RISK MANAGEMENT PRACTICE COMMITTEE

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

November 2012

Contents

1. About this Information Note

This Information Note was first published in September 2011 and was prepared by the Professional Standards Sub-committee of the Risk Management Practice Committee of the Actuaries Institute ("Institute"). It was updated, and released as an Exposure Draft for comment, in June 2012, and finalised in November 2012.

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) ("GPS 310"), and their related APRA Prudential Practice Guides. The Information Note outlines how Appointed Actuaries and actuaries in general, might satisfy themselves as to the suitability and adequacy 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. Actuarial input to shaping sound risk management and governance processes can contribute to protecting companies against a wide range of potential adverse scenarios, as well as assisting companies in taking advantage of opportunities as they arise.

It is intended that this Information Note will be developed into a Practice Guideline once greater consistency in actuarial practices in the review of risk management frameworks is achieved, and following further industry consultation.

2. Background

2.1 Purpose of this Information Note

The purpose of this Information Note is to provide information for life and general insurers' Appointed Actuaries and their support staff to consider in assessing the suitability and adequacy of their company's risk management framework, as required by APRA's risk management Prudential Standards (LPS 220 and GPS 220).

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 the Appointed Actuary is strongly encouraged to consider in forming this opinion.

While it is not a regulatory requirement (at this time) for superannuation, banking or health 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, banking and health are beyond the scope of this Information Note, actuaries may find the principles articulated in this Information Note useful in their work.

Any additional requirements imposed by any other Prudential Standard or Prudential Practice Guide, or any professional standard, including any other requirement for the Appointed Actuary to comment on the entity's risk management framework or Risk Management Strategy are outside the scope of this Information Note. 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 provides a level of financial security for policyholders, sound risk management and 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 that is suitable and adequate for the nature and scale of their operations.

It is recognised that large, diverse financial institutions, as well as businesses that are fundamentally complex in nature, 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. The Institute defines this concept as:

> "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 the 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 and roles of Appointed Actuaries and actuarial staff, and Annexure B outlines some examples 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 and providing an opinion on the suitability and adequacy of a company's risk management framework.

3.2 ERM frameworks

The Institute's definition of ERM is set out in Section 2.3 above. As outlined in LPS 220 and GPS 220, APRA describes a risk management framework as "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 [an insurer's] operations". In assessing the suitability and adequacy of a company's ERM framework, the Appointed Actuary is strongly encouraged to 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 conditions.

Some common ERM frameworks are described in Annexure B. 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 Appointed Actuary is encouraged to adopt a method that reflects the company's risk management framework, the size and complexity of the business, and also provides a reasonable basis for supporting the Appointed Actuary's opinion. Appointed Actuaries should come to their own views on what constitutes a suitable and adequate framework.

In forming their opinions, Appointed Actuaries are strongly encouraged to consider, but not be limited to, the following:

Risk appetite and related concepts

- The company's **risk appetite** (for example, as documented in a risk appetite statement). The Appointed Actuary is encouraged to be familiar with the level of executive and Board engagement in determining risk appetite, the determination of consistent risk tolerances, the reporting of exposures relative to those tolerances, and the proactive management and reporting of breaches across the business.

- The way in which the company's **capital models** are integrated with the business's risk appetite and risk limits.

- The **alignment of risk appetite, risk assessment, monitoring and capital management processes** and the links to the **company's business plan and strategic objectives**. In particular, risk management and capital management processes should inform one another and there should be clear linkages between them.

Risk management processes

- The findings of **internal reviews** (for example, audit reviews, regular or ad hoc) and the outcomes of **material incidents** that have arisen. However, as discussed further in Section 3.5, a review of the operating effectiveness of the risk management framework will typically not be performed by the Appointed Actuary for the purpose of LPS 220 and GPS 220.

- The **company's Risk Management Strategy and policy**. The Risk Management Strategy needs to meet the requirements of LPS 220 or GPS 220, and a company's risk management policies should be subject to regular review, implemented, and adhered to, across the business.

- The **processes, procedures, documentation and systems used** to support the operation of the risk management framework, including those used to identify, assess, mitigate and monitor all internal and external risks. This should have regard to past material issues and the extent to which risk management processes are intuitive and embedded in key decision making processes.

- The **processes used to inform the Board and senior management** of risk management issues, policies and practices within the company. Does the insurer monitor its risk profile? Are suitable and adequate processes and procedures in place and consistently adhered to, and do they function in a timely manner? What is the materiality level at which potential issues are escalated? What is the level of oversight of the Board when it comes to risk management?

- Consideration of **ongoing reporting and monitoring requirements**. In doing so, Appointed Actuaries could consider the reporting of business performance, ongoing control assurance processes, the execution of internal audit and assurance programs, progress updates on initiatives, reporting on key risk indicators, material business risks, regulatory activity, capital requirements and so on.

