
**ASSOCIATION ACTUARIELLE INTERNATIONALE**

**INTERNATIONAL ACTUARIAL ASSOCIATION**

# PRACTICE NOTE ON ENTERPRISE RISK MANAGEMENT FOR CAPITAL AND SOLVENCY PURPOSES IN THE INSURANCE INDUSTRY

**FINAL, 11 August 2008**

# Acknowledgements

Many people and organisations have been involved with the development of this Practice Note.

First and foremost the members of the IAA Enterprise and Financial Risk Committee are thanked for their efforts in promoting and supporting the development of the Practice Note. For more information about the committee, please visit http://www.actuaries.org and click on committees.

IAG (Insurance Australia Group) played a pivotal role facilitating the writing and development of the material included in the Practice Note. Particular recognition needs to be given to Tony Coleman, Chief Risk Officer who sponsored this project in IAG and Peter Sutherland, Head of Group Risk & Compliance who was principal author. A number of other IAG people also contributed thoughts, wrote case material and reviewed drafts.

Three companies were involved in the development of the case material. These companies were Ernst and Young, KPMG and PWC. As consulting companies they were able to draw on international material to provide rich illustrations of the practice points being presented.

In addition, Standard and Poors provided examples about approaches companies had used to implement Enterprise Risk Management in the context of their different organisation operating models from their published ERM criteria and from public rating report discussions of rated firms' ERM processes.

Finally, thanks go to the International Association of Insurance Supervisors. Members took a keen interest in the development of this Practice Note and dedicated time to review drafts at their Solvency and Actuarial Issues Sub-committee meetings in 2007 and 2008.

# TABLE OF CONTENTS

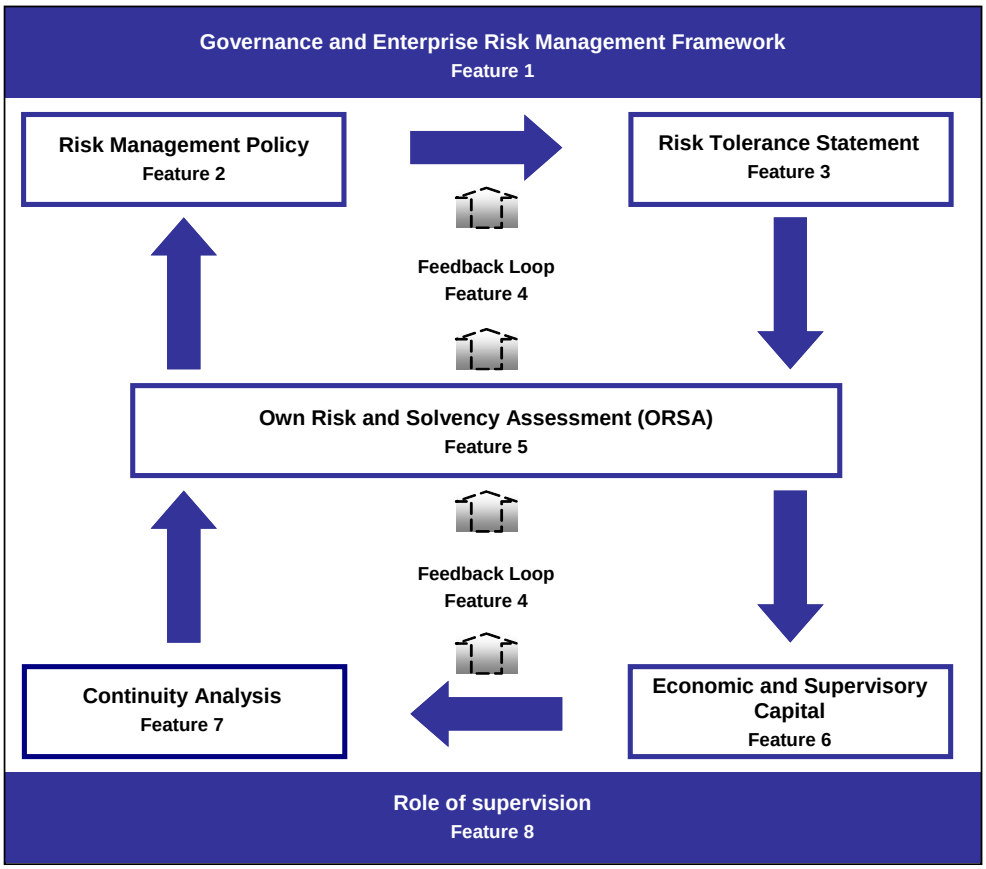
# LIST OF APPENDICES

# 1. Introduction

It is self evident that insurance and risk management are very closely linked. In recent years the concept of Enterprise Risk Management (ERM) has been embraced by an increasing number of insurers seeking to improve their management practices and the operating performance of their businesses. 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 supervisors 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.

This Practice Note has been developed by the IAA for insurers to support the Standards and Guidance materials developed by the IAIS for supervisors. It draws on industry experience, supervisors' supervisory practices, models and frameworks published by others and emphasises practical considerations. The Practice Note also seeks to help insurers assess risk framework maturity by reference to characteristics associated with different stages of development of risk management sophistication.

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. The material is presented as issues to consider and information about solutions others have used rather than a prescription to follow when implementing ERM. There is no 'one right way'; rather the appropriate approach will depend on the insurer's particular circumstances. Appendix 8 lists 'Useful References' that provide more information about the topics covered here.



## *1.1 Development of the Practice Note*

In developing this Practice Note, use has been made of standards issued by the Federation of European Risk Management Associations and Standards Australia, both of which have issued comprehensive Risk Management Standards. Additionally, extensive use has been made of material from consulting firms, supervisors, academics and industry professionals. A number of examples and tips have been included throughout the Practice Note to illustrate the points being discussed. In addition, a number of appendices have been compiled to provide more detailed case studies, guidance and suggestions for the implementation of an ERM risk management framework.

## *1.2 Working Assumptions*

This Practice Note has been developed for both life and non-life (general) insurance businesses. The breadth of experience and maturity in insurance businesses varies greatly in applying many of the concepts dealt within the Practice Note. However, the Practice Note attempts to provide a framework that is conceptually straightforward, based on practical principles that can be implemented in manageable steps – a series of building blocks to enable an insurance professional to move from ‘basic’ to ‘advanced’ ERM.

Many of the examples and frameworks provided are based on experiences in larger organisations. Nevertheless the information can equally apply to medium or small organisations. Smaller organisations can still be ‘advanced’ in ERM but may outsource some of the activities instead of completing all activities in house. Alternatively, smaller organisations may choose to undertake the essential activities for their organisation context rather than a full ERM implementation. This would be a business decision about balancing risk and return, a fundamental principle of ERM. Where possible, comments have been included to provide guidance to small and medium organisations.

This Practice Note is intended to support IAIS Standards and Guidance Notes for insurers in all jurisdictions by raising of awareness and building understanding among actuaries and other risk management professionals about ERM practices and the challenges associated with implementation.

## Setting the Scene

Much has been written on the topic of ERM. This represents a logical and evolutionary response to growing complexity, uncertainty and ambiguity associated with 21st century corporate life. Now all management is risk management. In a corporate context we encounter risk when we pursue our goals. Some risks are beyond our control but many may and should be managed – in a linear sense this means identifying, assessing, mitigating and, if necessary, transferring risk. In reality however the pattern of risk is anything but linear, involving a complex interplay of dynamic external influences and (unpredictable) human behaviour. At a conceptual level, the development of ERM is a rational acknowledgement that 'traditional' or silo risk management is not enough to sustain a 21st century insurance business.

The terms 'risk' and 'risk management' are commonly viewed through a lens of avoiding 'bad' things happening and limiting the downside. Whilst understandable, the more enlightened view emerging is one of connecting risk to value maintenance and creation. This includes, for example, the empowerment of people to exploit opportunities. Indeed, market watchers view the ability to anticipate and react to a market opportunity to be as important as readiness for a potentially significant business disruption. Moreover, the importance of the risk management culture is naturally being linked with effective ERM practices.

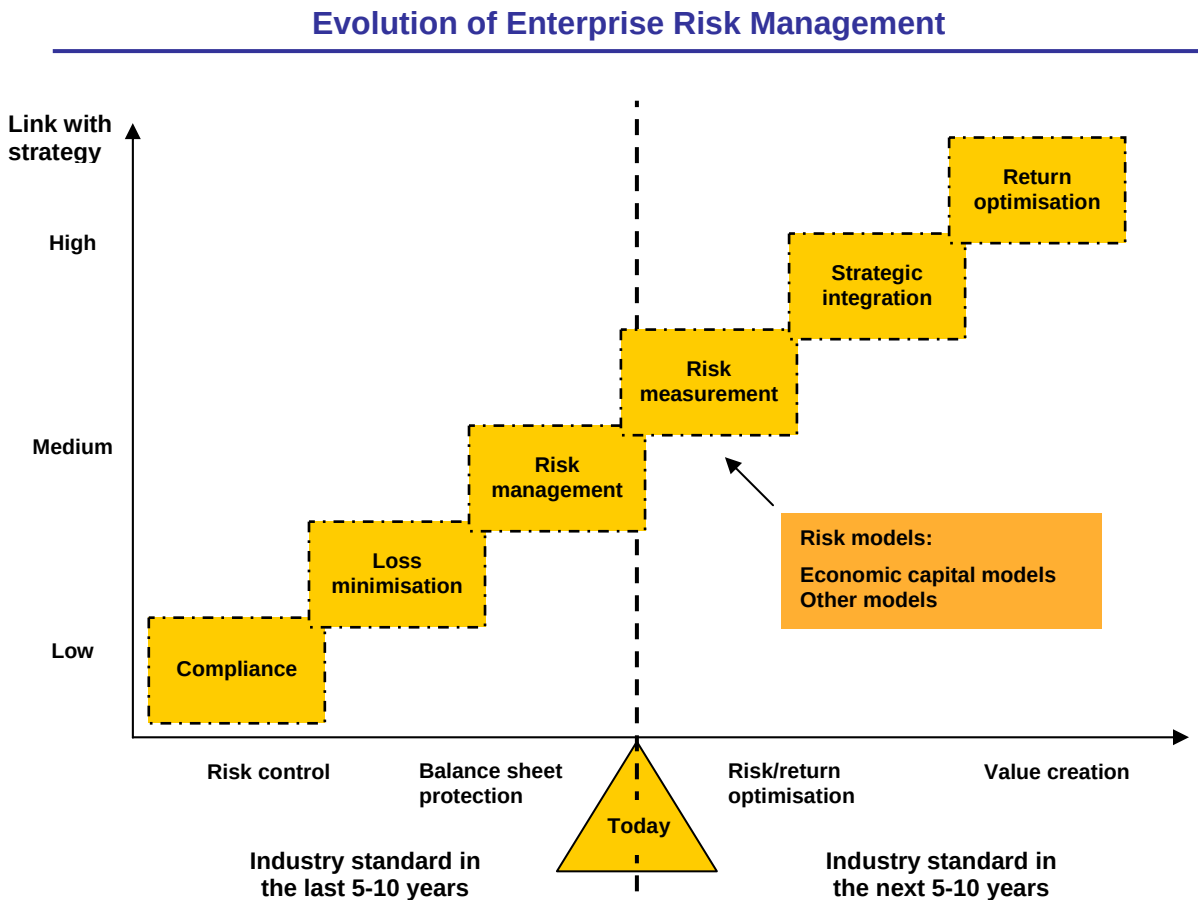
Effective ERM is inextricably linked with strategic planning for a business. When ERM is integrated in the business planning cycle of the insurer decisions of the company (e.g. growth of business lines, acquisitions, new product development, new channels) are made on a risk-adjusted basis and fully supported/informed by the ERM process. And, in turn, the annual risk budget/capital allocation by risk-type should be set in accordance with the business strategy of the enterprise. Finally, end-of-year capital measurement and performance measurement is conducted on a risk-adjusted basis, to complete the full circle of value creation.

Developing an effective enterprise wide approach to risk management is not a straightforward exercise or one that can be neatly added on to the responsibilities of an existing function. It requires new investments in modelling and analytical capabilities, a different way of looking at risk and capital, and cultural changes that would embed risk management in all activities of a corporation.[1]

ERM's importance is also reflected in the way supervisors and rating agencies increasingly expect insurers to apply its techniques for managing their business on a day-to-day basis.

[1] Risk Management Risk Opportunity, The 2006 Tillinghast ERM Survey.

## *1.3 Enterprise risk management history*




*'The Role of ERM in Ratings', Mark Puccia, Managing Director, Standard & Poor's March 30, 2007*

## *1.4 What is Enterprise Risk Management?*

There is no universally accepted definition of ERM and the very nature of the concept suggests that there may never be one. However, a number of recurring themes/terms appear in an ERM context. Terms like 'holistic', 'integrated', 'top-down', 'strategic approach' and 'value-driven' consistently appear in the various definitions found in ERM literature widely available today. It is not the intent of this Practice Note to add to the growing list of ERM definitions. Rather, the Practice Note has been developed having regard to the common themes and principles that emerge from the various definitions.

In summary, the Practice Note is underpinned by the following principles:

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

More specifically,

- ERM is concerned with 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
- ERM implies a common risk management 'language' across the operations of the insurer
- ERM involves systematic organisation of and coordination between risk functions i.e. specialist risk 'silos' operating in isolation from each other are inconsistent with ERM principles
- ERM includes both the management of 'downside' as well as 'upside' risks
- ERM seeks to quantify all risks but acknowledges that not all risks can be measured in currency/financial terms
- ERM is concerned with both behaviours (the risk management 'culture') and risk control processes
- ERM involves holistic 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).

Having framed the above principles it must be remembered that risk management remains the responsibility of all personnel in the insurer, and not just designated risk professionals. This reflects the fact that risk acceptance and management is integral to insurance. Moreover a series of 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 roles.

Insurers wishing to develop a formal definition of ERM for their business should review the various definitions that have been published. A list of a representative number of these can be found in Appendix 1 to this Practice Note.

For many insurers, implementation of ERM will not be straightforward nor a short term undertaking. For some, ERM will bring fundamental changes to governance and management structures, investing in different capabilities, implementing new processes and embarking on comprehensive change programs. Many of the insurers who have developed advanced practices describe ERM as a 'journey' implemented in waves and this is perhaps the more appropriate way to think about ERM when deciding on a course of action.

### *1.5 Strategic Considerations/Where does one Begin?*

It goes without saying that any directive, plan or recommendation to pursue an ERM implementation should emerge from careful research and analysis. Moreover, risk managers should avoid a 'quick fix' approach to ERM, irrespective of whether the driver is internal or external to the insurer.

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.

***EXAMPLE:***

***THE BOARD'S ROLE IN SETTING PRIORITIES***

*A large multinational, with operations in all continents around the world, set about developing an enterprise wide risk management strategy and framework to meet a number of needs for the organisation:*

- *Alignment of strategies and capital allocation demands from each of the regions*
- *Transparency and speed of communication*
- *Clarity and accountability for decision making*
- *Assurance to the Board on the effectiveness and efficiency of management practices, internal controls and processes.*

*The internal audit manager was charged by the Board to develop the risk profile for the organisation and the enterprise risk management strategy and framework. With an eye to internal audit and assurance responsibilities, they proposed to roll out a comprehensive program for implementation. Executive management became uneasy as they realised their investment of time in this program would focus mainly on audit needs with little attention to the growth or profitability of the business, their prime objectives. Therefore management began 'de-prioritising' time and involvement to this program. Implementation began to falter. Clearly a different approach was needed.*

*The Board initiated a re-engagement process with management to ensure that the significant ERM investment would meet the priorities and expectations of key stakeholders.*

- *The Board workshopped with management and the risk and assurance function to clarify each of the stakeholder needs, outputs and outcomes from any process/risk management activity*
- *The team prioritised and sequenced the activity and outcomes to reflect multiple stakeholder needs and business imperatives*
- *The Board gained commitment and accountability for the implementation plan and timetable and investment form all stakeholders.*

*Prioritisation and sequencing of the ERM focus areas enabled all three parties to gain clarity on the implementation path and how the business would realise the value and over what time frame.*

***Key Learnings***

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.*

ERM implementation programs are not immune from the problems typically encountered by large-scale projects impacting the whole of an insurer. Risk managers tasked with the job of 'implementing ERM' would benefit from studying lessons learned from 'failed' projects, particularly those projects involving complexity in both technology and business process change. Invariably, key learnings from an ERM context relate to:

- Setting clear objectives for the delivery of expected outcomes associated with the ERM project
- Assigning experienced and suitably skilled resources using a rigorous selection process, in particular with respect to project leadership and change management roles
- Sufficient detailed planning upfront to reflect realistic effort / timeframes
- Implementing rigorous processes to tightly manage scope, gated criteria for milestones and cost / benefits
- Clear executive-level ownership and accountability for delivery of all project aspects (appropriate project governance)
- Realism about the expected “pain” through early stages of implementation and support required
- Realism around complexity, cost and timeframes
- Thorough risk management / mitigation strategies and support processes
- An organisational culture that demands objective and transparent project reporting and rapid escalation (and welcoming) of “bad news” so that problems get addressed earlier and at less cost.

Rather than adopting a strategic approach, insurers have often tended in the past to develop their risk management frameworks in a piecemeal or ad hoc manner, usually in response to either new supervisory requirements or a business crisis (and sometimes these drivers are connected!). A not uncommon scenario involves the identification of a manager working in the disciplines of internal audit, finance, actuarial, compliance and/or operational risk and tasking them to build the appropriate framework. Such an approach, whilst generally resulting in the production of appropriate documentation and review processes, is unlikely to garner broad-based support across the organisation and will more likely reinforce a view that ERM is something more akin to a compliance exercise. More importantly, it does not take a strategic view about how ERM aligns with the insurer’s values, culture and approach.

Appendix 3 contains case studies to illustrate different approaches and issues involved in implementing ERM.

# 2. Governance and an Enterprise Risk Management Framework

***Key Feature 1***

***As part of its overall governance structure, an insurer should establish, and operate within, a sound ERM framework which is appropriate to the nature, scale and complexity of its business and risks. The ERM framework should be integrated with the insurer's business operations, reflecting desired business culture and behavioural expectations and addressing all reasonably foreseeable and relevant material risks faced by the insurer in accordance with a properly constructed risk management policy. The establishment and operation of the ERM framework should be led and overseen by the insurer's board and senior management.***

***For it to be adequate 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.***

## *2.1 Introduction*

This section of the Practice Note addresses a range of corporate governance, management, operational and cultural considerations relating to ERM.

One of the core IAIS principles relates to the concept of 'proportionality'. This principle of supervisory supervision establishes that supervision of regulated entities should be proportionate to the nature, scale and complexity of the risks to which the insurer is exposed to.

The proportionality principle can be equally applied in an ERM context. The ERM framework for a small motor insurer operating in one country will necessarily be different to the ERM framework adopted for a global insurer offering 'short tail' and 'long tail' non-life classes, as well as life insurance. The objective is for ERM frameworks to be proportionate to the nature, scale and complexity of the insurer.

This Practice Note provides case study and other examples relevant to small, medium and large insurers. Whilst the majority of these draw on the experiences of larger insurers, the learnings and themes can be applied to all insurers, irrespective of the nature, scale and complexity of the risks they manage.

Nevertheless, there are certain aspects of ERM typically observed in small insurers and certain aspects observed in large insurers. Smaller insurers will tend to have consolidated board and management structures for risk oversight (e.g. combined audit/risk/compliance committee), less resources applied to component risk disciplines and less sophisticated modelling and measurement methods. On the other hand, large global insurers are more likely to promote consistent frameworks that incorporate common risk language, standardised categories, extensive policy/guidance and training materials, common reporting templates and tools to facilitate aggregation of

risk information, and sophisticated systems for collecting, analysing and reporting risk information.

Cultural and behavioural characteristics of risk management will invariably be unique to an individual insurer, whether they be small, medium or large, reflecting the history, values and style of the insurer. An absence of a supportive culture will undermine the most sophisticated of ERM frameworks.

Appendix 2 to this Practice Note describes a risk management 'maturity' model. It lists components of an insurer's ERM framework and describes typical characteristics of early, intermediate and advanced stages of maturity. Insurers can use this model to benchmark their ERM maturity. It is very likely that insurers, irrespective of their size, will aim for different levels of maturity for different components, seeking to differentiate themselves on particular aspects of ERM appropriate to the nature, scale and complexity of their business.

## *2.2 Risk Management and Corporate Governance Generally*

Corporate governance is concerned with improving the performance and conformance of companies for the benefit of shareholders, policyholders, other stakeholders and the wider economy. It focuses on the conduct of, and relationship between, the board of directors, managers and the insurer's owners. Corporate governance generally refers to the processes by which organisations are directed, controlled and held to account.

In a corporate governance context risk management is best described as an enabling process in the sense that it enables and facilitates the exercise of direction, control and accountability. In practice, the link between corporate governance and risk management is manifested in the form of a board committee and/or board charter responsibilities.

To ensure that there is a proper joining of ERM with an insurer's corporate governance structure, it is self-evident that the scope of the board's and/or board committee's "risk" responsibilities include all types of risk to which insurer is exposed.

## *2.3 Risk Management and the Role of the Board*

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 supervisors, 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.

It is established practice for boards to form a dedicated committee to focus on matters relating to risk management. This committee may include risk, audit, financial reporting and compliance disciplines, or some combination of these.

The overarching objective of a risk committee with respect to risk management is generally described along the following lines:

> *To assist the Board of Directors to discharge its responsibility to exercise due care, diligence and skill in relation to the effective management of major risks to which the insurer is exposed and verify that the insurer's risk management and internal control systems are adequate and functioning effectively.*

Typical committee charter responsibilities relating to risk management include oversight responsibilities associated with at least:

- Effectiveness of the Insurer's Risk Management Framework
- Compliance with supervisory requirements
- Establishment of a suitably independent risk function with the authority, standing and resources to effectively execute its mandate
- Monitoring the adequacy of corporate insurance covers.

