Enterprise Risk Management

“All of life is the management of risk, not its elimination”
Walter Wriston, former chairman of Citicorp

October 1, 2008

Stuart Wason FSA, FCIA
Material for this presentation is based on the May 2008 draft of the IAA Practice Note on Enterprise Risk Management for Capital and Solvency Purposes
Key topics for this session

- Introduction
- Setting the Scene
- Governance & ERM Framework
- Risk Management Policy
- Risk Tolerance
- RiskResponsiveness & Feedback Loop
- Own Risk and Solvency Assessment
- Economic and Regulatory Capital
- Continuity Analysis
- Role of Supervision in Risk Management
Introduction

- Today, ERM is increasingly regarded as an appropriate response or indeed a solution to managing risk in today’s more complex and interdependent markets and operating environments.

- Insurance regulators have also played a leading role in setting standards and providing guidance to insurers on implementing appropriate frameworks for the management of risks faced by insurance companies.

- The IAIS Standard describes eight Key Features. The Practice Note ‘unpacks’ each of the ‘Key Features’ by explaining them in more detail, thereby assisting insurance executives address strategic and operational issues associated with implementing an ERM framework in their insurance business.
Governance and Enterprise Risk Management Framework

Feature 1

Risk Management Policy

Feature 2

Risk Tolerance Statement

Feature 3

Feedback Loop

Feature 4

Own Risk and Solvency Assessment (ORSA)

Feature 5

Feedback Loop

Feature 4

Continuity Analysis

Feature 7

Role of supervision

Feature 8

Economic & Regulatory Capital

Feature 6
Setting the Scene

- ERM is a logical and evolutionary response to growing complexity, uncertainty and ambiguity associated with 21st century corporate life. Now all management is risk management.

- ERM involves identifying, assessing, mitigating and, if necessary, transferring risk.

- In reality, risk involves a complex interplay of dynamic external influences and (unpredictable) human behaviour - ‘traditional’ or silo risk management is not enough to sustain a 21st century insurance business.
Setting the Scene

- Risk management is commonly viewed through a lens of avoiding ‘bad’ things happening and limiting the downside. The more enlightened view is one of connecting risk to value maintenance and creation.

- Effective ERM is inextricably linked with strategic planning for a business.

- Effective ERM requires new investments in modelling and analytical capabilities, a different way of looking at risk and capital, and cultural changes to embed risk management in all activities of a corporation.

- Regulators and rating agencies increasingly expect insurers to apply its techniques for managing their business on a day-to-day basis.
Evolution of Enterprise Risk Management

Risk models:
- Economic capital models
- Other models

Today
- Link with strategy: High
- Value creation
- Risk measurement
- Risk control
- Balance sheet protection

Industry standard in the last 5-10 years:
- Compliance
- Loss minimisation
- Risk management

Industry standard in the next 5-10 years:
- Return optimisation
- Strategic integration

‘The Role of ERM in Ratings’, Mark Puccia, Managing Director, Standard & Poor’s, March 30, 2007
Setting the Scene

What is ERM?

ERM is concerned with,
- All risks faced by insurers
- Creating value for the owners of an insurance enterprise whilst ensuring that promises made to policyholders are met.

Specifically, ERM
- Considers the totality of systems, structures and processes within an insurer that identify, assess, treat, monitor, report and/or communicate all internal and external sources of risk that could impact on the insurer’s operations
- Implies a common risk management ‘language’ across the insurer
- Involves systematic organisation of and coordination between risk functions
- Includes both the management of ‘downside’ as well as ‘upside’ risks
- Seeks to quantify all risks but not all risks can be quantified
- Is concerned with both behaviours and risk control processes
- Involves consideration of risk information relating to past events (e.g. losses), current performance (e.g. risk indicators) and future outcomes (e.g. the risk profile or risk assessment).
Setting the Scene
What is ERM?

- Strong enabling conditions must exist for ERM to take hold, namely:
  - Demonstrable executive management support is critical
  - Strong and direct linkages must be made between ERM and the insurer’s business strategy and its day-to-day operations
  - The insurer must establish clear accountabilities for the various aspects of risk management, distinguishing between those in line management roles and those in risk management

- Many of the insurers who have developed advanced practices describe ERM as a ‘journey’ implemented in waves
Setting the Scene
Where does one begin?

- Key to implementation is buy in and support from the Board. For this to occur, ERM needs to inform the board about issues they want and need to know about.

