Enterprise Risk Management
Organizational Structure & Sustainability

Leading Industry Practices

Insurance Conference
November 24, 2011

KPMG LLP
Table of Contents

SECTION 1.0 — Insurance Industry Risk Management Challenges
- 1.1 Enterprise Risk Management
- 1.2 Risk Capital
- 1.3 Risk Appetite
- 1.4 Operational Risk

SECTION 2.0 — Enterprise Risk Management - Organizational Structure and Sustainability - Leading Practices
- 2.1 ERM - Organizational Structure and Sustainability Challenges
- 2.2 CSA Q31001 – A Leading Practice Risk Management Standard
- 2.3 CSA Q31001 – Mandate and Commitment to Risk Management
- 2.4 CSA Q850 – Integration into Organizational Processes
- 2.5 Improving ERM Performance
- 2.6 Insurance Industry Risk Management Improvement Opportunities
- 2.7 An Integrated Approach

SECTION 3.0 — Enterprise Risk Management - Organizational Structure and Sustainability – Leading Practice Examples
- 3.1 - 3.4 Organizational Structure - Examples
- 3.5 Lessons Learned
- 3.6 Sustainability Questions

SECTION 4.0 — Enterprise Risk Management – Organizational Structure and Sustainability – Canadian Insurance Industry Examples
- 4.1 Example #1
- 4.2 Steps to Improve Your Risk Management Organizational Structure and Sustainability

SECTION 5.0 — Risk Management Challenges for Insurers

APPENDICES
Section 1.0

Insurance Industry Risk Management Challenges
1.0 Insurance Industry Risk Management Challenges

The insurance industry is facing a number of interrelated risk management challenges driven by economic, regulatory, operational and governance factors. Such challenges include:

1. The development and implementation of an enterprise risk management program reflective of international standards

2. Ensuring that risk capital meets regulatory requirements and maintains competitive product pricing

3. Meeting regulatory and governance requirements to develop more explicit and formal statements of risk appetite

4. Developing an operational risk management framework and measurement approach that meets economic capital requirements, mitigates high operational risk exposure and affords operational improvement opportunities
Section 1.1

Insurance Industry Risk Management Challenges – Enterprise Risk Management
1.1 AM Best ERM Expectations and Industry Views

**AM Best, Rating Agency Perspectives: ERM and Other Key Rating Drivers**

“Insurers’ ERM practices should be appropriate for their risk profile

Best expects “complex” companies to more fully adopt ERM and demonstrate usage of EC modeling in their decision making

Capital requirements will be closely linked to Best’s opinion of a company’s ERM strength and its “volatility”…”

---

**Colin Devine, Managing Director – Life Insurance, Citi US Equity Research in ACLI Global Leadership Forum, November 16, 2008**

“In this type of market, risk management is what separates the leaders from the rest.”

“I certainly see risk management as a core competency for some companies and others where it is noticeably less."

"The better risk management cultures are those companies being run by *actuaries* instead of *by sales people.*"
1.1 S&P ERM Expectations

Summary of S&P ERM Evaluations – “Strong“ ERM Rating (November 2007*)

To Qualify for a Strong ERM, Insurers must have ALL of:

- Strong or Excellent Risk Control for ALL key risks
- Adequate or better Emerging Risks Management
- Strong or Excellent Strategic Risk Management

Summary of S&P ERM Evaluations – Board Roles in ERM

- Oversight & Control
- Strategy
  - Risk Tolerance / Risk Appetite
  - Capital Budgeting:
    - Translate risk appetite & tolerance to risk limits
    - Based on full range of strategic concerns including risk reward information
  - Risk Profile
- Performance Evaluation
  - Monitoring risk adjusted value measures: RORAC, change in EV

S&P announcement (February 4, 2009)
“Although we are not changing Standard & Poor's baseline insurance risk-based capital adequacy model, we are applying incremental stresses for these asset classes across all confidence levels during this difficult economic period.”
1.1 Stakeholder Risk Management Expectations

- Optimize cost of capital
- Risk transfer via capital markets
- Direct relation between risk management and cost of funding
- Balancing growth, safety & security
- IFRS 4 Phase II
- Economic capital
- Changing solvency regulations
- Transparency and comparability
- Selective risk taking
- Benchmarking insurers
- Pricing
- Performance measurement
- Maintain/improve rating
- Increasing requirements of rating agencies and analysts
- M&A activity

... which requires integration of Risk, Performance and Capital Management through a leading practice risk management structure
1.1 Enterprise Risk Management Maturity Continuum

**Basic**
- Limited Board or senior-management emphasis/involvement in risk management
- Risk managed primarily in silos
- Incomplete coverage of critical risks
- No common approach and language in managing risk

**Mature**
- Board and senior-management support
- Risk committee formed
- Periodic risk profiling
- Recognized need for and growing acceptance of enterprise-wide risk management

**Advanced**
- Proactive Board and senior-management risk committees
- Risk managed and assessed across the entire organization
- Common language and approach (risk framework)
- Real-time analysis of risk portfolio
- Strong integration of governance, strategic, and operational risk
Section 1.2

Insurance Industry Risk Management Challenges — Risk Capital
1.2 Market Trends and Current Environment

**Current Trends**
- Board Accountabilities and Committees
- Executive Compensation Policies
- Prudential Regulatory Focus

**Regulatory Guidance**
- OSFI Corporate Governance Statements
- OSFI Updated Supervisory Framework
- Canadian Risk Standard – CSA Q31001
- OSFI Guidance on Advanced Solvency models

**International Guidance**
- Senior Supervisors Group Studies - *OSFI participation*
- BIS - *Principles for Enhancing Corporate Governance*
- Basel III
- Solvency II – *Pillar II Own risk solvency assessment*
- Standard & Poor’s – *Evaluating Risk Appetite*
1.2 Risk, Capital and Insurers