In developing an appropriate charter for a board risk management committee regard should be given to certain processes that 'enable' effective discharge of charter obligations. These include, but may not necessarily be limited to:

- Establishing a direct reporting line between the committee and the most senior risk executive in the insurer
- Scheduling regular one-on-one meetings between the chair of the committee and the most senior risk executive outside of formal committee meetings
- Setting aside time in formal meetings for private meetings without executive management being present
- Consultation of external experts by committee members
- Transparency of reporting by the insurer's risk function such that reports to the board risk management committee and to management are not subject to any form of 'filtering'.

In developing appropriate committee processes one must also bear in mind the essential reliance the committee places on the insurer's risk function. The relationship can be characterised as one of trust. Put simply, charter objectives are more likely to be met if they are accompanied by an organisational culture that fosters rapid escalation of significant risk issues and/or 'bad news'. Cultural and behavioural aspects of ERM are discussed further in section 3.8 of this Practice Note. An example of a Risk Committee Charter is provided in Appendix 4.

## *2.4 Board versus Management Accountabilities*

It goes without saying that the respective risk management responsibilities of the board and management should reflect natural boundaries and various legal and supervisory requirements in different jurisdictions. The (supervisory) board's role does not involve active day to day management of the risks faced by the insurer. Rather, it oversees and monitors management's role which should involve an active process for managing and reporting on all the insurer's risks.

Of particular importance for boards when articulating respective responsibilities and conducting board and/or committee meetings is for them to avoid a perception amongst

management that the board, or more particularly the board risk committee, is *managing* the insurer's risks.

Equally, a risk management committee of the board provides an appropriate forum for the committee to question and challenge management's assessment of key risks as well as the process put in place by management to settle its assessment of key risks.

**TIPS: WHAT SHOULD WE WATCH OUT FOR IN ORDER TO HAVE AN EFFECTIVE RISK COMMITTEE?**

- Check that the Risk Committee comprises of members of a diverse background with the appropriate qualities such as inquisitive / questioning minds, objectivity and relevant experience. Consider the inclusion of external committee members to create a broader band of experience on the committee. Knowledge of the organisation is also important.
- Ensure the Risk Committee "ask questions" of the reports submitted and of management rather than apply the "tick the box" approach.
- Ensure the Risk Committee directives have the support of the Board and the appropriate level of management "buy in".
- Consider the appropriateness of the level and volume of reporting to the Risk Committee and keep the "quality" of the reports tabled and discussed under review to ensure the right information is being communicated.
- Risks Committees should also be responsible for keeping track of leading practices, trends and aiming to continually evolve and improve the organisations risk management processes.
- Risk Committees should have an appropriate self-assessment program which includes Key Performance Indicators which are Specific, Measurable, Achievable, Realistic and Time bound.

## *2.5 Management Commitment and Leadership*

The critical link between the Board and management is the insurer's CEO.

If ERM or risk management generally is not seen by the wider organisation as important to the CEO, the Board will have a hard task convincing stakeholders that the culture of the company is aligned with the Board's philosophy and/or some stated commitment to ERM.

Perhaps the most tangible means of ensuring alignment of CEO and board priorities with respect to ERM is to include certain risk management responsibilities in the job description and performance evaluation of the CEO, for example:

- promoting a risk management and control framework that articulates clear and powerful risk tolerance boundaries
- providing periodic assurance to the Board about the effectiveness and adequacy of risk management and control systems

- supporting an environment that does not tolerate behaviour that might compromise prudent risk management practices.

Moreover, public statements by the CEO and the leaders of the insurer that describe risk management as an insurer's 'core competency' or in similar terms further reinforce the view that proper management of risk is seen as critical to the insurer's sustainability.

## *2.6 Establishing and Developing an Enterprise Risk Function*

Consider a scenario whereby the insurer's CEO and board have decided to implement an ERM framework. Furthermore, as a sign of leadership and demonstrable commitment to ERM, the board has agreed that its first act in this journey will be to source and recruit a Chief Risk Officer (hereafter referred to as 'CRO') who will report directly to the CEO, or possibly the CFO. The key roles and responsibilities together with an example of a generic CRO role description are in Appendix 5.

The first major challenge for the newly appointed CRO is likely to be a 'bringing together' of the various risk-related functions and specialists within the insurer under a common framework and structure.

A newly appointed CRO will typically encounter a fragmented series of risk structures within an insurer, for example:

- Actuarial and/or research functions in some business units
- An internal audit function
- A specialist business continuity team
- A reinsurance department or reinsurance buying function
- Treasury and credit risk functions
- A capital management function
- Market risk assessment staff within asset management operations
- Health and safety experts reporting to the HR function
- Fraud and investigations experts
- Compliance teams in business units or in a central location.

In addition to the above, the newly appointed CRO might observe some risk-related committees operating within various structures within the insurer.

Perhaps the most important steps to take early in such a situation involve undertaking a program of action which will address at least the following questions:

- Is there a clear, shared understanding throughout the Board and management of the insurer's risk tolerance
- Are the incentive arrangements for management aligned with prudent management of risk
- What is the quality, health and transparency of risk information flows
- Where are the capability gaps, if any
- Are there elements of the insurer's business that are destroying value on a risk adjusted basis
- How is risk management connected with capital management and/or pricing and/or reserving
- Is the true financial condition of the insurer transparent to stakeholders

- Do the governance structures really work when there are stressful issues to deal with? (i.e. is the scope, composition and location of risk management 'committees' and their relationship with the insurer's board governance structures adequate?)
- Is the management 'operating model' appropriate? (i.e. is risk management embedded in and aligned with the insurer's business model, required competencies, key processes, people and infrastructure?)

The nature of the CRO role inevitably introduces a new dynamic to an insurer's senior executive team. The typical insurer CRO has an actuarial or mathematical background, brings rigour, method and a typically dispassionate approach to management decision-making. It is not uncommon for 'sacred cows' to be challenged – are products delivering an acceptable return on capital? should the insurer exit certain lines of business? and so on. In this context, unless carefully and sensitively managed, the introduction or development of ERM can create natural tensions. It will therefore be important for the CRO to quickly establish the insurer's performance drivers and key internal and external stakeholders. Moreover the board's demonstrable support for the CRO's strategy and plans will be critical.

The relationship between the insurer's CRO and CFO is a very important one as, amongst other things, the CRO and CFO share the objectives of improving earnings predictability and limiting exposure to adverse variations in earnings. Managed well, the relationship can be a source of value creation for shareholders and security for policyholders. Policyholder security underpins capital requirements whilst shareholder needs underpin the setting of performance/value creation benchmarks. CFO and CRO strategies therefore need to be integrated, i.e. they need to generate adequate returns AND provide for an appropriate level of capital to protect all classes of policyholder.

Arguably the most important ERM decision for an insurer relates to the setting of its risk tolerance. One of the first tasks for a new CRO is to establish whether:

- a board-approved risk tolerance exists (and, if not, move to create and maintain one)
- if so, whether it is understood by people making day-to-day underwriting, investment, reinsurance decisions, and
- (perhaps most importantly), is it appropriate having regard to the insurer's strategic objectives?

The CRO is ideally placed to facilitate a dialogue and debate at management and board level about the insurer's risk tolerance. The CRO should lead the debate, both initially and over time.

Visibility and authority of the CRO are essential. A close position to the executive board or even a position in the executive board may be recommended.

Finally, it should be emphasised that the CRO role is one of coordinator of risk activities/measurement at the company level. This is to be distinguished from the role of the income-producing units in the insurer. These units are the ultimate 'risk takers'. In this context the CRO seeks to be a value-adding partner by helping them act on opportunities identified by the ERM function.

The above key considerations are by no means the 'standard' priority issues for an incoming CRO. Each insurer presents a unique set of circumstances. However, the CRO should establish, and gain consensus around, the particular priority issues as soon as practicable.

### *Management Governance – Considerations*

Oversight structures will need to have regard to:

- Transparency of decision making processes and the forums used to make key decisions
- The size and nature of the insurer and whether it is involved in life or general insurance, or both, or is part of a financial conglomerate
- The mix of risks faced by the insurer.

A typical management governance structure for a medium to large insurer will include the establishment of management committees at the group and business unit level with processes to ensure periodic reporting by business unit committees to the group risk committee. Another structuring option relates to forming oversight committees with a dedicated focus on particular risks. For example, a natural delineation might be to establish oversight committees for:

- Pricing and underwriting risk
- Balance sheet/market risk addressing investments, liquidity, reinsurance, credit risk matters, etc.
- Operational risk.

Smaller insurers typically combine risk oversight activities under one committee or integrate the process with executive management reporting and monitoring activities.

The risk management structure of the insurer should align with the distribution of management accountability. For example, if business units are run in a standalone manner with ‘end-to-end’ accountability, the centralisation of risk functions will potentially conflict with the desired accountability outcomes. For example end-to-end accountability means accountability for meeting premium growth targets and managing risks associated with pursuing growth targets.

Risk management committees should comprise senior management from business and risk management functions.

### *Structure of the ERM Function*

It may prove impractical or inappropriate for an insurer to combine all specialist risk functions within a management structure headed by a Chief Risk Officer. What is important however is that processes are established to ensure that risk functions act and are seen to be acting in a coordinated fashion. From a line management perspective, the various risk functions will be viewed through a common lens and therefore inconsistent business unit engagement and reporting processes will invariably dilute and undermine the effectiveness of ERM.

In the case of large and/or multinational insurers the structure will typically involve a central or group risk function plus risk functions in each of the business units or regions. In such cases there is always the possibility of risk functions operating in isolation from each other, inhibiting information flows and escalation of key issues. Whilst there may be a range of reasons for this to happen, a decentralised risk management structure supported by ‘matrix reporting’ clarifying respective roles and responsibilities serves to help create a more effective management of risk issues.

An insurer’s risk function should also comprise an appropriate mix of capabilities and skills to support the delivery of ERM objectives. This means for example ensuring the

function has the capability to implement ERM. Technical expertise may not be sufficient. The function will need to consider utilising project and change management skills as well as broader relationship management skills.

*Summary*

The form of the insurer's risk management structure will not of itself be the key determinant of the effectiveness of the ERM framework. An appropriate structure supported by consistently applied business unit engagement processes, a common risk language and standard risk management 'processes', agreed behaviours, appropriate reward systems, and clearly understand reporting and monitoring will help drive a sustainable ERM framework.

## *2.7 Importance of a Common Risk 'Language' in the Insurer*

It is not uncommon in businesses for there to exist a range of risk management terminology, tools, templates, rating systems and reporting protocols. Moreover, a number of supervisors have produced detailed guidance for insurers seeking to implement more structured risk management processes. For example, the traditional risk 'matrix' plotting risk likelihood and impact[2] can be presented in many different ways. In addition, internal auditors and external auditors (and supervisors) may not necessarily use the same methodology for rating risk issues. Another dynamic relates to introduced methods by third parties, typically consultants engaged by the insurer to assist with projects.

A plethora of 'competing' risk language can undermine the effectiveness of ERM in a number of ways:

- It inhibits business management 'buy-in' and the task of embedding ERM by tending to confuse people not directly involved in developing and maintaining the methodology
- A 'silo' approach is reinforced. Silos may exist in business units and across risk management functions
- A focus on 'form' over 'substance'. This could result in 'real' risks not being identified
- A proliferation of process inefficiencies and duplication.

In addition to the above, aggregation of risk across categories is made particularly difficult because of inconsistent measurement of risks. Attributes and practices associated with a common risk management language include:

- A universally understood 'top-down' risk rating system e.g. a set of both financial and non-financial parameters that define 'high' (or 'red') risks versus 'low' (or 'yellow') risks
- A rating system that relates risk rating to the level of management responsible for taking action to mitigate the risk
- Standard templates for use across the insurer and common risk categories
- Reporting and escalation thresholds e.g. guidance and/or rules governing what risk issues need to be reported to who, and when.

[2] Important to note that *Likelihood* and *Impact* are sometimes inappropriately characterized in this context as *Frequency* and *Severity* – see footnote on page 39.

***EXAMPLE: 'BUT WE IDENTIFIED MORE RISKS THAN OUR COMPETITORS…'***

*An international insurer with a number of overseas branches was seeking accreditation under an advanced supervisory regime. However over time the insurer had developed different definitions of the risk classifications (such as Credit, Operational, Market, Fraud, etc) across many of the various jurisdictions that it operated in.*

*The lack of a common language created both operational and supervisory problems. The inconsistent and vague definitions created multiple risk identification, management and capital allocations of what could have been single risks. Some key risks were omitted from the risk management process which in turn, resulted in an inefficient business management structure. In addition, the lack of a common language meant that applications for accreditation could not be progressed until this could be resolved creating extra cost for the business and impacting on performance outcomes.*

*The company learnt to its cost that risk definitions should be precise enough to allow for the correct identification and classification of the 'real risks' to the organisation's business objectives, enabling economic value drivers within an organisation's risk management framework. In addition, risk language needs be consistently applied and communicated effectively across the organisation, enabling the organisation to take an enterprise-wide view of risk management, aware that all risks have been defined, classified and assessed consistently. Moreover a common risk language is essential to meet increasingly global supervisory requirements, no matter what size your company.*

## *2.8 Risk Management 'Culture'*

Simply put, culture is the combination of the behaviours of people in the organisation – often described as 'the way we do things around here'. All organisations have a risk management culture. The only issue is whether it is supporting the appropriate goals, activities and outcomes and mitigating the risks of not achieving desired outcomes. Therefore a question to ask when considering promotion of ERM is: "What are the behaviours you want people to use in relation to management of risk?" Appropriate risk management behaviours may vary according to the organisation, the industry context, the location of operations both within and across national boundaries together with the resultant jurisdictional requirements. However behaviours that allow responsibility for dealing with risk to be unclear, that inspire a culture of fear or retribution, that allow "shooting the messenger" or that help "bad news to travel slowly" are not likely to be conducive to good risk management.

However deciding on behaviours is not sufficient to create or reinforce an appropriate risk management culture. There needs to be effective implementation of risk frameworks and processes. Furthermore, people need to be willing and able to use the appropriate behaviours to support risk related activities. It is these behaviours that over time will create the desired risk management culture. Therefore it can be said that human behaviour and capability are key to effective ERM.

Experience has shown that the most effective way to introduce these behaviours is as 'part of good business practice' rather than a 'big launch' which can be perceived as a 'fad' by employees. Positioning these behaviours as 'business as usual' also serves to bind the whole organisation to the concept because everyone is on the implementation team. In reality this takes significant time and effort. Typically adoption of new behaviours requires at least three years to start to take hold and longer to embed into the corporate culture.

***EXAMPLE: PROMOTING A PROACTIVE RISK MANAGEMENT CULTURE***

*An international general insurer based in Asia Pacific saw an opportunity to improve management risk by encouraging people to be more proactive. There were several potential benefits for working on the cultural side of ERM in this way. Being proactive meant that risks could be prevented or detected earlier, when smaller and were therefore typically quicker and less costly to remediate. Being proactive and encouraging speaking up about things 'not right' could enable speedier detection of issues. On the upside, hearing about ideas for improvements could support innovation, a key to business growth.*

*However it was recognised that changing the culture would take a number of years. So a program to embed proactive risk management behaviours was developed. The first step was to define the elements of a proactive risk culture, shown in the model below. Then behaviours associated with this model were incorporated into the annual staff survey. These questions form a risk culture index that not only enabled tracking of progress but also correlated with operational performance.*


*Initiatives to promote proactive behaviours were designed and implemented, all framed around the tag line of* **It's all about being proactive.**

- *Inclusion of proactive principles in the Risk Management Strategy and Group policies and practices*
- *A corporate risk goal for senior managers based in improving the risk culture index*
- *Proactive behaviours included in role definition, performance management and succession/talent development processes*
- *Training programs developed for managers and staff in face to face and online/blended formats and inclusion of the proactive principles in other training*
- *Information placed on the company intranet including incident reporting portals.*

*Several years on, measurable progress is being made however the challenge is to continually invigorate the program to ensure being proactive stays at the top of people's minds.*

The following sections expand on two of these challenges: the development and measurement of an appropriate risk management behavioural model and designing an effective implementation plan.

## *2.9 Developing a Risk Behaviour Model*

There are arguably three aspects to consider in addressing the behavioural aspects of risk management. The first is a proposition that risk management is not about eliminating risk, as this would inhibit growth and change. Rather, it is choosing the risks the organisation is willing to take and then managing them well. Therefore it is useful to adopt the description from various risk standards (e.g. the Australian Risk Management Standard AS4360) about the core risk behaviours of prevention, detection and recovery combined with continuous improvement.

Supporting this is a second core concept that people need to feel confident to speak up about in this risk management context. This may involve full and frank discussion of the risks being considered, whether they are minor process issues in a call centre or risks associated with a potential acquisition. It also means people feeling confident to communicate 'bad news' promptly when things go wrong without fear of retaliation. This requires managers to provide an encouraging environment at all levels.

Underpinning both of these is a third aspect involving people having the skills, capability and empowerment (role clarity and accountability) to undertake the behaviours necessary to manage risk situations. Interestingly, these three aspects also link strongly to supporting innovation and therefore growth of the business. In this way the behavioural aspects of risk management can be positioned as addressing the 'downside' and supporting the 'upside' of risk management (refer also to Section 3.11 below).

## *2.10 Developing an Implementation Plan*

It is important to operationalise appropriate risk management behaviours by developing a common language to describe them in a way that everyone in the organisation can use. These descriptions should be incorporated into descriptions of core competencies and/or capabilities, talent assessment and development and all risk and compliance training. These activities should be supported strongly by executive management and the insurer's board who need to demonstrate a keen interest in progress across the business.

The organisation should measure the above elements each year to observe areas where the risk management culture is strong and where there is opportunity for improvement. Rather than creating an entirely new measure and an extra burden on the business in time, the first step should be to identify if there are measures already available to use. These could include existing employee surveys, performance data and audit reports. Consideration could be given to augmenting existing measures identified so they can be used to assess the strength of the risk management culture. Using additional measures also has the benefit of 'shielding' the measurement from gaming to achieve a good result, especially if bonuses are dependent on results. The key word is simplicity, both for the model and the measurement approach.

In summary, people, behaviours and resultant cultures are a fundamental building block for the development of effective and sustainable ERM. Implementation of a 'culture' component of ERM should address the following aspects:

- Consideration and development of a risk management behavioural model that suits the insurer's broader culture and operating environment. The model should be precise in describing behaviours in measurable and observable terms

that can be incorporated into training, reporting, bonus and performance management systems
- Securing support of senior management and development of their risk awareness. This could be facilitated by training, focus groups, education and briefing of executive management and by examining how risks have been managed in the past together with better approaches. 'War stories' help understanding and engagement
- Ensuring that the 'right' behaviours are embedded in the design of frameworks and processes so they have integrity within the ERM framework and also are reinforced at every available opportunity
- Design of an implementation plan over a realistic time frame, appropriately resourced
- Reinforce behaviours through multiple influencing channels
- Benchmark behaviours before starting the implementation program and measure at least annually to assess progress. Be ready to make adjustment to the design and change program if required, particularly if external events indicate the need
- Link the measures to measurable business outcomes to prove the value add of the desired risk management culture.

**TIPS FOR IMPLEMENTING RISK CULTURE CHANGE PROGRAMS**

**Leverage** – Use existing organisation-wide programs rather than starting new ones to both lessen the load of managers and staff and facilitate embedding as business as usual as soon as possible.

**Language** – Focus on behaviours which people feel they can change rather than 'culture' which can be considered amorphous and intangible.

**Change skills** – Hire or engage people with skills to assist the risk function such as people skilled in change management, learning, human resources, project management etc.

**Embed Principles** – Ensure the change initiatives to promote the new cultural principles are embedded into the people processes so the program is continually reinforced and maintained.

**Measures and Consequences** – Benchmark the culture then measure progress and ensure the Board/Risk Committees are supportive of the program and aware of improvement. Reinforce good behaviours and reorient inappropriate behaviours through use of levers such as bonus payments.

## *2.11 'Upside' Risk Management*

It is commonly accepted that risk management involves both the management of potential adverse effects and, conversely, the realisation of potential opportunities. Whilst practices associated with managing adverse effects are well understood and follow established patterns, the same cannot be said for the realisation of opportunities. This of course is not to say that insurance managers miss opportunities. Rather, it reflects a relative lack of consistently applied *risk management processes* for the management of opportunities (or 'upside risk').

Perhaps the best way to illustrate this relative gap is to reflect on the information generally presented in management reports dealing with risk. These will typically highlight key risks, incidents, issues and trend in risk indicators etc. However these reports rarely include an analysis of key opportunities and therefore are arguably incomplete in addressing the full spectrum of risk. Of course insurers do report on opportunities, typically via CEO and business head reporting. However the assessment of the value of these opportunities is invariably disconnected from the assessment of the value of the insurer's risks. Effective ERM implies an integrated assessment of adverse effects and opportunities.

The real challenge then for insurers is to create an environment around the development of their ERM framework that facilitates better integration of the management of upside and downside risks. Some of the practices that will support integration include:

- Ensuring the risk function is involved in strategic planning
- Including both risks and opportunities in reports prepared by risk functions (and internal audit functions). Some examples of opportunities can be:
    - Reduce costs by removing excessive or ineffective controls
    - Leveraging risk management controls to achieve other business goals (such as utilising work from home solutions not just as a BCP risk control but also to achieve a human resourcing goal to establish more flexible working conditions to attract / retain staff)
- Reward systems that encourage calculated risk taking
- Reporting on emerging, industry-wide, cross-border, and longer term risks.

The risk management process (Section 7.2) can be equally applied to the assessment of risks and opportunities. The discipline of the process requires people to quantify both risks and opportunities using consistent rating methods.

Effective upside risk management is underpinned by a mindset that views all risks as opportunities:

- Opportunities to implement mitigation or risk transfer strategies for identified risks
- Opportunities to develop plans to proactively prepare for low likelihood – high impact scenarios e.g. by running crisis simulations
- Opportunities to invest in new capabilities to manage longer term risks potentially impacting future profitability.

Involvement of the risk function in upside risk management provides a real opportunity for the function to actively participate in strategic activities and add value to the insurer.