- **Key Lessons**
  1. ERM is one of the few truly enterprise wide business capabilities that both provides an opportunity to change the way an organisation does business, but also can be ‘used’ to drive certain agendas that may not be aligned to the business imperatives, and stakeholder needs.
  2. The output of ERM may not suit all stakeholders, so Board buy-in with management is critical to ensure needs and expectations are met and the ERM investment delivers maximum return and minimises any agency/stakeholder bias.
  3. The Board is well placed to take a strategic and holistic perspective to ensure long term sustainability of the ERM investment.
Governance & Enterprise Risk Management Framework

Key Feature 1

- **ERM framework must be appropriate to the nature, scale and complexity of insurer’s business and risks.**

- **ERM framework should be fully integrated with (and embedded in) the insurer’s business operations.**

- **ERM framework should be led and overseen by the insurer’s board and senior management.**

- **For capital management and solvency purposes, the framework should include provision for the quantification of risk for a sufficiently wide range of outcomes using appropriate techniques.**

- **Measurement of risk should be supported by accurate documentation providing appropriately detailed descriptions and explanations of risks.**
The role of an insurer board with respect to risk management is broadly well understood and reflects an ‘ultimate responsibility’ for the insurer’s risk management framework. Stakeholders, including regulators, interpret this ultimate responsibility to mean, amongst other things:

- Approving the insurer’s overall risk management strategy and/or policy
- Overseeing the process of ensuring the insurer’s ‘responsible persons’ are fit and proper
- Setting the risk appetite of the insurer
- Monitoring key risks by ensuring the implementation of a suitable risk management and internal controls framework.
TIPS FOR AN EFFECTIVE RISK COMMITTEE

- Diverse member background with appropriate qualities such as inquisitive/questioning minds, objectivity & relevant experience.
- Ensure RC “ask questions” of the reports submitted and of management rather than apply the “tick the box” approach.
- Ensure RC directives have support of Board and the appropriate level of management “buy in”.
- Appropriateness of level & volume of reporting to RC - ensure the right information is being communicated.
- Responsible for keeping track of leading practices & trends.
- Have an appropriate SMART self-assessment program.
Governance & Enterprise Risk Management Framework

- Board versus management accountabilities
- Management commitment and leadership
- Establishing and developing an enterprise risk function
- Importance of a common risk language
- Risk management culture
- Developing a risk behavior model
- Developing an implementation plan
- Upside risk management
- Performance measurement and reward systems
Reporting and monitoring: At the highest level risk reporting should seek to identify the following (for example):

- Current and emerging key risks in the business and within the wider environment, and changes over time (the risk profile of the insurer)
- Changes in risk indicators (measures influencing risk likelihood and/or impact)
- Capability for identifying and managing risks
Many stakeholders rely on quality risk information:
- Audit Committees – Monitoring material financial risks and their mitigation
- Executives - Reviewing risk information for completeness
- Managers - Reviewing risk information for completeness and changes in risk profile or control effectiveness
- Risk Owners - Updating risk information and escalating changes in likelihood, impact or control effectiveness as required
- Control Owners - Updating status of treatments for controls that they are responsible for
- Internal Audit - Reviewing the effectiveness of internal control measures
- External Stakeholders – Reviews by regulatory bodies.
A succinct dashboard is the most effective way to report so the information can be assessed at a glance. Supporting information can be attached for those who require more detail. Some of the key categories of a dashboard may include:

- **Top 10 residual risks**
- **Key risk indicators**
- **Scoring chart for risk severity and control effectiveness**
- **Heat map of all substantial inherent and residual risks**
- **An additional commentary section**
- **Significant project progress.**
An insurer should have a risk management policy which outlines the way in which the insurer manages each relevant and material category of risk, both strategically and operationally. The policy should describe the linkage with the insurer’s tolerance limits, regulatory capital requirements, economic capital and the processes and methods for monitoring risk.
Risk Management Policy
Aspects to consider

- A clear risk management philosophy – for example outlining why risk management is important and the linkages with value creation
- The relationship between risk management and the insurer’s purpose or mission, values and strategic objectives
- How risk management is embedded in the related processes of capital management, pricing, reserving and performance management
- Scope of activities to which the policy applies. For example, the policy should be sufficiently flexible to cater for multiple ownership structures (e.g. wholly-owned, majority-owned, joint venture etc.)
- Appropriate regulatory requirements and considerations
- Requirements with respect to acquisition of new businesses e.g. time frame for integration with the insurer’s ERM framework
- Categories of risk and risk definitions and how these map to internationally accepted categories/definitions
- In addition to risk categories, the policy should define risk ‘terminology’ used e.g. ‘risk’, ‘risk management’, risk management framework’
Risk Management Policy
Aspects to consider

- Most importantly, the insurer’s risk appetite should be set forth in the policy
- Governance and oversight aspects
- Board, board committee structures, responsibilities
- Management structures, roles, responsibilities
- Roles and responsibilities of the various corporate and business unit risk functions
- Role of internal and external audit
- Compliance aspects, including consequences associated with policy breach
- Behavioural expectations of all staff
- Minimum process-level requirements that apply across the insurer
- Requirements for the conduct of the insurer’s ‘Own Risk and Solvency Assessment’
- The process for reviewing and updating the policy.
An insurer should establish and maintain a risk tolerance statement which sets out its overall quantitative and qualitative tolerance levels and defines tolerance limits for each relevant and material category of risk, taking into account the relationships between these risk categories.