In addition to regulators, other interested parties include:

- **Owners/investors** – want to know that decision-making is based on assessment of both risk and capital needs

- **Capital markets** – expect use of capital to reflect comprehensive risk assessment approach

- **Rating agencies/analysts** – increasingly interested in insurers’ risk management practices

- **Boards of directors/management** – want improved decision making, reputation concerns

- **Policyholders** – solvency concerns

**Transparency: a common interest**
1.2 EU: Solvency II - the “Three Pillars”

Three-pillar approach

**Pillar 1:** Quantitative capital requirements
- Technical provisions
- Minimum capital requirements
- Use of internal models
- Investment principles

**Pillar 2:** Qualitative requirements
- Supervisory review
  - Governance, risk management and required functions
  - Own risk and solvency assessment (ORSA)
  - Supervision process

**Pillar 3:** Reporting, disclosure, and market discipline
- Transparency
- Disclosures
- Support of risk-based supervision through market mechanisms

Market-consistent valuation and risk-based requirements
Business governance Risk-based supervision
Disclosure, transparent markets
1.2 Risk and Capital Management - Much More than Financial Modelling

- Understanding the risks that threaten your objectives
- Defining risk appetite, and identifying risks outside your risk appetite
- Dealing with more subjective risks (e.g. reputational)
- Aligning risk management with business objectives
- Aligning management incentives with risk management
- Embedding risk and capital management in the management and governance of the enterprise
1.2 Benefits of Integrated Risk and Capital Management

- Improved understanding of risks and their true cost to the organization
- Increased management accountability
- Company culture with a greater awareness of risks and a consistent definition and application of risk appetite
- Stronger ability to quantify risk adjusted capital adequacy position to regulators and rating agencies
- Transparency – if they can’t see/read it, it doesn’t exist
- Improving corporate governance and the perception of corporate governance to external parties
- Providing a prospective view of the capital requirements of the organization
1.2 Capital Planning Cycle – Isolated Planning Functions Need to be Integrated

**Business Planning**
- Board and Senior Executive approval
- Capital allocation and limit setting
- Contingency planning based on implications of planning and stress results

**Risk & Capital Planning**
- Revision of business and risk strategy
- Scenario definition and evaluation
- Assessment of impact on B/S, P&L, and capital adequacy

**Stress Testing**
- Assessment of performance (e.g., risk adjusted profitability) of businesses
- Target setting exercise
- Development of detailed BU plan

Diagram illustrates the cycle with steps 1 to 9, indicating the integration of planning functions.
Section 1.3

Insurance Industry Risk Management Challenges – Risk Appetite
1.3 Governance of the Risk Management Function

Risk Management

In recent papers and speeches, OSFI has highlighted several areas of focus and improvements in the governance program implemented at financial institutions:

- The role of the Board – active engagement; setting and limiting risk appetite
- Risk appetite - linkage to strategic and capital planning processes; how defined, measured, monitored, controlled and reported
- Board composition and experience – risk literate; expectations are rising
- Role of the Board in compensation
- Board and Senior Management oversight of risk
- Operational controls

The mandate of the new corporate governance unit at OSFI is to conduct reviews of the risk governance practices across the largest of the Canadian institutions.
1.3 Industry Guidelines – Canadian Risk Management Standard

**CSA Q31001**

- Risk appetite is informed by risk mitigation decisions made during the risk management process.

- Determination of risk appetite can be through development of a strategic policy set at the governance or organizational level or via a bottom up summation of risk mitigation decisions.

- Risk appetite is informed by stakeholder input, organizational experience, lessons learned, resources and capacity, and changing external or internal business context.

- Risk appetite should recognize the balance of positive and negative consequences of risk decisions (e.g. the health benefits and the negative health consequences of particular vaccines).
1.3 International Observations on Risk Appetite

Findings include:

- In some cases there is no clear statement of Risk Appetite, or no obvious understanding of what it actually is in concept.
- There is a wide range of approaches to articulating Risk Appetite - from short high-level statements to a few pages of detailed thoughts.
- The quality of the statement of Risk Appetite ranges from poor to quite good.
- A lack of analysis of Risk Appetite through the use of scenario analyses, stress testing etc.
- Not always clear that the board has been heavily engaged in setting the Risk Appetite.
- In some cases there is a disconnect between the Risk Appetite statement and its translation into operational management.
- With some subsidiaries or branches of foreign-owned insurers, group risk management practices are adopted without necessarily full and proper engagement of local management and/or board.
1.3 Risk Appetite Statement Specification

Definition of the risk appetite statement:

- Risk appetite is the total impact of risk an organization is prepared to accept to achieve its strategic objectives.
- It represents the aggregation of all risks within each risk category, including strategic, capital management, liquidity, insurance, investment, credit & concentration, legal & regulatory and operational risk.
- The amount of risk an organization accepts will vary from organization to organization.
- Factors, such as the external environment, people, business systems and policies can influence an organization’s risk appetite.
- Organizations can exercise different methods to measure risk appetite, ranging from simple qualitative measures to complex quantitative models of economic capital and earnings volatility.

