PACICC

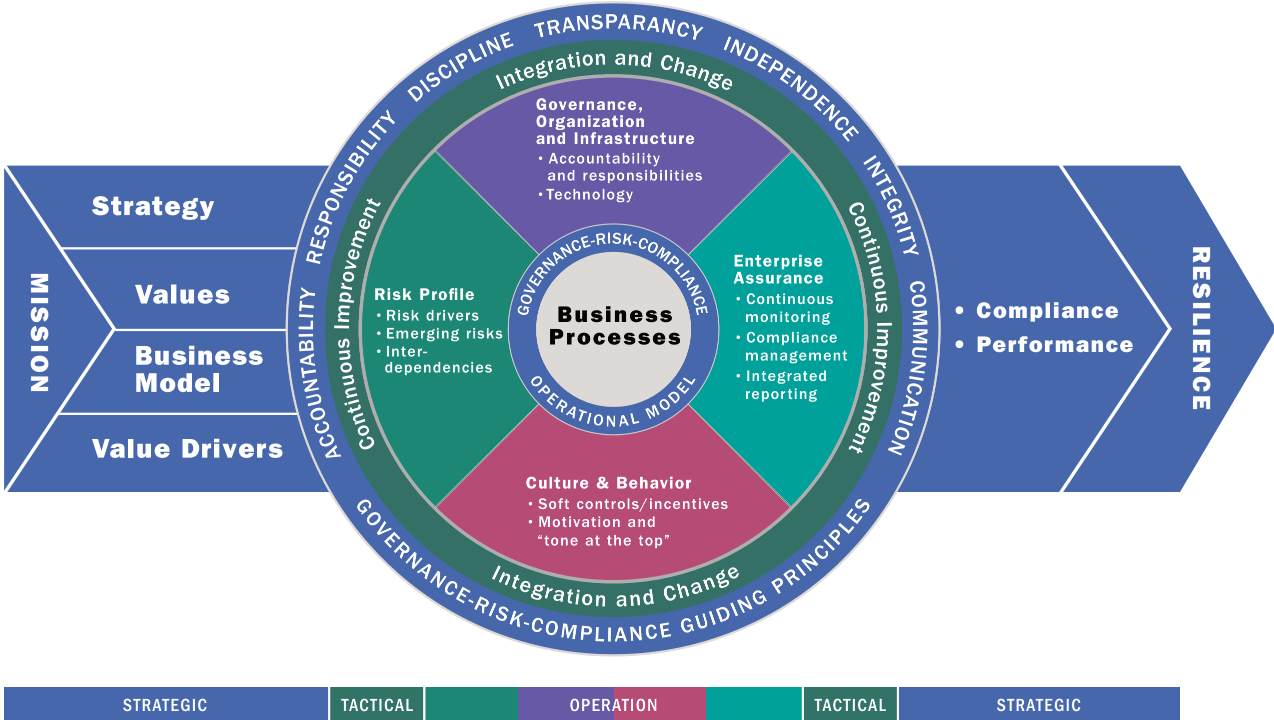
Property and Casualty Insurance Compensation Corporation
Société d'indemnisation en matière d'assurances IARD

Helping Canadian property and casualty insurers implement ERM best practices

March 2013

A holistic model of risk governance and risk management

See page 19 for details



©2012 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Helping Canadian property and casualty insurers implement ERM best practices

March 2013

Contents

Executive summary 1

Each enterprise is unique 2

Defining key concepts 3

Operationalizing Risk Appetite 5
- Developing a Risk Appetite Framework 5
- Constructing Risk Appetite Statements 6
- Embedding Risk Appetite 8
- Experiences implementing Risk Appetite at Aviva Canada and Intact Insurance 9

Creating an effective Enterprise Risk Management culture 13
- Elements of an effective risk culture 13
- Measuring risk culture 15

The Chief Risk Officer 16
- Opportunities for Chief Risk Officers 16
- Attributes of successful Chief Risk Officers 17
- Roles of Chief Risk Officers 18

Implementing Risk Governance and Risk Management 19
- A “Holistic” approach to Risk Governance 19
- Responsibilities of the Board 20
- Responsibilities of senior management 21
- Risk Committee 22
- Governance maturity 23

Conclusion 24

Executive summary

During 2011, PACICC began work on a project to promote the use of effective enterprise risk management (ERM) practices by its member companies. As part of this effort, PACICC conducted a survey of its member companies to benchmark their use of ERM practices.[1] The survey results made it clear that Canada's P&C industry has embraced ERM and that much work has been done to establish ERM within their enterprises. It also became clear, however, that the task of integrating effective ERM practices into daily insurance operations remains a work in progress for many enterprises, and that they welcome assistance in this endeavour, particularly in the form of practical advice about how to achieve tangible improvements in ERM on an enterprise-by-enterprise basis.

Accordingly, in the fall of 2012 PACICC collaborated with KPMG to sponsor a three-part series of ERM seminars for its members. Several critical sub-themes identified through PACICC's ERM benchmark survey were examined in the seminars, including essential elements of a successful ERM strategy, establishing clear guidance with regard to risk appetite, and resources and responsibilities surrounding risk governance and risk management.

PACICC is grateful to KPMG for contributing its expertise to this important and timely discussion, with special thanks to Neil Parkinson, KPMG Partner, National Insurance Sector Leader, for helping to organize and lead the seminars, and Elizabeth Murphy, Peter Heimler, and Rudolph Persaud, Associate Partners, Financial Services Advisory, for presenting at each of the seminars. PACICC is also grateful to members of its ERM Advisory Committee, particularly Susan Meltzer, Brandon Blant, Ron Bilyk and John Cairns,[2] for sharing their knowledge and personal experiences with developing and executing ERM within the P&C industry. Response to the seminar series was enthusiastic, with more than 100 member insurer representatives participating in the series.

PACICC retains an interest in supporting enhanced ERM capabilities in Canada's P&C insurance industry. Possible future initiatives may include further member surveys to help gauge progress in implementing ERM, as well as continuing education.

Paul Kovacs
President & CEO
PACICC

[1] Property and Casualty Insurance Compensation Corporation, "ERM Benchmark Survey Report," December 2011.

[2] Susan Meltzer is Vice President, Enterprise Risk Management, Operational & Regulatory Risk for Aviva Canada; Brandon Blant is Vice President, Risk Management for Intact Insurance Financial Corporation; Ron Bilyk is Director, Compliance for Zurich Canada; and John Cairns is Senior Vice President and General Counsel for Chubb Insurance. The views expressed in this report represent the personal views of participants and in no way reflect the views of any Canadian insurer.

Each enterprise is unique

Although this paper sets out some proven approaches and best practices to implementing ERM, a recurring theme among participants in all of the seminars was that each enterprise is unique, and that therefore the appropriate structure of the ERM program will differ for each enterprise.

