Institute of Actuaries of Australia

RISK MANAGEMENT PRACTICE COMMITTEE

Information Note: Actuarial Advice regarding Risk Management of a Life Insurer (LPS 220) or General Insurer (GPS 220)

September 2011

Contents

1. Status of Information Note

This Information Note was first published in September 2011 and was prepared by the Professional Standards Subcommittee of the Risk Management Practice Committee of the Institute of Actuaries of Australia ("Institute").

This Information Note does not represent a Professional Standard or Practice Guideline of the Institute. It has been prepared to assist Appointed Actuaries in their roles of providing actuarial advice regarding the suitability and adequacy of risk management frameworks, as required under APRA Prudential Standards LPS 220 (Risk Management) (issued in March 2007) ("LPS 220"), GPS 220 (Risk Management) (issued in July 2008) ("GPS 220") and GPS 310 (Audit and Actuarial Reporting and Valuation) (issued in July 2010), and their related APRA Guides. This Information Note suggests ways in which Appointed Actuaries, their support staff and actuaries in general might satisfy themselves as to the appropriateness of their organisations' risk management frameworks.

Although the primary objective of this Information Note is to provide information to Members concerning the actuarial requirements relating to risk management under relevant APRA Prudential Standards and Prudential Practice Guides, references are also made to the ways in which actuaries may more specifically assist in strengthening the risk management frameworks of life insurers and general insurers. Actuaries can contribute by identifying opportunities to appropriately enhance a company's risk management framework. Taking opportunities to assist in shaping sound risk management and governance processes can assist in protecting companies against a wide range of potential adverse scenarios.

Feedback on this Information Note is encouraged and should be forwarded to the Professional Standards Subcommittee of the Risk Management Practice Committee using the email address michael_thornton@amp.com.au. It is expected that this Information Note will evolve over time.

2. Background

2.1 Purpose of this Information Note

This Information Note provides information for life and general insurers' Appointed Actuaries and their support staff in assessing the suitability and adequacy of their company's risk management framework, as required by APRA's risk management Prudential Standards.

APRA defines a company's risk management framework as follows in section 9 of LPS 220:

> "the risk management framework is the totality of systems, structures, policies, processes and people within the life company that identify, assess, mitigate and monitor all internal and external sources of risk that could have a material impact on the life company's operations".

A life or general insurance Appointed Actuary must include an assessment of the suitability and adequacy of the company's Risk Management Framework as part of the annual investigation of the company's financial condition. This Information Note outlines a number of issues that an Appointed Actuary could consider in forming this opinion.

While it is not a requirement (at this time) for superannuation or banking actuaries to assess the suitability of risk management frameworks, actuaries are often asked to do so (for example, as a part of a Financial Condition Report). While superannuation and banking is beyond the scope of this Information Note, actuaries may find the principles articulated in this Information Note useful in their work.

Outside the scope of this note is any additional requirements imposed by any other prudential standard or guide, or any professional standard, including any other requirement by the actuary to comment on the entity's risk management framework or risk management strategy. To illustrate this point, this Information Note focuses on the suitability and adequacy of the risk management framework and more details on the technical requirements contained in Professional Standard 305 (Financial Condition Reports for General Insurance) are outside the scope of this Information Note.

2.2 Rationale for review of risk management framework within Prudential Standards / Prudential Practice Guides

APRA notes, in LPS 220, that:

> "Risk management is an essential component of a life company's ability to deal with its internal and external sources of risks and, therefore, its capacity to reduce and manage any adverse effects on its policy owners, operations and reputation."

Whilst regulatory capital can provide a level of financial security for policyholders, sound risk governance processes can provide broader protection for a broader group of stakeholders.

In 2007 and 2008, APRA released two prudential standards relating to risk management – LPS 220 and GPS 220 – that aim to ensure that companies maintain a risk management framework and strategy appropriate to the nature and scale of their operations.

It is recognised that large, complex financial institutions will typically require sophisticated risk management frameworks, whilst smaller, simpler organisations might use less sophisticated approaches, yet both may be deemed valid. In other words, one size does not fit all.

2.3 Enterprise risk management

In considering the requirements of LPS 220 and GPS 220, the concept of 'enterprise risk management' is important. For present purposes, this is defined as follows:

> "Enterprise Risk Management is the process by which organisations in all industries assess, control, exploit, finance, and monitor risks from all sources for the purpose of increasing the organisation's short and long term value to its stakeholders."

Broadly, enterprise risk management ("ERM") is the management of all risks across the whole organisation, in a structured and consistent manner, reflecting the inter-relationships between risks. It involves identifying risks and opportunities relevant to the organisation's ability to meet its objectives, assessing the likelihood and severity of those risks, determining an appropriate response, and the ongoing monitoring of risks and the management actions taken to address them.