Characteristics of a well-defined risk appetite statement

- Reflective of strategy, including all key aspects of the business - organizational objectives, business plans and stakeholder expectations.
- An acknowledgement, willingness and capacity to take on risk.
- Documented as formal risk appetite statements.
- Considerate of the skills, resources and technology requirements to manage and monitor risk exposures in the context of risk appetite.
- Inclusive of a tolerance for loss or negative events that can be reasonably quantified.
- Periodically reviewed and reconsidered with reference to evolving industry and market conditions.
- Reviewed by the Board.
### 1.3 Components of a Risk Appetite Statement

<table>
<thead>
<tr>
<th>Metric</th>
<th>Illustrative possible components of definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quantitative</strong></td>
<td></td>
</tr>
<tr>
<td>Target rating</td>
<td>■ Define capital requirements</td>
</tr>
<tr>
<td></td>
<td>■ May reference ratings set by rating agencies</td>
</tr>
<tr>
<td>Earnings volatility</td>
<td>■ Specify desired earnings forecast by more than X% at a XX% confidence level</td>
</tr>
<tr>
<td></td>
<td>■ Target dividends</td>
</tr>
<tr>
<td>Diversification</td>
<td>■ Allocation of capital into various business, markets or franchisees</td>
</tr>
<tr>
<td>Liquidity headroom</td>
<td>■ Available liquidity resources to meet requirements at a percentage confidence interval</td>
</tr>
<tr>
<td><strong>Qualitative</strong></td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td>■ Key statements of expected ethical behaviour and corporate culture</td>
</tr>
<tr>
<td>Regulation</td>
<td>■ Statements regarding regulatory compliance</td>
</tr>
<tr>
<td>Governance</td>
<td>■ Statements regarding organizational governance expectations</td>
</tr>
<tr>
<td>Strategy/growth</td>
<td>■ Overview of approach regarding risk strategy / growth expectations</td>
</tr>
<tr>
<td>Geopolitical/</td>
<td>■ Statements regarding geopolitical or cultural risk factors</td>
</tr>
<tr>
<td>Cultural</td>
<td></td>
</tr>
</tbody>
</table>

Source: Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward
Examples Risk Appetite statements

- The minimum continuing capital and surplus requirement ratio preferred operating range is the minimum operating level of XXX% plus 20 percentage points
  - It must not fall below the internal capital target level of XXX
- The company must meet all regulatory solvency and capital requirements
- The Liquidity Ratio is to be maintained between XXX% and XXX% for both immediate and ongoing liquidity needs
- Change in total surplus for the year must be between X-Y%
- The return on equity for insurance is a minimum of X% plus 3 percentage points
- The recovery time objective for critical operations is 24 hours
- Administrative expenses must decrease from prior year by a minimum of x% with a target of 10%
- The company will not:
  - Breach any laws or regulations of the jurisdictions in which it operates
  - Risk any degradation to its rating agency or regulatory ratings
  - Risk any significant damage to its reputation or its competitive position
  - Risk over concentration in its investment or business activities
Section 1.4

Insurance Industry Risk Management Challenges – Operational Risk
1.4 The Operational Risk Challenge

Definition: The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events

- The definition includes legal risk, which is the risk of loss resulting from failure to comply with laws as well as prudent ethical standards and contractual obligations.
- It also includes the exposure to litigation from all aspects of an institution’s activities.
- The definition does not include strategic or reputational risks.

Alternate definition: An attempt to frame the unframeable, to assuage fears about the uncontrollable ‘rogue others’ and to tame the man-made monsters [of the financial system].

Prof Michael Power, Organized uncertainty: designing a world of risk management (2007)
In the past few years, financial institutions have been through an intense period of change that has greatly increased the potential for operational risk.

Increased regulation, mergers and acquisitions, internal restructuring and changes to distribution, systems and technology bring management up against a potential minefield of risks and issues.

The way financial sector organizations manage these risks is under greater scrutiny than ever before, as they are liable to policy holders, shareholders, regulators, and other stakeholders.

Insurers have been ahead of banks and other financial institutions in modeling most risks, but operational risk is an exception to this.

The Solvency II and Basel II accords provide comprehensive frameworks for the governance and management of risk, including operational risk.
## 1. 4 Operational risk – Regulatory Guidance

<table>
<thead>
<tr>
<th>DATE</th>
<th>SOURCE</th>
<th>PUBLICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superceded</td>
<td>OSFI</td>
<td>Sound business and financial practices framework, reported on in PARC for life insurers.</td>
</tr>
<tr>
<td>May 2006</td>
<td>OSFI</td>
<td>Corporate Governance at TSA &amp; AMA Institutions</td>
</tr>
<tr>
<td>Ongoing</td>
<td>Solven</td>
<td>QIS models for measuring capital required, including specific amounts for operational risk</td>
</tr>
<tr>
<td>development</td>
<td>cy II</td>
<td></td>
</tr>
<tr>
<td>June 2011</td>
<td>BCBS</td>
<td>Principles for the Sound Management of Operational Risk</td>
</tr>
<tr>
<td>June 2011</td>
<td>BCBS</td>
<td>Operational Risk - Supervisory Guidelines for the Advanced Measurement Approaches</td>
</tr>
<tr>
<td>August 2011</td>
<td>OSFI</td>
<td>Memo to Banks referencing BCBS - Principles for the Sound Management of Operational Risk:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“OSFI believes that the principles outlined in the 2011 paper establish sound practices that are relevant to all deposit-taking institutions, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>expects institutions to take account of the nature, size, complexity and risk profile of their activities when assessing their practices against</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the updated principles in the Principles paper in the course of normal compliance reviews. Institutions should develop a plan to remedy any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deficiencies that come to light during their assessments.”</td>
</tr>
</tbody>
</table>
### 1.4 Some Examples of Reported Operational Risk Events