Insurance regulators recognize this reality. Accordingly, they have deliberately avoided imposing a set of ERM practices and methodologies across the industry, choosing instead to articulate a set of principles to guide implementation of sound ERM strategies. This approach recognizes, as the Office of the Superintendent of Financial Institutions stated in its Guideline issued January 28, 2013 regarding Corporate Governance of Federally-Regulated Financial Institutions (FRFIs), "that FRFIs may have different corporate governance practices depending on: their size; ownership structure; nature, scope and complexity of operations; corporate strategy; and risk profile."[3] Despite the importance of the Corporate Governance Guideline, it should be noted that additional regulatory guidance will affect an insurer's ERM framework – such as internal capital and Own-Risk Solvency Assessment (ORSA).

Such a principles-based approach is extremely useful for P&C insurance companies. It sets out in clear language what is expected in terms of ERM best practices within the industry, actively encouraging enterprises to develop ERM strategies but providing them with the opportunity to develop individual ERM identities by testing different strategies and determining what best suits their own risk profile.

[3] Office of the Superintendent of Financial Institutions Canada, "Guideline: Corporate Governance," January 2013, p. 1.

Defining key concepts

Traditionally within the financial services sector, information sharing has been hampered by the silo effect, where treasurers typically focus on finance risks, compliance officers manage compliance issues, desk traders hedge market risks, and so forth. Risk managers can begin to dissolve silos by creating a common language across the enterprise with clear definitions of key terms that might otherwise mean different things to groups with different backgrounds and responsibilities. It is also important to note that one of the key challenges when communicating about risk in any enterprise is being jargon-free as much as possible.

Defining key concepts on an enterprise-wide basis is also useful in setting the appropriate tone from the top about the importance of ERM, creating positive and informed attitudes toward governance and risk management throughout the enterprise, and properly equipping employees at all levels to participate in risk assessment as part of day-to-day decision-making.

The following definitions are based on PACICC's understanding of key risk concepts as defined by leading ERM sources of guidance, including the COSO Framework and ISO 31000. The definitions are also informed by best practices guidelines supplied by KPMG.

"It's very important to make sure that people understand the definitions... [defining key concepts was important for] making sure that people around the table could be on the same page when we were using certain ERM terms."

Brandon Blant, Intact Insurance

Risk: The positive or negative effect of uncertainty on an enterprise's objectives.

Risk capacity: The outer limits of risk that an enterprise could take. Risk capacity is the enterprise's total ability to take risk or absorb losses. For example, "we cannot expose more than $X m of available capital to all risks." This information then needs to flow down through the enterprise, addressing what it means for the enterprise's overall strategy and what individuals should be doing on a day-to-day basis to ensure that the enterprise does not exceed its risk capacity.

Risk tolerance: The specific maximum risk levels the enterprise allows itself to take regarding each relevant risk, beyond which it is not comfortable proceeding. These levels can be thought of as "tripwires" that alert the enterprise to an impending breach of tolerable risks. Risk tolerance is often expressed in absolute terms; for example, "we will not expose more than X percent of our capital to losses in a certain line of business, or "we will ensure that business interruptions last no longer than X business days."

Risk targets: Optimal levels of risk an enterprise wishes to take in pursuit of specific business goals. For example, "we will accept a staff turnover of 15% and a target claims loss ratio for product X of 50%."

Risk limits: Thresholds to monitor that actual risk exposures do not deviate excessively from risk targets and stay within the enterprise's risk tolerance and risk appetite. Exceeding risk limits will typically trigger management action; for example, "X corrective action will be triggered when Y number of consumer complaints is reached."

Risk appetite: The total amount and type of risk an enterprise is willing to accept in pursuit of its business objectives, provided there is a commensurate return. For example, "we will maintain $X in excess of economic capital over a Y-year time horizon with Z profitability," or "we will maintain a credit rating of AA or better." Risk appetite can only be defined in the context of a known and effective risk capacity. It reflects the enterprise's risk management philosophy, and in turn influences its culture and operating style. Risk appetite is fluid; it will change as the enterprise's capacity improves or deteriorates, and as relevant economic conditions change. (The next section of this paper discusses risk appetite in greater detail).

> **"If you think back a few years ago – post-Enron – there was a lot of emphasis on having financial literacy on boards of directors. Now, when you look through to what OSFI is expecting from board members, [OSFI] is also asking for something that I would paraphrase as 'risk literacy'."**
>
> *Neil Parkinson, KPMG*

Risk appetite statement: A specific statement that articulates and documents the enterprise's risk appetite, setting the tone for risk management and providing direction and boundaries for the amount of risk that can be accepted at various levels of the enterprise. It also defines the control and sanctions environment, and describes limits, thresholds and key risk indicators. Contents of a risk appetite statement could include desired overall net risk, risks by category, reporting and monitoring, and conditions requiring review. Examples include enterprise-wide measures that can be disaggregated (for example, earnings at risk or capital at risk), liquidity preferences (for example, mix of liquid assets or funding sources), hedging strategies (for example, the use of insurance or derivatives), or operational controls (for example, internal system requirements, or tolerance for outsourcing arrangements).

Risk appetite framework: The enterprise-wide process that translates risk appetite objectives into key performance indicators and targets.

Operationalizing risk appetite

The most robust discussion among seminar participants centered on topics related to risk appetite. This focus reflects an understanding of the increasing importance of the risk appetite framework, and a desire for direction in terms of clearly defining, executing and communicating risk appetite through the enterprise.

An effective risk appetite framework can influence decision-making for management and employees regarding acceptable financial and performance limits, selection of strategic options, delegations of authority, and short and long-term target setting. It can also help to define the appropriate set of controls for the enterprise, and it can help to create consistent behaviors throughout the enterprise by directly informing policies, procedures and controls. The focus on risk appetite also reflects a sense among participants that it is possible to improve the way in which risk appetite is operationalized at a business level.

"One of the benefits of the risk appetite is that it defines the sandbox within which management can operate."

Brandon Blant, Intact Insurance

The task of determining the enterprise's risk appetite is best suited to the board and senior management because risk appetite is closely linked to defining the enterprise's overall strategic direction. Once set, however, the risk appetite must flow through all levels of the enterprise to make certain that it is appropriately operationalized at a business level. Broad steps to operationalize risk appetite include communicating the risk appetite across the enterprise in a way that allows employees to understand how they should adjust their decision-making, applying risk appetite consistently to all relevant risks and business units through risk targets, limits and tolerance levels, and assigning specific roles and responsibilities to individuals at different levels within the enterprise.

Developing a risk appetite framework

One approach to developing a risk appetite framework has been proposed by KPMG. Certain principles are considered fundamental to the overall design and implementation of an effective risk appetite framework. First, risk appetite is not a single, fixed concept; rather, there is a range of risk appetites that are appropriate for the risk categories faced by each enterprise. These risk categories must be monitored as they will vary over time to reflect changes in the business environment and the enterprise's market strategy. It is also important to take into account different stakeholder needs at levels of detail that reflect a strategic and operational perspective. Different views of risk appetite will occur at different levels of the operation. Risk appetite must also reflect its business context, market strategies and stakeholder perspectives. Finally, risk appetite constraints must be integrated into the enterprise's set of controls and embedded into decision-making processes at both the strategic and business levels.

