extraordinary event or any failure of risk mitigation.

– by Gaetano Geretto

What is Our Risk Capacity?

Financial institutions face a broad range of risks and opportunities, and for many the potential exposures can be significant. It is therefore important that these organizations understand the maximum level of risk that they are able to take on, or their "risk capacity", and manage their operations accordingly.

Since financial capital represents the most readily accessible resource available to fund unexpected losses, risk-taking capacity is often closely associated with the amount of capital that the organization already holds, or can reasonably access, if and when required. Financial capital can be determined on either a regulatory or economic basis and either one of these may ultimately become the limiting constraint when it comes to assessing an organization's overall risk-taking capacity.

However, while financial capital is indeed a key determinant of risk-taking capacity, it is important to recognize that various other organizational factors and attributes also contribute to an entity's overall risk-taking capacity. For example, in addition to financial capital, the following (non-exhaustive) list of quantitative and qualitative factors also warrant careful consideration when deriving a more comprehensive and holistic assessment of that capacity:

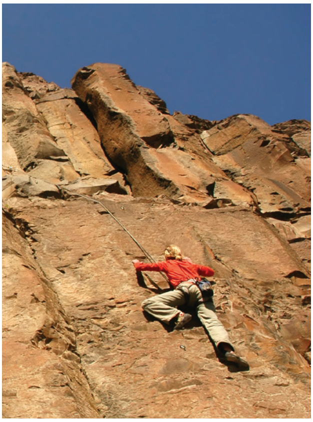
- **Earnings**
  For many public companies, earnings volatility often represents a key consideration in determining risk-taking capacity. Moreover, over the course of the economic cycle, various stakeholders may shift their focus between the statement of operations and balance sheet when assessing the organization's current risk capacity and profile, making earnings an important structural complement to capital-based risk capacity metrics.
- **Liquidity**
  Risk capacity can often be a function of not just the amount but the form of available financial resources, including, in particular, how readily these resources can be converted to cash to fund unexpected commitments.
- **Third-Party Credit and Claims-Paying Ability Ratings**
  The ability to refinance existing capital and access new capital, and the cost of funds associated with these financing activities, are key determinants of risk-taking capacity that are all impacted by third-party ratings. The deterioration of third-party ratings can also be a key strategic risk for many financial institutions, since existing or potential customers may qualify their prospective providers based on minimum accepted third-party rating levels.

- **Brand Equity**

An organization's brand equity can also be a key consideration in determining its risk-taking capacity, particularly when considering business issues or opportunities that may involve high levels of reputation risk.

- **Risk Management Capabilities and Expertise**

Management resources and capabilities often represent the most important enablers, or constraints, in shaping an organization's risk capacity. These resources include the broad range of risk management capabilities and expertise, business processes, operational and technology infrastructure, and governance and control framework used in the ongoing process of identifying, assessing, managing, monitoring, reporting, and communicating risk in the day-to-day pursuit of its business strategy and goals.



It is sometimes argued that, because financial capital is highly fungible and can therefore be converted into any of these other elements, any assessment of risk capacity can be focused entirely upon it. However, this argument fails to recognize the often extended time frame over which the proposed form of conversion can reasonably occur. This can materially amplify the execution, market, and valuation-related risks inherent in such conversion, and thereby severely undermine the ultimate effectiveness to the point where it would clearly not be appropriate to rely on financial capital alone when assessing risk-taking capacity. Moreover, the additional management perspectives and insights that derive from a more holistic, multidimensional interpretation of risk capacity result in richer understanding of the risks, and the full range of options for managing them.

Risk capacity provides an important benchmark for assessing the organization's risk appetite (the amount of risk the organization is willing to take) and risk profile (a point-in-time assessment of risk levels actually being assumed). Because the risk exposures underlying these concepts are subject to inherent misestimation, deterioration, cyclicality, and volatility over time, it is important to establish an appropriate risk buffer relative to the articulated risk capacity, and maintain active surveillance and review of these risk buffers through formal risk monitoring and reporting protocols. If the organization's risk appetite or current risk profile exceeds its risk capacity (i.e., it has a negative risk buffer), then it needs to appropriately curb its enthusiasm for risk and/or find ways to increase its risk capacity so that appropriate positive risk buffers can be established.

However, whenever considering the latter strategies, management should recognize that the expected costs and lead times involved in actually building risk-taking capacity are themselves often subject to significant levels of inherent risk.

– by Mike Stramaglia

What is Our Risk Appetite and How Do We Know We're Operating Within It?

Risk appetite has always been at the heart of the enterprise's vision and strategy. This is because institutions and organizations are often in the business of risk-taking. The products and services we provide inherently involve assuming some level of risk on behalf of our customers that they otherwise could not bear, or at least not at a reasonable price. The risks that we choose to aggregate, the amount that we accept, and the markets we choose to serve, are an expression of risk appetite.