<table>
<thead>
<tr>
<th>LOSS CATEGORY</th>
<th>COMPANY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft and Fraud</td>
<td>Co-operators General Insurance (2003)</td>
<td>Missing hard drive contained client names, addresses, bank account details, beneficiaries, social insurance numbers, pension fund values, pre-authorized checking information, and mothers' maiden names.</td>
</tr>
<tr>
<td>Unauthorised Activity</td>
<td>UBS (2011)</td>
<td>UBS said it had lost around $2 billion due to rogue dealing by a London-based trader at the Swiss bank and police said they had arrested a man on suspicion of fraud.</td>
</tr>
<tr>
<td>Suitability, Disclosure and Fiduciary</td>
<td>Manulife (2005)</td>
<td>Manulife Securities had a referral arrangement with the Portus hedge fund and failed to disclose to its clients the syndication fees that comprised part of its compensation from the referral arrangement. Aggregate cost to Manulife of its compensation offer to its clients was $246 million.</td>
</tr>
<tr>
<td>Clients, Products and Business Practices</td>
<td>Prudential Insurance</td>
<td>$2 billion settlement of class action lawsuit</td>
</tr>
<tr>
<td>Clients, Products and Business Practices</td>
<td>Providian Financial</td>
<td>$400 million settlement &amp; restitution</td>
</tr>
</tbody>
</table>
## 1.4 Some Examples of Common, But Usually Unreported Risk Events

<table>
<thead>
<tr>
<th>LOSS CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft and Fraud</td>
<td>• Fraudulent claims – fabricated events by fraud rings; exaggerated claims.&lt;br&gt;• Unreported deaths for annuities and pensions.&lt;br&gt;• Jumbo commissions on fraudulent life policies.</td>
</tr>
<tr>
<td>Unauthorised Activity</td>
<td>• Internal collusion with external claims or other service providers.</td>
</tr>
<tr>
<td>Suitability, Disclosure and Fiduciary</td>
<td>• Failure to comply with training and sales practices requirements by sales force.&lt;br&gt;• Failure to provide adequate selection and oversight of sales force.</td>
</tr>
<tr>
<td>Clients, Products and Business Practices</td>
<td>• Failure to apply underwriting or claims settlement standards.&lt;br&gt;• Over-rides of underwriting or claims settlement standards.</td>
</tr>
<tr>
<td>Clients, Products and Business Practices</td>
<td>• Errors in product design or pricing.</td>
</tr>
<tr>
<td>System Failures</td>
<td>• Interface errors between billing and receivable systems.&lt;br&gt;• System configuration errors affecting complex computations.&lt;br&gt;• Loss of data.</td>
</tr>
</tbody>
</table>
Section 2.0

Enterprise Risk Management
Organizational Structure and
Sustainability
Leading Practices
2.1 ERM – Organizational Structure and Sustainability Challenges

- A narrow risk management perspective primarily focused on compliance
- An immature ERM governance and accountability structure
- A lack of a vision or understanding of the linkages between enterprise, financial and operational risk using a common framework
- A plethora of financial and operational risk management activities throughout the organization with multiple methods, frameworks, etc.
- No apparent motivation to look at the myriad of frameworks to identify similarities, efficiencies and integration opportunities
- A process focus rather than a decision-making focus to risk management
- Over reliance on siloed or specialty risk management expertise
- Lack of communication and interaction of individual business units or operational risk managers both horizontally and vertically within the organization
- No clear reporting or governance structure to surface operational risks which may quickly become strategic risks (threats and opportunities)
- Passive engagement by the Board of Directors in major emerging, strategic or reputational risks
2.1 ERM – Organizational Structure and Sustainability Challenges Cont’d

Serious and often devastating impacts on an insurance business can be attributed to:

1. **Board Skill and non-executive director (NED) Control**: Risks arising from limitations on board skills and competence and on the ability of NEDs effectively to monitor and, as necessary, control the executive arm of the company.

2. **Board Risk Blindness**: Risks from board failure to recognize and engage with risks inherent in the business, including risks to business model, reputation and ‘license to operate’, to the same degree as they engage with reward and opportunity.

3. **Inadequate Leadership on Ethos and Culture**: Risks from a failure of board leadership and implementation on ethos and culture.

4. **Defective Internal Communication**: Risks from the defective flow of important information within the organization, including up to board level.

5. **Risks from Organizational Complexity and Change**: This includes risks following acquisitions.

6. **Risks from Incentives**: This includes the effects on behaviour that results from both explicit and implicit incentives.

7. **Risk ‘Glass Ceiling’**: Risks arising from the inability of risk management and internal audit teams to report on and discuss, with both executive and non-executive directors, risks emanating from higher levels of their company hierarchy, including risks from ethos, behaviour, strategy and perceptions.

Source: Roads to Ruin, A study of Major Risk Events: Their Origins, Impact and Implications, A Report by Case Business School on behalf of Airmic
The following developments will have to occur to create a mature and sustainable risk management culture:

1. The scope, purpose and techniques of risk analysis and management will need to be rethought in order to capture risks that are not routinely covered by current approaches.

2. Risk professionals may need to extend their skills so that they become competent to identify, analyze and discuss risks emerging from the ethos, culture and strategy of their company and the activities and behaviour of their leaders.

3. The role and status of risk professionals will have to change so that they can safely evaluate, report and discuss all they find on these underlying risks at all levels, including at the board level.

4. Boards, and particularly the Chairman and non-executive directors (NEDs), need to recognize the importance of risks that are not captured by current approaches – they also need to focus on how to ensure missing risks are captured.

Source: Roads to Ruin, A study of Major Risk Events: Their Origins, Impact and Implications, A Report by Case Business School on behalf of Airmic
Unlike previous risk management standards which could be implemented as independent activities, this new Canadian risk management standard requires:

- an integrated approach with risk management activity being fully embedded and indistinguishable from an organization’s regular arrangement of governance as illustrated in the chart on the next slide.