By identifying and addressing risks in this manner, and by focusing on upside (the sound management of business opportunities) as well as downside risks, businesses will be better protected and positioned for profitable and sustainable growth, improving and protecting stakeholder value.

Two key elements differentiate ERM from traditional risk management:

(a) ***ERM applies risk management techniques consistently across the whole enterprise***. ERM aims to avoid a 'silo' approach to risk management, allowing management to understand interactions and interdependencies between risks faced by different business units. It also aims to ensure that the organisation's risk exposure is considered after allowing for diversification and concentration of risk across business units and risk types.

An example of a common 'silo' approach is the management of underwriting risks solely within the underwriting team, where there is no regard to the overall product offering or the organisation's tolerance for the insurance risks being accepted.

(b) ***ERM requires integration of risk management and measurement into business processes***. This includes incorporating risk considerations into strategic planning and decision making processes, ensuring that a company's strategy is aligned with its risk

appetite, and ensuring that key management decisions are made in a 'risk aware' manner.

Further, a distinguishing feature of ERM is a focus on managing risk to maximise the value to shareholders. This can be extended in some situations to maximising value for other stakeholders.

Annexure A outlines the ERM responsibilities of Appointed Actuaries and actuarial staff, and Annexure B outlines some samples of common enterprise risk management frameworks.

3. Considerations in assessing the suitability and adequacy of risk management frameworks

3.1 Introduction

This section outlines considerations for an Appointed Actuary in assessing the suitability and adequacy of their company's risk management framework. As the Appointed Actuary must consider the entire company's risk management framework, assessing risk management in the context of ERM is important. For this reason, ERM is referenced on many occasions in the rest of this Information Note.

3.2 ERM frameworks

As outlined in LPS 220 and GPS 220, an ERM framework is the totality of systems, structures, policies, processes and people within the company that identify, assess, mitigate and monitor all internal and external sources of risk that could have a material impact on the life company's, or general insurer's, operations. In assessing the appropriateness and effectiveness of a company's ERM framework, the Appointed Actuary might consider:

1. risk appetite and risk culture of the Board;
2. maturity, size and complexity of the business;
3. nature, complexity and magnitude of the risks faced by the company; and
4. cost / benefit tradeoffs.

A company's ERM framework should be capable of identifying emerging risks, as well as being flexible enough to cope with changing company and industry circumstances.

Some common ERM frameworks are described in Annexure B to this Information Note. Actuaries are encouraged to keep up to date with future developments to ERM frameworks,

as these may provide useful reference points in assessing a company's risk management framework.

3.3 Assessing the suitability and adequacy of a company's risk management framework

Whilst there is no single process for forming an opinion on a company's risk management framework, the method adopted should reflect the company's risk management framework, the size and complexity of the business, and provide a reasonable basis for supporting the Appointed Actuary's opinion.

Considerations that Appointed Actuaries may take into account in forming their view on a company's risk management framework might include:

- Considering views on the company's risk management framework from those involved in monitoring risks and controls – for example, the Chief Risk Officer, internal audit, compliance, and operational risk managers will have views on the adequacy of the framework.

  Specific matters that might be discussed with such staff might include: details on major risk incidents and "near misses", insights into their ERM concerns, views on opportunities for improvement, emerging risks, risk culture, and the risk awareness of the executive team and the Board. Risks that have impacted other companies and industries may also be considered to identify any risks that are not currently being appropriately addressed by the company's ERM framework.

- Consideration of key risk management issues that have emerged over the year (many of which will need to be reviewed in any event, as part of the Financial Condition Report), the severity, speed and adequacy of management's response, and the ongoing management of these issues.

- Reviewing action items that have been identified in previous risk management reviews, to ensure these have been addressed in a timely manner.

- Considering the company's risk appetite: the executive and Board engagement in determining risk appetite; the determination of consistent risk tolerances; the reporting of exposures relative to those tolerances, and the pro-active management and reporting of breaches across the business.

- Considering the risk management culture across the business: the speed and transparency with which issues are escalated and acted upon, and the organisation's response to "bad news", might be relevant in this regard. Other relevant items might include the proactive management of key risks, the level of oversight by the Board, and the level of resourcing and capability of the risk management team.

- Consideration of the processes used to inform the Board and senior management of risk management issues, policies and practices within the company, and their appropriateness.

- Consideration of the effectiveness of the risk management framework – whilst the framework itself may be suitable and adequate, it also needs to be effective within the context of the organisation. For example, LPS 220 requires a sign off on the effectiveness of the risk management framework by the audit function, and this could be considered by the Appointed Actuary.

- Consideration of the suitability and adequacy of the company's risk management policy, the structure of the risk management function and the risk management responsibilities within the business, as well as people risk management capabilities.