However, being explicit about that appetite is important because it brings transparency to the risks that enable strategies (those that directly drive value) and risks of implementing strategies (that should be mitigated considering the cost benefit of those actions). These discussions reveal areas where the company has the demonstrated strength and capability to manage risk in a manner that provides some level of competitive advantage, or where greater capabilities are needed to prudently execute some of the company's strategic aspirations. A company's risk appetite validates its strategy and provides clear guidance on the level of risk it is willing to take to achieve those objectives.

Transparency then facilitates governance of the organization. It is impossible to separate the board's and management's risk appetite from the individuals and/or management teams they rely on to execute the company's strategy and manage its risks. Risk appetite has to be set at the highest level of the organization and then cascaded throughout the company. An overall risk appetite framework is a comprehensive system of governance, roles and responsibilities, monitoring, and decision-making.

The system of risk appetite statements, limits and key performance indicators, and how they are cascaded through the organization, involves delegation of authority. As the company's risk exposure fluctuates, specific risk limits serve as the triggers to ensure that the right conversations, evaluations, and escalation to the appropriate layer of authority are occurring. Executive management and business units are supported in their articulation of risk appetite and its management by the functional areas of the company, including risk management, actuarial, and finance.

Finally, risk appetite is of little use if you do not periodically evaluate your exposure in relation to it. Winston Churchill once said, “However beautiful the strategy, you should occasionally look at the results”. Risk appetite is a reflection of the business plans, expectations, and assumptions in place when it is set. No matter how rigorous the planning process, things will rarely turn out exactly as planned. Risk reporting focused on how the company operates within its risk appetite, and the action required to periodically make course corrections if needed, is critical.

These reports should also demonstrate how the company might look under stress, and offer a view on emerging, but not yet materialized, risks facing the organization to create a holistic view of risk appetite. With this we are well-positioned to continually evaluate and ensure we remain within an appropriate risk appetite.

– by Rahim Hirji

How Do We Know That We Have Identified Our Key Risks?

There are three main aspects to this question.

1. Are we omitting the most important types of risks?

Board members expect ERM measures of firm volatility to be based on a full consideration of all key risks. ERM programs usually do capture the volatility of financial and insurance risks. Unfortunately, many ERM programs fail to include the volatility of strategic risks (such as strategy execution risk and competitor risk) and operational risks (such as human resources-related risks and technology risks). The failure to capture the volatility of these risks is particularly disturbing because industry studies consistently show that strategic and operational risks account for the bulk of a firm’s volatility, even for financial services companies.

Failing to include strategic and operational risks in expressions of firm volatility represents a major distortion and can lead to a dangerous underestimation of the organization’s risk exposure.

2. Are we focusing on the wrong key risks?

It is common practice during the risk identification process to use a qualitative risk assessment (QRA) process to narrow down a long list of potential risks to just the key risks that can significantly impact the firm. The QRA process involves asking a broad group of individuals to suggest potential key risks and then score their likelihood and severity using qualitative categories such as very high, high, and medium. The key risks are selected via a combined ranking of these scores. This is a necessary first step in the ERM process.

Unfortunately, many ERM programs proceed directly to using this information for decision-making, such as which risks to mitigate, to what level to mitigate them, etc. This often leads to poor decision-making, including over- and under-mitigating, and, more importantly, focusing on the wrong risks. This is because the QRA process is intended only as an initial screening, and its results must then be vetted via risk quantification, which involves developing and quantifying a set of robust risk scenarios for each potential key risk using a rapid, but deeper-dive, process.

The prioritization produced by the risk scenario development and quantification process replaces the one produced by the QRA process, for the key risks, because it is superior in three ways:

a) It leverages information from subject matter experts specific to each risk, rather than relying on a broad group of individuals;

b) It develops multiple specific risk scenarios for each risk, rather than relying on a single amorphous risk, providing more clarity of focus; for example, rather than worry about "data breach" risk, we learn that we are really most concerned with "an internal data breach in system X by system administrators who have access to 100 percent of customer privacy data records"; and

c) It provides quantitative point-estimate impacts, rather than qualitative categories which often span wide ranges (e.g., "high" may involve an impact of 10–20 percent).

3. Are we missing some of the biggest threats?

Many ERM programs, after quantifying the impact of each key risk scenario and finding that no single risk event is devastatingly large, infer that the organization is invulnerable, since it can withstand any potential risk event. This can provide a false sense of security. Industry studies show that what most often takes down an organization is the combination of two or more risk events occurring simultaneously. To identify the biggest threats to firm survival, ERM programs must use models that simulate multiple concurrent risk events.

– by Sim Segal

How Are We Measuring Risk?

ERM asks simple questions. The answers, however, are often elusive, obfuscated by complex and correlated risks, masked by risk volatility, and shrouded in a litany of organizational decisions. Much of this confusion stems from an unclear sense of what risk measures are appropriate for the task at hand: evaluating an entity's risk profile.