- decisions and managerial activities be carried out using the risk management process, including those of the senior decision-making body that should use it in their strategic planning and governance activities

- The standard fully supports regulatory and rating agency pronouncements about improving enterprise risk management practices
2.3 CSA Q31001 – Mandate and Commitment to Risk Management

Mandate and commitment to risk management is demonstrated when senior management:

- integrates it into existing governance, planning, execution and performance management processes
- specifies how and when risk will be managed through the approval of a risk management framework and policy and encourages it to be integrated at all levels of the organization (strategic, operational and project levels)
- requires monitoring and reporting of the organization’s risk management framework regularly to ensure it is still appropriate
- sets and manages the risk appetite of the organization
- leads by example in applying risk management to its own activities
- renews commitment to effective risk management regularly as time, events, and senior leadership change

Note: See Appendix A CSA Q31001 – Risk Management Framework
2.4 CSA Q850 – Integration into Organizational Processes

Organizations should ensure that risk management is never a separate activity, but fully integrated with all decision-making processes. Risk management should be integrated into (among other things):

- strategic planning
- operational planning
- policy development
- governance frameworks and structures
- resource management
- major investments (e.g. joint ventures, mergers, key supplier relationships)
- budgeting
- performance evaluation
- internal control over financial reporting
- legislative compliance
- information technology
- project management
- business continuity management planning

The risk management governance and management structure should reflect this multi-disciplinary perspective.
2.5 Improving ERM Performance

Figure 3: Best-in-Class Actions to Improve ERM Performance

- Integrate risk and performance management for more accurate, timely, and fiscally-responsible business decisions: 35% (Best-in-Class), 31% (All others)
- Establish & enforce an enterprise-wide framework with consistent policies and procedures for risk management activities: 32% (Best-in-Class), 25% (All others)
- Converge risk and compliance activities for improved efficiency and accountability: 27% (Best-in-Class), 18% (All others)
- Ensure executive-level commitment to risk management initiative: 27% (Best-in-Class), 27% (All others)

Source: Aberdeen Group, February, 2009
## 2.6 Insurance Industry Risk Management Improvement Opportunities

<table>
<thead>
<tr>
<th>Topics</th>
<th>What are we hearing from the insurance industry?</th>
<th>What changes are being considered?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Culture</td>
<td>Risk management often perceived as compliance exercise rather than a business issue</td>
<td>Risk management will be a strategic function. Integration of risk function and business is critical</td>
</tr>
<tr>
<td>ERM Organization Structure</td>
<td>Important factor in ERM and a contributor to the recent economic problems – absence of risk committees, lack of independent risk function</td>
<td>Re-evaluate roles of CROs and business owners. Establish risk committees and governance to address various issues such as roles &amp; responsibilities, independence, and interdependency of risks</td>
</tr>
<tr>
<td>Senior Management and Board Members</td>
<td>Unbalanced focus on profits vs. risk management. Lack of risk management expertise at senior level</td>
<td>Executive team must demonstrate leadership in ERM (“tone at the top”), which will be better embedded into company’s culture and operations</td>
</tr>
<tr>
<td>Risk Tolerance and Appetite</td>
<td>High level definition. Not operationalized at business level. Not clearly communicated and not enforced on a real time basis</td>
<td>Clearly defined and better communicated. Executable and enforced. Linkage to economic capital modeling</td>
</tr>
<tr>
<td>Operational Risk</td>
<td>Remains as a weak spot in ERM with simplistic assumptions</td>
<td>Strengthen ORM with other interdependent risks. More sophisticated scenario testing and better linkage to economic capital. Greater focus on model validation</td>
</tr>
<tr>
<td>Economic Capital Model</td>
<td>Effective usage of EC is lagging behind. Not fully utilized in decision making and capital allocation</td>
<td>Clearly understand model limitations. Greater forward looking view. Embed EC into decision making and performance management</td>
</tr>
<tr>
<td>Scenario Analysis and Testing</td>
<td>Lack focus on interdependency of risks. Emphasis on historical events, reactive, not forward looking. Shocks and stresses too weak</td>
<td>Key focus will be on risk interdependencies, especially in the operational risk area. Greater consideration of more severe scenarios and stress testing. Enhancements through dedicated data collection, both internal and external.</td>
</tr>
<tr>
<td>Reporting &amp; Systems</td>
<td>Reports with multiple views of the same risk, not available on a timely basis. Inadequate IT systems and processes</td>
<td>Enhance discipline of single view of risk. Improve effectiveness through common Governance, Risk and Compliance platform</td>
</tr>
</tbody>
</table>
2.7 An Integrated Approach
Section 3.0

Enterprise Risk Management
Organizational Structure and Sustainability
Leading Practice Organizational Structure Examples
3.1 Organizational Structure – Example # 1

- Board of Directors
- Audit Committee
- Risk Oversight Committee
- Operational Senior Management
  - Operational Risk Management
- Commercial Senior Management
- Chief Risk Officer
- Enterprise Risk Management
- Chief Financial Officer
- Chief Internal Auditor
3.2 Organizational Structure – Example # 2

Board of Directors

Audit Committee

Risk Oversight Committee

Operational Senior Management

Commercial Senior Management

Chief Financial Officer

Director of Risk Management

Operational Risk Management

Chief Internal Auditor

Enterprise Risk Management & Middle Office
3.3 Organizational Structure – Example # 3

- Board of Directors
  - Governance & Risk Committee
    - Planning & Risk Oversight Committee
  - Audit Committee
- Operational Senior Management
  - Operational Risk Management
- Commercial Senior Management
- Vice President – Strategic Planning
  - Director of Planning and Risk Management
    - Enterprise Risk Management
- Chief Financial Officer
- Chief Internal Auditor
3.4 Organizational Structure – Example # 4

Board of Directors

Governance & Risk Committee

Audit Committee

Enterprise Risk Management Committee

Commercial Senior Management

Operational Senior Management

Operational Risk Management

Chief Financial Officer

Executive Vice President – Legal Counsel & Corporate Secretary

Director of Strategic Planning and Risk Management

Enterprise Risk Management

Chief Internal Auditor
3.5 Lessons Learned

- The ideal structure reflects the size, complexity, culture, risk management resources and leadership within a company.