Culture and capability

- The **risk management culture** and **level of staff engagement** across the business. This may include considering: how staff perceive and interact with the risk management framework; how this relationship influences the speed, transparency and management of risks escalated through the governance structure; how the organisation responds to "bad news"; use of post-implementation reviews when new processes or change management programs are implemented; and whether key lessons learned from previous issues are identified and reflected in the risk management framework.

  Other relevant items might include the proactive management of key risks, the level of awareness and training provided to the business.

- The management of **conflicts of interest**, where the interests of staff or entities within a group may not be aligned with one another, or with the interests of customers. Policies and supporting processes should be in place, well understood and adhered to, and be subject to regular independent assurance.

- **Risk management responsibilities and the structure of the risk management function**. The ownership of risks should be clear and governance frameworks should be understood and effective, clearly reflecting relevant roles and responsibilities and ensuring an appropriate level of independent oversight, challenge and assurance. The risk management function's structure and reporting lines should reflect the activities required and performed. Where appropriate, for material risks, a "three lines of

defence" approach may assist in clarifying roles and responsibilities, and for creating a segregation of duties between those actively managing risk and those responsible for independent oversight, challenge and assurance to management and boards. This approach is briefly described in Annexure B.4.

- **Risk management capabilities within functional units and within the specialist risk management function**. Do the functional units and specialist risk management functions have the skills, authority, level of independence, remuneration structures and incentives needed to perform their roles? The sufficiency of resourcing, the capability of people, and the use of technology are all relevant.

Risk management issues and exposures

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

- **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 are all relevant.

- **Internal and external views, where relevant, on the company's risk management framework from those involved in monitoring risks and controls** – for example, views of functional unit heads, compliance and operational risk managers, the Chief Risk Officer and internal audit on the adequacy of the framework. Specific matters recommended to be discussed with such staff include details on material incidents and "near misses", insights into their ERM concerns, views on opportunities for improvement, risk culture, and the risk awareness of the executive team and the Board.

- The **risks to which a company is exposed or contributes**. The potential for losses 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.

- The **fundamental complexity of the business**, and how this in itself impacts on risk management.

- The approach the company takes to **horizon-scanning**, including both emerging risks and risk events that have impacted other relevant companies. As a test of the risk management framework, the Appointed Actuary may themselves consider any publicly-reported major risk incidents that have occurred to other relevant organisations, including what controls are in place to prevent or mitigate such incidents, if the same set of circumstances were to occur within their company.

- The company's **response to the identification and potential impact of "extreme" events**. An Appointed Actuary might assess whether scenario analysis, or the stress testing, of plausible but "extreme" events is considered and an assessment made of the business's ability to continue operating following such events. Examples of events may include a 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, it is important that the Appointed Actuary 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 identifies any potential gaps.

An opinion on a company's risk management framework is a matter of judgment. It is considered good actuarial practice that the judgment should be reasonably formed, supportable, and be clearly articulated (as discussed in Sections 3.4 and 3.5 below).

3.4 Forming an objective opinion on a company's risk management framework

Good actuarial practice is that an Appointed Actuary forms an objective opinion on a company's risk management framework, and outlines the process adopted in determining such an opinion.

The Appointed Actuary may form an opinion 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 is encouraged to form a holistic view of the suitability and adequacy of the company's risk management framework and the control environment is one important element in forming such a view.

A way to assess the extent of this risk awareness may be to consider how well risks have been identified, quantified, reported and managed. For example:

- how clearly can the Board articulate the top risks the organisation faces?
- 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 insights been implemented adequately?
- how frequently and by what method have the risks been quantified?

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 opinion 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, to provide context, and to ensure that the company has the ability to respond in a timely and appropriate manner. There may be situations where the Appointed Actuary disagrees with management, in which case it may be appropriate to document management's view in the Financial Condition Report.

If the Appointed Actuary does form an opinion that there are material inadequacies, then particular care will be needed to effectively communicate this within the company (see Section 3.5). 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 company staff, and ultimately with the Board, the Appointed Actuary is encouraged to seek to play an appropriate role in facilitating improvements to the company's risk management framework. For example, it may be appropriate to support the company in developing an action plan and closely monitoring its implementation.

If the Appointed Actuary feels their exposure or interaction with the Risk Management Strategy is such as to limit their ability to perform a review, provide an opinion, or recommend improvements on the risk management framework, they are encouraged to seek to ensure suitably skilled staff are made available to conduct such a review, subject to the Appointed Actuary being comfortable with the scope of, and taking ultimate responsibility for, the resulting review and opinion. For an external Appointed Actuary, it is recognised that it may be more difficult to identify suitably skilled staff.

Conversely, where the Appointed Actuary has not had suitable access to enable a review of the risk management framework, or has been unable to access suitably skilled staff to review

aspects of the framework, they are strongly encouraged to document the potential limitations on their opinion and may need to consider their ability to continue with the engagement.

