RISK MANAGEMENT PRACTICE COMMITTEE
EXPOSURE DRAFT
Information Note: Actuarial Advice regarding Risk Management

May 2019

Contents

1. About this Information Note

This Information Note supersedes the previous document dated November 2012.

This Information Note does not represent a Professional Standard or Practice Guideline of the Institute. It has been prepared to assist Actuaries in their roles of providing advice in relation to risk management frameworks, as required under APRA Prudential Standards:

- GPS 110 (Capital Adequacy) (issued in January 2015) ("GPS 110");
- CPS 220 (Risk Management) (issued in July 2017) ("CPS 220");
- CPS 320 (Actuarial and Related Matters) (to be effective July 2019) ("CPS 320"); and
- APRA Prudential Practice Guides related to these documents.

The Information Note is also intended to assist actuaries in general on how they might provide advice on their organisations' risk management frameworks and to assist those actuaries who perform Chief Risk Officer or equivalent roles.

2. Background

2.1 Purpose of this Information Note

APRA defines an APRA regulated institution's risk management framework as follows:

> "the risk management framework is the totality of systems, structures, policies, processes and people within an institution that identify, measure, evaluate, monitor, report and control or mitigate all internal and external sources of material risk. Material risks are those that could have a material impact, both financial and non-financial on the institution all internal or on the interests of depositors and/or policyholders."

Paragraph 26 of CPS 220 describes Material Risks.

As part of assessing the financial condition under CPS 320, a life, health, or general insurance Appointed Actuary must make general observations on the overall risk management framework, with a focus on financial risks, and how these risks are managed by the insurer.

Actuaries may also be engaged to carry out an independent review of an institution's Internal Capital Adequacy Assessment Process (ICAAP) under paragraph 13 of GPS 110, and/ or an independent comprehensive review of an institution's risk management framework under paragraph 45 of CPS 220.

The ICAAP review requires an opinion "on whether the ICAAP is adequate and effective", and the CPS 220 review requires a comprehensive review on "the appropriateness, effectiveness and adequacy of the institution's risk management framework".

Under paragraph 47 of CPS 220, the independent comprehensive review of the risk management framework must, at a minimum, assess whether:

- The framework is implemented and effective;
- It remains appropriate, taking into account the current business plan;
- It remains consistent with the Board's risk appetite;
- It is supported by adequate resources; and
- The RMS adequately documents the key elements of the risk management framework that give effect to the strategy for managing risk.

This Information Note outlines a number of issues that the Actuary is encouraged to consider in forming these opinions.

While it is not a regulatory requirement (at this time) for superannuation actuaries to assess the suitability of risk management frameworks, these actuaries may find the principles articulated in this Information Note useful in their work.

3. Considerations in advising on risk management frameworks

3.1 Assessing the suitability, adequacy and effectiveness of a company's risk management framework

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

Risk appetite and related concepts

- The company's **risk appetite** (as documented in its Risk Appetite Statement). The Actuary should 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 since the previous review.

- The **company's Risk Management Strategy and policy**. The Risk Management Strategy needs to meet the requirements of CPS 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, 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, 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.

- **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 the **previous risk management review**, to ensure these have been addressed in a timely manner.

- **Key risk management issues that have emerged** since the last review, 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 breadth and 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 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**. The 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 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.

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

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

The 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 Actuary may conclude that part of the risk management framework is adequate, whilst some components have weaknesses that should be enhanced. However, 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 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 Actuary might consider the company's ability to effectively respond to emerging risks.

If the 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 Actuary disagrees with management, in which case it may be appropriate to document management's view in the review documentation.

If the 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 3.3). 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 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 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 Actuary being comfortable with the scope of, and taking ultimate responsibility for, the resulting review and opinion. For an external Actuary, it is recognised that it may be more difficult to identify suitably skilled staff.

Conversely, where the 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.

3.3 Communicating the Actuary's opinion within the Company and to the Board

In communicating their opinion, the 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 3.2, and disclosing any material departures from Section 3.2, 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 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 since the previous review, where appropriate cross-referencing these items with relevant parts of the previous review report;
- clearly highlight areas where improvements have been made since the previous review, and improvements that are recommended for the future; and
- identify and document any barriers that have impeded the Actuary in conducting the review and the resulting limitations on the opinion.

It is important that the scope of the Actuary's opinion is clearly understood. For the avoidance of doubt, and to avoid misunderstanding, any limitations on the scope of the review and the opinion provided should be documented.

3.4 Conflicts of interest

There is a potential for a conflict of interest to arise for an Actuary. The presence of a conflict of interest may depend on how an 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 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.