- The risk management organizational structure should support existing governance and accountability structures within the organizations.

- More structure does not necessarily mean better enterprise risk management - cultural and behavioural factors can lead to adverse risk management.

- The structure has to be designed to reinforce strong risk management leadership and encourage active risk management discussion, debate and, ultimately, decision-making.

- The structure and risk management polices must reinforce the Q31001 principles:
  - Risk management is not distinct from the organization’s planning, management, performance measurement and accountability structure and processes.
  - Risk management exists to support both strategic and day-to-day decision-making.
  - The structure should promote a highly interactive, engaged and holistic discussion and debate about risk from multi-disciplinary perspectives across the organization.
3.6 Sustainability Questions

- **Do we need to establish a separate risk committee as part of our governance structure to unencumber our audit committee?**
  - The trend is toward establishing a Risk Review or Oversight Committee to focus on the broader enterprise risk profile and mitigation strategies linked to the firm’s strategy.

- **Do we need to create the position of the Chief Risk Officer to establish the framework and steward the risk management policy and process?**
  - If our size does not warrant it, do we need to ensure that equivalent responsibilities are assigned to an executive lead?
3.6 Sustainability Questions Cont’d

- **What processes do we put in place to identify, validate and verify the high exposure risks and the mitigation strategies**
  - Business unit involvement
  - Interactive workshops
  - Escalation protocols
  - Risk repository and dashboard reporting
  - Validation – by a risk department, internal audit, or third parties

- **What is the right frequency for refreshing our risk profile?**
  - Quarterly reporting to the Board is common
  - Leading practice is often aligning the refresh with the annual business planning process or multi-year strategic planning process
3.6 Sustainability Questions Cont’d

- How do we establish strong risk management literacy at the Board, Management and Staff levels of our organization?
  - Equivalent to establishing financial literacy on the Board
  - ERM 101 sessions for management and staff
  - Adopting a common standard such as Q31001
  - Developing a common ERM framework and supporting policies and procedures
  - Integrating risk management with existing planning, performance management and reporting accountabilities within business units
Section 4.0

Enterprise Risk Management
Organizational Structure and Sustainability
Canadian Insurance Industry Examples
4.1 Canadian Insurance Industry Example

Risk Management Overview

- The Corporation has a comprehensive risk management framework and internal control procedures designed to manage and monitor various risks in order to protect its business, clients, shareholders, and employees.

- The company’s board of directors, directly and in particular through its Audit and Risk Review Committee, oversees its risk management programs, procedures, and controls.

- The Board is assisted by the risk management department through the Chief Risk Officer, internal auditors, and independent auditors.

- The company has established an Enterprise Risk Committee which comprises senior officers and is chaired by the Chief Risk Officer. It meets on a quarterly basis and oversees and endorses the company’s risk management priorities, assesses the effectiveness of risk management programs, policies, and actions of each key function of its business, and reports on an ongoing basis to the company’s management.
4.1 Canadian Insurance Industry Example Cont’d

Risk Management Structure

• The company’s internal structure is designed to gain a sustainable competitive advantage by fully integrating risk management in its daily business activities and strategic planning.

• The company believes that each of the employees and management teams has a responsibility to take an appropriate action to mitigate risks and ensure compliance with all the legal and regulatory requirements:
  - Heads of departments have primary responsibility and accountability for the effective control of risks/challenges affecting their respective departments. They are responsible for the execution of the risk management policies set by the Enterprise Risk Committee.
  - Risk management members exercise their functions to partner with and support heads of department in the execution of risk management activities.
  - The Internal Audit department provides an independent review of the design and effectiveness of internal controls over the company’s business operational risks. In carrying out this work, this department provides specific recommendations for improving governance, risk, and control framework.
  - The corporate governance and compliance department reviews, analyzes, and reports current and developing legal and regulatory requirements in order to ensure continued compliance.
4.1 Canadian Insurance Industry Example Cont’d

Board of Directors

- Conduct Review and Corporate Governance Committee
- Audit and Risk Review Committee
- Human Resources Committee
- Investment Committee

Enterprise Risk Committee

- Operational and Other Risk Committee
- Senior Management Committee
- Operational Investment Committee
- Profitability Committee
- Reserve Review Committee
- Insurance Committee
- Large Loss Committee

Corporate Governance and Compliance
4.1 Canadian Insurance Industry Example Cont’d

**Notable Features of the Risk Management Structure**

- Risk management is integrated into the strategic planning and day-to-day decision making of the company in keeping with Q31001

- Through the Executive Heads, risk management policies are operationalized and accountability rests with the business units

- An overarching Enterprise Risk Management Committee has been established which provides a multidisciplinary perspective to risk decisions

- Specialty risk committees exist for investments, large losses and operational risk

- The Audit Committee is unencumbered through additional risk management focus of the Conduct Review and Corporate Governance Committee, the Investment Committee and the Human Resources Committee
4.1 Canadian Insurance Industry Example Cont’d

Challenges of the Structure

- Coordinating the risk management decision making of the management and Board committees
- Defining risk appetite statements across the company that supports risk taking decisions in a consistent manner
- Ensuring that risk dashboard reporting and monitoring data are real time

Note: See Appendix B Supplementary Insurance Industry Example
4.2 Steps to Improve Your Risk Management Organizational Structure & Sustainability

Board activities:

- Provide enterprise risk management education at the board level
- Establish buy-in at board level for risk appetite and risk strategy
- Develop “ownership” of risk management oversight by the Board
- Periodic review of the “top” risk profile and mitigation strategies of the enterprise