3.5 Communicating the Appointed Actuary's opinion to the Board

In communicating their opinion to the Board, the Appointed Actuary is encouraged to:

- briefly outline the process and diligence used to support their opinion. This could be addressed by outlining the process adopted in conducting the review of the risk management framework, noting the considerations outlined in Section 3.3, and disclosing any material departures from Section 3.3, as well as any potential limitations on the opinion provided;

- ensure that the documentation on the process used to support their opinion does not detract from the results of the review, the opinion provided, or any recommended improvements, by considering the needs of the audience and not providing excessive detail. Where appropriate, further detail on the process adopted and the results of the review might be disclosed in an appendix or the Appointed Actuary's working papers;

- provide an update on items and recommended improvements raised in previous reviews;

- demonstrate an understanding of new items that have emerged over the year, cross-referencing these items with other relevant parts of the Financial Condition Report;

- clearly highlight areas where improvements have been made over the year, and improvements that are recommended for the future; and

- identify and document any barriers that have impeded the Appointed Actuary in conducting the review and the resulting limitations on the opinion.

It is important that the scope of the Appointed Actuary's opinion regarding the suitability and adequacy of the risk management framework is clearly understood. In particular, whilst the Appointed Actuary would review material incidents that have arisen over the year, for the purposes of LPS 220 and GPS 220, a review of the operating effectiveness of the risk management framework will typically not be performed by the Appointed Actuary. For the avoidance of doubt, and to avoid misunderstanding, this limitation on the scope of the review and the opinion provided could be documented.

Subject to this potential limitation, the Board is encouraged to view the Appointed Actuary's assessment and opinion as one that supplements 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 for an Appointed Actuary. The presence of a conflict of interest may depend on how an Appointed Actuary has been involved in prior activities that are subsequently related to a later activity. This may involve multiple occasions of involvement with a product, business process or other activity.

Potential examples include involvement in:

- product development/pricing and the subsequent valuation of those product liabilities;
- recommending reinsurance structures and/or asset-liability structures and subsequent capital requirement assessments; and
- the design/ implementation of the risk management framework and subsequent review of the suitability and adequacy of the company's risk management framework. For example, the Appointed Actuary may have a role in the oversight of risk across the business and/or is acting as a Chief Risk Officer.

In these examples, the potential conflict of interest may be managed via:

- making appropriate disclosure of the conflict and any resulting limitations on the opinion; and
- seeking, or placing reliance on, other independent reviews of the risk management framework.

Members are reminded that any such conflict of interest must be managed in accordance with the Institute's Code of Professional Conduct.

Annexure A: ERM responsibilities and roles 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 suitable and adequate for 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.

For life insurers, LPS 220 states that "[t]he 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 currently 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 strongly 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 are encouraged to develop an understanding of the risks that could adversely affect the company's ability to meet these obligations, and that could adversely affect business objectives and strategic plans.

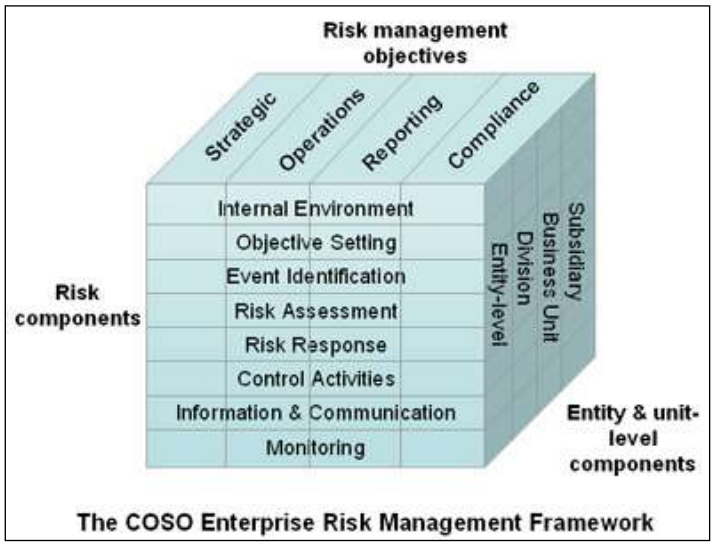
Actuaries are well placed due to their training and technical capabilities to serve a valuable role in ERM, and to make important contributions to protect the financial soundness of institutions. This includes considerations relating to the identification, analysis, evaluation and reporting of risks.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

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 Commission ("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."[1]



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.

---

[1] Committee of Sponsoring Organisations of the Treadway Commission, "Enterprise Risk Management – Integrated Framework", Executive Summary, September 2004, page 2 (available at: http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf).

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".[2]

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				

[3]

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

2 Casualty Actuarial Society, "Overview of Enterprise Risk Management", May 2003, page 8 (available at: http://www.casact.org/research/erm/overview.pdf).

3 *Id*, page 9.