As described in Section 3.8 above, the insurer's organisational culture is critical to the effective management of upside risks.

## *2.12 Performance Management and Reward Systems*

The discussion above about organisation culture reinforces that performance management and/or incentive systems should include a recognition or inclusion of a risk management component. For example, a broad scope ERM implementation that is not accompanied by management incentives tied to clearly defined risk management outcomes will, most likely, fail.

Care should be taken when constructing incentive programs that include a component aimed at improving risk management practices or extracting value through better risk management. Key considerations include:

- Getting the balance right and, for example, ensuring that the relative size of the incentive for improving risk management does in fact motivate targeted individuals and/or groups
- Deciding which individuals or groups to include. If senior management reward systems are not inclusive of a risk management goal then the insurer will struggle to evolve its ERM framework
- Establishing clarity about what to measure and what are appropriate measurement 'proxies'. Consideration should be given to activity-based measures (e.g. milestone completions), financial measures (e.g. value at risk over time), audit results/performance and staff surveys
- Making linkages between risk management performance and talent management and capability development processes. For example, if it is understood that leadership potential is in part measured by an individual's capacity to create an environment that fosters proactive management of risk, then the insurer's board can gain comfort that managers will actively support ERM
- Ensuring that incentive programmes are targeted at the appropriate level of staff and that they do not have unintended consequences. For example, linking staff incentives to results of staff surveys/feedback is likely to skew the results of the surveys.

***EXAMPLE: ENCOURAGING THE 'WRONG' BEHAVIOUR***

*A large financial services organisation announced significant losses relating to the activity of their proprietary trading division. It seemed that people had used various methods of concealment so they could continue reporting profits despite the significant losses being incurred. One of the motivations appeared to have been the desire to achieve budgeted profits and receive bonus payments.*

*Investigations confirmed this link to incentives. The following observations were made regarding the culture:*

- *There was an excessive focus on process, documentation and procedure manuals rather than on understanding the substance of issues, taking responsibility and resolving matters.*
- *Risk measures and reporting were not relied upon or believed to characterise the risk exposure correctly and therefore were ignored*
- *There was arrogance in dealing with warning signs*
- *Issues were not escalated to the Board and its Committees and bad news was suppressed.*

*The prevailing culture fostered an environment that provided the opportunity to incur losses, conceal them and escape detection despite ample warning signs from the formal risk management processes, structures and systems. The employees did not behave honestly and the risk management processes failed.*

*As a result of these significant financial losses, several senior managers resigned, there was considerable damage to the organisation's reputation; significant fall in share price; heightened supervisory supervision with associated increased management time and cost; and criminal proceedings and convictions of the traders.*

***Example: Encouraging the wrong behaviour - Key learnings***

1. *Listen to the warning signs and ACT*
2. *Prioritise the correction of known control breakdowns*
3. *Consider the unintended consequences of incentive plans*
4. *Risk management needs all its elements to work together to reduce 'gaps'*
5. *A poor culture and misaligned incentive plan can override the best of formal systems and controls.*

## *2.13 Reporting and Monitoring*

Effective ERM relies heavily on quality risk management information because better risk management information means better decisions. The insurer's risk management function should form a view as to whether executive management and the board are receiving the 'right' information. Typically, insurers produce detailed information about insurance, market/investment and credit risk. However this is not always the case with operational risk and the overall portfolio of risk – the enterprise-wide risk report. At the highest level risk reporting should seek to answer the following kinds of questions, such as:

- 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.

The table below provides, by risk category, an indicative list of the sort of information typically associated with enterprise risk reporting:

| Risk Category | Information |
|---|---|
| Enterprise /all risk categories | • Enterprise risk profile (refer also section 7.2 for sample risk profile layout)<br>• Capital adequacy ratios<br>• Significant regular engagement<br>• Significant losses, incidents<br>• ERM framework improvements<br>• Changes in key risk indicators (KRIs) |
| Underwriting (including reinsurance) | • Risk aggregations (sum insured) by region, peril, distribution channel<br>• Reserve strengthening/release |
| Market | • Value at risk (VAR)<br>• Stress and scenario test results |
| Credit | • Counterparty credit quality and diversity for assets and liabilities – credit rating analysis |
| Liquidity | • Proportion of liquid assets to total assets |
| Operational | • Analysis of key risks (operational risk profile)<br>• Change in key risk indicators<br>• Internal audit results |
| Other | • Benchmarking of emerging industry risks<br>• Business, insurance cycle data |

The following is an example of dashboard reporting.

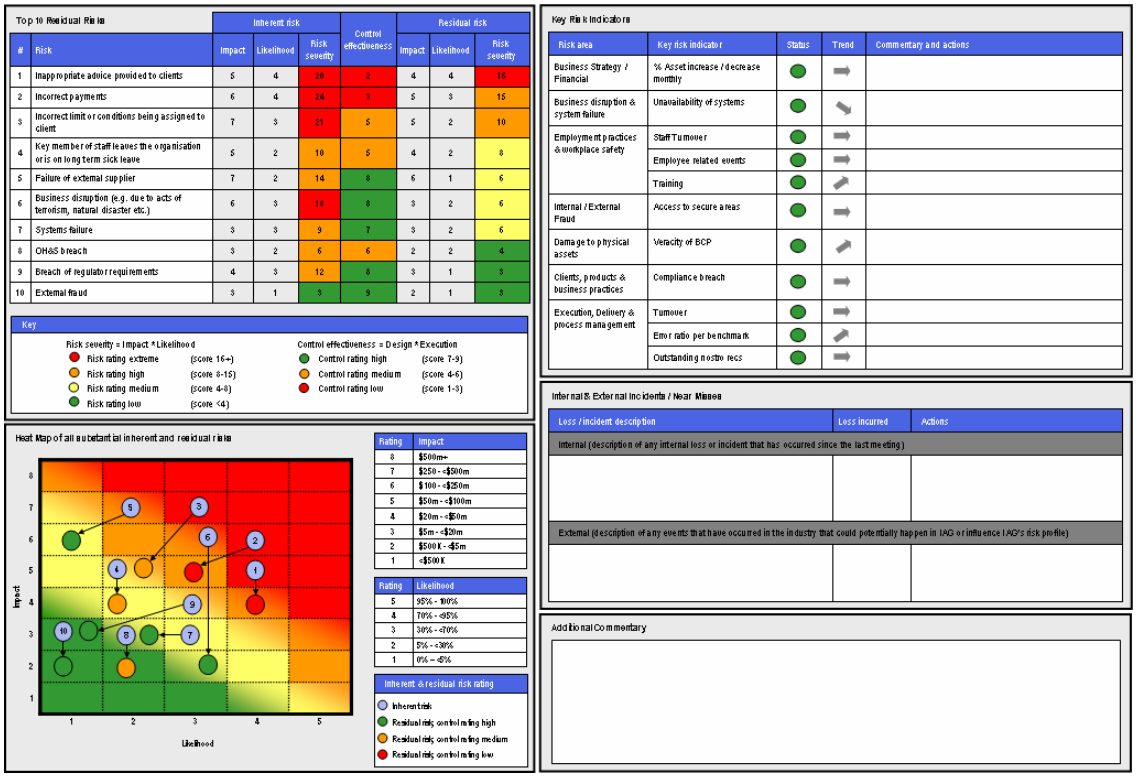
***EXAMPLE: 'ANYTHING TO REPORT?'***

*Many stakeholders rely on quality risk information:*

- *Audit Committees – Monitoring material financial risks and mitigation of those*
- *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 supervisory 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*
- *Heatmap of all substantial inherent and residual risks*
- *An additional commentary section*
- *Significant project progress.*



## *2.14 Role of Internal Audit*

It is not uncommon practice for the role of developing an insurer's risk framework to be allocated to an insurer's internal audit function. This reflects a view that there is a good match of the desired skill sets for ERM implementation and those of internal auditors.

This practice may deliver short term assurance benefits and give insurer boards a sense that progress is being made but is unlikely in the medium to longer term to deliver a truly effective or embedded ERM framework. Moreover, the practice can potentially undermine the necessary independence of the internal audit function by putting it in the position of creating processes that it is consequently conflicted from 'checking'. Perhaps more importantly, it sends a message to the wider organisation that ERM is essentially an assurance or compliance exercise rather than a process that is ultimately intended to optimise value created within an agreed risk appetite. A number of national supervisors have recognised this inherent conflict by introducing standards that define the role of an insurer's internal audit function with respect to risk management.[3]

Emerging best practice in this area is to clearly delineate the roles of internal audit and the function tasked with developing and maintaining an insurer's ERM framework. In this way, the independence of internal audit is not compromised but rather is preserved and directed at providing assurance to the board, and typically via the board audit committee, about the effectiveness of the insurer's ERM framework over time.

## *2.15 Dealing with New Activities*

An insurer's ERM framework needs to extend to new activities as these are invariably sources of new risks that can significantly affect an insurer's risk profile. 'New activities' could include:

- Product changes and introduction of new products
- Changes in corporate and management structures
- Commissioning of major projects to build and/or upgrade computer systems and networks
- Due diligence, acquisitions, divestments and other 'corporate transactions' e.g. capital raisings
- Outsourcing and off-shoring strategies.

It is important for the insurer's risk function to be familiar with the range of change or 'pipeline' activity under way at any given time. Moreover, strong working relationships between the insurer's risk function and functions driving the pursuit of new activities or strategies increase the likelihood that the 'risk voice' will be appropriately heard and considered. In practice this means involvement of the risk function at the planning stage of new activities and agreeing details of the role and responsibilities of the risk function with respect to such activities.

The insurer's risk function should therefore develop close, transparent and systematic relationships with functions such as strategy, finance, product development, IT, legal and human resources, amongst others.

[3] For an example refer APRA Prudential Standard GPS510, Governance, para's 46, 47.

There are a number of ways that the insurer's risk function can become involved in new activities, including:

- Involvement in due diligence work where the skills of the actuary and other risk management professionals can be utilised to help identify and assess risks and to assist with valuation and modelling aspects
- Working with the insurer's strategy team to ensure the strategy incorporates an appropriate assessment of risks attaching to the chosen strategic direction
- Preparing and/or facilitating risk assessments for major projects or new product launches
- Managing and coordinating engagement with relevant supervisors with respect to pursuit of new activities
- Working with newly acquired businesses to help them adapt to and implement the insurer's risk management framework.

Engagement by the insurer's risk function in these kinds of activities fosters strong relationships, facilitates better management decisions and aligns the risk function with the objectives of sustaining and creating value. In this way ERM disciplines and processes become naturally embedded in change activities.

## 3. Risk Management Policy

***Key Feature 2***

***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, supervisory capital requirements, economic capital and the processes and methods for monitoring risk.***

The insurer's risk management policy provides an important opportunity for the insurer to establish and communicate philosophy and minimum requirements for the management of the portfolio of risks to which the insurer is exposed. Risk management policy should be set by the insurer's board. In a number of jurisdictions it is also a supervisory requirement for risk policy to be approved by the board. A list of the typically topics included in a risk management policy together with a suggested structure is provided in Appendix 7.

The process of developing and setting risk management policy should involve many stakeholders, take some time and be tested with those responsible for implementing and complying with the policy. An 'in-use' policy should be regularly reviewed, at least on an annual basis.

In formulating risk management 'policy' the insurer should address at least the following aspects:

- 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 supervisory 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'
- Most importantly, the insurer's risk appetite should be set forth in the policy (refer Section 6 below) for further discussion on risk tolerance
- 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 universally across the operations of the insurer e.g. risk management training, risk profiling, business process documentation, risk reporting and escalation, risk monitoring and assurance
- Requirements for the conduct of the insurer's 'Own Risk and Solvency Assessment' (refer Section 7 below)
- As appropriate, specific requirements attaching to defined risk categories
- The process for reviewing and updating the policy.

The above 'shopping list' may be suggestive of a policy document of some considerable length. This should not necessarily be the case. Care should be taken to avoid writing a long policy document that is not read or understood by the wider organisation. Therefore, the writer or policy custodian should consult widely to formulate an appropriate strategy for communicating the board's expectations with respect to ERM. This may involve the development of a suite of documents, including a high level set of policy principles, tailored to different 'audiences' within the insurer.

Development of new policy or renewal of existing policy provides an excellent opportunity to assess attitudes to and understanding of risk management in the organisation. If ERM policy implementation is carried out in a top-down fashion with limited engagement of business functions, then it is unlikely that ERM requirements will be properly integrated with and embedded into the day-to-day operations of the insurer.

## 4. Risk Tolerance Statement

***Key Feature 3***

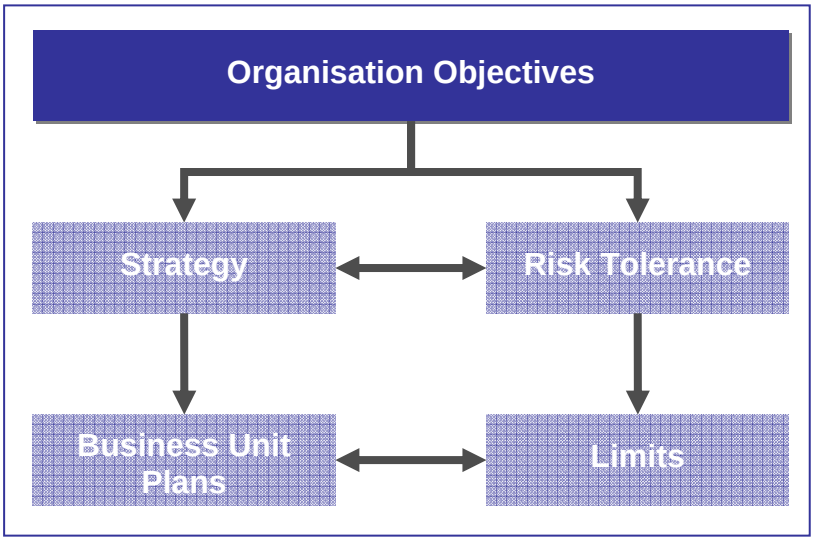
***An insurer should establish and maintain a risk tolerance statement which sets out its overall quantitative and qualitative tolerance levels and defines tolerance limits for each relevant and material category of risk, taking into account the relationships between these risk categories.***

***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.***

This section discusses the concept of 'risk tolerance', the relationship between risk tolerance and the insurer's strategy and provides guidance for insurers on some of the practical aspects of setting and updating risk tolerance.

Establishing an insurer's risk tolerance involves making strategic choices. The process must be connected with setting strategy and longer term direction. Whilst 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.

The insurer's risk tolerance is framed having regard to the insurer's strategy and business plan. The risk tolerance shares the same time horizon as corporate strategy, typically three to five years, and therefore should not respond to, for example, annual budget targets/business plans. Put another way, it would be highly unusual for an insurer's risk tolerance to change every year. The relationship between risk tolerance and strategy is illustrated in the diagram below:



The insurer's risk tolerance articulates boundaries for how much risk the insurer is prepared to accept. 'Limits' are more in the nature of thresholds that warn insurers that achievement of plans may be 'at risk':

- Risk tolerance is a higher-level statement that considers broadly the levels of exposure to risks that the Board deems acceptable
- Limits are narrower and set the acceptable level of variation around objectives associated with an insurer's annual business plan and budget. In particular, Limits translate the risk tolerance into language that can be used by the business on a day to day basis.

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 supervisory criteria incl. 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'
- Maintaining a buffer level of capital in excess of the minimum supervisory capital
- 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)
- Minimum acceptable pricing principles
- Descriptions of unacceptable operational risk scenarios typically disruptive of the continued and efficient operation of the insurer
- Setting 'go/no-go' criteria for corporate transactions and strategic projects e.g. acquisitions, divestments, capital raisings, projects spanning multiple business units and/or entities within an insurance group etc.

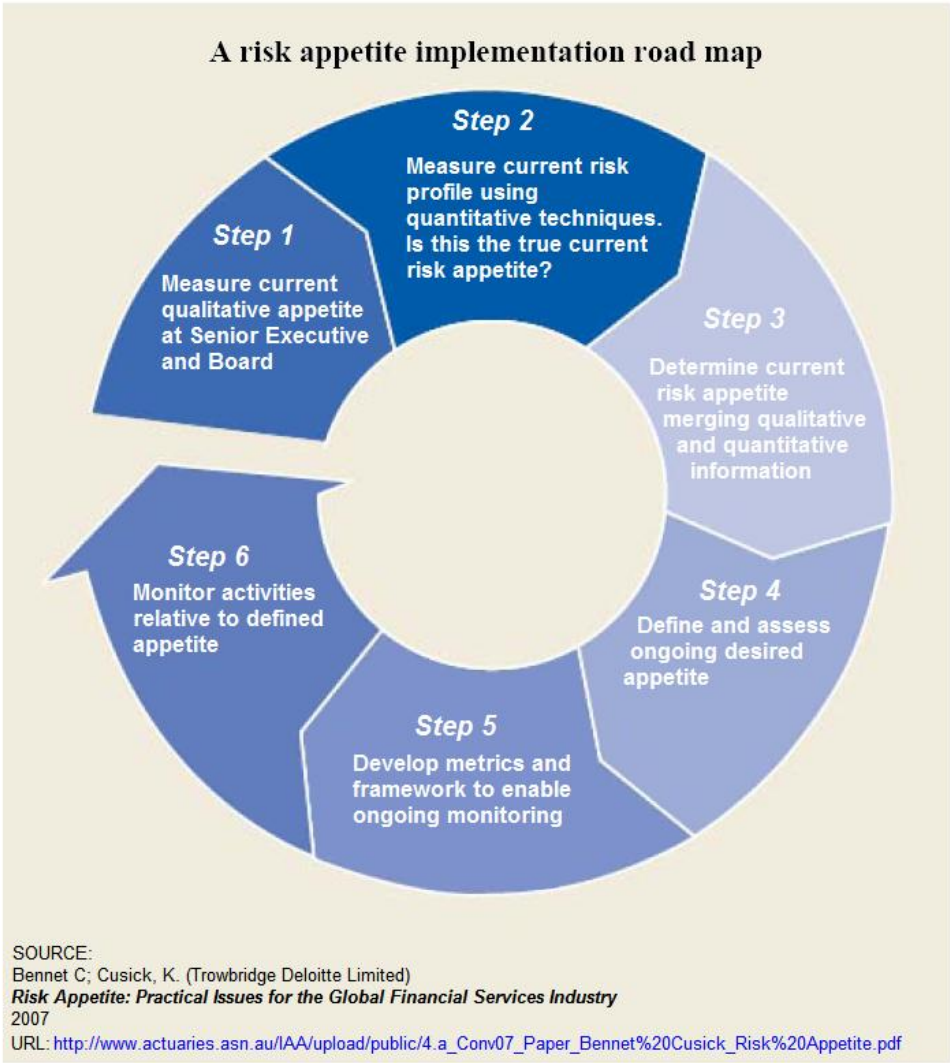
On the other hand limits, being narrower in scope, tend to operate at the risk category level. Staying within limits should mean that an insurer will stay within its overall risk tolerance. Example of risk limits include:

- 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 insurance reserves to target an explicitly quantified 'probability of adequacy'
- 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, health & safety and project delivery, amongst others.

As can be seen from the above, limits are more transparent to business managers. Moreover it is becoming increasingly common for business managers to utilise Key Risk Indicators (KRIs) to highlight how and when limits may be exceeded or are reaching key thresholds. It is therefore important that the insurer, usually via its risk function, establishes clear linkages between risk tolerances and limits. This delivers governance benefits (board assurance that risk policy is appropriately 'operationalised') and performance management benefits (fewer surprises and reduced earnings volatility). In addition, it is important to consider when calibrating risk tolerance by reference to target credit ratings, that insurers should also undertake their own appropriate rating analysis to 'triangulate' external data supplied by ratings agencies, and other third parties.

It is important that each insurer develop a statement of risk tolerance appropriate to its own circumstances. Some insurers may choose to develop high level statements of risk tolerance whereas others may define risk tolerance at the risk category level, and even within the risk category level. The diagram below shows a typical roadmap of the steps to establish a risk tolerance.



More details about this process can be found in the Useful References in Appendix 8 particularly the source referenced in the diagram.

Whatever path is chosen, the following should be borne in mind when settling an insurer's risk tolerance:

- It must support the achievement of business strategy
- It must be supported by appropriate financial and other policies that translate higher level statements of risk tolerance into operational limits.

***EXAMPLE: HOW TO DEVELOP A RISK TOLERANCE***

As shown in the following graphic, risk tolerance is about which risks to take and why, not just how much risk to take.


1. ***Risk Profile:*** the current and emerging risks facing the business
2. ***Risk Capacity***: The financial, reputational and operating capacity or comparative advantage of the business to withstand or manage the risk exposures
3. ***Risk Tolerance***: Whether the risk profile is appealing within the context of our risk capacity, strategy, market positioning and business competencies

When developing a position on risk tolerance the questions to ask are;

- How comfortable are we in the continuing exposure to an individual or basket of risks given our Risk Profile (current and future), our Risk Capacity (current and future) and within the context of our strategic options or choices?
- Is there a build up or concentration of risk that makes us uncomfortable?
- In light of the risk exposure, are we satisfied with the level of return (and capital requirements) expected from the decision?
- What would be the level of regret if we took an alternative option/decision or bet under different future scenarios?

# 5. 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.***

## *5.1 Nature of Feedback Loops*

A key test of the effectiveness of an insurer's ERM framework is the extent to which it caters for change. A framework geared only towards 'business as usual' (BAU) activity may fail to prepare the organisation for shifts in market dynamics, supervisory change, changing customer preferences, global trends and so on.

The insurer's risk profile over time will be influenced by:

- Outputs from periodic risk assessments at the enterprise and business unit levels that have regard to BAU activities, new initiatives/strategies and external events (*looking forward*)
- Movements in key risk indicators (*the present*)
- Unexpected losses, and significant control failures or incidents (*looking back).*

Taken together these three influences provide valuable ongoing information about the effectiveness of the insurer's internal control environment. The insurer's ERM framework should therefore include formal and systematic processes to collate information from the above three sources (past, present, future).