Management activities:

- Create a high-level risk strategy (policy) aligned with the strategic business objectives
- Create a risk management organizational structure and ensure clear reporting lines
- Develop and assign responsibilities for risk management
- Communicate the Board vision, strategy, policy, responsibilities and reporting lines to all employees across the organization
- Tie performance incentives to good risk management practices
4.2 Steps to Improve Your Risk Management Organizational Structure & Sustainability Cont’d

Establish a common risk culture:
- Use a common language and concepts
- Communicate about risk using appropriate channels and technology
- Develop training programs for risk management
- Identity and train “risk champions”
- Provide success stories and identify quick wins
- Align risk management techniques with the company culture
- Develop a knowledge sharing system

Create risk accountability/responsibility:
- Include risk management activities/responsibilities in job descriptions
- Incorporate ERM concepts into personal goals
- Empower managers with defined risk boundaries
4.2 Steps to Improve Your Risk Management Organizational Structure & Sustainability Cont’d

**Embed risk activities into ongoing business process:**

- Align and integrate risk management activities within business processes
- Embed real-time controls related to risk into digital systems
- Develop continuous improvement processes related to risk

**Measure and monitor risk:**

- Identify key performance indicators and critical success factors related to risk
- Establish success measures for risk strategy and activities
- Provide a periodic process for measuring risk/return
- Identify and implement monitoring processes and methods of feedback
4.2 Steps to Improve Your Risk Management Organizational Structure & Sustainability Cont’d

- Embrace Q31001
- Conduct awareness and training sessions on the standard for the Board, the executive team and risk management staff
- Conduct a maturity assessment of your risk management structure and practices against Q31001
  - The standard defines attributes of leading risk management practices & provides a maturity continuum
- Identify gaps and challenges in your current structure against the leading practices
- Include strong representation from the Board, Executive Management, staff and the Board in the (re)design of the risk management organizational structure to fully support strategic, financial, operational, performance management and day-to-day risk-based decision making
- In keeping with Q31001, introduce a continuous risk management improvement effort including:
  - Periodic independent reviews of the risk management structure, policies and practices
  - Ongoing Board, Executive Management and Staff risk management training and development
Section 5.0

Risk Management Challenges for Insurers
5.1 Advancing Your Organization’s Risk Management Practices

<table>
<thead>
<tr>
<th>Questions</th>
<th>Possible actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>How can we put a comprehensive ERM framework in place?</td>
<td>Enterprise risk management framework/policy development and implementation</td>
</tr>
<tr>
<td>Have we identified the full range of significant risks? Have we identified the most significant ones? Do we keep this up to date?</td>
<td>Conduct board and management workshops Outside challenge of key risk list</td>
</tr>
<tr>
<td>How does our risk management stack up: • against leading practices? • against regulatory expectations?</td>
<td>Enterprise risk management • maturity assessment vs. leading practices • Gap analysis vs. regulatory expectations</td>
</tr>
<tr>
<td>Do we have a clear idea of what our “risk appetite” is? Is it consistent with our business and strategic plan? Is it expressed clearly? Do our people understand it?</td>
<td>Risk appetite policy development – quantitative and qualitative perspectives</td>
</tr>
<tr>
<td>Do we have a capital plan? Are our regulatory capital and economic capital requirements the same or different? How do we monitor and model capital adequacy?</td>
<td>Capital planning and management • Policy development and assessment • Leading practice assessment and independent model evaluation</td>
</tr>
</tbody>
</table>
### Questions

<table>
<thead>
<tr>
<th>Questions</th>
<th>Possible actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are we managing operational risk effectively? Are we measuring:</td>
<td>• Operational risk management framework development and model assessment</td>
</tr>
<tr>
<td>• the costs of operational risk events?</td>
<td>• Root cause analysis of losses</td>
</tr>
<tr>
<td>• leading indicators of operational risk?</td>
<td>• Development and reporting of key risk indicators</td>
</tr>
<tr>
<td>Do we make full use of stress testing to understand and monitor the</td>
<td>• Consider wider range of stress test scenarios than in regulatory requirements</td>
</tr>
<tr>
<td>organization’s vulnerabilities?</td>
<td>• Use of “reverse stress testing”</td>
</tr>
<tr>
<td></td>
<td>• Board and management participation in planning of scenarios to be tested</td>
</tr>
<tr>
<td>Are our reporting and escalation procedures up to scratch?</td>
<td>Assessment vs. leading practices for reporting of:</td>
</tr>
<tr>
<td></td>
<td>• risk levels and indicators</td>
</tr>
<tr>
<td></td>
<td>• significant risk events/losses/adverse change</td>
</tr>
<tr>
<td></td>
<td>• “trip wires” requiring notifications, remedial actions or enhanced reporting</td>
</tr>
<tr>
<td>Are the responsibilities for the management and governance of risk</td>
<td>Assessment of:</td>
</tr>
<tr>
<td>clear and appropriate?</td>
<td>• risk governance framework – management role and board governance role</td>
</tr>
<tr>
<td></td>
<td>• linkages between risk and compensation</td>
</tr>
<tr>
<td>Date</td>
<td>Topic</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>May 31, 2011</td>
<td>Risk Appetite</td>
</tr>
<tr>
<td>June 13, 2011</td>
<td>Capital Management and Risk Capacity</td>
</tr>
<tr>
<td>July 13, 2011</td>
<td>ERM Organizational Structure and Sustainability</td>
</tr>
<tr>
<td>October 25, 2011</td>
<td>IT Governance</td>
</tr>
<tr>
<td>November 16, 2011</td>
<td>Operational Risk</td>
</tr>
</tbody>
</table>

*Presentation copies available if you missed the above sessions*

*Future sessions on these and new topics to be announced in early 2012*
Thank you
Appendix A