The risk tolerance levels should be based on the insurer’s strategy and be actively applied within its ERM framework and risk management policy. The defined risk tolerance limits should be embedded in the insurer’s ongoing operations via its risk management policies and procedures.
Risk Tolerance

- Establishing an insurer’s risk tolerance involves making strategic choices.

- The process must be connected with setting strategy and longer term direction.

- While top-level management may be heavily involved in debating the appropriate risk tolerance to match a given strategic direction, it is the Board who must decide on risk tolerance and the insurer’s strategy.

- The CRO should be involved in but not responsible for defining the insurer’s risk tolerance.
Risk Tolerance

For an insurer, the following parameters are typically used to articulate risk tolerance across financial and non-financial risks:

– Lines of business that the insurer will/will not accept
– Earnings volatility
– Requirements to meet regulatory criteria (including allowance for unexpected events)
– Desired capital ‘strength’, usually by reference to a defined rating level of a recognised credit rating agency
– Maintaining levels of economic capital by reference to a specified chance of meeting policyholder obligations or target return periods for ‘risk of ruin’
– Maximum exposure to aggregation of risk
– Dividend paying capacity (for listed company insurers)
– The maximum net loss the insurer is prepared to accept in any given year in the event of a catastrophic loss (general insurers)
Risk Tolerance

Limits, being narrower in scope, tend to operate at the risk category level. Examples of risk limits include:

- Establishing counterparty credit limits for investments and reinsurers
- Setting an overall target for credit quality for a reinsurance buying program, usually by reference to credit rating
- Establishing concentration limits for lines of business/products, geographies and counterparties
- Maintenance of underwriting and pricing principles and limits
- Setting liquidity benchmarks by reference to the amount of investment assets to be held in ‘highly liquid’ assets
- Investment mandates setting limits for the investment of policyholder and shareholder funds in traded instruments
- Limits on the use of financial derivatives
- Establishing operational risk policies that include limits for outsourcing, business interruption, fraud etc.
Risk Responsiveness and Feedback Loop

Key Feature 4

- The insurer's ERM framework should be responsive to change.

- The ERM framework should incorporate a feedback loop, based on appropriate and good quality information, management processes and objective assessment, which enables the insurer to take the necessary action in a timely manner in response to changes in its risk profile.
Risk Responsiveness and Feedback Loop

An effective feedback loop is underpinned by:

- Establishment of thresholds for reporting significant issues
- Protocols for escalation of issues to various levels and management and, if necessary, regulators
- Reporting of risk aggregations to identify where limits (and potentially risk tolerance) may have been exceeded.
Emerging risks are developing or already known risks which are subject to uncertainty and ambiguity and are therefore difficult to quantify using traditional risk assessment techniques.

Insurers are interested in emerging risks for a number of reasons including, whether emerging risks will:
- Influence the organisations strategy
- Impact the performance of the underwriting portfolios – unexpected (latent) claims / claims frequency / claims costs
- Impact on the operational risks facing the organisation
- Present opportunities for new types of insurance products?

One way to evaluate high impact/low probability events is through scenario planning, which can augment statistical models and help companies prepare for specific events. Scenario planning is a powerful tool that helps executives assess the resilience of the organisation to internal and external shocks.
An insurer should regularly perform its own risk and solvency assessment (ORSA) to provide the board and senior management with an assessment of the adequacy of its risk management and current, and likely future, solvency position. The ORSA should encompass all reasonably foreseeable and relevant material risks including, as a minimum, underwriting, credit, market, operational and liquidity risks. The assessment should identify the relationship between risk management and the level and quality of financial resources needed and available.
ORSA involves carrying out a combination of quantitative and qualitative techniques to identify, assess and manage risk.

The core process of risk management involves the systematic identification, analysis, evaluation and treatment of risks.

Typically, the ‘context’ is framed around objectives of a business process or project or indeed the broader insurance enterprise.