A particular source of relevant feedback is incidents and issues. These could be generated by customer complaints, audit findings, project or system failures, crisis events and supervisory action. The insurers ERM framework should incorporate processes for the formal review of incidents/issues above certain thresholds, including the analysis and reporting of 'root causes'. This practice supports a culture of learning from mistakes and continuous improvement.

An effective feedback loop is underpinned by:

- Establishment of thresholds for reporting significant issues (see also Section 2.13 above)
- Protocols for escalation of issues to various levels and management and, if necessary, supervisors
- Reporting of risk aggregations to identify where limits (and potentially risk tolerance) may have been exceeded.

## *5.2 Emerging Risks*

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.

**TIP: WHY INSURERS WANT TO KNOW ABOUT EMERGING RISKS**

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?

The answers to these question may have a direct impact on policy wording, claims reserving strategies, reinsurance arrangements and the insurer's own operational risk strategies.

Having a clear set of emerging risk objectives linked to the organisation's context and strategy is critical before starting this step. Some examples of the context setting characteristics to consider include:

- Geographical scope - local / country / regional / global
- Time Horizon – long time horizon for long tail classes of insurance, or, short time horizon
- What types of impacts – physical damage to property; liability exposures; health issues; or multiple types of impacts.

Appendix 8 provides some useful 'emerging risks' websites.

Once the objectives and scope are established this will provide some direction to help identify emerging risks. The identification can be done using a variety of methods ranging from reviewing the press and trade publications, work shops, the opinions of external experts, etc.

Emerging risks may lead to claims with a high loss potential but may also represent a new business opportunity akin to 'first mover advantage'. The earlier these sorts of risks and/or opportunities are identified, the greater the room for action. A mature ERM framework will be addressing emerging risks and creating the conditions for dialogue between business functions and risk functions about strategies for dealing with them.

The common characteristics of emerging risks are:

- High uncertainty as there is little information available and the frequency and severity[4] is difficult to assess
- Difficulty in quantification as risk is uncertain and the risk transfer may be questionable

[4] *Frequency* and *Severity* are both probability distributions as opposed to *Likelihood* and *Impact* which are dimensions of a matrix.

- No industry position as no single insurer wants to make the first move for fear of losing market share
- Difficulties for risk communication as there is the danger of reacting to phantom risks
- Supervisory involvement often being necessary.

In 2005, the Chief Risk Officers (CRO) Forum founded the *Emerging Risks Initiative* (ERI) with the aim of raising awareness of and communication about emerging risks that are relevant to the insurance industry. The ERI focuses on identifying, prioritising and communicating information on emerging risks relevant to the insurance industry. The CRO Forum Emerging Risk Initiative (http://www.croforum.org/emergingrisc.ecp) has so far published three positions papers: pandemic; terrorism; climate change & tropical cyclones.

An insurer implementing ERM needs to establish a process for dealing with emerging risks relevant to its own business, working through the risk processes identified in Section 7.2 below. In addition the following information about emerging risks frameworks may assist in formulating an approach.

### *5.3 Scenario Planning*

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 can take the form of facilitated workshops, crisis simulations and think tanks. It can also provide opportunities for collaboration on industry issues.

Scenario planning is a powerful tool that helps executives assess the resilience of the organisation to internal and external shocks. Assumptions about the real nature of the risks and operation of controls and contingency plans are tested and often result in changes being made.

A number of insurers have invested in capabilities to help them cope better with the ‘unexpected’. In particular, the practice of Business Continuity Management, or BCM, has evolved rapidly in recent years. BCM teams typically run a schedule of crisis simulations under a range of scenarios and managers who participate in simulations typically will report that they feel better prepared for a ‘real crisis’ having experienced a simulated one. This is particularly the case when simulations affect multiple business units and require participation of senior executives. (Refer Section 8.3 for further details).

# 6. Own Risk and Solvency Assessment (ORSA)

***Key Feature 5***

***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.***

## *6.1 Introduction*

ORSA involves carrying out a combination of quantitative and qualitative techniques to identify, assess and manage risk. It is important that this involves the regular actuarial control cycle that essentially examines experience from decisions and actions taken and provides the feedback from this experience into future decisions and actions. This section discusses the basic 'building blocks' of the 'risk management process' and also suggests appropriate methods for assessing different kinds of risk.

## *6.2 The Risk Management Process - Risk Profiling*

The core process of risk management involves a systematic identification, analysis, evaluation and treatment of risks having regard to an appropriate context. Typically, the 'context' is framed around objectives of a business process or project or indeed the broader insurance enterprise. In addition, a critical aspect of context involves the setting of the risk tolerance (Section 4, above). 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).

Risk profiling and related governance and/or framework activities should not be confused with capital modelling (refer Section 7, below). The latter process is primarily concerned with statistical and actuarial methods and processes whereas risk profiling is more in the nature of an operational process, sharing similar characteristics with activities like business planning and project management. 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'. A working definition of these terms is shown in the table below[5].

| Inherent Risk | Residual Risk |
|---|---|
| The risk to an entity in the absence of any actions management might take to alter the risk's likelihood or impact | The remaining risk after management has taken action to alter the risk's likelihood and impact |

[5] Enterprise Risk Management-Integrated Framework, The Committee of Sponsoring Organisations, September 2004

This aspect of the risk management process can be tedious and counter-intuitive in the hands of, say, an underwriting manager who may view the underwriting process through the lens of controls 'built-in'. Nevertheless, assessing both inherent risk and residual risk highlights 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*).

More broadly, the value in risk profiling revolves around bringing people together to debate risk and its management. New insights are gleaned and awareness of the nature of risks is raised. The process is important because it promotes and reinforces:

- Consistency and understanding, by collating and presenting a shared view of the most significant risks from time to time. The process also forces management to assess risks relative to each other
- Transparency to the board and an opportunity for the board to review management's formal assessment of significant risks
- Organisational efficiency by ensuring that management effort/risk mitigation is prioritised to the areas of greatest assessed risk
- Learning and continuous improvement through taking action to alter and ideally reduce the risk profile
- A culture of proactive risk management that supports innovation and sustainability.

It is not the purpose of this Practice Note to discuss the mechanical, workflow and or task-level steps associated with developing a risk profile. However, a risk profile will typically include the following information:

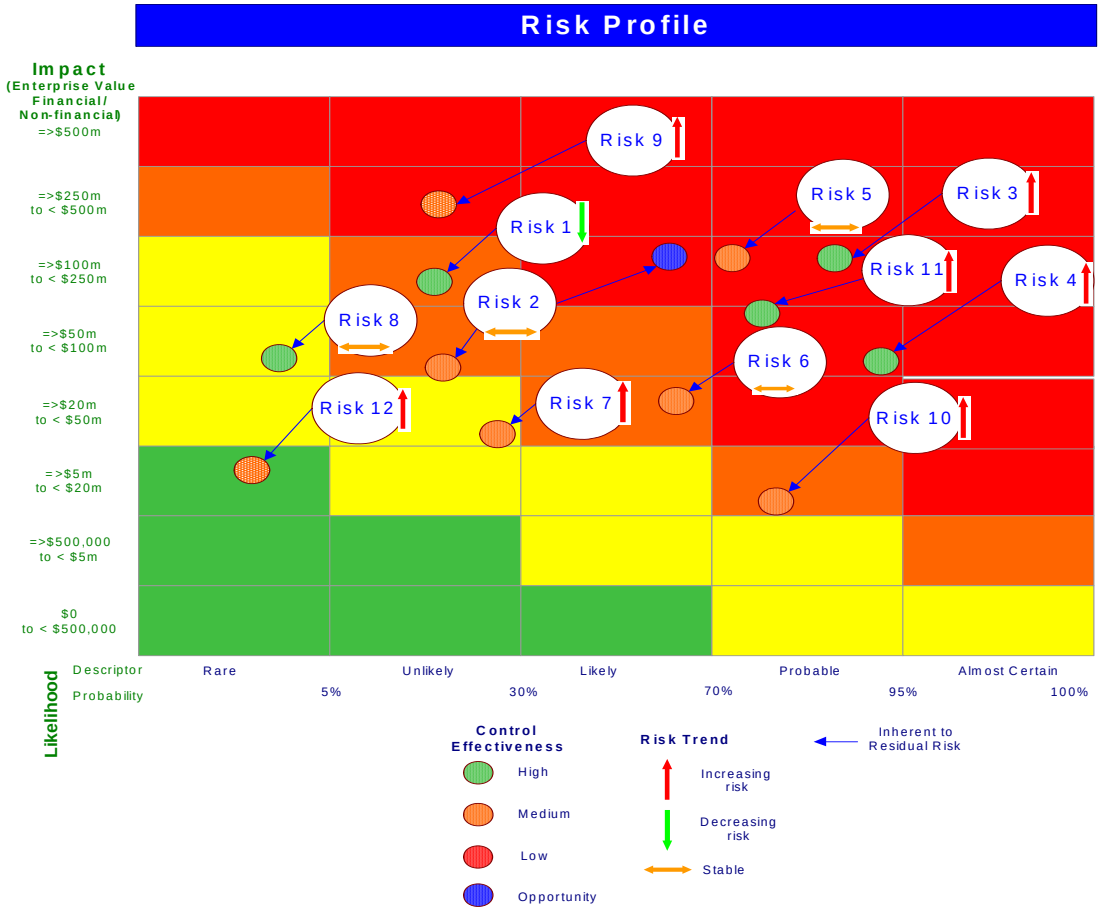
- A description of risks in enough detail for each risk to be understood in isolation
- The cause(s) or underlying conditions giving rise to a given risk actually occurring or crystallising
- The consequence(s) of the risk. These are typically expressed in both financial and non-financial terms e.g. loss of customers, supervisory sanction, cost over-runs etc
- An appropriate categorisation of each risk. This is particularly important where an insurer comprises multiple business units and there is a requirement to perform some form of risk aggregation at the enterprise level
- An inherent risk assessment that considers likelihood/frequency of risk occurrence and impact of the risk. It is best to establish clear rating criteria for the risk assessment e.g. establishment of financial and/or non-financial proxies for, say, 'high', 'medium', or 'low' risks
- An assessment of the effectiveness of controls and/or risk mitigation strategies. This assessment should consider both design and performance aspects of controls and note control ownership
- A residual risk assessment after taking into account the effectiveness of controls
- A description of the action(s) to be taken to bring unacceptable residual risk within appropriate limits.

Risk profile documents are typically 'signed off' by the responsible executive. This could be the insurer's CEO in the case of the 'enterprise risk profile' or business unit head in the case of a business unit risk profile.

Insurance company managers tend to be very comfortable with the assessment and quantification of risk. After all, it should be core business for them. However this can also result in a tendency amongst insurance managers to seek to quantify non-insurance risks in financial terms. Many risks, in particular those of a strategic or operational nature may not behave stochastically nor readily lend themselves to statistical or actuarial analysis. In such cases it is perhaps better to opt for more simple or qualitative criteria to quantify the risks.[6]

Risk practitioners should also be careful to ensure that the risk profiling process does not become stale or be seen as an end in and of itself. Much of the work is done in creating the risk profile and less work is required to maintain it. Typically the risk profile does not change significantly over the short term unless the business is rapidly changing or growing. Therefore, risk practitioners need to be mindful of this and look for opportunities to ensure the risk profile remains relevant to management decision-making over time.

A risk profile report should provide 'snapshot' management information about significant ('top 10') risks – an assessment of the inherent risk, effectiveness of controls, residual risk and the risk trend. The graphic below provides an example of how this information could be presented on 'one page'.




[6] Aust standard, COSO etc for examples

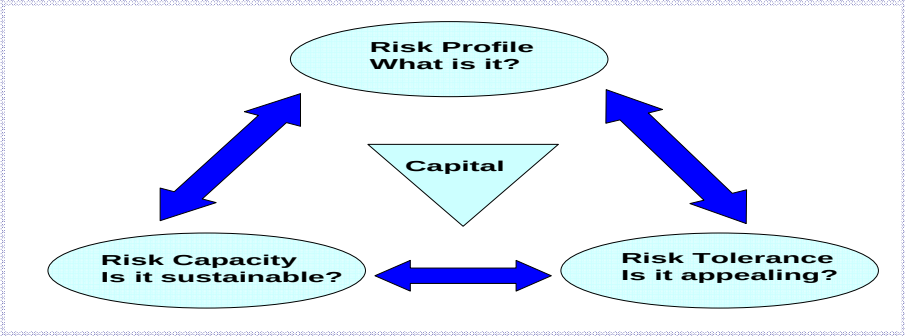
## *EXAMPLE: 'WHAT IS THE RISK PROFILING PROCESS?'*

*The risk profiling process is comprised of three main phases:*

***1. Preparation** - The objective of risk profiling is to provide the business with a structured approach to recording and assessing risk. This facilitates the common understanding and articulation of risk. Therefore, it is useful to prepare any existing material prior to the risk profiling exercise to assist the process of identifying and assessing risk and controls.*

***2. Risk Profiling Exercise** - The risk profiling exercise should be facilitated by a risk champion from the business to provide guidance and help drive consistency of the process. Business involvement is key to the successful completion of the risk profile as it effectively ensures an accurate capture of risks. There will need to be an initial investment of time to complete the risk profile and an ongoing commitment to maintain it. The amount of time required will vary dependent on the approach used to complete the risk profiling exercise (e.g. workshops vs. one-on-one meetings).*

***3. Review** - Following the risk profiling exercise, a review should be undertaken by the risk champion to ensure the outputs of the meeting have been recorded accurately and agreed by management.*




***Key benefits of this approach are:***

- *A structured process that promotes consistency for risk profiling across the organisation*
- *Collation of risk related material before the risk profile exercise provides participants with a good starting position for risk profiling*
- *Both risk expertise and business knowledge being used to risk profile*
- *Promoting transparency of risk profiling*
- *Time efficiency for risk profiling*
- *Clear linkage between risks and controls.*

***However watch out:***

- *Providing existing material may cause participants to focus on known issues, rather than future issues – always ensure they also consider potential risks*
- *Sometimes used as a 'once a year' approach which could discourage updating of the risk profile outside of the workshop – promote the risk profile as a living document and ensure it is relevant for the effective running of the business.*

## *6.3 Risk Modelling Techniques*

Apart from the process of risk profiling, a range of statistical and other modelling techniques are commonly used by insurers to quantify insurance risks. The table below lists a range of modelling and statistical techniques considered appropriate for the quantification of insurance risks. Refer to Appendix 8 – Useful References for more details on these techniques.

| Risk Category | Modelling Technique(s) |
|---|---|
| Enterprise /all risk categories | • Dynamic Financial Analysis |
| Underwriting (including reinsurance) | • Financial Condition Report (FCR) and/or underwriting modelling or reviews |
| Market | • Value at risk (VAR) or Tail VAR<br>• Interest rate models<br>• Scenario tests |
| Credit | • Credit risk models |
| Liquidity | • Asset/Liability modelling |
| Operational | • Internal loss data<br>• External loss data<br>• Scenario analysis, simulations |

***Comment: The 'black swan' dilemma – is ERM enough?***

*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 or something perceived as impossible actually occurring.*

*Black swan events have occurred throughout history. More recently the events of 9/11 and the sub prime meltdown in the USA spring to mind. While some may argue that people did and could have predicted these events people were still surprised when they occurred, particularly the magnitude of the impacts that reached far into the financial services sector.*

*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.*

*Some argue that developing an emerging risks register will prevent surprises. One topical example of an emerging risk is nanotechnology. However, apart from the fact that if we know about them they are not surprises, the question of cost benefit comes into play. To what extent is it worth spending money to prevent something that might happen, particularly if we are not sure of its exact manifestation?*

*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 impacting, especially surprises, however it is a lot better than not having any preventative framework at all.*

[1] Learning to Expect the Unexpected by Nassim Taleb, The New York Times, April 8, 2004

# 7. Economic and Supervisory Capital

***Key Feature 6***

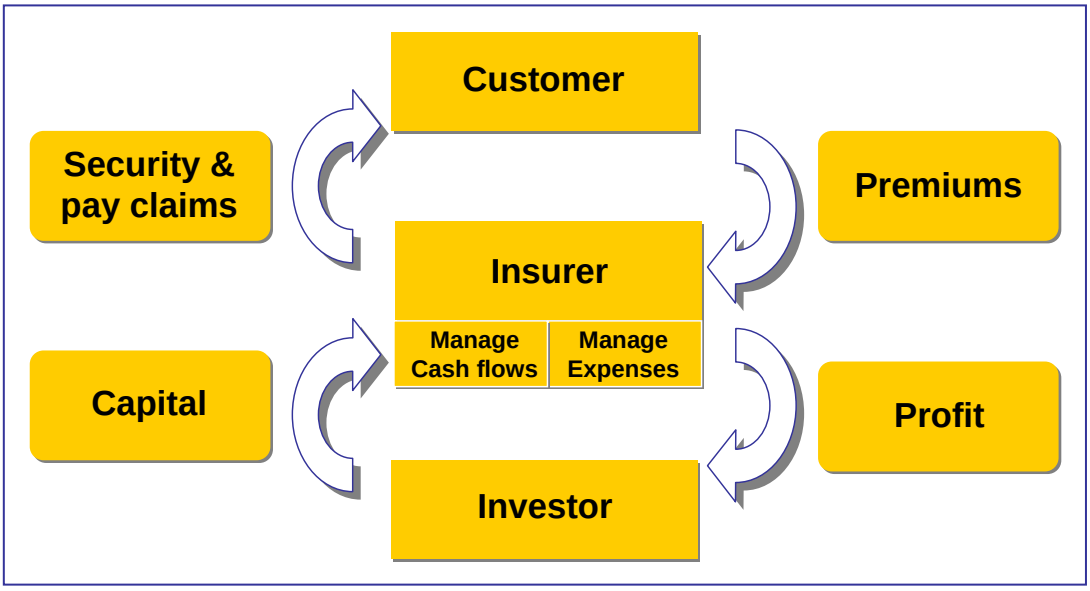
***As part of its ORSA an insurer should determine the overall financial resources it needs to manage its business given its own risk tolerance and business plans, and to demonstrate that supervisory requirements are met. The insurer's risk management actions should be based on consideration of its economic capital, supervisory capital requirements and financial resources.***

## *7.1 Introduction*

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. Based on this principle, enterprises will propose business ventures that require capital and indicate the return they will provide in this capital. The owners of capital will assess these proposals and provide their limited capital to the best available proposals, allowing for the potential risks of each proposal. Over time the track records of countries, industries and companies are established and the continued provision of capital and the return expected is refined.

In the Insurance context, the Insurer essentially needs to charge the 'correct' premium for the promises it makes to pay claims and to manage expenses and cash flows efficiently. In the running of this insurance business the insurer is exposed to many risks that may reduce the profit it can pay to the capital providers, and hence the management of these risks is an important part of running the insurance business. The dominant risks will vary by insurer according to such factors as their stage in life-cycle (e.g. start-up versus run-off), relative size and nature of business written.

Figure 1 below illustrates this relationship in the Insurance context.



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 a model can provide indications of what profit will emerge under many different assumptions and provide a guide to management of the insurer of how specific decisions may impact the expected level and volatility of future profit. The models can also provide indications of the risk of failure of the insurer. These models are often referred to as Economic Capital Models. They are used by capital providers, supervisors and companies.

The capital providers and supervisors will have more generic models that they apply to individual companies with some refining to attempt to allow for the individual company characteristics. The management of companies will generally have a model that is developed internally and therefore should be more accurate. This 'internal economic capital model' is usually able to provide more accurate assessments of the need for capital and provide better insights for input into key management decisions.

The 'best practice' internal economic capital models are able to break up the overall capital and return of the company into smaller parts for which individual decisions can be made. A key example of this is where different products sold within the company have different risk and profit profiles. By knowing which products are enhancing or diluting the company's overall profit relative to capital required enables corrective action to be taken so as to ultimately improve the company's overall return on capital.

***EXAMPLE: RATING STRENGTH***

*One of the roles of pricing is to ensure premiums are competitive and that an adequate return on capital is achieved.*

*For the insurer overall, the capital required will usually be determined using the insurers risk appetite, market or regulator expectations and their Economic Capital Model (ECM). The insurer will also set an overall planned return on this capital.*

*However, the insurer will be relying on the pricing function to deliver these overall results, usually based on many decisions at lower levels of detail for various risk classes. For the pricing function to fulfil this role effectively it will need a robust and accurate Economic Capital Model (ECM) that can allocate the capital requirements of the overall insurer down to the underlying risk classes for it to understand the return on capital performance of each risk class, and to adjust pricing, risk class features or business volumes in order to steer the outcome for the overall return on capital for the insurer.*

*For example, column (A) in the table below shows the pricing measure, for example insurance profit margin, that is required to achieve at a desired return on capital based on the capital allocated to that risk class using the ECM.* ***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.*** *Based on this example in the table below, the insurer could adopt actions, for example, that focus its limited resources on writing more volume of risk class X and consider increasing the pricing for risk class Y to improve the overall return on capital.*

| Risk Class | Pricing Measure to Achieve X% RoC | Actual Pricing Measure | Rating Strength | Actual Business Volumes |
|---|---|---|---|---|
| | (A) | (B) | (B / A) | |
| X | 10% | 11% | 1.10 | 100 |
| **Y** | **5%** | **4%** | **0.80** | **200** |
| Z | 7% | 7% | 1.00 | 70 |
| Total | | | 0.92 | 370 |

*Taking the example above to a lower level of detail, if the ECM can provide capital requirements at for Risk Class Y at a lower level of detail, i.e. Y1 and Y2, then more effective management decisions are likely to be made by understanding the source of the underperformance of risk class Y. For example the more focused action is likely to be made to correct the pricing or limiting volumes of risk class Y2.*

| Risk Class | Pricing Measure to Achieve X% RoC | Actual Pricing Measure | Rating Strength | Actual Business Volumes |
|---|---|---|---|---|
| | (A) | (B) | (B / A) | |
| X | 10% | 11% | 1.10 | 100 |
| **Y1** | **5%** | **6%** | **1.20** | **67** |
| **Y2** | **5%** | **3%** | **0.60** | **133** |
| Z | 7% | 7% | 1.00 | 70 |
| Total | | | 0.92 | 370 |

## *7.2 Economic Capital Model*

The purpose of an Economic Capital Model (ECM) is to provide a holistic assessment of the key risk drivers within an organisation and to devise risk management techniques to address these risks.