- Consideration of systemic risks to which a company is exposed or contributes. Capital requirements that increase as experience deteriorates, and risk management arrangements where investments have to be sold (or derivatives purchased) in declining markets, might be an area of focus.

- Consideration of the way in which the company's capital models are used in determining risk appetite and risk limits in the business.

- The company's response to "extreme" events may also be considered. An Appointed Actuary might assess whether scenario testing of plausible, or "extreme", situations is regularly considered. For example, testing the business' ability to continue operating following a significant business continuity event, low liquidity, or a breach of desired surplus above capital adequacy.

Finally, the relevant risk management Prudential Standards and Prudential Practice Guides provide a benchmark, and mandatory considerations in certain cases, for the key components of an ERM framework. As a result, the Appointed Actuary should ensure that he or she has a good understanding of the process used to review compliance with these Prudential Standards and relevant Prudential Practice Guides, with a view to ensuring that the compliance process is appropriate and effective in identifying any potential gaps.

Inevitably, any opinion on a company's risk management framework is a matter of judgment, but that judgment should be reasonably formed and clearly articulated.

3.4 Forming a view about a company's risk management framework

An Appointed Actuary may form the view that a company's risk management framework is materially inadequate or unsuitable. Such a view will necessarily be based on judgment and is not a simple conclusion.

Alternatively, the Appointed Actuary may conclude that part of the risk management framework is adequate, whilst some components have weaknesses that should be enhanced. Having noted this, risks do not function in isolation, and control deficiencies in one area may suggest control weaknesses in other areas, or a heightened level of risk in one, or more, parts of the company. The Appointed Actuary needs to form a holistic view of the suitability and adequacy of the company's risk management framework and the consistency of the "risk-aware" control environment is one important element in forming such a view.

A way to consider the appropriateness of controls and capabilities may be to consider how well risks have been identified, reported and managed previously. For example:

- how well have "warning signals" or "alarm bells" of events been communicated?
- how rapidly were these escalated and addressed?
- has the process for reporting and managing new risks been effective?
- how frequently, or materially, have risks in excess of the company's risk tolerance arisen?
- how well have risks or incidents been reported?
- have there been material control failures during the year?
- have the follow up remedial actions and learnings been implemented adequately?

Even if no material issues have arisen during the year, the Appointed Actuary might consider the company's ability to effectively respond to emerging risks.

If the Appointed Actuary begins to form the view that the company's risk management framework is materially inadequate or unsuitable, it would normally be appropriate to raise questions with those individuals responsible for the inadequacy at the earliest opportunity – to reduce any potential misunderstanding and to provide context.

If the Appointed Actuary does form a view that there are material inadequacies, then particular care will be needed to effectively communicate this within the company, and to APRA if required (see the following section). Actuaries may find it useful to seek advice, or a

second opinion, from a senior actuary or other specialist especially if their views may prove controversial. Although responsibility for any areas of concern may lie with other staff members within the company, and ultimately with the Board, the Appointed Actuary should seek to play an appropriate role in facilitating an improvement to the company's risk management framework. For example, it may be appropriate to develop an action plan and closely monitor its progress.

3.5 Communicating the results of the review to the Board and APRA

In communicating the results of the review to the Board and to APRA, the Appointed Actuary should seek to demonstrate the process and diligence used to support their opinion. This might be addressed by:

- outlining the process used to conduct the review;
- providing an update on items raised in previous reviews;
- demonstrating an understanding of new items that have emerged over the year, cross-referencing these items with other parts of the Financial Condition Report; and
- clearly highlighting areas where improvements have been made over the year, and enhancements that might be made in the future.

The Board should be encouraged to view the Appointed Actuary's assessment of the risk management framework as one that complements that of internal and external audits, as well as an opportunity for the Appointed Actuary to highlight potential areas of concern.

3.6 Conflicts of interest

There is a potential for a conflict of interest to arise as the Appointed Actuary reviews the suitability and adequacy of the company's risk management framework. This might arise where the Appointed Actuary also has a role in the design and implementation of the framework, notably if they are also acting as a Chief Risk Officer. With respect to this assessment, this may be managed via:

- appropriate disclosure of the conflict; and
- independent reviews of the risk management framework.

Annexure A: ERM responsibilities of Appointed Actuaries and actuarial staff

A.1 Mandatory requirements for risk management

APRA's Prudential Standards LPS 220, GPS 310 and GPS 220 aim to ensure that a company maintains a risk management framework and strategy that is appropriate to the nature and scale of its operations.

The prime responsibility for the risk management framework and strategy rests with the Board of directors of the company or, in the case of an eligible foreign company, with the Compliance Committee.

LPS 220 states that "The Appointed Actuary must include an assessment of the suitability and adequacy of the risk management framework as part of the Financial Condition Report".