The output of the risk management process is usually described as a ‘risk profile’, ‘risk register’, ‘heat map’ and/or ‘risk control self assessment’ (hereafter described as a risk profile).

The process of risk profiling can be applied at the insurance enterprise level, business unit, key business process level (e.g. underwriting, claims) or be applied in the management of projects. Risk profiling involves an assessment of risk at both the levels of ‘inherent risk’ and ‘residual risk’. 
Inherent and residual risk highlight important management information not otherwise readily apparent:

– Those risks whose management rely heavily on the continued and effective operation of key controls (*high inherent risk/low residual risk*)

– Those risks whose nature does not significantly alter following the application of controls. This highlights that certain controls may be ineffective and that resources might be utilised better elsewhere, or that different controls are needed (*high inherent risk/high residual risk*)

– Those risks that may be over-controlled (*low inherent risk/low residual risk*).
ORSA
Risk profile elements

- Description of risks in enough detail for each risk to be understood in isolation
- Cause(s) or underlying conditions giving rise to a given risk
- Consequence(s) of the risk - in both financial and non-financial terms (e.g. loss of customers, regulatory sanction, cost over-runs etc)
- Categorisation of each risk - especially important where an insurer comprises multiple business units and risk aggregation is required at the enterprise level
- Inherent risk assessment that considers likelihood/frequency of risk occurrence and impact of the risk.
- Assessment of controls and/or risk mitigation strategies.
- Residual risk assessment after taking into account the effectiveness of controls
- Action(s) to be taken to bring unacceptable residual risk within appropriate limits.
<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Modelling Technique(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise /all risk categories</td>
<td>• Dynamic Financial Analysis</td>
</tr>
<tr>
<td>Underwriting (including reinsurance)</td>
<td>• Financial Condition Report (FCR) and/or underwriting modelling or reviews</td>
</tr>
<tr>
<td>Market</td>
<td>• Value at risk (VAR) or Tail VAR</td>
</tr>
<tr>
<td></td>
<td>• Interest rate models</td>
</tr>
<tr>
<td></td>
<td>• Scenario tests</td>
</tr>
<tr>
<td>Credit</td>
<td>• Credit risk models</td>
</tr>
<tr>
<td>Liquidity</td>
<td>• Asset/Liability modelling</td>
</tr>
<tr>
<td>Operational</td>
<td>• Internal loss data</td>
</tr>
<tr>
<td></td>
<td>• External loss data</td>
</tr>
<tr>
<td></td>
<td>• Scenario analysis, simulations</td>
</tr>
</tbody>
</table>
Nassim Taleb\(^1\) coined the phrase “black swan” to describe something that is a large-impact, hard-to-predict, and rare event beyond the realm of normal expectations. The metaphor here is that most people would expect a swan to be white (at least until black swans were discovered in the 17th Century in Australia) and therefore a black swan is a surprise.

Black swan events have occurred throughout history. More recently the events of 9/11 and the sub prime meltdown in the USA are examples.

But here is the dilemma. Since black swan event are surprises they cannot happen twice because once they have occurred they are within know experience. Planning to avoid repeated events of this nature is a good idea but cannot prevent further surprises. Even a forensic understanding of such events will do little to prevent the next black swan.

Good risk practices are our only real preventative measure – and honesty that surprises will happen. Through an appropriate ERM framework we can be well placed to manage surprising situations appropriately and decrease the impact.

So ERM is probably not enough to prevent all manner of risks, especially surprises, however it is a lot better than not having any preventative framework.

\(^1\) Learning to Expect the Unexpected by Nassim Taleb, The New York Times, April 8, 2004
As part of its ORSA an insurer should determine the overall financial resources it needs to manage its business given its own risk tolerance and business plans, and to demonstrate that supervisory requirements are met. The insurer's risk management actions should be based on consideration of its economic capital, regulatory capital requirements and financial resources.
Economic and Regulatory Capital

- One of the basic principles behind capitalism is that the market will allocate capital to the most productive activities and organisations as measured by their ability to provide a return on that capital.

- Owners of capital will assess proposals for the use of their capital based on their risk vs reward and provide their limited capital to the best available proposals.

- A key component to managing these risks is to have a model that attempts to simulate the environment in which the insurer is operating.

- Such models provide a guide to management of how specific decisions may impact the expected level and volatility of future profit. They can also provide indications of the risk of failure of the insurer. Referred to as Economic Capital Models, they are used by capital providers, regulators & companies.
Economic and Regulatory Capital

It is the ability of the ECM to allocate the capital down to the level of detail where ‘localised’ decisions can be made that is crucial to the success of the pricing function.