"How much risk is right for us?"
"What risk sources will we tolerate?"
"Are our risk measures fit for purpose?"

Senior leadership and the board need a set of appropriate tools and information to make informed decisions regarding these questions. As much as risk measurement is about evaluating an organization's risk profile, it's also about developing a clearer sense of how organizational decisions will change that risk profile, and by how much.

For many insurance companies, underwriting leverage, reliance on investment income, and comfort with particular types of insurance risks, for example, may be at the core of an entity's risk profile. Each risk profile will have its advantages, providing particular opportunities, and sometimes the luck of the draw in terms of losses and investment environments will determine which option wins. Organizations survive and thrive using all types of risk profiles.

While risk categories can vary by industry, identifying the most common categories of risk is a key step. As an example, for a P&C company they would include the following: catastrophe, underwriting, reserve, and asset. The data sources often used to measure these differ:

- Catastrophe risk is measured by third-party vendor catastrophe (cat) models;
- Underwriting risk is calculated by a combination of company and industry loss ratios (ex-cat);
- Reserve risk is measured by a combination of company and industry loss triangles (a table of loss experience showing total losses for a certain period at various, regular valuation dates); and
- Asset risk is assessed by market and credit risk information from third-party vendor models.

The time horizons are also different:

- Catastrophe models use historical records to produce a catalogue of possible events (an event set);
- Underwriting risk typically uses 7–10 years of loss ratios;
- Reserve risk often uses the entire loss triangle; and

- Asset risk (depending on the sub-category) could use data ranging from 90 days to 10 years.

Each category differs in how the risk is measured:

- Catastrophe models are measured using a company's actual exposure information (e.g., by location, construction type, occupancy, year built, and number of stories). The models run each event from an event set over those properties, and determine a range of how much damage they would suffer.
- Underwriting risk is measured from observed volatility, similar to margin of error concepts in political polling.
- Reserve risk is measured based on our historical track record of reserving accuracy—how well did prior year reserve estimates play out? Generally a number of actuarially sound models are run and management makes picks, which are used to develop final reserve estimates.
- Asset risk is measured in a similar fashion, by looking at historical fluctuations in the value of certain types of investments as markets moved up and down.

The measurement of risk is as much art as science, so human judgment will continue to play a key role in the assessment of a company's risk profile.

– by Don Mango & Judy Jackson

This booklet was created by the ERM Applications Committee of the Canadian Institute of Actuaries.

Members:

Hélène Baril, FCIA, FSA, Chair	Jill Knudsen, ACIA, ASA, CERA
Danielle Harrison, FCIA, FCAS, Vice-chair	Pierre-Paul Renaud, FCIA, FSA
Patrick Duplessis, FCIA, FSA, CERA	Martin Roy, FCIA, FSA
Gaetano Geretto, FCIA, FSA, CERA	Mark Struck, FCIA, FCAS
Kim Girard, FCIA, FSA	Kathleen Thompson, FCIA, FSA
Diane Gosselin, FCIA, FSA	Ella Young

The Canadian Institute of Actuaries (CIA) is the national voice of the actuarial profession in Canada. With more than 5,000 members, the Institute puts the public interest ahead of its own, and is dedicated to providing actuarial services and advice of the highest quality.

Actuaries are risk management experts who evaluate and provide guidance on the financial implications of uncertain future events. They apply their knowledge of mathematics, finance, statistics, and risk theory to ensure the financial security of organizations and individuals. In Canada their profession is governed by the Canadian Institute of Actuaries (CIA). Actuaries turn numbers into knowledge.

Opinions expressed are those of the authors.

Our thanks to the following individuals who contributed articles to this booklet:

Gaetano Geretto, FCIA, FSA, CERA, founder and President, Pelecanus Strategic Advisory Services

Rahim Hirji, FCIA, FSA, executive vice-president and chief risk officer, Manulife

Judy Jackson, President and CEO, NLC Insurance

Minaz Lalani, FCIA, FSA, FCA, CERA, founder and managing principal, Lalani Consulting Group

Don Mango, Vice-chair of enterprise analytics, Guy Carpenter

Shannon Patershuk, FCIA, FSA, CERA, regional manager, retiree program relations, Johnson

Sim Segal, FSA, CERA, President and founder, SimErgy Consulting

Mike Stramaglia, FCIA, FSA, CERA, executive in residence, Global Risk Institute

Mark Struck, FCIA, FCAS, vice-president, enterprise risk management, Wawanesa Mutual Insurance

[1] https://stats.oecd.org/glossary/detail.asp?ID=6778.

[2] http://www.td.com/about-tdbfg/corporate-governance/committees-of-the-board/committees.jsp.

[3] *Risk Management and Corporate Governance*, OECD Publishing. http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf.

[4] Recommendation of the Council on the Governance of Critical Risks, adopted on May 6, 2014. http://www.oecd.org/mcm/C-MIN%282014%298-ENG.pdf.