At a high level, KPMG employs a six-step process to develop a risk appetite framework. The process begins by setting the broad context within which the enterprise exists and accepts risk, then it moves to setting risk appetites, and finally to specifying controls:

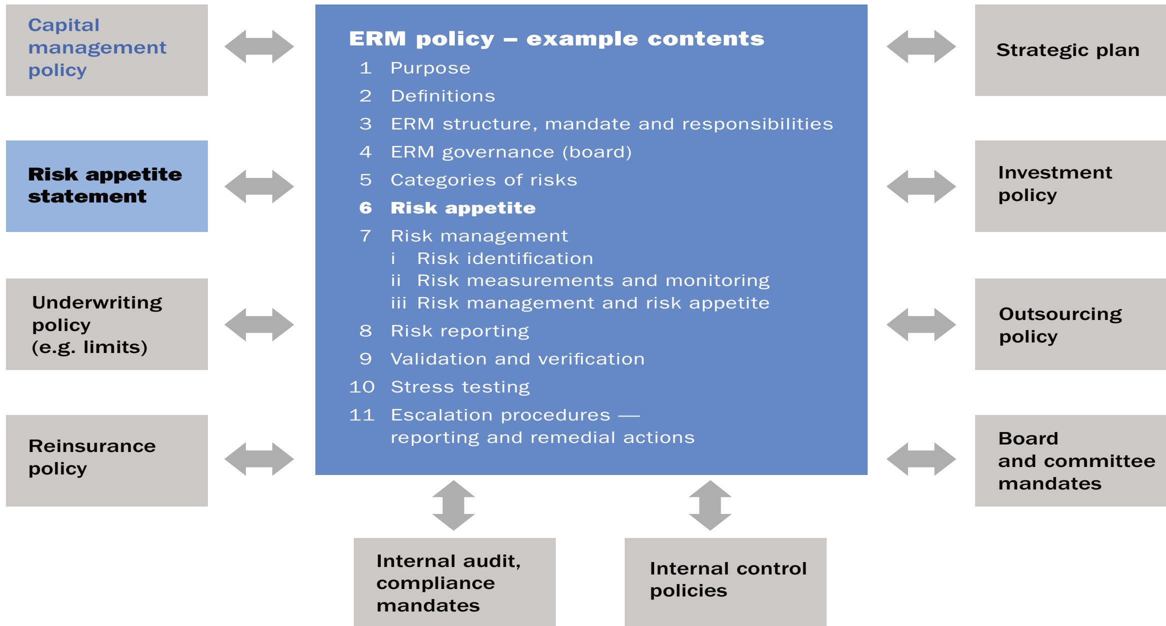
1. Understand the business environment, market strategies and perspectives of key stakeholders. For example, conduct key stakeholder interviews and analysis, and review strategy, governance structure, roles and escalation procedures;
2. Consolidate the findings of Step 1 into a set of principles related to risk-taking activities, and establish the material risk exposures that the enterprise is willing to accept;
3. Specify high-level risk appetite statements and align key risk indicators with each statement so these can be used to monitor the risk profile;
4. Establish risk appetite constraints and make them more detailed in terms of tolerances and limits, and identify any gaps in controls that need to be addressed;
5. Establish a system of monitoring and aggregation processes. This step requires infrastructure that affords day-to-day monitoring of risks and reporting processes that reflect the constraints, tolerances and limits as they are implemented;
6. Update the risk management approach to ensure that it reflects new risk constraints and measurement, monitoring and reporting processes.

Constructing risk appetite statements

The risk appetite framework begins with a risk appetite statement that establishes the boundaries for business focus and the board's desired approach to a variety of businesses, risk areas, and product types.

Risk appetite statements should be fully integrated into the broader risk management policy framework, as illustrated on the next page.

Risk appetite and the risk management policy framework



©2012 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Specific components of risk appetite statements might include:

- Change in total surplus for the year must be between X% and Y%.
- No policies will be accepted outside accepted underwriting standards.
- Administrative expenses must decrease compared to the prior year by X%, with a target of 10%.
- The enterprise will not breach any laws or regulations of the jurisdictions within which it operates, or risk over-concentration in its investment or business activities.
- The liquidity ratio must be maintained between X% and Y% to meet both immediate and future liquidity needs.
- Return on equity for a P&C insurer must be a minimum of X%, plus three percentage points.

A structured approach to creating risk appetite statements includes four key elements. The first is setting organizational and strategic objectives to understand the enterprise's drivers, including market share, reputation, earnings stability and growth, investor returns, regulatory standing, capital adequacy and external credit ratings. Second is identifying material risks by aligning the risk profile with business and capital plans through such factors as measuring the enterprise's aggregate risk profile and the level of unexpected losses that it is willing to accept in the event a risk occurs. Third, using stress testing to determine risk tolerance ranges for specific risks to ensure the risk appetite remains within the bounds of the capital management and/or business plan. Fourth, formalizing and ratifying risk appetite statements by documenting the risk appetite framework and submitting it for board approval, and establishing a program to communicate the details of the framework to the wider enterprise.

Risk Appetite Statements should contain quantitative and qualitative elements

Targets	Defining capital requirements or ratings set by rating agencies
Earnings volatility	Specifying desired earnings forecasts
Diversification	Allocating capital to various business lines, markets or franchises
Liquidity headroom	Specifying resources available to meet liquidity requirements at various confidence levels
Reputation	Statements of expected ethical behavior and corporate culture
Regulation	Statements regarding regulatory compliance
Governance	Statements regarding organizational governance expectations
Strategy and growth	Overview approach regarding risk strategy and growth expectations
Geopolitical and cultural	Statements regarding risk tolerances in these areas

Embedding risk appetite

Successfully embedding risk appetite through the enterprise depends on several critical factors:

- Ensuring it reflects the enterprise's strategic vision as developed by management and approved by the board;
- Providing strong leadership and support for the risk appetite development process, and ensuring that this support is visible to employees across the enterprise;
- Defining risk appetite such that it articulates the actual risks the enterprise can take and those it should avoid, including specific targets and tolerances;
- Capturing sufficient data to allow the enterprise to assess performance in relation to risk appetite;

- Ensuring that the risk appetite is consistent with the enterprise's controls and capability;
- Recognizing that risk appetite is dynamic and will change with the enterprise and evolve as the maturity of its ERM program advances, and therefore reviewing the risk appetite framework periodically.