<table>
<thead>
<tr>
<th>Risk Class</th>
<th>Pricing Measure to Achieve X% RoC</th>
<th>Actual Pricing Measure</th>
<th>Rating Strength</th>
<th>Actual Business Volumes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(A)</td>
<td>(B)</td>
<td>(B / A)</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>10%</td>
<td>11%</td>
<td>1.10</td>
<td>100</td>
</tr>
<tr>
<td>Y</td>
<td>5%</td>
<td>4%</td>
<td>0.80</td>
<td>200</td>
</tr>
<tr>
<td>Z</td>
<td>7%</td>
<td>7%</td>
<td>1.00</td>
<td>70</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>0.92</td>
<td>370</td>
</tr>
</tbody>
</table>
Taking the example to a lower level of detail, if the ECM can provide capital requirements for Risk Class Y at a lower level of detail, i.e. Y1 and Y2, then more effective management decisions can be made by understanding the source of the underperformance of risk class Y.

<table>
<thead>
<tr>
<th>Risk Class</th>
<th>Pricing Measure to Achieve X% RoC</th>
<th>Actual Pricing Measure</th>
<th>Rating Strength</th>
<th>Actual Business Volumes</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>10%</td>
<td>11%</td>
<td>1.10</td>
<td>100</td>
</tr>
<tr>
<td>Y1</td>
<td>5%</td>
<td>6%</td>
<td>1.20</td>
<td>67</td>
</tr>
<tr>
<td>Y2</td>
<td>5%</td>
<td>3%</td>
<td>0.60</td>
<td>133</td>
</tr>
<tr>
<td>Z</td>
<td>7%</td>
<td>7%</td>
<td>1.00</td>
<td>70</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>0.92</td>
<td>370</td>
</tr>
</tbody>
</table>
Economic and Regulatory Capital

- Regulatory capital requirements are just one input into capital requirements. There can be a multitude of others including:
  - Desired rating agency ratings
  - Desired earnings volatility
  - Desired shareholder return, dividend and capital growth
  - Market expectations

- Key potential differences between a regulatory prescribed method and an ECM would often include:
  - The volatility of various classes of business
  - Different allowances for diversification (often performed by correlation matrices, or sometimes via copulas) between risk types and within risk types
  - Different focuses driving capital (i.e. different aims)

- Capital management focuses on turning risk into shareholder value
Capital Management

Risk Management

Performance Management

Capital

Pricing

Reserving
Continuity Analysis

Key Feature 7

- As part of its ORSA, an insurer should analyse its ability to continue in business, and the risk management and financial resources required to do so over a longer time horizon than typically used to determine regulatory capital requirements.

- Such continuity analysis should address a combination of quantitative and qualitative elements in the medium and longer term business strategy of the insurer and include projections of the insurer’s future financial position and modelling of the insurer’s ability to meet future regulatory capital requirements.
Continuity Analysis

An ECM allows an insurer to look further into the future than most regulatory prescribed methods are based on. This will require explicit decisions to be made regarding (amongst other things):

– What time period of modelling should be used
– Should the financial position of the insurer be assessed at a future point in time, or once all relevant liabilities are modelled to have run-off
– What management actions are likely should results turn to the worst
– What capital reduction (e.g. dividend) / capital injection policy can be assumed
– How reliable are an insurer’s longer term forecasts and are they sufficient to form the basis of an ECM.
Continuity Analysis

A truly integrated ECM will be used for a wide range of purposes within an insurer. For example, it can be used to provide analysis relating to:

- Economic capital requirements
- Investment strategy
- Mergers, acquisitions and divestments
- Capital allocation
- Reinsurance programmes
- Optimal business mix
- Reserving volatility
- Capital outflow / inflow
- Financial Condition Report
- Business Continuity Planning
Role of Supervision in Risk Management

Key Feature 8

- The supervisor should undertake reviews of an insurer's risk management processes and its financial condition. The supervisor should use its powers to require strengthening of the insurer’s risk management, including solvency assessment and capital management processes where necessary.
Role of Supervision in Risk Management

Supervisors increasingly expect insurers to apply ERM as part of the on-going management of their business on a day-to-day basis.

- ERM is consistent with the aims of risk-based supervision and the protection of policyholders
- Supervisors will wish to be kept informed in an appropriate and regular manner of all the ERM Features noted in this Practice Note
- Supervisors will seek confirmation that ERM satisfies the “Use” test within the insurer.
- Supervisors have a range of interests in ERM from Board level governance to the technical specifications involved with internal model approvals for regulatory capital (for example)
- Insurers should aim to adopt ERM practices which are sound and forward-looking and be proactive in communications with their Supervisor.