An ECM generally comprises integrated asset and liability models and simulates the out-turn of asset and liability cash flow experience over future periods. Typical output from an economic capital model comprises forecast future balance sheet, profit and loss accounts cash flow statements, and projected distributions of profit; capital and return on capital. This is based on running many iterations of the model. The distributions enable management to take a view on the probability of key indicators

falling outside an acceptable level (one possible definition of risk tolerance) and hence are a critical input to the determination of capital needs. Such models are sometimes also referred to as “internal models”, but that term can also apply to less holistic modelling of part of an insurer’s business performance and risks. Reference should also be made to the IAIS Guidance paper on the use of internal models for risk and capital management purposes by insurers (Oct 2007).

The asset model component of an ECM should be based on well researched financial market models. Inputs incorporate both economic and financial parameters and the model allows for correlations in returns from different asset classes and correlations in returns over time. For multinational insurers, an allowance for potential exchange rate fluctuations is advantageous.

The liability model examines the relationship between premiums and claims and their variability. Examples of causes of variability to be taken into account would include general economic conditions, future claims deterioration (or improvement), changes to market share and the effects of the underwriting cycle. Reinsurance and correlations between classes should also be considered.

A link between asset and liability models through some economic variables (inflation, interest rate etc.) has to be established. The uses and benefits of a dynamic model include:

- Improved understanding of the dynamics in the balance sheet arising out of the insurer’s current strategy
- Consideration of the effects of implementing different asset and liability (and reinsurance) strategies
- Examining relative impacts of different sources of capital (e.g. reinsurance; future profits; retained earnings; capital markets; reserves etc)
- Due diligence support for acquisition and divestment decisions
- Capital allocation by region and product
- Assessment of risk adjusted performance of different business units
- Determining the optimal asset mix
- Financial condition reporting
- Understanding the possible impact of extreme events on the financial position of the insurer.

It should be noted that the model is only a tool and is heavily reliant on the integrity of inputs. In addition, some subjectivity is unavoidable. It is often not the modelling results themselves which are of key benefit; rather it is the deeper understanding of the risks and drivers of the business that has resulted from going through the modelling process.

A dynamic model will need to consider and allow for the extent to which a company chooses to match (or mismatch) the cash flows from its assets and those required to meet its liabilities. The model will need to take into account any specified liquidity requirements of the insurer. An ECM will typically also include rules in relation to the investment and reinvestment policy of a company and rules specifying the switching and rebalancing of the investment portfolio to changing financial circumstances of the insurer.

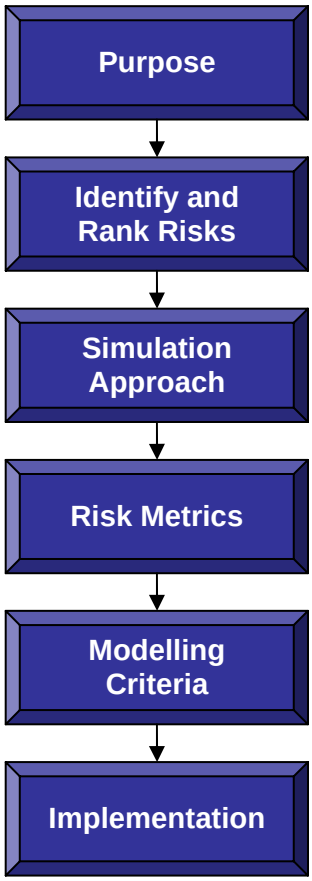
A dynamic model also enables management to systematically understand the factors driving volatility of earnings and provides a sound basis for the development of targeted risk management strategies to reduce earnings volatility.

A key decision that will affect the form and use of the ECM will be to what degree the ECM will be integrated into the day to day operations of the business. Various alternatives for this could include:

- Real time running of the ECM for changes (actual or potential) to the business
- Translation of the ECM output into “rules of thumb” that can be used by the businesses on a day to day basis
- Processes used to control centralisation of the ECM, which would usually involve many aspects of the business having their own detailed model which a centralised model could then incorporate to produce more summarised output at a group level that is nevertheless built on a consistent foundation throughout all the insurer’s activities.

### *7.3 Economic Capital Model Process*

The ECM process entails a number of steps. The flowchart below provides an elevated summary.




Each step of the ECM process is explained in the following sections.

a) Purpose

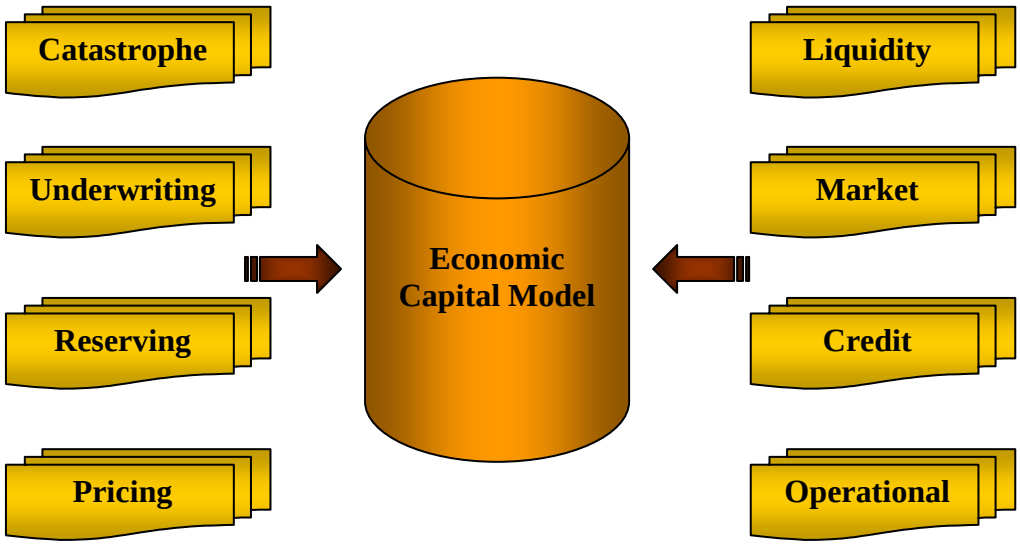
Will the ECM be used for supervisory capital requirements or the insurers own solvency assessment? An ECM for supervisory capital purposes must comply with the

IAIS solvency requirements for Internal Models[7]. This Practice Note supports the use of an ECM for an insurer's own solvency assessment and capital management purposes. It is important to clarify the purpose of the ECM as it will have a significant impact on:

- Who should be responsible for the ECM
- What level of controls and processes need to be incorporated around the ECM
- How flexible and dynamic does the ECM need to be
- What level of detail and accuracy is required from the ECM
- What level of resourcing is required?

b) Identify and Rank Risks

The risks that need to be assessed and ranked according to the particular requirements of each insurer are illustrated below. The dominant risks will vary by insurer.




The sophistication of the model will reflect the risk hierarchy i.e. key risks require more detailed modelling and analysis.

Any diversification recognised between risks (and within risks) is generally built into the model. This may, for example, be via correlation matrices, copulas or other approaches.

Given the scope of operational risk, there needs to be clearly defined guidelines to ensure consistency across the domestic and international insurance industry. An example here is the Basel II definition of operational risk for banks[8].

[7] IAIS Guidance paper on the use of internal models for risk and capital management purposes by insurers (Oct 2007)
[8] International Convergence of Capital Measurement and Capital Standards – A Revised Framework, Basel Committee on Banking Supervision, June 2004

*"Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputation risk."*

Basel II outlines three methods for calculating operational risk. These methods are outlined below in increasing degree of sophistication:

(i) Basic Indicator Approach

- Operational risk capital is a fixed percentage (15%) of positive annual gross income averaged over the previous three years.

(ii) Standardised Approach

- Operational risk capital is a fixed percentage (12%, 15% or 18%) of annual gross income measured for each of eight specified business lines. The positive total across all business lines is averaged over the previous three years.

(iii) Advanced Measurement Approaches

- Operational risk capital is calculated using an approved internal model.

The Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS) outlines in their last quantitative impact study (QIS3 spring 2007) a methodology to calculate the capital charge for operational risk. Operational risk is the minimum of two values:

- A fixed percentage (30%) of the Basic Standard Capital Requirement
- The maximum of a fixed percentage (2% for Non Life and 3% for Life) of total earned premium and a fixed percentage (2% for Non Life and 0.3% for Life) of insurance technical provisions.

The choice of method is a function of the corporate structure (mono-line insurer, multi-line insurer, conglomerate of insurance and non insurance), the maturity of capital modelling within an organisation, resources and cost.

The challenge for the international insurance industry is the establishment of processes to separately record operational losses. There is limited historical data on operational risk which currently limits the sophistication and reliable application of stochastic modelling of this risk.

c) Simulation Approach

There are several techniques to quantify risk which could be used by an insurer to construct its model. In broad terms, these could range from basic deterministic scenarios to complex stochastic models. Deterministic scenarios would typically involve the use of stress and scenario testing reflecting an event with a set probability to model the effect of certain events (such as a drop in equity prices) on the insurer's capital position, in which the underlying assumptions would be fixed. In contrast, stochastic modelling (such as Monte Carlo simulation) often involves multiple scenarios with varying likelihoods, in order to reflect the likely distributions of the capital required by the insurer.

The choice is a function of cost, time and benefit.

Deterministic testing highlights key risks and provides a reasonable check on more sophisticated simulation methods. It is particularly important to understand the interaction between risks and to understand how this interaction changes under stressed scenarios (e.g. previously unrelated impacts may become related under severe stress). A key input into the ECM is often qualitative and subjective decisions that would be considered by the insurer's management at the time of distress (for example changing asset mix or reinsurance levels).

d) Risk Metrics

Traditional risk metrics associated with an ECM includes:

- VaR versus TailVaR
- Time horizon
- Confidence level.

These are a function of the insurer's strategy and risk tolerance.

e) Modelling Criteria

Some examples of modelling criteria include:

- Exit value as measured by absolute ruin
- Ongoing business criteria as measured by supervisory intervention
- Attaining a certain investment rating.

An insurer should seek to apply multiple criteria for each segment of its business.

f) Implementation

Two main approaches can be taken to the development of the ECM:

- A fully integrated model that considers the interactions of the entire operation or
- A univariate model that considers each division individually and then integrates all components using some combination method (e.g. copulas).

A fully integrated model can readily be applied to mono-line insurers while a univariate model lends itself to multi-line organisations that are involved in insurance and non-insurance business.

The type of model used should be appropriate to the nature, scale and complexity of the insurer's business.

## *7.4 Relationship with Capital Management*

Supervisory capital requirements are just one input into capital requirements. As discussed there can be a multitude of others including:

- Desired rating agency ratings
- Desired earnings volatility
- Desired shareholder return – dividend and capital growth
- Accumulation of risks
- Market expectations.

An ECM will generally present a more accurate and/or complete picture of a business than the application of a supervisory capital prescribed methodology.

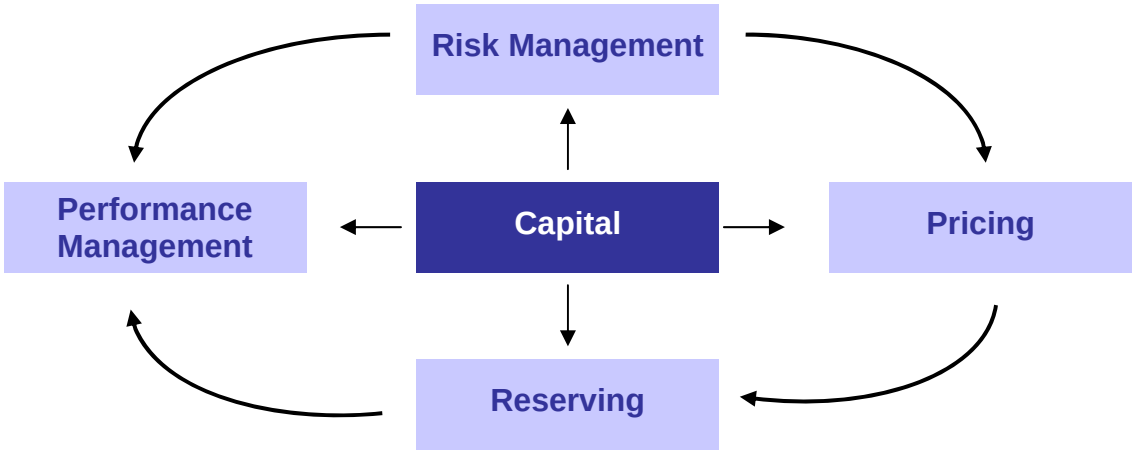
Key potential differences between a supervisory prescribed method and an ECM would often include:

- Different views as to the volatility of various classes of business (both absolute and relative to other classes)
- 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)
- Inclusion of different risk types (e.g. operational risk may not be included or may be implicitly included in supervisory prescribed methods, but may be included explicitly in the ECM)
- Different views may be expressed regarding the availability of various assets for capital (e.g. tax benefits; goodwill; etc).

Even an ECM will likely need to calculate and project supervisory prescribed method capital as the relevant supervisor will want to understand the relativities.

Effective capital management is focussed on turning risk into shareholder value. In operational terms this means ensuring that the “right” amount of capital is ascribed to the appropriate risks so that suitably informed decisions can be made.

The following schematic seeks to articulate the relationship between capital and the core elements of capital management.




*Capital* plays a central role in the cycle of turning risk into value. It finances growth, capital expenditure and business plans. It also provides support in the face of adverse outcomes from insurance activities, investment performance and support activities.

From a market perspective, one of the roles of *pricing* is to ensure premiums are competitive and that an adequate return on capital is achieved. Operationally, the objectives of the pricing process are to meet expected claims and operational / administration expenses. Of course, pricing includes other aspects, including consideration of the need to cover fixed costs as well as meeting supervisory requirements where appropriate.

The *reserving* process establishes a central estimate for outstanding claims, provides a margin to cover the value of uncertainty (the risk margin) and ensures that insurance liabilities are adequate having regard to experience and expectations about future experience and cover against any expected premium rate deficiency.

The allocation of capital to business units / lines commensurate with risk underpins the *performance management* process and enables measurement of outcomes and returns against those expected. Effective performance management incorporates early warning mechanisms so that the risk management, reserving and pricing processes can be adapted to improve outcomes.

From a capital management perspective, the role of *risk management* is threefold – establishment of the overall risk 'tolerance', identification / assessment of risks, and keeping risks "in control". The process of establishing risk tolerance relies on systematically deciding which risks to take and which risks to shed. As discussed previously, the articulation of risk tolerance can ultimately be expressed in terms of target financial strength (an acceptable "risk of ruin") but can also encompass strategic components e.g. target credit rating and acceptable earnings volatility.

# 8. 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.***

## *8.1 Introduction*

A key benefit of the use of an ECM is the ability to examine scenarios outside of those prescribed by regulation. For example, supervisory capital requirements are often performed on a run-off basis, rather than on an ongoing basis. Likewise, an ECM allows an insurer to look further into the future than most supervisory 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.

The modelling approach and the assumptions, fundamentally depend on the time horizon over which risks are modelled. For a one year time horizon actions of an insurer's management can be neglected. However, for modelling over the longer term, the actions of the insurer become more important.

For longer time-horizon models, assumptions based on a static business and asset mix in the absence of actions of the insurer would make the calculations and projections less effective. However when long-horizon models consider assumptions such as the insurer's strategy and management actions, since these are rather subjective, the results of the model need more interpretation and the limitations of the modelling need to be clearly articulated.

Long-term modelling can necessitate the development of separate models from those used for shorter time horizons. For example, in order to model financial market risk over a longer time horizon requires models that project the relevant risk factors consistently. This requires the use of more explanatory models rather than models that rely to a large degree on purely historical data.

A key part of models that project over longer than one year time horizons is the modelling of management actions and strategies. This encompasses:

- Premium setting: what is the strategy of the firm in case of losses or inadequate profits emerging? Does the firm try to retain or gain market share when prices are low? What is the strategy of the firm during an insurance cycle?
- Asset allocation: How does the firm react in cases of financial stress?
- Discretionary policyholder benefits: What is the insurer's strategy for discretionary policyholder benefits in particular in cases (a) where the firm alone experiences financial distress and (b) where the whole market experiences financial distress
- Dividend policy: What is the dividend strategy, in particular in cases where the firm experiences losses
- Risk mitigation strategy: Reinsurance strategy, ALM strategy, securitizations and other transfers of risk to the market etc.

## *8.2 Quantitative Analysis - Capital Planning*

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

- *Economic capital requirements*
  The ECM is the primary vehicle to calculate the capital requirements based on the risk profile of an organisation. The output of which should be closely integrated into the capital management process of the insurance company.

  However the model can also be utilised to link capital more closely to the way in which the business is managed. It can be used to help clarify or define the risk appetite of the organisation. This could consider for example, the calculation of the risk of ruin, the risk of "regulatory ruin" or as a measure of earnings volatility.

- *Disaster Planning*
  The ECM can also be used to analyse the eventuality of financial distress. This should include a detailed analysis of the legal and supervisory requirements of the jurisdictions in which the firm operates. Included in the analysis should be the potential limitations in capital fundability. The output of this exercise can then be used to alter the capital management strategy, implementing, where appropriate, instruments that mitigate potential capital mobility problems, e.g. via contingent capital solutions.

- *Investment strategy*
  An organisation's approach to their investment strategy considers a number of elements such as risk tolerance and the objectives of the insurer. The future capital need of the organisation also plays a part in this equation. The investment strategy will vary according to the future need for capital in the business.

- *Mergers, acquisitions and divestments*
  ECM can be used to assist the business understand the impact of any mergers, acquisitions and divestments. That is, it can be used to model the effect of diversification of risk on capital requirements and by quantifying the actual dollar amount of additional capital required (or released) due to merger /

divestment activity. Economic Capital can also be used as a mechanism to assist in the valuation of acquired (or divested) entities.

- *Capital allocation*
  Capital allocation is one of the primary methods used to measure the performance of Business units. There is not ‘one way’ of allocating capital to businesses, but the approach should be risk based and provide incentives for the business to effectively manage their risk (demand for capital) and measures to ensure they earn a suitable return on deployed capital.

  The approach taken to capital allocation will depend on the organisation’s aim, for example, if it is to build an "optimal portfolio" (in terms of the spread of risk) the risk measures may be derived more from the extremes of the distributions of outcomes by class rather than the middle of the distribution that simple growth targets may suggest. Issues that need to be overcome in the allocation of capital include the treatment of support (i.e. non revenue generating business units) and the approach used; top-down allocation or bottom-up calculation (or a combination of both).

- *Reinsurance programmes*
  An ECM can be used to assess the capital required based on the risk profile of the organisation. The more risk that is on an organisation’s books the more capital is required to be set aside. Reinsurance is one of the main mechanisms available to insurers to ‘pass on’ some of this risk to another party, therefore decreasing the amount of capital they are required to hold. Therefore in this instance, the value of reinsurance is derived from it acting as a proxy for capital. The cost of holding capital versus the cost of reinsurance can be considered by an organisation, allowing a more information decision to be made.

- *Optimal business mix*
  Setting the optimal business mix is related to the effective allocation of capital to the business. If capital is allocated on the basis of the underlying riskiness of the business, then the risk adjusted performance can be measured. The risk adjusted performance management can then be used to optimise the product or business mix and assist management to make decisions in line with the organisation’s strategy. Although capital will not be the only factor considered it provides a good measure for assessing relative performance.

- *Reserving volatility*
  In this case, the model acts to effectively treat the risk margins in the claim and premium reserves as "policyholders' capital" (as opposed to the "shareholders' capital" designated by the difference between assets and liabilities in the balance sheet).

- *Capital outflow / inflow policies*
  This is could be considered a subset of Economic Capital Modelling, but is important to treat it separately as it considers risk tolerance in a specific way. (i.e. examining the capital adequacy "range" for the entity).

The Solvency II Cost of Capital risk margin (with its origins in the Swiss Solvency Test) actually requires the projection of the capital needs for the existing business. This requires organisations to also assess the long term impact of their business. As a minimum risk management must be able to at least quantify the capital requirements of insurance business over the whole life time of the liabilities.

The OSFI (Canadian regulator) already requires longer term projections via their DCAT (Dynamic Capital Adequacy Testing) requirement (10 year projections of plausible adverse scenarios). (See also 'The use of internal models for determining liabilities and capital requirements' by Allan Brender, April 2002, North American Actuarial Journal).

Some supervisors require a more formal assessment of the financial viability of an insurer, often called a Financial Condition Report (or FCR). The FCR usually covers the broad spectrum of risks that are faced by an insurer, and is most useful when it provides a holistic view of the insurer for the Board and supervisor. An FCR usually covers not only the explicit numerical financial condition of the insurer (including financial statements and the outcomes of the ECM mentioned above) but it also usually covers the range of harder-to-quantify risks faced by an insurer, for example operational risks and reputation and brand related risks. The FCR usually includes an assessment of the effectiveness of the risk management framework of an insurer.

## *8.3 Qualitative Analysis - Business Continuity Planning*

Business continuity management is an essential part of operational risk management. Business continuity planning enables a business to anticipate, identify and assess business interruption risks. A properly documented and tested Business Continuity Plan (BCP) reduces the impact of interruptions on key business processes and, most importantly, protects reputation. A robust BCP also allows a business to explain to stakeholders and industry supervisors that risks associated with potential business interruptions can be managed.

## *8.4 Crisis Management and Contingency Planning*

A Crisis Management Plan minimises business impact and loss in the event of a significant incident by providing a clear and organised response strategy supported by predefined response procedures. It outlines the basic actions to be performed by, say, a Crisis Management Group (CMG) during an incident to assess its nature and severity, decide if the incident requires crisis level response and initiate the appropriate actions by management and employees.