For general insurers, GPS 310 requires the Appointed Actuary to prepare a Financial Condition Report, which must include a "high-level assessment of the suitability and adequacy of the risk management framework (as defined in GPS 220)".

Whilst this Information Note aims to assist in providing support to Appointed Actuaries in making this assessment, it is noted that there are a number of statutory requirements in LPS 220, GPS 310 and GPS 220 that must be complied with, and the reader is encouraged to review the requirements of these Prudential Standards in more detail.

A.2 Role of the actuary in risk management

Actuaries are concerned with the financial soundness of institutions and their ability to meet their obligations to policyholders, as well as acting as trusted advisers to businesses. As such, actuaries should be concerned with the risks that could adversely affect the company's ability to meet these obligations, and that could adversely affect business objectives and strategic plans.

Actuaries are well placed due to their training and technical capabilities to serve a valuable role in ERM, and to make important contributions to protect the financial soundness of institutions. This includes considerations relating to the identification, analysis, evaluation and reporting of risks. Consideration should be given to upside risk (the sound management of business opportunities) as well as downside risks, along with risks which are not directly quantifiable. Whilst not part of the traditional role of an actuary, a valuable contribution can be made in the recommendation of appropriate management responses.

A.3 Role of the Appointed Actuary in risk management

The main requirement of the Appointed Actuary is to include an assessment of the suitability and adequacy of the risk management framework, as part of the annual investigation of the company's financial condition. The Appointed Actuary should ensure that he or she uses a sound process to support this opinion.

A.4 Actuarial risk management within legal and prudential frameworks within Australia

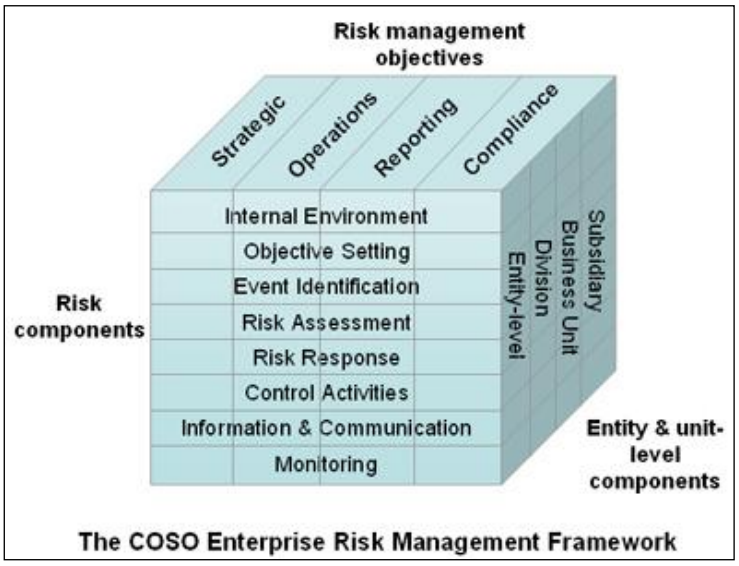
Risk management has long been a feature of the actuary's role within the Australian insurance industry. However, it historically related to the Appointed Actuary's assessment of the company's ability to meet financial obligations to policyholders, and as part of actuarial advice regarding the terms and conditions of products, pricing, reserving and reinsurance.

Annexure B: Enterprise risk management frameworks

Some common ERM frameworks are described below. These may provide useful reference points in assessing a company's risk management framework.

B.1 COSO ERM framework

The Committee of Sponsoring Organisations of the Treadway Commissions ("COSO") is an American private sector organisation sponsored by professional accounting associations. It has issued a set of definitions and standards against which organisations can assess their internal control systems. ERM is defined by COSO as "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."



The COSO Enterprise Risk Management Framework

B.2 ISO 31000

The International Organisation for Standardisation is an international standard setting body that has issued a set of standards relating to risk management known as ISO 31000. The purpose of ISO 31000 is to provide principles and generic guidelines on risk management.

ISO 31000 seeks to provide a universally recognised paradigm for practitioners and companies employing risk management processes.

B.3 CAS ERM framework

The US Casualty Actuarial Society adopted an ERM framework addressing hazard, financial, operational and strategic risks. ERM is defined as "the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders".

ERM Framework				
	Types of Risk			
Process Steps	Hazard	Financial	Operational	Strategic
Establish Context				
Identify Risks				
Analyze/Quantify Risks				
Integrate Risks				
Assess/Prioritize Risks				
Treat/Exploit Risks				
Monitor & Review				

B.4 Three lines of defence model

The three lines of defence model is used across a variety of industries and situations, and primarily relates to governance across organisations:

- First line: the day to day running of the business, and includes management and staff.
- Second line: the monitoring of the business via risk, control and monitoring functions.
- Third line: independent internal and external assurance processes.

END OF INFORMATION NOTE