Key steps to developing a risk appetite framework

1. The Board should approve the risk appetite framework, aligning it with the enterprise's corporate strategy, financial and capital plans, business unit strategies, and day-to-day operations.
2. To ensure effective monitoring and governance, the risk appetite should incorporate a balanced mix of both quantitative and qualitative measures.
3. An active, iterative process should be used by the Board – working with management – to shape risk appetite statements.
4. The right people need to be empowered throughout the enterprise to assist in implementing the risk appetite framework.
5. Once approved by the Board, the risk appetite framework should be implemented by senior management through the enterprise as an integral part of the overall ERM framework.
6. Effective control, monitoring and reporting systems and procedures should be developed to ensure ongoing operational compliance with the risk appetite framework, including regular reports to the Board and routine assessment by Internal Audit or Compliance.

Experiences implementing risk appetite at Aviva Canada and Intact Insurance

The previous section outlined practices and approaches that have proven effective in developing risk appetite, risk appetite statements, and the risk appetite framework. However, each enterprise's approach must fit with its unique culture and structure. As such, an opportunity exists for each enterprise to define and operationalize risk in its own way.

> **"Risk appetite is very much driven by who you are."**
>
> *Susan Meltzer, Aviva Canada*

For Susan Meltzer, the process of setting risk appetite at Aviva Canada began five years ago qualitatively and two years ago quantitatively. The first step was to ask "who are we?" as an enterprise. For example, a monopoly has a different attitude toward risk-taking than competitive enterprises. Meltzer believes that answering this question is somewhat different for insurers because they already believe that they are professional risk takers and that they understand their underlying risk appetite. Nonetheless, the first question of "who are we?" still applies to an insurance enterprise.

The answer for Aviva Canada was: "we are the wholly-owned subsidiary of a UK-based company, predominated by life insurance operations." The second and third questions were: "what does that mean?" and "what measures are important to us?" Susan Meltzer found after answering these questions and following the process described above that Aviva Canada's Board and senior management already shared an understanding of the enterprise's risk appetite. And when they considered if the enterprise's business strategy fit with its risk appetite, the answer was a resounding "yes." She believes this synergy existed because the same people set both the strategy and the risk appetite. Within her enterprise, no conflict existed between the two.

Key questions for Boards regarding risk appetite

- What are the enterprise's strategic objectives? Are they clearly stated? What is explicit and what is implicit in those objectives?
- What are the enterprise's three most profitable activities?
- Is the board clear about the nature and extent of the significant risks the enterprise is willing to take in achieving its strategic objectives? Are these risks compatible with our strategic objectives?
- Can board members articulate the enterprise's risk appetite?
- Does the board need to establish clearer governance over the risk appetite and tolerance of the enterprise?
- Is the course of action being proposed compatible with our risk appetite?
- Are the enterprise's line management and staff aware of the risk appetite and do they use it to guide their daily decisions?
- What steps has the board taken to ensure that it provides appropriate oversight to senior management with respect to the enterprise's risks?

There was, however, some difference of opinion early on about the appropriate levels of risk to assume. For example, at one point the Board decided that the risk managers were too conservative when presenting qualitative statements about operational risk. As a result the risk managers were asked to re-draft these risk statements to find a way to express that the enterprise needed to take a cost-benefit approach to its risk appetite for operational risks. Aviva Canada now has a separate risk committee of the board, and that committee examines the enterprise's risk appetite every quarter and makes necessary adjustments.

For Brandon Blant of Intact Insurance, setting risk appetite at his enterprise took more than a year, beginning with defining key terms for Board members and senior management, such as risk appetite, risk tolerance, and risk capacity. Determining risk appetites began with a series of preliminary interviews with Board members and senior management on macro questions such as "what are the types of risks we like to take?" and "what are the things we don't like to do?"

> **"[ERM] is by no means a one-size-fits-all approach."**
>
> *Brandon Blant, Intact Insurance*

Blant sat in on each of the individual interviews with Board members and senior management, and an external consultant was also engaged to help lead discussions at the Board and senior management levels. While some views were widely shared on certain key questions, in other areas different views emerged. But that was expected. The point of the exercise was to bring the views of the Board and senior management closer together.

Once all the information was collected, Brandon Blant and his team developed a set of preliminary statements that were "pitched" to a risk appetite sub-committee of the Board risk committee. Members of the sub-committee were asked: "does this statement embody what we are already doing?" The goal was to "articulate" the risk appetite while making sure that any disagreements were explored and understood to be either differences in wording or something more substantial. Then, risk managers went back to the full Board with a draft for discussion, incorporating certain final adjustments into the document and finally receiving Board approval.

Writing down specific risk appetite statements can be particularly challenging. Brandon Blant believes that it is easy to underestimate the difficulties involved in this part of the process. Part of the solution was to enlist help from Intact Insurance's corporate communications team to review the risk appetite statements and to help better express what the risk managers were trying to achieve.

At Aviva Canada, the key to creating effective risk appetite statements was to use words that helped drive behavior at the front line. Susan Meltzer found it useful to divide risk appetite statements into two components: first, a quantitative statement or the very measurable statement that could be reported to stakeholders (which might include the parent, regulators, rating agencies, and the Board); and second, a communications statement that could drive behavior through the business.

While differences are evident in the approaches to risk appetite taken by Aviva Canada and Intact Insurance, a number of consistent themes emerge and should be noted as they reflect best practices. These include:

- A high level of buy-in from the Board and senior management;
- Constant two-way communication between the risk management team and the Board and senior management;

- A corporate culture that appropriately integrates risk appetite into everyday business activities;
- A belief that responsibility for risk appetite belongs to the Board and senior management, not the risk management staff;
- Recognition that ERM is dynamic so that, once developed, the risk appetite should be considered fluid and therefore subject to regular updating. Likewise, the risk appetite statement is a "living document" that needs to be reviewed periodically to reflect major changes to the business;
- Acknowledgement that the process of developing an effective risk appetite framework takes time, even if the enterprise already enjoys a high level of "buy-in" at the board and senior management levels.

Creating an effective enterprise risk management culture

The previous section emphasized the board's responsibility in setting the enterprise's risk appetite framework. It also emphasized, however, that a healthy and well-functioning risk culture across the enterprise facilitates improved management of risk and underpins an enterprise's ability to work within its risk appetite. Risk culture is at the heart of the human decisions that govern the daily activities of the enterprise. It is the behaviors of individuals and departments within the enterprise that determine the enterprise's overall ability to identify and understand, openly discuss and act on, its current and future risks. The enterprise's ability to manage and monitor its risk appetite will depend to a large extent on the quality and maturity of the risk management culture within the enterprise.

> **"If you're going to spend a nickel on process, you should spend a dime on culture – maybe a quarter in today's world."**
>
> *Peter Heimler, KPMG*

John Cairns of Chubb Insurance noted that creating a risk culture should begin with creating a "culture of integrity," where senior managers make ethics and integrity a key component of the corporate message. Moreover, although a statement of ethics and integrity is a positive step forward, management actions should support the message with appropriate training for employees highlighting integrity and ethics issues.