One way of treating consequences is to undertake planning and preparedness for contingencies so that an insurer can act quickly to take advantage of unexpected gains or stem losses and prevent or limit disruption. This requires plans to be well founded in good risk management principles, tested and up-to-date. When an event occurs, the organisation’s management may need to respond quickly to mitigate the impact of the event on the achievement of business objectives such as revenue stream, product quality, corporate reputation or customer satisfaction. In most circumstances, these impacts may be managed as part of normal management processes. However, when the scale of the event overwhelms management’s normal capacity to cope, a systematic approach to critical incident management is needed.

At the core of critical incident management is Business Continuity Management (BCM), which provides an organisation with a disciplined capability to continue to operate sustainably in the face of potential significant business disruption. Appropriately implemented, BCM can provide a robust framework for addressing disruption risk exposures in a cost effective and timely manner. It provides a key component for the organisation to sustain good corporate governance, maintain its customer base and market share, retain the confidence of its stakeholders, and manage its reputation in

the face of an increasingly turbulent economic, industrial and security environment. As a minimum response, effective BCM will prevent an emerging crisis from becoming more persistent or widespread.

***EXAMPLE: UNDER WATER AGAIN!***

> "QUEENSLAND is facing a damage bill of hundreds of millions of dollars as flood waters surge through the state, cutting roads, swamping coal mines, destroying agricultural stock and forcing people from their homes. The state's booming mining industry expects tens of millions of dollars in coal production to be lost from the Bowen Basin. The flooding has caused massive stock losses for some farmers, while irrigation infrastructure and crops have also been destroyed."
> (news.com.au 22 January 2008)

*Climate change is a major challenge for the insurance sector and the increasing incidence of extreme weather events is a likely manifestation of the changing global environment. In the Australian context, extreme weather events account for the bulk of major property damage and are therefore the key focus for property and casualty insurers. The floods in Queensland were just one of the most recent weather related disasters that the Australian insurance industry has had to respond to, one compounded by the number of remote locations involved.*

*From a business continuity perspective, what is the appropriate response of an insurer with a focus on customer service and what should their response be if their own buildings or data centres are affected?*

*In 2008 one 'resilient' insurer had, in line with regulatory requirements, a proven and tested recovery strategy, well-rehearsed continuity plans, clear crisis management procedures and a culture of awareness of the need to ensure that critical services continue to operate. Moreover, with a geographically spread customer base, this insurer had implemented a resilient service model with processing of claims as a number one priority for business function recovery. This operational model ensured that processing was not dependent on any single building, location or data centre. While parts of its infrastructure may be damaged, other parts can take on the workloads in the short term and the impacted areas are quickly brought back on line in alternate facilities.*

*An important initial response to customer needs used by this insurer was to send mobile assessors into a disaster area. Those assessors were equipped with the necessary technology and authority to accept and process claims, make payouts on claims, approve emergency accommodation and respond to other particular requests for assistance that are within the scope of its policy commitments. The insurer has surplus mobile telephony infrastructure on stand-by for prompt deployment to all personnel so that they are always connected. This insurer also worked in close cooperation with disaster relief and emergency services personnel to ensure that access of its personnel into the affected area was conducted in a responsible manner and did not place people at risk.*

*Although very rare, large-scale catastrophic events can throw significant challenges at the insurance community and may overwhelm individual insurers. In these circumstances, responsible insurers will work with the national industry umbrella organisation under catastrophe coordination arrangements that have been prepared and rehearsed. By establishing working parties composed of state and federal government agencies, insurance industry organisations, insurance ombudsman services and associations of brokers and loss adjusters, a broad combined response will be mobilised to meet these challenges.*

*Responding to disasters affecting customers is a benchmark challenge for property and casualty insurers. Maintenance of a culture of resilient operations and effective plans for recovery of any damaged infrastructure is essential for an insurer, not only to comply with government regulations, but also to maintain their obligations to policy holders and their reputation in the wider community.*

# 9. 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.***

## *9.1 Introduction*

This Section seeks to provide assistance to insurers in developing constructive, transparent and proactive relationships with supervisors.

## *9.2 The role of the Supervisor*

Prudential supervision[9] is accepted worldwide as an integral component of the regulation of financial institutions. The fundamental premise underpinning the supervisory role is that the primary responsibility for financial soundness and prudent risk management within a supervised institution rests with the Board and senior management. In this context the primary emphasis of supervision is on avoidance of problems rather than penalizing those who may be found to have caused problems.

In relation to insurance, prudential supervision involves establishing a system of:

- Financial oversight
- Mandatory licensing
- Ongoing operational requirements e.g. prudential standards
- Procedures and processes for monitoring compliance with licence conditions and ongoing operational requirements
- Where necessary, undertaking enforcement action either to force a non-compliant insurer into compliance or remove it from the industry.

Supervisors adopt a risk-based approach to supervision. In practice this means that institutions facing greater risks receive closer supervisory attention. Therefore, in order to effectively manage the supervisory process, supervisors must form their own view of risks, and the effectiveness of the management of risks, for each supervised institution.

It is also worth noting that supervisors find themselves in the unique position in a given market of seeing the broad totality of risk management practices in operation across the supervised sector. They are exposed to the full spectrum of 'worst' to 'best' practices. Insurers seeking to improve their risk management practices should

[9] A term used to describe the supervision/regulation of financial institutions such as banks, insurers, building societies, friendly societies where the supervising authority seeks to ensure that the protection of depositors/policyholders is maintained by the institution in question being financially sound.

therefore not lose sight of the opportunity to engage with supervisors with a view to improving the management of risks.

## *9.3 Risk-based Supervision*

The supervisor's understanding of an insurer typically begins with consideration of the nature of the insurer's business, governance arrangements, strategic/business plans, financial condition reports and strategies and processes to manage risk. Licensing and ongoing supervisory activities typically involve review of documents relating to these areas.

Insurers should proactively engage with supervisors to help them understand, and test, these key aspects of the business. If a supervisor does not have a level of comfort about the strategic and higher level aspects of an insurer's risk management framework, they are more likely to adopt a more intensive supervisory approach than would otherwise be the case. Insurers should therefore seek to promote ongoing and transparent dialogue with supervisors about strategy and framework matters. This will foster a more open and productive relationship over the medium to longer term.

## *9.4 Supervisor Relationship Management*

*Relationship Management Principles*

Insurers should consider adopting a set of high-level principles to guide engagement with supervisors. In developing a set of appropriate principles, insurers should have regard to:

- Alignment with supervisory objectives
- Preservation and enhancement of corporate reputation
- Proactive and early engagement
- Communication transparency
- Relationship management accountability and coordination.

*Strategic Approach*

The supervisor is one of the key stakeholders for any insurer and therefore insurers should have a comprehensive understanding of supervisory objectives and processes. A strategic approach to supervisory relationship management involves, amongst other things, maintaining a profile on key supervisors. This includes key contacts at the supervisor and within the insurer, forward supervisory priorities and objectives, pressure points, specific risk areas for focus, relationship analysis, relationship development plans and opportunities for engagement.

*Nature of interaction with supervisors*

Insurers will typically have a range and variety of interactions and communications with the Supervisors which regulate the various jurisdictions in which they operate. These can be broadly classified as follows:

- Operational / Procedural
    - Submitting standardised, periodic returns and statistics

    - Responding to routine queries relating to standard operations (e.g. claims performance benchmarks).

- Non-standard / Unusual
    - Responding to a supervisor in relation to matters arising from a customer complaint
    - Responding to supervisor about industry issues and company exposure to them e.g. surveys about exposure to Hurricanes/Cyclones/Typhoons
    - Communications from supervisors initiating investigation and/or enforcement action
    - Results from supervision visits reported by supervisors to senior management
    - Reporting material incidents and breaches to a supervisor
    - Seeking relief/ exemption from current/proposed legislation
    - Advice of fines or 'please explain' requests
    - Developing strategy, tactics in response to industry or entity-level enforcement actions
    - Responding to non-standard communications (e.g. enforceable undertaking)
    - Any non-routine enquiry which has the capacity to result in the insurer being subject to disciplinary action or adverse consequences.

- Strategic
    - Submission on current/proposed legislation/policy
    - Encouraging a change in a supervisor's policy position
    - Public statements (e.g. to media and or government) relating to an insurer's views and policy position
    - Consulting with supervisors in relation to strategic initiatives (e.g. acquisitions, corporate transactions).

In the context of this wide variety of interaction many insurers (and most large insurance groups) develop accountability mechanisms and protocols to ensure the 'right people' are engaging supervisors appropriately. For example, supervisor engagement with respect to proposed acquisitions should involve the most senior management of the insurer.

A common approach is for insurers to allocate overall accountability for the supervisory relationship to a single executive, typically the Chief Risk Officer or Chief Financial Officer. In this way supervisory engagement can be effectively planned and coordinated. Under this approach, all 'non-standard' and 'strategic' engagement is transparent to the ultimate relationship manager.

*Supervisory Policy Development*

It is critical for insurers to engage with supervisors in the area of policy development. This is because insurers are in the best position to assess the practical implications of proposed supervisory change. Supervisors look for constructive feedback on their proposals and look to insurers to test the robustness and proportionality of new proposals.

Supervisors typically set time frames for submissions on new proposals. Insurers should adopt a strategic and proactive stance with respect to responding to submissions. A submission process that involves only written correspondence delivered on the final due date is likely to result in poor outcomes. Rather, insurers

should use the policy development process as an opportunity to meet with supervisors to explore implications of proposal and to understand the rationale for change.

In today's environment supervisors are moving in a direction of 'principles-based supervision'. Therefore, insurers should avoid arguments about being 'unique' unless there are compelling reasons for doing so. Instead, insurers should make use of industry bodies to coordinate submissions on proposed new policy.

*Supervisory Visits*

Supervisory visits provide the supervisor with an opportunity to 'deep dive' into particular aspects of an insurer's operations and/or risk management processes. Insurers should work with supervisors in the first instance to assist them with shaping the overall supervisory plan, typically spanning a 1-year time horizon.

Having agreed the overall plan, insurers should seek to work with supervisors to coordinate site visits - agenda development, document submission and overall visit logistics. This process provides an excellent opportunity to strengthen the relationship at an operational level.

Requirements and recommendations arising from supervisory visits should be welcomed, and taken seriously. To the extent that insurers seek to unreasonably challenge supervisory requests and requirements, this may be viewed by the supervisor as in indicator of underlying cultural issues and potentially have the effect of resulting in even more intensive supervision. Insurers should therefore look for every opportunity to promote openness and free exchange of views during site visits.

*Reporting of Incidents and/or Breaches*

One of the key tests of an effective supervisory relationship is how the insurer deals with the management and reporting of breaches of requirements. In the vast bulk of cases, breaches are inadvertent human and/or process errors as opposed to blatant disregard of rules.

Supervisors typically establish requirements for the mandatory reporting of breaches. These establish materiality thresholds to ensure that only significant matters reach the attention of supervisors. Insurers should therefore seek to 'operationalise' supervisory breach reporting requirements by translating these into processes that result in internal reporting and escalation of material matters and clear accountabilities for reporting to supervisors.

The identification, management and reporting of breaches should be viewed as a process improvement opportunity. No one expects zero breaches. Ironically, an absence of breach reporting to supervisors for an extended period could be viewed as an indicator of ineffective risk management and/or cultural activities.

*International Considerations*

Insurers operating in multiple jurisdictions have the added complexity of managing multiple supervisor relationships. In these situations the principles outlined above equally apply. There is even a greater need to establish clear accountabilities for relationship management at the country/local level and at the corporate/group level. Insurers should assume that supervisors themselves will establish protocols for the sharing of appropriate information cross-border and therefore establish agreed and

transparent processes that recognize this dynamic in the context of international insurance groups.

*Governance Aspects - Transparency of Supervisory Engagement*

Boards have a key role to play in setting the tone for engagement with supervisors. They should monitor important engagement between the insurer and the supervisor. In particular, strategic and non-standard engagement should be transparent to the board or appropriately delegated committee. For example, summary details of strategic and non-standard engagement should be reported on a periodic basis to the board or relevant board committee. This will enable the board to ensure that its expectations with respect to supervisor relationship management are being met on an ongoing basis.

**TIPS: HOW TO ENGAGE WITH SUPERVISORS LOCALLY AND GLOBALLY**

KPMG: *Bringing regulation into the boardroom – A global survey of the supervisory function in the communications sector* (December 2007) noted that "With an increasing focus on regulation, companies must be able to both shape and respond to the supervisory agenda in traditional and, increasingly, emerging markets".

With the increasing demands of regulation and supervisors throughout the world, insurers should incorporate regulation as part of every day operations. Regulation should be part of the "DNA" of the business. The question however is, "how can this be done"? How can we "engage" with supervisors?

Tips:

1) Embracing and understanding the principles of the overall supervisory framework and its mandates / standards throughout all levels of the organisation with the Board / governance committees driving the implementation of the compliance strategy. This should involve linking the supervisory strategy with the overall corporate strategy.

2) Implementation of a transparent and comprehensive supervisory strategy which is communicated to the supervisory bodies and throughout the organisation. The supervisor should be able to evidence the extent of the success of the organisation in achieving its supervisory strategy and the organisation must be able to demonstrate how their supervisory strategy leads to compliance with the standards mandated by the supervisors.

3) Be practical in your feedback on proposed supervisory changes presented by the supervisors e.g. incorporating examples, financial and market impacts, to support the organisations' view and present an unbiased argument at all times, focussing primarily on the critical issues. Never feel the pressure to comment on every aspect of the supervisor's discussion paper.

4) Adopt best practice before it is mandated. The Board / governing committees and senior management should adopt a "forward thinking approach" to ensure compliance with regulations.

5) Be proactive, anticipating supervisory changes and working with industry bodies to influence the supervisors to create the most favourable environment to the business / industry. This will include demonstrating a willingness to participate in supervisory consultations and surveys.

6) Engage in open and regular communication with the supervisors. Establishing a good working relationship with the supervisors' supervisory contacts will therefore be important. This is relevant for all types of communication, and not just relating to matters concerning risk management.

7) Be proactive in the provision of relevant information which will allow the supervisor to discharge its responsibilities. This should encompass: keeping supervisors updated with the progress and results of certain risk management qualification and quantification exercises (and not just providing the results of these when they are due) – i.e. being open in relation to potential issues and how the firm intends to rectify matters. However, it will be important to establish expectations initially since supervisors will not want to be overwhelmed with large volumes of information, not all of which may be relevant to them.

8) Manage the perception of the supervisors internally within the firm. Where the relationship with the supervisor is seen to be confrontational and negative, engagement tends to be on defensive terms, seeking to justify actions as opposed to engaging in open communication by treating the supervisor as a partner and significant stakeholder of the business.

9) Liaise with the supervisor on where they see the next challenges emerging and working with them to minimise the anticipated impacts on the industry.

In summary, an insurer's ERM framework will not be complete if it does not incorporate as a key component the effective management of the relationship with the supervisor. Insurers are therefore encouraged to focus on this aspect as part of the ongoing development of the overall ERM framework.

# Appendix 1
# Published Definitions for Enterprise Risk Management

*"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

COSO: Enterprise Risk Management – Integrated Framework Executive Summary (September 2004)

*ERM is the discipline by which an organisation in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organisation's short- and long-term value to its stakeholders."*

CAS ERM Research Committee: Overview of Enterprise Risk Management (2002)

*"Enterprise Risk Management, as described here, is a holistic management process applicable in all kinds of organisations at all levels and to individuals. ERM differs from a more restricted 'risk management' used in some sectors. For example, in some areas the terms 'risk management' or 'risk control' are used to describe ways of dealing with identified risks, for which we use the term 'risk treatment'. Some other terms used in this document also have different usages. For example the terms 'risk analysis', 'risk assessment' and 'risk evaluation' are variously used in risk management literature. They often have overlapping and sometimes interchangeable definitions, and they sometimes include the risk identification step."*

Guideline to the Australian Standard AS/NZS 4360 (2004)

*"ERM is a structured and disciplined approach aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing the uncertainties the enterprise faces as it creates value."*

KPMG: Enterprise Risk Management - An emerging model for building shareholder value (November 2001)

*ERM is the process of planning, organising, leading, and controlling the activities of an organisation to minimise the effects of risk on an organisation's capital and earnings.*

KPMG: Viewpoint for Consumer Markets (August 2005)

*ERM is defined as a process, effected by an entity's board of directors, management, and other personnel; applied in a strategy setting and across the enterprise; designed to identify potential events that may affect the entity; and manage risk to be within its risk appetite to provide reasonable assurance regarding the achievement of entity's objectives.*

The Institute of Internal Auditors: What is ERM and what role in it does internal auditing play? (September 2004)

# Appendix 2
# Stages of Enterprise Risk Management Maturity

| Framework Sophistication | Definitions used in this Attachment |
|---|---|
| **Early** | Risk management and internal control activities exist in part, are inconsistently applied and not well understood by management and the relevant employees in limited business areas. Significant opportunities for enhancement remain. |
| **Intermediate** | Risk management and internal control activities are established, yet not consistently applied or fully understood by management and relevant employees in key functions/business areas. Moderate opportunities for enhancement remain. |
| **Advanced** | Risk management and internal control activities are established, consistently applied and well understood by management and relevant employees across the organisation. Opportunities for enhancement remain to align and coordinate activity across the organisation. |

| | **Early** | **Intermediate** | **Advanced** |
|---|---|---|---|
| **Role of the Board** | Board not closely involved in risk management. | Board responsibility for creating the environment and the structures for risk management. | Dedicated board risk management sub-committees, and roles and responsibilities of these committees are publicly available. |
| | Statement of risk management responsibility. | Board approves the Risk Management Policy. | Board reviews Policy and sets best practice objective. |
| | No defined risk tolerances. | Board sets the Risk Tolerances. | Any proposed variation to the organisation risk tolerance requires the prior approval of the Board. |

| | Early | Intermediate | Advanced |
|---|---|---|---|
| | | | The Board or relevant committees ensures that the risk management framework is appropriately resourced consummate with the risk profile of the organisation. |
| | | | The Board and Committee sets the appropriate 'tone from the top' with regards to the importance of risk management in the organisation. |
| **Risk Appetite** | Risk tolerances are implied in corporate plan but not explicitly applied. | Both risk tolerance and risk limits set boundaries for how much risk the organisation is prepared to accept. | Risk tolerance is determined having regard to organisation's strategy and long term (i.e., over 3 years) Strategic Plan. |
| | Risk appetite is not tangible, but is understood by the Board and Senior Management for the decision-making process. | Risk appetite is set by the Board and articulated sufficiently to the majority of the organisation. However, not completely embedded within strategic and operational decision-making process. | Risk appetite is set by the Board, articulated sufficiently to the majority of the organisation. It is effectively communicated to internal stakeholders and assists the strategic and operational decision-making process. |
| | | | Strategic decisions are independently reviewed against the risk appetite. Areas of weakness are remediated. |
| **Risk Management Policy** | Formal policies occasionally set out internal controls responsibilities. | Risk Management Policy outlines the requirements for the management of risk.<br>Policies are supported by protocols, standards and guidelines. | Risk Management Policy covers all major elements of an ERM program. |
| | Internal controls not linked formally to other corporate governance (e.g. strategy) | Risk Management Policy directly supports the organisation's purpose, and identifies roles and responsibilities for risk management. | Clear alignment between strategic objectives and risk management.<br>Complementary activities on improving the external environment.<br>New acquisitions are integrated into the Risk Management Policy |
| | Compliance with local laws and supervisory requirements. | Risk management relates to compliance and operational risks. | Risk management linked to business objectives. |

| | Early | Intermediate | Advanced |
|---|---|---|---|
| | Policies are developed ad hoc. | Risk Management Policy reviewed regularly by the Enterprise-wide Risk Function. | Policy framework exists and is reviewed every 12 months. |
| **Management Accountabilities** | Statement of responsibility for internal control is prepared but not owned by CEO or executive team. | Executive management implements the Risk Management Policy. | Management committees oversee Risk Management Policy. |
| | Do not see business value of compliance activities. | Risk management is integral part of doing business. | The risk management programme outcomes are measurable and value creating. |
| | A senior person (e.g. internal auditor) is responsible for risk management. | Business Units have appropriate structures and processes to meet the requirements contained in the Risk Management Policy. | The Business Unit Risk Functions have a dual matrix reporting line to the management of the Business Unit and Enterprise-wide Risk Function. |
| | Informal procedures exist for managing risk. | Each Business Unit has a Risk Function that develops tailored Risk & Compliance plans. | Risk functions undertake control self assessments and develop action plans |
| **Management Commitment & Leadership** | Risk management seen as responsibility of specialist area (e.g. internal audit). | Managers at all levels are responsible for using the Risk Management Policy in their normal processes and procedures. | Managers see risk management as source of competitive advantage and reflected in employees. |
| | Internal controls responsibilities not generally included in job descriptions and performance appraisals. | Identification and management of risk is the responsibility of all employees.<br>Roles are formally defined for each employee. | Support and promote the proactive risk management behaviours<br>Encouraging others to report any issues or incidents. |
| **Enterprise Risk Function** | Internal controls are delegated to Internal Audit. | A CRO position has responsibility for the Risk Management Policy. | The Enterprise-wide Risk Function develops and maintains the Risk Management Policy. |
| | Resources provided to specialist risk area. | Executive management is responsible for establishing Business Unit Risk Functions sufficiently resourced and supporting their activities. | Efficiency and effectiveness of risk resourcing is periodically reviewed. |
| **Risk 'Language'** | No common usage of risk terms. | Shared understanding of risk language. | Use of consistent risk management terminology/lexicon, internationally accepted risk categories, ratings, and reporting. |