CSA Q31001

Risk Management Framework
Organizational Governance
Including mandate for Risk Management framework

Commit and Mandate
- Policy Statement
- Standards
- Guidelines
- RM Plan and RM Process
- Assurance Plan

Communicate & Train
- Stakeholder analysis
- Training needs analysis
- Communication strategy
- Training strategy
- Network

Structure & Accountability
- Board RM Committee
- Executive RM Group
- RM Working Group
- Manager, Risk Management
- RM Champions
- Risk and Control Owners

Review & Improve
- Control assurance
- RM Plan progress
- RM Maturity Evaluation
- RM KPIs
- Benchmarking
- Governance reporting

Process for Managing Risk
1. Establish context
2. Risk assessment
   - Identify risks
   - Analyse risks
   - Evaluate risks
3. Treat risks

Management Information System
- Risk Registers
- Treatment Plans
- Assurance Plan
- Reporting templates

Framework Implementation
- Framework Continuous Improvement Cycle

Framework Continuous Improvement Cycle

Framework Implementation
Appendix B
Supplementary Insurance Industry Example
Risk Management Overview

- The company uses an Enterprise Risk Management framework to categorize, monitor and manage its risks.

- The major categories of risks are:
  - Market
  - Credit
  - Insurance
  - Operational
  - Strategic

- Through its existing enterprise risk management procedures, the company reviews the various risk factors identified in the framework and report to senior management and to the Risk Review Committee of the Board quarterly.

- The framework recognizes the role of risk culture in the effective management of enterprise risk.

- Its risk culture is supported by a strong ‘tone from the top’, which is reinforced from the Board of Directors and the Board Committees to the executive officers, line management and staff.
A.1  Canadian Insurance Industry Example #2

The risk management framework sets out key processes for managing risk in the following areas:

Risk Management Processes

- Risk Appetite
- Risk Identification
- Risk Measurement & Assessment
- Risk Response
- Monitoring & Control
- Risk Reporting & Communication
A.1  Canadian Insurance Industry Example #2 Cont’d

Risk Management Structure

• The Board of Directors is responsible for ensuring that risk management policies and practices are in place and they are appropriately identified and managed.

• The Board of Directors has delegated this function to its Risk Review Committee, which is a standing committee of the Board of Directors.

• The Risk Review Committee oversees the review and approval of risk management policies, ensuring the identification of major areas of risk facing the company and the development of strategies to manage those risks, and to review compliance with risk management policies implemented by the company.

• The Risk review committee works in collaboration with the Investment Oversight Committee and the Governance and Conduct Review Committee to monitor compliance with risk management policies.

• The company’s governance model for risk management also includes oversight from various functional heads in the Corporate Office.

• There are functional heads for all key business oversight functions such as the Chief Compliance Officer, the Chief Privacy Officer and the Chief Internal Auditor.

• All the functional heads support the Chief Risk Officer in the development and communication of the company’s enterprise risk management function.
A.1 Canadian Insurance Industry Example #2 Cont’d
A.1 Canadian Insurance Industry Example #2 Cont’d

Notable Features of the Risk Management Structure

• The Enterprise Risk Management framework reflects leading practice established in Q31001

• An overarching Risk Review Committee of the Board of Directors has been established which provides a focused and multidisciplinary perspective to risk decisions at the governance level

• Specialty risk committees exist for investments, compliance and privacy risks at the Board level

• The functional heads for investment, compliance privacy and internal audit work in conjunction with the Chief Risk Officer to support the enterprise risk management framework

• The framework emphasizes the importance of risk culture and tone at the top and how they influence risk taking behaviours
A.1 Canadian Insurance Industry Example #2 Cont’d

Challenges of the Structure

• Coordinating the risk management authority decision making of the various risk chiefs including enterprise risk, privacy, compliance investment and internal audit

• Coordinating and integrating the risk oversight roles and decision making of the various risk committees at the Board level

• Monitoring the effectiveness of risk appetite statements across the company that supports risk taking decisions in a consistent manner

• Ensuring that business unit heads and staff own and are accountable risks that may pose opportunities and threats to their business objectives
Contacts

Neil Parkinson
Partner, Insurance Industry National Leader

KPMG LLP
Suite 4600
Bay Adelaide Centre
333 Bay Street
PO Box 31
Toronto, ON M5H2S5
nparkinson@kpmg.ca

Tel (416) 777-3906
Fax (416) 777-8462

Jacqueline Friedland
Partner, Actuarial Practice Leader

KPMG LLP
Suite 4600
Bay Adelaide Centre
333 Bay Street
PO Box 31
Toronto, ON M5H2S5
jfriedland@kpmg.ca

Tel (416) 777-8320
Fax (416) 777-8462

Elizabeth Murphy
Associate Partner, Insurance Industry

KPMG LLP
Suite 4600
Bay Adelaide Centre
333 Bay Street
PO Box 31
Toronto, ON M5H2S5
elizabethmurphy@kpmg.ca

Tel (416) 777-8279
Fax (416) 777-8462

KPMG LLP, a Canadian limited liability partnership.
Contacts Cont’d

Peter Heimler
Associate Partner
Enterprise Risk Management

Suite 4600
Bay Adelaide Centre
333 Bay Street
PO Box 31
Toronto, ON M5H2S5
pheimler@kpmg.ca

Tel (416) 777-3509
Fax (416) 777-8462

Rudolph Persaud
Associate Partner
Financial Risk Management

KPMG LLP
Suite 4600
Bay Adelaide Centre
333 Bay Street
PO Box 31
Toronto, ON M5H2S5
rppersaud@kpmg.ca

Tel (416) 777-8957
Fax (416) 777-8462
© 2011 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.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.