Elements of an effective risk culture

At an enterprise-wide level, the following requirements need to be present for a risk culture to thrive:

- Maintain a focus on education and dialogue to ensure that a robust risk culture is constructed across the entire enterprise. Establishment and articulation of the enterprise's overall direction for integrating risk management, including vision, objectives and operating principles, supports successful integration of the risk management function into the enterprise;
- Boards and senior management must continue to transform from a "compliance focus" to a "strategic advisor" focus. Complying with regulatory requirements is clearly important, but it must be balanced with a value-added approach;
- An appropriate culture around risk may be developed broadly by the board, which sets the tone and direction in terms of developing culture. But it is implemented largely by senior management, which sets performance expectations for mid-level managers in terms of overall leadership and day-to-day direction;
- Identify individuals in the enterprise who can function as good subject matter experts. Such individuals bring technical expertise to the concept of risk management. For example, a team of subject-matter experts could be assembled from every level of the enterprise to engage in debate about the potential advantages and disadvantages that different types of risk pose for the enterprise. Over time, the hope is that risk management will disseminate through the ranks of the enterprise in a positive way;

- Risk management must interconnect with the enterprise's planning, management, performance measurement and accountability structure and process;
- There must be visible and consistent role modeling of desired behaviors and standards by senior management;
- The board must challenge senior management on a regular basis as a key part of instilling a risk management culture.

Steps to help improve the organizational structure and sustainability of risk management include:

- Providing the board with appropriate risk management education;
- Developing "ownership" of risk management oversight by the board and periodically reviewing the enterprise's top risk profile and mitigation strategies;
- Creating within management a high-level risk strategy or policy that is aligned with the strategic business objectives;
- Creating a risk management organizational structure for the entire enterprise and ensuring that clear reporting lines exist and are conveyed to employees;
- Developing and assigning specific responsibilities for risk management. This must be conveyed as a positive effort, one that engages employees and makes them feel involved in the enterprise's success. Partly this includes the chief risk officer identifying "risk management champions" with strong technical skills and creativity;
- Communicating the board and senior management vision, strategy, policy, responsibilities and reporting lines to employees across the enterprise;
- Linking performance incentives to good risk management practices and to the overall health of the enterprise.

KPMG lists the following specific measures to promote an effective risk culture:

- Use common language and concepts throughout the enterprise;
- Develop training programs for risk management; for example, train a core set of risk managers to act as role models and provide mentorship for others;
- Ensure that top risks are included in status reports and circulated to managers and key stakeholders;
- Identify quick "wins" and share success stories;
- Develop a knowledge sharing system, including developing IT systems that support effective risk management;

- Include risk management activities and responsibilities in job descriptions and make performance on risk issues an important part of how job performance is assessed;
- Align and integrate risk management activities within business processes and develop continuous improvement processes related to risk;
- Identify key performance indicators and critical success factors related to risk. Provide a periodic process for measuring risk and return;
- Ensure that an effective system exists for reporting risk information enterprise-wide;
- "Risk literate" board members and senior management will be better positioned to demonstrate leadership in ERM by setting the tone at the top and to oversee the embedding of the corporate risk agenda and strategy throughout the enterprise.

Measuring risk culture

Straightforward measures of risk culture do not exist, although measurement does take place. According to Towers Watson, the best approach to measuring risk culture is to engage directly with employees responsible for risk management, as well as with identified risk "champions" throughout the enterprise. This is accomplished either by having risk managers regularly interview these people, or by administering periodic surveys of attitudes and activities and comparing results from one period to the next.

In the absence of interviews or periodic surveys, certain questions can be posed by risk managers at regular intervals, such as:

- How can board members and senior managers become more supportive of those actively engaged in seeking to understand and manage risks? Is a risk "champion" structure in place to support managers in better managing risks? Have the efforts of risk "champions" been appropriately recognized through the performance management process? Have risk accountabilities been captured within role descriptions and performance targets?
- Has the board and senior management succeeded in setting clear expectations for risk management across the enterprise? How deep within the enterprise have expectations been set? Has senior management actively encouraged management information related to risks to travel quickly across the enterprise? Have lessons, both positive and negative, from risk events been communicated sufficiently and in timely manner to people across the enterprise?
- What level of resources has it taken to develop and implement a risk appetite framework across the enterprise? Was this level of resources appropriate? Should it be amended going forward?

The Chief Risk Officer

Opportunities for Chief Risk Officers

Debate continues about the right mix of risk management talent that each enterprise requires, especially whether the enterprise needs a chief risk officer, or a risk committee consisting of a team of executives that collectively lead the ERM effort, or both. There is no single correct answer. Each enterprise must decide for itself how best to organize the risk management function.

> **"It is the role of the chief risk officer to help the board articulate questions and to anticipate what [board members] don't know and to be able to guide them to a better understanding."**
>
> *Susan Meltzer, Aviva Canada*

Brandon Blant of Intact Insurance pointed out that the right corporate structure is necessary to support the success of the chief risk officer, including reporting lines that are conducive to the role. This could mean a direct line to the CEO or a dotted line to the board, or both. It is most important that the chief risk officer's stature within the enterprise is significant enough that people understand that he or she has a "seat at the table" and that his or her views are heard so that there is an opportunity to escalate issues.

For large, complex and multi-line insurance companies, a separate chief risk officer is normally deemed essential. However, for small and medium-sized companies, or those of less complexity with more predictable and easily diversifiable risks, individuals with responsibility for risk management may perform other functions. The challenge with the latter arrangement is being able to demonstrate that the board, CEO, senior management and regulators can rely upon the risk management processes to a sufficiently high degree, and that the multiple responsibilities of the officer assuming responsibility for risk management are compatible. A good test appears to be that the chief risk officer is independent of business operations and revenue generation.

The advantages of appointing a chief risk officer are many, including:

- Improving communication among senior management and between senior management and other levels of the enterprise;
- Reporting to senior management, key individuals in control functions, and to the board on the insurer's risk profile, risk exposures and related mitigation actions as appropriate;
- Helping to nurture the risk expertise of senior managers so that they know which questions to ask about risk-related issues as they arise;
- Maintaining an aggregated view of the risk profile of the insurer at a legal entity and at a group-wide level.

Attributes of successful Chief Risk Officers

For Susan Meltzer of Aviva Canada, attributes of a successful chief risk officer for a P&C insurer include being persuasive, understanding how to challenge the business without confronting board members or senior management, and being able to assist the enterprise to take the risks it wants to take. For her, this could fit anybody from an actuary to a lawyer to an insurance purchaser. Brandon Blant pointed out that, like many other senior roles, attributes of a successful chief risk officer include diplomacy and an ability to communicate well on complex topics to people at various levels. The chief risk officer should not always be a constraint on the business by saying "you can't do this." It is more important to be an enabler who helps the business move forward subject to the agreed risk appetite and tolerance.

> **"The risk manager's dream is to prove that you add value."**
>
> *Susan Meltzer, Aviva Canada*

Effective chief risk officers attempt to gain a "big picture" understanding of their enterprise's assortment of risks. They assess the unknowns – 'What have we missed? What if...?' They identify hidden risks, possible future risks, and risks that may already have been incurred but were previously unidentified. According to Susan Meltzer, her team was able to identify an area of the enterprise that was taking risk well below its stated risk appetite compared to risks being taken elsewhere in the enterprise. As a result, risk appetite was re-aligned in that area, thereby improving profit for the enterprise.