| | Early | Intermediate | Advanced |
|---|---|---|---|
| | Definitions provided do not materially assist the identification and management of risks. Some risks that have been identified and managed are not material risks, but causes or consequences. | Definitions provided allow for sufficient identification and management of material risks. A significant amount of risks have been incorrectly classified. | Definitions clear, concise and allow for all risks to be identified and categorised correctly, enabling the efficient management of these risks. |
| **Risk Management Culture** | Corporate plan refers to values. | The organisation aims to ensure:<br>Role Clarity<br>Training<br>Accountability | Developed a behavioural model to underpin and promote the desired proactive risk management culture.<br>Executive promotes and reinforces the risk management culture.<br>Processes exist to identify, evaluate, assess and exploit opportunity risks |
| | Code of Conduct exists and training is included in orientation for new staff. | Training to support people in understanding how to use proactive behaviours. | Measurement each year of the risk management culture. |
| | Employees do not see internal control as a personal responsibility. | Risk Management Policy is reflected in employee and management training. | Employees take responsibility for proactively managing risk to benefit the business. |
| **Performance Management & Reward Systems** | Incentives exist for employee performance. | Some incentives for management aimed at encouraging a proactive risk management culture. | Each year a risk goal is set as part of an incentive bonus scheme. |
| **Own Risk & Solvency Assessment** | Ad hoc analysis on a reactive basis. | An Economic Capital Model provides assessment of the key risk drivers and risk management techniques to address these risks. | Economic capital model comprises forecast future balance sheet, profit and loss accounts, and projected distributions of profit; capital and return on capital. |
| | | | The allocation of capital to business units / lines commensurate with risk underpins the performance management process and enables measurement of outcomes and returns against those expected. |

| | Early | Intermediate | Advanced |
|---|---|---|---|
| **Risk Management Processes** | Controls are not explicitly linked to risks. | There is a clear identification of all the relevant risk categories. | Materiality limits for reporting incidents/risk issues are agreed on at least an annual basis by the executive management. |
| | Controls are generally detective in nature. | Risk management processes are applied. | Risk management processes are applied & the risk assessment includes the quantification of operational risk. |
| | A formal risk management plan is produced on a periodic basis that includes actions to be taken in respect of risks. | Risk Profiling is undertaken regularly at Business Unit level and organisation level. | Process for identifying and evaluating emerging risks (i.e., developing subject to uncertainty and difficult to quantify). |
| | Financial and compliance objectives and taken into account in the risk assessment process. | The risk analysis and treatment processes allows for the assessment and quantification of 'Inherent' and 'Residual' risk and the effectiveness of controls. | Scenario planning is used to evaluate high impact/low probability events. |
| | Loss events are monitored by central function (e.g. internal audit), | Loss events and risk profiling undertaken. | Able to integrate loss events with key risk indicators (lead and lag) and risk profiling. |
| | Controls focus on financial reporting and compliance. | Controls are all risk based and reviewed regularly. | Control activities cover all risks and undertaken within each Business Unit and business processes are documented and incorporate policies and procedures. |
| **Reporting & Monitoring** | Reporting of significant control weaknesses are communicated to certain parties e.g. internal audit, and without a strong sense of urgency. | Any breaches of these requirements are reported to the Enterprise-wide Risk Function. | Assurance is provided to executive management, the Audit Committee, and the Board via controlled risk self-assessments.<br>The responses to the controlled risk self-assessments are reviewed by the internal audit team, and the results of their review are reported to a Board Committee. |

| | Early | Intermediate | Advanced |
|---|---|---|---|
| | Information captured sometimes enables line management to effectively identify and deal with risks. | Internal risk reporting covers all key aspects of the Risk Management Policy.<br>Risk & Compliance plans developed by the Business Units identify the external reporting requirements, timings and responsibilities. | The Enterprise-wide Risk Function undertakes the:<br>Central collection, collation and analysis of enterprise-level risk-related data<br>Establishment of common reporting standards, tools and risk management information systems<br>Production of risk management reports. |
| | Some oversight / monitoring of middle management actions and the organisation's activities. | Business Unit are responsible for monitoring control activities. | Consistent Key Risk Indicators are applied across the organisation, enabling aggregation. |
| | Employees are encouraged to raise issues with management regarding inappropriate behaviour. | Formal internal channels exist for raising inappropriate behaviour. | Formal and independent channels exist for raising inappropriate behaviour, and these are used. |
| | Internal Audit plays integral role in reviewing effectives of controls. | Management undertakes overall responsibility for periodic reviews of the risk management system. | Risk management is monitored and evaluated on an ongoing basis by management and employees. |
| **Internal Audit** | Internal audit has limited access to Executives or Audit Committee. | Effective implementation and compliance with the Risk Management Policy is monitored by the Internal Audit Function, as well as the organisation's external auditors. | Internal Audit Function conducts an annual audit of the Risk Management Policy, and the Enterprise-wide Risk Function. |
| **New activities** | Major projects have cost benefit analysis with risk factored in. | Risk and controls exist for major projects. | Risk, controls and assurance testing new programmes, projects and ongoing change tasks, and strategic developments (e.g. acquisitions). |
| **Continuity Analysis** | A disaster recovery plan exists for information system applications | A properly documented and tested Business Continuity Plan. | Risk & financial condition assessment of the ability of the insurer to stay in business for more than one year. |
| | | | 'Crisis Management Plan' that minimises business impact and loss in the event of a significant incident. |

# Appendix 3
# ERM Implementation Case Studies

**ERM Implementation – Incorporating a Capital Model**

A large insurer was seeking to implement an ERM strategy throughout the organisation, and an integral aspect of this strategy was building a capital model. There were several drivers for insurance companies to build capital models. Supervisors and rating agencies now considered capital modelling incorporated into an ERM framework as vital for a well run insurance company. As well as reducing capital requirements, capital models provide employees with a tool to better understand the risks in their business, and therefore manage those risks more effectively.

Before the project started, the insurer recognised that it is important to get support within the business to develop a capital model. This is possibly the most important step, since building a capital model that will be useful for the business as a whole required input from across the organisation. Therefore, the project sponsor for the European capital model was the Chief Actuarial Officer (who was part of the Board Executive), and the project sponsor for the Group capital modelling project was the Chief Executive Officer of the Group. This high profile project sponsor provided a clear vision to implementing the ERM strategy. This in turn was helped increase the businesses' enthusiasm to participate in the project and enabled the project team to overcome obstacles through the project's lifetime.

Next a steering committee was formed to monitor development of the modelling. Membership included a good mix of business skills to help resolve any major issues. For instance, the European capital model steering committee consisted of:

- Chief Actuarial Officer (Chair)
- Chief Executive Officer
- Chief Finance Officer
- Chief Underwriting Officer
- Two operations directors
- Two senior underwriters.

Use of project disciples with a well-developed project plan ensured effective tracking of progress and ability to report in a timely and comprehensive manner to the Steering Committee.

During the implementation phase, the key internal stakeholders were managed through the steering committee, and a concerted effort was also made to extend publicity as far as possible. External stakeholders were also brought on-board at an early stage. The insurer recognised that it is much easier to include them on the capital modelling journey, rather than hand them a large report at the end of the project, for which they do not have the necessary resources to review. With the European model, the insurer held a number of meetings with the two UK supervisors; Lloyd's of London and the FSA. These meetings were beneficial in that it provided consensus that the general approach was sound. During the development phase of the capital model, the modelling team held one hour meetings with most of the underwriting teams within the business.

Incorporating all key risks into the capital model, as part of a wider ERM implementation, required the insurer to include the following:

- Underwriting risk – It was found that employees were familiar with the risks that business they are currently writing faces, and the underwriters were familiar with considering the uncertainty around business they are about to write
- Credit risk - The most common source of credit risk was external reinsurers, since this was typically one of the larger debtors on the balance sheet. The insurer incorporated reinsurance credit by considering the credit quality of the different reinsurers on the insurer's balance sheet
- Asset (market) risk – In seeking to avoid too much investment risk, the insurer was investing in high quality corporate bonds. Yet, even though these are secure, due to their market value being dependant on the prevailing yield curve, the market value of the bonds were modelled stochastically
- Liquidity risk – Although liquidity risk tends to be an immaterial risk for non-life insurance companies, in the event of a natural catastrophe, there could be a liquidity crunch. To allow for liquidity issues, the insurer considered short-term cash flows within the model
- Operational risk – The insurer combined a robust operational risk scenario analysis along with a risk register as the operational risk assessment within the capital model.

Once the various parts of the capital model were assessed, they were reviewed by the relevant business experts:

- Underwriters and pricing actuaries for underwriting risk
- Reinsurance function and security committee for credit risk
- Investment function for market risk
- Risk management for operational risk and group risk
- Senior management and Board for overall reasonableness of the aggregate capital model.

Due to the comprehensiveness of the capital model, as part of a wider ERM strategy, the ERM implementation process achieved a high confidence level with the Board of this insurance organisation. However, the insurer also recognised that a continual review of their ERM strategy is necessary in order to increase focus on managing risk at an organisation-wide level and to effectively address pragmatic issues.

**ERM Implementation – A Cautionary Tale**

A large insurer initiated a project to design and implement an ERM process throughout the organisation. Project management and project ownership was assigned to the Internal Audit department because they were considered the owners of risk identification. Internal Audit quickly set about identifying the risks for each business unit and creating a draft Risk Profile. However the risk profiles produced were limited because they only addressed the areas which were understood and monitored by Internal Audit. Not only did the Executive not accept these risk profiles as true reflections of their businesses but some "key risks" were omitted entirely. As a result of this resistance the process of implementing ERM was significantly slowed down.

In response to the problems being experienced in the implementation of ERM, the Board decided to reassign ownership of the ERM project to the business units. The business units worked collectively to establish a project team of people with the right

attitude for the project. However, these individuals ended up being part time resources due to their continued responsibility for their day to day roles and again the project ran into delays.

Additional risk champions in the businesses were identified. These were managers with full day jobs already who were not part of the risk community. Due to budgetary constraints and time availability no training was provided to these new champions. It was considered that they were talented mangers who would soon pick it up. By now the Board had decided that to ensure ERM was implemented to be 'leading practice' in the industry. This added pressure to the project team and the new champions as they strove to meet these higher level criteria for success. Nevertheless after several months the ERM implementation was complete.

A post implementation survey of business managers was conducted to assess both the project and views about the usefulness of the ERM framework. The feedback was quite critical. The ERM process was considered "over-engineered" in some areas and the implementation patchy in other areas of the business. They also observed that there was a lack of training and support provided to the business unit risk teams / risk champions and that the solution for the risk management tool was decided before the development of the Group framework. In addition, the roll-out would have benefited from detailed implementation planning. This lead to frustrations and actually resulted in risk awareness going backwards. People found it was difficult to understand what the objectives were, what the desired inputs were and what output and benefit was being received. The process became very user-unfriendly.

The Board subsequently initiated a new project to "simplify" the existing ERM process and noted the following learning to avoid problems in future:

- Board and senior management "buy-in" into the ERM process is required from the beginning; with a clear vision and agreed achievable outcomes
- The project owner of ERM design and implementation should never be just one department within the organisation, always include ownership across the business from the start
- Use project plans, project disciplines and full time resources, don't ask people to do this work in addition to their day jobs, build the project over time
- Engaging risk champions at the lower levels of the organisation is critical prior to roll-out and ensure they receive the relevant training
- The time and resources for a roll-out of a Group framework should not be under-estimated
- Introducing new technology is typically harder than expected so plan for the worst not the best case scenario
- Understand that implementing ERM involves cultural change which will take time so build these expectations into the project plan
- AND do not over-engineer the process; keep it easy and simple.

**ERM Implementation: Success is whatever you define success to be!**

A large Global Insurer embarked on an ERM implementation program. Taking the prevailing standards, guidance and academic material the organisation set out to deliver 'holistic', 'strategic', 'integrated' risk management to the entire enterprise to meet the needs of supervisors, investors, customers and policy holders and management all in one program.

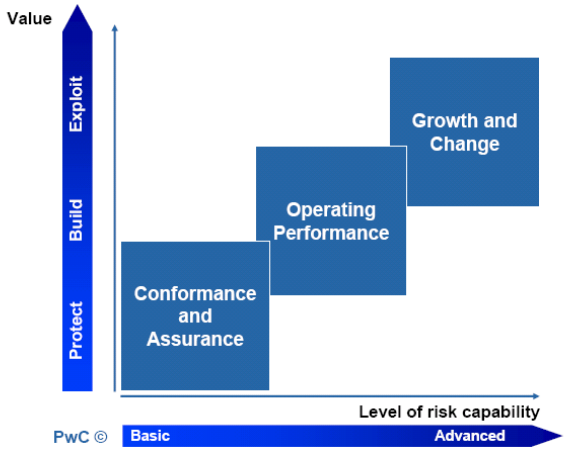
The ERM program defined measures of success in terms of project activities, achieving project milestones, number of workshops, frequency and volume of reporting outputs, sophistication of tools and techniques and many 'process or activity' related success measures. But the outcome was unsuccessful and much of the work and investment was unwound and written off. Many of the staff in the risk management function lost their jobs.

So what went wrong? Fundamentally, the ERM program did not have a definable impact on business objectives or outcomes. There was:

- No significant changes to the risk profile or risk management capability of the organisation
- No defined business outcomes for ERM that were aligned/sufficiently connected to the business objectives and outcomes
- Increased cost, work load and time put on management that did not deliver any greater insight to the business than already obtained through other management practices and capabilities
- Duplication of existing analysis, processes and reports for little marginal economic benefit.

What should be done differently? The definition of success for ERM needs to be defined in terms of the business outcomes and value contribution to the business.

1. Be very specific on the scope and focus of the ERM activity. For example the illustration below provides a view on where ERM is to have an impact;




a) Conformance and assurance; reduction in losses or greater cost avoidance
b) Operating performance; reduction in uncertainty or **downside** variability in operational costs and outcomes – operational stability and cost avoidance
c) Growth and change; increase the likelihood or probability of success in growth and change decisions – taking the right bets with greater confidence

Where is the primary business focus for the ERM implementation?

2. There must be qualitative, quantitative and economic measures of success and impact of ERM on the business.
3. The Stakeholders must agree and support the measures of success, with the ERM sponsors held accountable for delivering this success
4. There must be continuous assessment and challenge of the status quo to ensure the investment in ERM continues to be relevant to the business outcomes.

# Appendix 4
# Example of a Risk Committee Charter

**What should be included in a risk committee charter?**

- The purpose of the Risk Committee e.g. *to perform centralised oversight, policy setting, information gathering, and communication to senior management and the Board of Directors, regarding important risks and its related risk management activities*
- Outline of the responsibilities of the Risk Committee e.g. *identify and monitor important existing and emerging risks to the achievement of the company's strategic and operating objectives, formulate appropriate policies and monitoring and reporting frameworks etc.*
- Minimum pre-requisites for its members / committee composition e.g. *nominated by senior management, a third of the committee members are required to be external etc.*
- Frequency of meetings for the Risk Committee e.g. *meet one month in advance of each Board of Directors' meeting*
- Outline of the Key Performance Indicators ("KPI") which will be used by the Risk Committee to annually assess its performance e.g. *number of policies considered by the Risk Committee in a year, number of policies recommended for adoption to the Board which were adopted in a year, number of meetings held during the year, number of policies approved for adoption by the Board which were successfully implemented etc.*
- Outline the resources which the Risk Committee shall have direct access to and open communication with e.g. *senior management, assistance / liaison from internal audit, internal legal, finance and other advisors within and external to the organisation*.

**Example Charter**

## *1. PURPOSE*

The Risk Committee's primary purpose is to perform centralised oversight, policy-setting, information gathering, and communication to the Board of Directors, regarding important risks and its related risk management activities. In addition, the Committee shall assist the Board of Directors in fulfilling its oversight responsibilities related to the company's risk assessment and management processes.

## *2. RESPONSIBILITIES*

The Risk Committee shall be responsible for the following activities:

- Identify and monitor important existing and emerging risks to the achievement of the company's strategic and operating objectives.
- Formulate appropriate policies and monitoring and reporting frameworks to support effective management of important risks.

- Review and evaluate the effectiveness of management processes and action plans to address such risks.
- Advise on and recommend to senior management any significant actions or initiatives that the Committee believes necessary to effectively manage risk.
- Ensure that activities of discrete risk management disciplines within the company are appropriately coordinated.
- Report to the Board of Directors on the status of the company's important risks and related risk management processes.

## *3. MEMBERSHIP AND MEETINGS*

The Chief Executive Officer / Board hereby resolves to establish a Risk Committee consisting of representatives from the Board of Directors. The Risk Committee shall have a Chair appointed by the Board / Chief Executive Officer, who will be responsible for providing overall leadership of Committee activities and setting agendas for the Committee meetings.

The Risk Committee shall meet [bi-monthly / quarterly] and additionally when needed.

## PERFORMANCE AND CHARTER

Annually, the Risk Committee shall perform a self-assessment against the Key Performance Indicators ("KPIs"), a review of the Committee membership and recommendations as to any changes thereto. In addition, the Committee shall annually review its Charter and make any recommended changes thereto.

## RESOURCES AND AUTHORITY OF THE COMMITTEE

The Committee shall have direct access to and open communication with senior management and liaison / assistance from internal audit, internal legal, finance function and other advisors to assist with decision making and monitoring. The Committee shall also have access to external advisors to assist if required.

## KEY PERFORMANCE INDICATORS FOR ASSESSMENT OF COMMITTEE PERFORMANCE

Examples:

- Number of policies approved by the Committee per annum;
- Number of policies considered by the Committee per annum;
- Number of meetings held per annum; and /or
- Average number of attendees at each Committee meeting.

# Appendix 5
# Chief Risk Officer – Key Roles & Responsibilities

## Chief Risk Officer

The Chief Risk Officer will oversee market risk, asset/liability management, credit risk, investment risk, operational and supervisory risk and actuarial issues throughout the organisation and service the Risk Committee and its sub-committees.

In accordance with the organisation's Operating Philosophy, the role of the Chief Risk Officer is to provide:

- Policy Guidance and establish Minimum Standards for the conduct of risk management activities throughout the organisation
- Oversight of risk management activities across the organisation to ensure Minimum Standards are met, including monitoring of aggregate risk data
- Lead the risk committee and ensure it adheres to its charter
- Functional leadership for the organisation's specialist personnel involved in risk management activities throughout the organisation to ensure a professional cadre of risk management personnel operates at high standards throughout the organisation
- Monitor leading practice trends to ensure the organisations ERM program continually evolves
- Research capability to ensure the organisation is kept abreast of the latest developments and harnesses such developments for the benefit of the organisation
- Ensure there is an independent view on the effectiveness and efficiency of the risk management arrangements
- Liaise with ratings agencies and provide the relevant information as required
- Provide additional services deemed necessary by the organisation or at the request of individual operating units that does not conflict with their role
- The Chief Risk Officer where necessary, challenges business decisions on key risk areas and has the ability to escalate issues that cannot be resolved with individual operating units to the Operating Units Managing Director / Chief Executive Officers. In the very rare event that a matter of significant business risk cannot be resolved with an Operating Unit Managing Director, then the matter is referred to the Chief Executive.

In addition the Operating Unit Managing Directors / Chief Executive Officers ensure that appropriate consultation takes place with the Chief Risk Officer on all issues involving organisational policy or otherwise within their remit.

The following example is how these responsibilities might be described in a role specification.

## Generic Role Specification

Reports to: INSURER Group Chief Executive Officer

### *Principle Role & Accountability:*

*The Chief Risk Officer is responsible for the leadership, direction and co-ordination of the Group-wide application of risk management at INSURER including line management responsibility for [Group Risk Management, Internal Audit, Health, Safety, Welfare and Environment.] and to ensure that the principles and requirements of managing risk are consistently adopted throughout the Group, and to establish a risk management framework and appropriate resource to assist the Group in its realisation of business objectives and continual development.*

### *Principle Responsibilities:*

Policy and Strategy

a) To design and oversee the group-wide risk management strategy, aligning all risk management and associated internal control activities to support the delivery of shareholder value in the INSURER Group.

b) To present INSURER Group risk management policy for discussion and approval by the INSURER Group Risk Management Committee and/or INSURER Group Board.

c) To canvass senior management views on the continual development of risk management across the Group and review whether organisational structure to support the INSURER Group risk management strategy remains appropriate.

d) To maintain awareness of trends and developments in risk management that may be significant to the INSURER Group and its operating subsidiaries.

e) To oversee the procurement of all Group insurance, broker and underwriter contracts and where appropriate, identify professional advisors to support the delivery of best practice risk management across the INSURER Group.

f) To facilitate the integration of risk management policy and strategy into all INSURER Group business strategy and activity, including the consideration of risk management in investment decisions.

g) Ensure that appropriate information regarding risk and internal controls is provided to the investment market including shareholders in conjunction with the Chairman and Chief Executive Officer.

h) To liaise with the Supervisors on existing regulations, new regulations and emerging regulations. Liaison will include participation in providing feedback to the Supervisors on framework and principles as well as responding to the Supervisors questions and requests.

Risk Identification & Assessment

a) To monitor and report to the INSURER Group Risk Management Committee on the total level of INSURER Group risk exposure.

b) To maintain independent challenge on risk and assurance issues through the management of INSURER Group risk and assurance functions.

c) Ensure that risk identification and assessment activities performed across the INSURER Group and operating subsidiaries are reviewed and challenged where necessary and appropriate escalation procedures are in place at the highest level.

Management and Reporting Framework

a) To be responsible for management and co-ordination of Group Risk Management [(to include Group Insurance), Internal audit and Health, Safety, Welfare and Environment (including Corporate Social Responsibility).]

b) To ensure appropriate risk management and reporting frameworks are in place across the INSURER Group and operating subsidiaries, commensurate with risks to Group.

c) To provide an annual INSURER Group risk management performance report to the INSURER Chief Executive Officer.

Reporting and Stakeholder Engagement

a) To monitor the overall risk management performance at Group level and to ensure the effective and timely reporting of risk management information within the Group operating subsidiaries and at Group level.

b) To be an attendee of the INSURER Group Risk Management Committee and ensure that the Committee engages in the development of best practice risk management across the INSURER Group.

c) To present, discuss and challenge Strategic Risk Review summary reports, reporting key risks and associated internal control procedures, to the INSURER Group Risk Management Committee.

d) To represent INSURER Group risk management positions, strategy and experiences at internal and external forums to maintain a high reputation.

e) To develop and maintain appropriate engagement processes with INSURER Group stakeholders, and ensure that equivalent and consistent risk management processes are implemented within INSURER Group operating subsidiaries.

f) With Strategy & Communications and others as appropriate, to advise the investment community, Credit Rating Agencies, on risk management performance, particularly with reference to Socially Responsible Investment.