Brandon Blant finds that one way to support the work of the chief risk officer and of the ERM program in general is through enhanced corporate communications. If a communications function already exists, it can be used to reinforce the way in which risks are presented to the enterprise-such as reviewing definitions being used in the corporate culture, or the risk appetite statements.

Susan Meltzer agrees, adding that "words help drive behavior." For her, getting the words right is one of the keys to receiving enterprise-wide "buy-in." She also believes in formal training in ERM practices for employees across the enterprise. Two levels of training are suggested; first, for technical personnel – such as actuarial, finance, human resources, product design – in economic capital and economic capital allocation using case studies, where they actually allocate capital amongst a number of products; and second, for other personnel, with training about risk management as it applies to the enterprise, including the enterprise's risk appetite, followed by training of the "what if" variety, such as discussing with IT personnel what will happen if they fail to operate a particular control properly.

Roles of Chief Risk Officers

Four key roles of the chief risk officer are outlined below. Elizabeth Murphy of KPMG observed that the responsibilities of the chief risk officer will vary between enterprises, depending upon the organizational structure and size. In other models, "challenging" may be called "counseling," "coordinating" may be called "teaching," "monitoring" may be called "policing," and "challenging" may be called "leading" or "business leading."

Four key Chief Risk Officer roles

Advising on...	Coordinating...	Monitoring...	Challenging...
✔ Risk strategy ✔ Risk framework ✔ Risk appetite and limits ✔ Key performance/risk indicators and targets, limits, thresholds ✔ New product approvals ✔ Stress testing and scenario analysis ✔ Risk mitigation ✔ Model standards and related governance	✔ Internal Capital Adequacy (ICA)/Solvency II ✔ Interactions in relation to the business planning cycle, encompassing risk and funding/capital management ✔ Risk reporting from Divisional flows and analysis ✔ Regulatory interactions ✔ Training, knowledge management and awareness ✔ Disaster recovery coordination	✔ Risk capacity vs. risk profile ✔ Limit breaches ✔ Cascade/escalation processes ✔ Performance of "Line 1" ✔ Remediation actions and escalating reports/findings	✔ Business strategy ✔ Key/emerging trends, variances and anomalies ✔ Major projects/change management programs/M&A ✔ The extent of embedding ✔ Via the use of intensive reviews/testing/ validation

The Developing Role of the Risk Function (under Solvency II), April 1, 2011, Sajib Azab, Senior Risk and Technical Specialist, Prudential Risk Division, FSA.

KPMG further noted that expanding the focus from the more traditional or reactive role of monitoring to encompass the other three roles allows the chief risk officer to use an expanded skill set. In particular, it requires more of the so-called "soft" skills that were highlighted by Susan Meltzer and Brandon Blant, such as negotiation, facilitation, education, and communication. This is especially true for effectively executing the roles of "advising" and "challenging."

Implementing risk governance and risk management

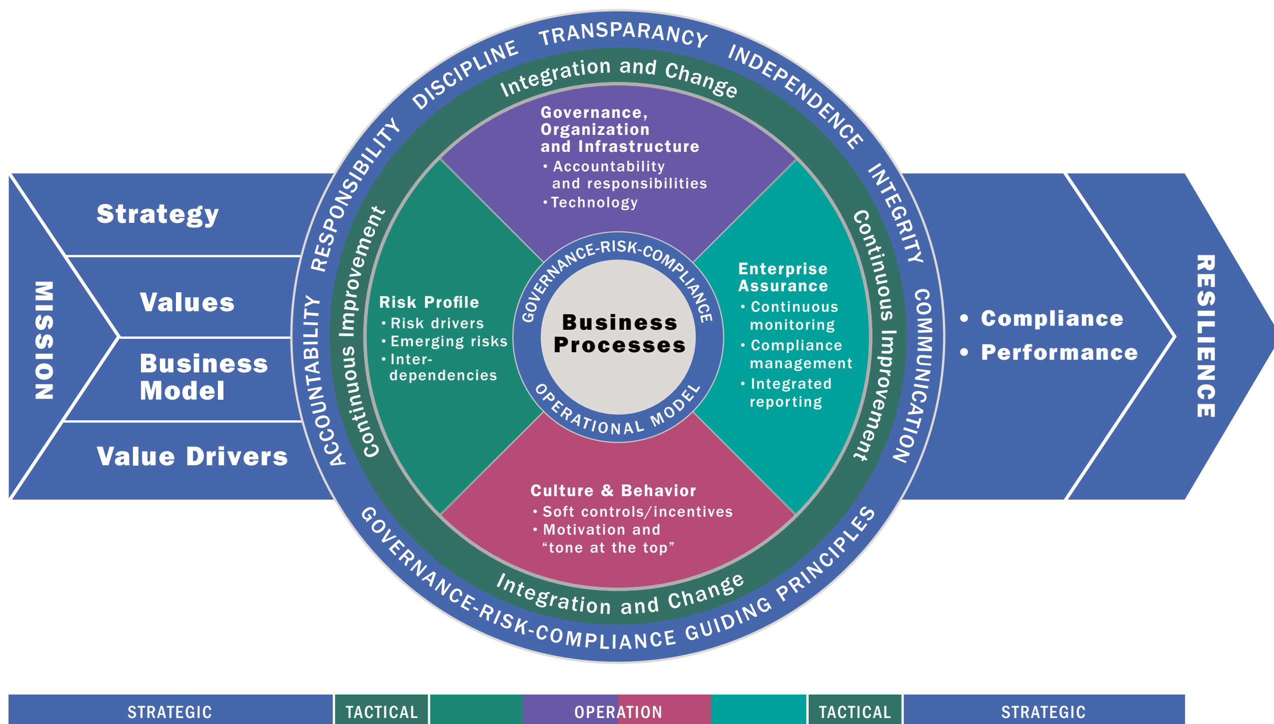
According to the Conference Board of Canada, risk governance is “the system through which senior management and the board of directors establish the enterprise’s attitude toward risk, manage risk, and oversee the management of risks to achieve the organization’s objectives.” In this respect, risk governance is an important component of corporate governance.

A “Holistic” approach to risk governance

Enterprises should ensure that risk management is never a separate activity, but is fully integrated with all decision-making processes, including governance structures, strategic planning, operational planning, major investments (for example, joint ventures, mergers, primary supplier relationships), internal control over financial reporting, and legislative compliance.

The chart below depicts KPMG’s “holistic” approach to risk governance, which aligns both complex and disparate risk and compliance activities with corporate strategy.