Line Support and Knowledge Sharing

a) To facilitate risk management knowledge and best practice sharing across the Group, with reference to external indices and benchmarks as appropriate.

b) To Chair the INSURER Group Risk Management Co-ordinators Forum, providing expertise and support and communicating risk and associated internal control procedures arising from the INSURER Group Risk Committee and act as an information conduit for the Forum to the Risk Management Committee.

c) To support senior management with any aspect of risk management development and oversee key risk management training initiatives including key senior management training and to incorporate risk management into employee induction programmes.

# Appendix 6
# Topics and structure of a typical risk management policy

## 1 INTRODUCTION

1.1 Definitions of Risk and Enterprise Management

1.2 Objective of Enterprise Risk Management

## 2 RISK MANAGEMENT POLICY

2.1 Objectives of Risk Management Policy

2.2 Categories of Risk and Definitions

[*Example risks for an insurer:*

- Operational
- Corporate and strategic
- Underwriting and pricing
- Reserving
- Liquidity
- Credit
- Market
- Legal and compliance
- Financial]

2.3 Potential Benefits of ERM

2.4 Success Criteria

## 3 RISK MANAGEMENT STRUCTURE

*[Include organisational chart along with details on the roles of each position.]*

3.1 Risk management organisational structure

3.1.1 Role of Risk Committee
e.g., Performs centralised oversight, policy-setting, information gathering, and communication to executive management and Board of Directors.

3.1.2 Role of CEO

3.1.3 Role of CRO

3.1.4 Role of Executive Management

3.1.5 Role of Risk Sponsors

e.g., Represents each of the Company's major business units and support functions, and to whom given risks are "assigned" for helping to ensure that the Committee's objectives are carried out.

3.1.6 Role of Risk Owners
e.g., Individuals responsible for managing a specific risk or risks.

3.1.7 Role of Risk Manager

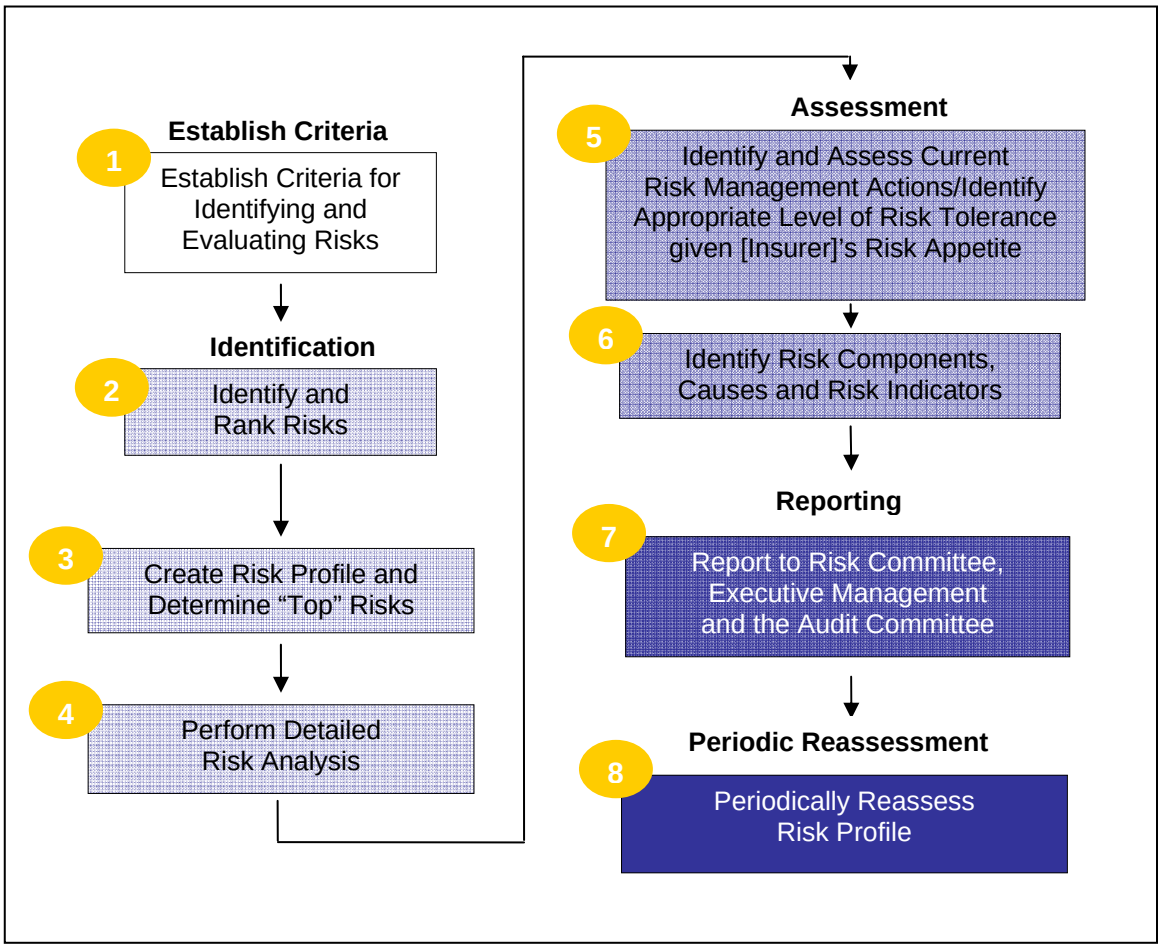
3.1.8 Role of Monitors
e.g., The company's risk control processes are monitored at the Risk Owner and Risk Committee level, as well as by risk control functions (e.g., Internal Audit, Compliance, and Legal)

## 4 RISK IDENTIFICATION AND ASSESSMENT PROCESS

*[Define the enterprise identification and assessment process.]*

4.1 Overview of the risk assessment process

The overall risk assessment process is illustrated in the following diagram. Each of the steps is explained further below.



4.2 Step 1 – Establish Criteria

4.2.1 Risk Ranking Criteria

4.2.2 Current Risk Management Action Effectiveness Score

4.2.3 Risk Appetite

4.2.4 Risk Tolerance

4.3 Step 2 – Identify, Assess and Rank Risks

4.4 Step 3 – Create Risk Profile and Determine “Top” Risks

4.5 Step 4 – Perform Detailed Risk Analysis

4.6 Step 5 – Identify and Assess Current Risk Management Actions / Identify Appropriate Level of Risk Tolerance Given [Insurer]’s Risk Appetite

4.6.1 Identify and Assess Current Risk Mitigating Actions

4.6.2 Identify Appropriate Level of Risk Tolerance Given [Insurer]’s Risk Appetite

4.7 Step 6 – Identify Components, Causes and Risk Indicators (applicable to Top Risks only)

4.8 Step 7 – Report to Risk Committee, Executive Management and the Audit Committee

4.9 Step 8 – Periodically Reassess Risk Profile

## 5 RISK REPORTING

*[Define the risk reporting process and include example template where applicable.]*

5.1 Format and timing of the risk reporting

For Example:

| Reporting to | Frequency of reporting | Reporting format |
|---|---|---|
| Risk Committee | *Quarterly* | |
| Executive Management | *Quarterly* | |
| Audit Committee | *Quarterly for Top Risks* | |

## APPENDICES

**Appendix A: Risk Committee Charter**

**Appendix B: List of Risk Committee members**

**Appendix C: Risk Register Template**

**Appendix D: Risk Ranking Criteria (Likelihood and Consequence)**

**Appendix E: Current Risk Management Action Assessment Criteria**

**Appendix F: Risk Profile**

**Appendix G: Sensitivity Analysis for Top Risks**

**Appendix H: Top Risk Management Actions Report**

**Appendix I: Effectiveness in Light of Risk Tolerance**

**Appendix J: Risk Status Report – Top Risks**

**Appendix K: Risk Status Report – Remaining Risks**

**Appendix L: Risk Content Report**

## GLOSSARY OF TERMS

For Example:

- *Risk Committee:* reviews the Company's policies with respect to risk assessment and risk management, and contingent liabilities and risks that may be material
- *Enterprise Risk Management (ERM):* a structured and disciplined approach aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing risks a company faces as it creates value
- *Monitoring:* the Company's risk control processes are monitored at the Risk Owner and Risk Committee level, as well as by risk control functions
- *Risk:* the threat of an event, action, or loss of opportunity that, if it occurs, may adversely affect values of the Company
- *Risk Appetite:* phrase used to express the overall level of risk the Company is willing to take to achieve its objectives.
- *Risk Committee:* performs centralised oversight, policy setting, information gathering, and communication to executive management and Board of Directors
- *Risk Owners:* individuals responsible for managing a specific risk or risks
- *Risk Sponsors:* represent each of the Company's major business units and support functions, and to whom given risks are "assigned" for helping to ensure that the Committee's objectives are carried out
- *Risk Tolerance:* quantitatively defines the level of risk we are willing to accept with respect to each of the Company's important risks.

# Appendix 7
# Useful 'Emerging Risk' web links

CRO Forum home page: http://www.croforum.org/

CRO Forum Emerging Risks Initiative page: http://www.croforum.org/emergingrisc.ecp

CRO Forum Emerging Risks Initiative – *"Position paper - Climate change & tropical cyclones"*: http://www.croforum.org/emergingrisc.ecp

CRO Forum Emerging Risks Initiative *"Position paper – Pandemic"*: http://www.croforum.org/publications/20080201_1_resource/File.ecr?fd=true&dn=cro_pandemie_final

CRO Forum Emerging Risks Initiative *"Position paper – Terrorism"*: http://www.croforum.org/publications/20072711_resource/File.ecr?fd=true&dn=terrorismpositionpaper_nov07

Swiss Re emerging risk initiate: http://www.swissre.com/pws/media%20centre/online%20magazine/market%20trends/the%20cro%20emerging%20risk%20initiative.html

Ernst & Young report - *"Strategic Business Risk 2008 – the Top 10 Risks for Business with Oceania Perspectives"*: http://www.ey.com/Global/assets.nsf/Australia/AABS_Strategic_Business_Risk/$file/SBR.pdf

Ernst & Young report - *"Property/Casualty Insurance Industry 2007 Outlook"*: http://www.ey.com/Global/assets.nsf/International/Industry_Insurance_US_Property_Casualty_Insurance_Industry_Outlook_2007/$file/EY_USProperty_Casualty_Insurance2007Outlook.pdf

Ernst & Young report - *"Strategic Business Risk - Insurance 2008"*: http://www.ey.com/Global/assets.nsf/International/Industry_Insurance_StrategicBusinessRisk_2008/$file/Industry_Insurance_StrategicBusinessRisk_2008.pdf

World Economic Forum report *"Global Risks 2008 - A Global Risk Network Report"*: http://www.weforum.org/pdf/globalrisk/report2008.pdf

OECD Report – "*Emerging Risks in the 21st Century – An OECD International Futures Project":* http://www.oecd.org/dataoecd/23/56/19134071.pdf

Economist Intelligence Unit Report – *"Risk 2018. Planning for an unpredictable decade"*: http://www.btglobalservices.com/business/global/en/docs/other/risk_2018_planning_for_an_unpredictable_decade.pdf

Deloitte report – "2008 Industry Outlook. Insurance overview. A look around the corner": http://www.deloitte.com/dtt/cda/doc/content/us_2008CrossIndustryOutlook_insurance.pdf

# Appendix 8
# Useful References

**Note: All websites accessed on 1 July 2008.**


Acharyya, M. 2007. ***Proposing a conceptual framework to measure the performance of Enterprise Risk Management from an empirical study of four major European insurers***
http://www.egrie2007.de/EGRIE%20Papers/EGRIE_2007_Acharyya.pdf

A.M. Best. 2006. ***A.M. Best Comments on Enterprise Risk Management and Capital Models*** http://www.ambest.com/ratings/methodology/enterpriserisk.pdf

American Academy of Actuaries. 2001. ***Risk Management in the Insurance Industry***
http://www.actuary.org/pdf/finreport/risk_09dec01.pdf

Bennet C; Cusick, K. (Trowbridge Deloitte Limited) 2007. ***Risk Appetite: Practical Issues for the Global Financial Services Industry***URL:
http://www.actuaries.asn.au/IAA/upload/public/4.a_Conv07_Paper_Bennet%20Cusick_Risk%20Appetite.pdf

Bohn, C; Kemp, B. 2006. ***Enterprise Risk Management Quantification - An Opportunity*** http://www.soa.org/library/monographs/other-monographs/2006/july/Bohn-abstract.pdf

Casualty Actuarial Society. May 2003. ***Overview of Enterprise Risk Management***
http://www.ucop.edu/riskmgt/erm/documents/overview.pdf

Committee of Sponsoring Organizations of the Treadway Commission. 2004 ***Enterprise Risk Management — Integrated Framework: Executive Summary***
http://www.coso.org/publications/ERM/COSO_ERM_ExecutiveSummary.pdf

Continuity Central. 2007. ***Emerging Governance Practices in Enterprise Risk Management*** http://www.continuitycentral.com/feature0439.htm

D'Arcy, S. 2006. ***Enterprise Risk Management in the Insurance Industry***
http://www.business.uiuc.edu/~s-darcy/present/ERM%20Symposium%20-%202006%20-%20Workshop%202%20(D'Arcy%203-31-06)%20with%20Template.ppt#258,2,Overview

Deloitte. 2006. ***The Risk Intelligent Enterprise: ERM Done Right***
http://www.deloitte.com/dtt/cda/doc/content/us_risk_RIPOV.pdf

Ernst & Young. 2006. ***Insurance Risk Leadership Roundtable: Setting Risk Appetite, Tolerance and Limits***
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Insurance_Risk_Leadership_Roundtable_Corporate_Risk/$file/AABS_RAS_Insurance_Risk_Leadership_Roundtable_CorporateRisk.pdf

Ernst & Young. 2006. ***Insurance Risk Leadership Roundtable: Preparing for the new ERM Environment***

http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Insurance_Risk_Leadership_Roundtable/$file/AABS_RAS_Insurance_Risk_Leadership_Roundtable.pdf

Ernst & Young. 2005. ***Managing Risk across the Enterprise: Connecting New Challenges With Opportunities***
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Managing_Risk_Across_Enterprise/$file/AABS_RAS_Managing_Risk_Across_Enterprise.pdf

Ernst & Young. 2006. ***Managing Risk Across the Enterprise: The value of Enterprise Risk Management***
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Value_ERM/$file/RAS_Value_ERM.pdf

Ernst & Young. 2007. ***Managing Risk Across the Enterprise: Building a Comprehensive Approach to Risk***
http://www.ey.com/Global/assets.nsf/International/AABS_RAS_Manag_Risk_Enterprise/$file/AABS_RAS_Manag_Risk_Enterprise.pdf

Financial Services Authority. 2006. ***Insurance Sector Briefing: Risk Management in Insurers*** http://www.fsa.gov.uk/pubs/other/isb_risk.pdf

Financial Services Authority (McDonnell, William). 2002. ***Managing Risk: Practical Lessons from Recent "Failures" of EU insurers***
http://www.fsa.gov.uk/pubs/occpapers/OP20.pdf

Gates, Stephen. 2006. Incorporating Strategic Risk into Enterprise Risk Management XVème Conférence Internationale de Management Stratégique, Annecy / Genève 2006 http://www.strategie-aims.com/aims06/www.irege.univ-savoie.fr/aims/Programme/pdf/SP26%20GATES.pdf

Hoyt, R.E; Liebenberg, A.P. 2008. ***The Value of Enterprise Risk Management: Evidence from the U.S. Insurance Industry***
http://www.ermsymposium.org/pdf/papers/Hoyt.pdf

Ingram, D. 2003. ***Life Insurance Industry Risk Management***
http://www.iafe.org/upload/Ingram_Talk.pdf

Institute of Internal Auditors. 2004. ***The Role of Internal Audit in Enterprise-wide Risk Management*** http://www.ucop.edu/riskmgt/erm/documents/erm1.pdf

International Association of Insurance Supervisors. 2007. ***Guidance Paper On Enterprise Risk Management For Capital Adequacy And Solvency Purposes***
http://www.iaisweb.org/__temp/2_2_6_Guidance_paper_on_enterprise_risk_management_for_capital_adequacy_and_solvency_purposes.pdf

International Association of Insurance Supervisors.2007. ***Guidance Paper On The Use Of Internal Models For Risk And Capital Management Purposes By Insurers***
http://www.iaisweb.org/__temp/15__Guidance_paper_No__2_2_6_on_the_use_of_internal_models_for_risk_and_capital_management_by_insurers.pdf

International Electrotechnical Commission (IEC). ***Draft IEC 31010 Risk Management - Risk Assessment Techniques***
http://www.rmia.org.au/LinkClick.aspx?fileticket=uXc91tcaLVU%3d&tabid=85&mid=634

International Organisation for Standardization (ISO). 2008. ***Draft International Standard ISO/DIS 31000: Risk management — Principles and guidelines on implementation***
http://rmia.org.au/LinkClick.aspx?fileticket=AWkZuS%2bB6Wc%3d&tabid=85&mid=634

KPMG. 2001. ***Enterprise Risk Management: An Emerging Model for Building Shareholder Value*** http://www.kpmg.com.au/aci/docs/ent-risk-mgt.pdf

KPMG. 2006. ***Risk and Capital Management for Insurers***
http://www.kpmg.cz/czech/images/but/Risk_Capital_Management_for_Insurers_2006.pdf

Lam, J. 2000. ***Enterprise-wide risk management and the role of the chief risk officer*** http://www.erisk.com/Learning/Research/011_lamriskoff.pdf

Matthews, A; Wang, S; Cassidy, P: Faber, R; Newton, T. 2007. **Enterprise Risk Management and Exploring Best Practice in Commercial Insurance Pricing and Underwriting**
http://www.actuaries.asn.au/IAA/upload/public/2.c_Conv07_Paper_Matthews_putting%20enterprise%20risk%20mgt%20into%20best%20practice.pdf

McConnell, Patrick. 2004. ***A 'Standards Based' approach to Operational Risk Management under Basel II*** http://www.m-bryonic.co.uk/library/ORStandards.pdf

PWC. 2004. ***Enterprise-wide Risk Management for the Insurance Industry - Global Study***
http://www.pwc.com/extweb/pwcpublications.nsf/docid/57b887e9d239274785256e470020a3a5

Rech, J. E. 2005. ***Enterprise Risk Management for Insurers: Theory in Practice.***
http://www.contingencies.org/novdec05/enterprise_1105.asp

Schmidt Bies, S. 2006. ***A Bank Supervisor's Perspective on Enterprise Risk Management,*** BIS Review, publication 34/2006.
http://www.bis.org/review/r060502d.pdf

Shamieh, C. 2007. ***Implementing EC – Recent experience***
http://riskisopportunity.com/files/pdf/2007-chicago-shamieh.pdf

Society of Actuaries, 2006. ***Enterprise Risk Management Specialty Guide***
http://soa.org/library/professional-actuarial-specialty-guides/enterprise-risk-management/2005/august/spg0605erm.pdf

Standard and Poor's. 2005. ***Enterprise Risk Management For Financial Institutions: Rating Criteria And Best Practices***
http://www.mgt.ncsu.edu/erm/documents/sp_erm_busdevbk.pdf

Standard and Poor's. 2007. ***Enterprise Risk Management Can Help U.S. Commercial Lines Insurers Ward Off Irrational Pricing***
http://www.rims.org/resources/ERM/Documents/ERMReportCard4-30-07.pdf

Standard and Poor's. 2006. ***Insurance Criteria: Refining The Focus of Insurer Enterprise Risk Management Criteria***
http://www.actuaries.org.hk/doc/ET060808_Ref4.pdf

Teuten, P. 2005. ***Enterprise Risk Management: Its Evolution And Where It Stands Today*** http://www.keanebrms.com/portals/0/JLR-Fall%202005.pdf

Tillinghast - Towers Perrin. 2000. ***Enterprise Risk Management: An Analytic Approach*** http://www.towersperrin.com/tillinghast/publications/reports/Enterprise_Risk_Management_An_Analytic_Approach/erm2000.pdf

Tillinghast - Towers Perrin. 2001. ***Creating Value Through Enterprise Risk Management — A Practical Approach for the Insurance Industry*** http://www.towersperrin.com/tillinghast/publications/reports/Creating_Value_through_Ent_Risk_Mgmt/2002051306.pdf

Treasury Board of Canada. 2004. ***Integrated Risk Management – Implementation Guide*** http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/guide01_e.asp

Tripp, M.H; Chan, C; Haria, S; Hilary, N; Morgan, K; Orros, G.C; Perry, G.R; Tahir-Thomson, K. 2008. ***Enterprise risk management from the General Insurance perspective*** http://www.actuaries.org.uk/__data/assets/pdf_file/0017/132038/sm20080428.pdf

UK Cabinet Office. Government Strategy Unit Report. 2008. ***Risk: Improving Government Ability to Handle Uncertainty*** http://www.cabinetoffice.gov.uk/strategy/work_areas/risk.aspx

Wang, S; Faber, R. 2006. ***Enterprise Risk Management for Property-Casualty Insurance Companies*** http://www.ermii.org/Research/downloads/erm_paper080106.pdf

Warrier, S.R; Chandrashekhar, P. 2006. ***Enterprise Risk Management: From the boardroom to shop floor*** http://www.infosys.com/industries/insurance/white-papers/enterprise-risk-management-paper.pdf

Wason, S. 2007. ***Repositioning ERM*** http://www.actuaries.asn.au/IAA/upload/public/1.a_Conv07_Paper_Wason_repositioning%20ERM.pdf

Yow, S; Sherris, M. 2007. ***Enterprise Risk Management, Insurer Pricing, and Capital Allocation*** http://wwwdocs.fce.unsw.edu.au/actuarial/research/papers/2007/iisyowsherrisfinal.pdf