A holistic model of risk governance and risk management



©2012 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

As Rudolph Persaud of KPMG noted, a holistic approach achieves the following:

- Demonstrates a commitment to aligning governance, risk and compliance to the enterprise's strategy and mission;
- Supports informed decision-making driven by robust governance structures and appropriate reporting (such as dashboards showing current and historical trends of an enterprise's key performance indicators);
- Enhances consistency, transparency and operational efficiency by rationalizing overlapping risk management efforts, controls, assurance structures and processes;
- Supports a suitable and sustainable approach to tackling challenges posed by evolving risks and rapidly changing regulatory requirements;
- Embraces governance, risk, and compliance as a source of competitive advantage by making the enterprise more resilient and responsive to new events- such as mergers and acquisitions, new regulatory requirements, expanded territories, or increased competition.

"It's just human nature for people who are risk owners to tend to underestimate the severity of risk and to overestimate the effectiveness of the controls that they've put in place to deal with [risk]."

John Cairns, Chubb Insurance

Responsibilities of the Board

John Cairns of Chubb Insurance pointed out that boards are now responsible for approving the oversight of internal controls, including the personnel, policies, processes, limits, and other aspects of the enterprise that support the achievement of its objectives. In effect, the board is being asked to approve and promote the culture of the enterprise, emphasizing to management a culture of integrity, a culture of compliance, and a culture of risk management. For example, embedding integrity across the enterprise can be achieved by taking a firm stand when a senior manager comes too close to an ethical line.

"You need to ensure that you have some sort of an umbrella governance framework in order to consolidate and coordinate all of your assurance functions."

Ron Bilyk, Zurich Canada

Cairns also noted that effective risk governance requires the board to set the appropriate "tone from the top," while making sure that senior management is engaged in the implementation process and that risk management is not seen as simply a compliance requirement.

He cautions that there are additional challenges when the enterprise is a subsidiary of a foreign parent because the parent might have a number of international strategies, including risk management processes to which all of the subsidiaries worldwide are expected to comply. The key in this scenario is to provide the board with high quality and thorough information. While the risk manager may be giving the board a "Canadian version" of an international risk management program, it is still possible to develop a sufficiently robust process that can be probed thoroughly.

For Ron Bilyk of Zurich Canada, a primary responsibility of the board is to regularly assess the enterprise's risk profile, which is critical for determining how to adequately and appropriately assign duties and responsibilities among senior managers. He also noted that the board needs to be well-informed about the regulatory environment. While regulatory guidance is often flexible and provides opportunities for the board to structure its activities in relation to its size and other circumstances, senior management must ensure that the board is aware of the specifics of guidance, such as guidelines for investment, capital management, and reinsurance.

KPMG suggests that certain high-level questions should be asked routinely by board members to confirm that the enterprise is on the right track regarding its commitment and approach to risk governance. These questions could include:

- Where is the business headed?
- How do we govern the different assurance advisors and external consultants providing support to the governance and financial processes?
- What are the expectations of regulators, shareholders, policyholders, and rating agencies?
- Which board committees are required? Is there a transparent mandate for each committee? Is a separate risk committee appropriate?
- Does the board possess the necessary "risk literacy" to oversee the risk management function?
- How should the interface between the board and its relevant committees be structured within the risk strategy and in relation to risk management issues?
- What is the mandate of the risk function and what is the chief risk officer's role? How does the chief risk officer go from being "controller" to "advisor"?
- How are the interfaces between CEO, CFO, chief risk officer and actuary defined, and how will they function in practice? How should the enterprise demonstrate independent and effective oversight functions?

Responsibilities of senior management

Ron Bilyk commented on the importance of ensuring that senior managers communicate their knowledge up to the board on a regular and timely basis. This is important because senior managers likely have superior access to the first-hand knowledge about emerging issues and trends from their internal management information systems, or from the collective body of intelligence that they have within the enterprise. Creating a regular stream of communication and awareness up to the board ensures that if any change to process or regulation comes to light, the board is made aware of it on a timely basis and understands it so that appropriate action can be taken.

"The role of the board is to oversee, and the role of senior management is to implement [the ERM program], and one has to be very careful not to cross those lines."

John Cairns, Chubb Insurance

For John Cairns, it is important that senior managers routinely set aside time to spend with board members to review the details of the most important risks, such as the enterprise's top-10 risks. Senior managers should also provide the board with details about the controls that have been placed on these risks, and the system used to make the assessments about the effectiveness of controls.

Risk committee

When is it appropriate to establish a risk committee of the board to oversee risk management on an enterprise-wide level? The consensus is that it depends on the nature, size, complexity and risk profile of the individual enterprise, and therefore should be decided on a case-by-case basis. For John Cairns, the most important factor is the risk profile. A small enterprise with a complex risk profile may wish to establish a risk committee, whereas a larger enterprise that is not overly complex may decide against establishing a separate committee. For Ron Bilyk, more important than having a separate risk committee is to have people on the board who think about risk in appropriate detail on a regular basis.

> **"You have to have some way of making sure that if there is any significant change in the organization – any process change, any regulatory change – that the board is made aware of it and understands it soon enough so that they can take the appropriate action."**
>
> *Ron Bilyk, Zurich Canada*

If the enterprise decides that it could support a separate risk committee, the committee should be given a clear mandate and appropriate status and visibility throughout the enterprise. All committee members, including the chair, should be independent of senior management. In terms of "risk literacy," some committee members should have sufficient knowledge of risk management within financial institutions and, where appropriate, the committee should include individuals with technical knowledge in risk disciplines that is significant to the enterprise.

A board-level risk committee's mandate is likely to include:

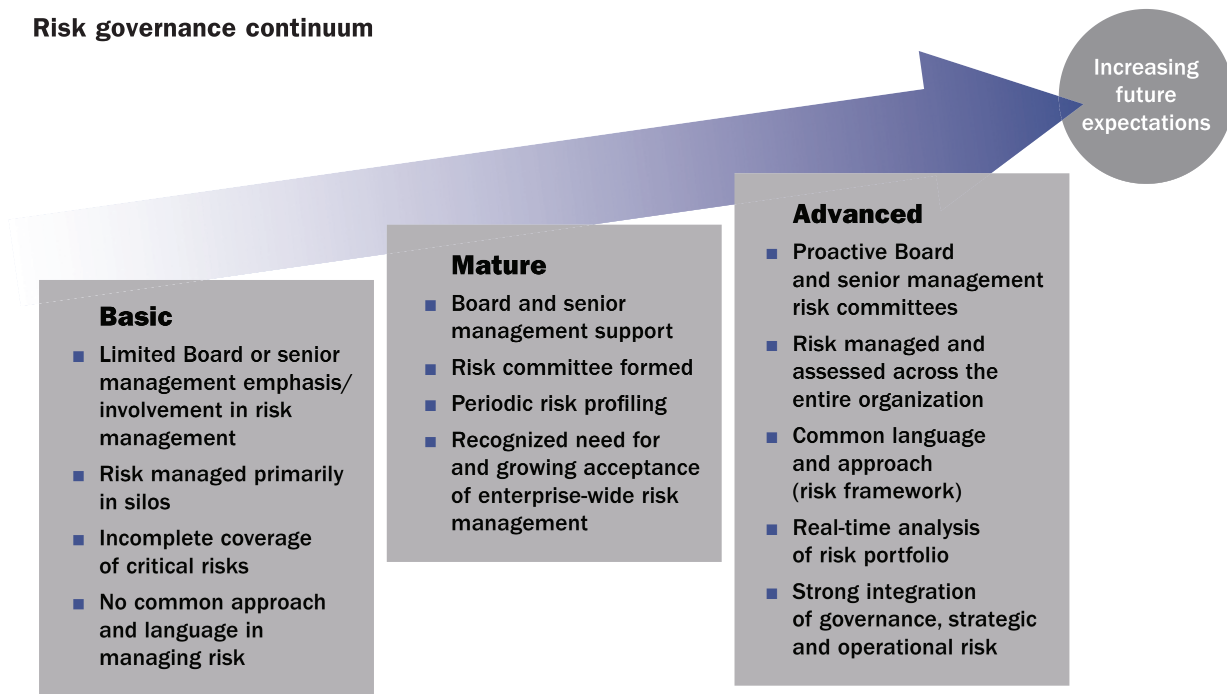
- Approving the enterprise's risk appetite statements and risk appetite framework;
- Seeking assurance from the chief risk officer that oversight of risk management activities of the enterprise is independent of operational management and adequately resourced, and that risk information or analysis prepared by business lines is objective;
- Establishing processes to verify assurances provided to the committee;
- Maintaining an awareness of material changes to the enterprise's business strategies, corresponding risk appetite and the limits within which the enterprise is authorized to act, as well as internal controls;
- Receiving timely and accurate reports on significant risks to the enterprise and to exposures in relation to approved limits;

- Being satisfied that material exceptions to policies and controls are identified, monitored, measured and controlled in a timely manner;
- Maintaining an awareness of the techniques and systems used to identify, measure, monitor, mitigate and report on risks;
- Approving the mandate, competencies and resources of the chief risk officer, at least annually, and approving the chief risk officer's performance review;
- Overseeing succession planning for the chief risk officer position and other key positions within the risk management function.

Governance maturity

The accompanying chart highlights that no matter where the enterprise is on the ERM maturity continuum today, there is an expectation that what might seem mature today will seem basic in two to three years time, with activities that are currently on the advanced portion of the graph becoming normal going forward.

Risk governance continuum



©2012 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

That being said, developing and implementing a risk management structure and culture that is effective for each enterprise takes time, as well as some trial and error. The key for P&C insurers is to make steady and tangible progress toward a greater understanding and management of their enterprise-wide risks.

Conclusion

Seminar discussions with P&C insurers revealed certain consistent practical lessons in implementing ERM. Some of the main lessons from this report are summarized below. They highlight the necessity of combining organizational consensus, strong executive leadership, and technical expertise to effectively implement ERM.

Define the value to the enterprise of an ERM program. Concerns were raised about the difficulty in demonstrating the value of ERM across the enterprise. This is largely because traditional investment metrics (for example, return on investment and return on equity) cannot capture the value of ERM. The business case for ERM examines shareholder value, risk mitigation, and silo elimination. These tend to be goals, and goals can be difficult to measure and to articulate to the board and to management. This is why finding ways to demonstrate "value creation" is important to many ERM practitioners. Identifying the benefits and impacts that the enterprise expects to achieve from its ERM program is useful, which may include improved decision-making at the strategy level, improved corporate governance, greater efficiency of operations, and enhanced capital allocation.

Define risk terminology on an enterprise-wide basis. Experienced ERM practitioners felt that each enterprise needs to develop its own glossary of key risk terms at the start of the ERM implementation process. This will ensure that all members are "on the same page" with respect to commonly used definitions. At a minimum, the enterprise needs to agree on definitions for such key terms as risk management, risk tolerance, risk capacity, and risk appetite.

Assign responsibility for ERM. Depending on the size and complexity of the enterprise, a risk committee of the board and/or a chief risk officer may be required. Participants agreed that the decision should be made on an enterprise-by-enterprise basis. However, whether or not either is necessary, it was considered imperative that the board include members who are "risk literate" and systematically consider risk management as part of their mandate.

Take stock of what the enterprise is currently doing right. Many enterprises have existing controls in place for well understood risks, such as business interruption, environmental liability, or workplace injury. In most cases, individuals responsible for these controls also conduct risk assessments. Searching out existing practices allows the enterprise to leverage these practices within the broader ERM environment.

Build a risk management culture. Many parts of the enterprise have a stake in risk management and a risk-aware culture is necessary to ensure that ERM becomes institutionalized within the enterprise. Risk training at every level of the enterprise was recommended by many participants and speakers. Also, it is considered imperative that "risk champions" are identified and nurtured at all levels within the enterprise. Seek out individuals who are knowledgeable about the enterprise and able to influence others. It is also vital that risk "fixes" are delegated to whoever is accountable for managing the business function most closely associated with the risk. This may be one individual, or it may be a group. Even when a specific individual is not obviously accountable, it was felt that a "risk owner" should be assigned to each risk.

Measure performance and report on progress. Regular monitoring throughout the risk management process is important to ensure currency of risk information since the environment in which the enterprise operates is constantly shifting, as are the risks it faces. Regular monitoring also continuously improves ERM practices. Measuring risk management performance should include both quantitative and qualitative measures. Measures need to be efficient in terms of demands on time, effort and resources, and the results need to be presented in a format that facilitates learning and improvement throughout the enterprise. Moreover, risk managers need to regularly report to the board and senior management on successes and new challenges connected with the ERM program. Progress reports are an opportunity to highlight the differences that ERM is making in the enterprise.

Develop "soft skills". Effective communications skills are necessary to demonstrate the positive value of risk management and to achieve the necessary "buy-in" at different levels of the enterprise. For example, risk managers need to be able to articulate how employees can contribute in their own way. Constant communication also allows risk managers to learn from stakeholders, and to obtain an enhanced understanding of the context, risks, and effect of the risk management plan. Communication also includes consulting with internal and external stakeholders at each step of the ERM process to ensure that those responsible for implementing ERM – as well as those with a vested interest in the outcome of the ERM process – understand the basis upon which decisions are made and why certain actions are necessary.

Integrate ERM into performance management. From a human resources perspective, goal-setting linked to ERM should be one component of an individual's performance management plan. While there are competing theories about how this can be accomplished, it is believed to be an important component to developing an effective ERM culture.

Build a unique ERM plan. Perhaps the most consistent theme to emerge in discussions, and one that is highlighted at several junctures in this report, is the idea that there is no one path to success in implementing ERM. Each enterprise is unique, and each path should therefore be unique.

Property and Casualty Insurance Compensation Corporation
20 Richmond Street East, Suite 210
Toronto, Ontario M5C 2R9
Phone (416) 364-8677
Fax (416) 364-5889
www.pacicc.ca