INSURANCE COUNCIL OF AUSTRALIA

Mr Neil Grummitt
General Manager, Policy Development
Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001

Email: riskmanagement@apra.gov.au

10 July 2013

Dear Mr Grummitt

HARMONISING CROSS-INDUSTRY RISK MANAGEMENT REQUIREMENTS

The Insurance Council of Australia (Insurance Council) welcomes the opportunity to comment on APRA's consultation package on harmonising cross-industry risk management requirements. The Insurance Council shares APRA's commitment to ensuring that risk management plays its part in providing protection for Australian policyholders and strongly supports the maintenance of effective risk management practices by its members.

However, the Insurance Council is concerned that there are many elements in CPS 220 and CPS 510 that would require the abandonment or severe modification by its members of established risk management practices for no appreciable improvement in policyholder security. The Discussion Paper on harmonising cross-industry risk management requirements (the Discussion Paper) refers to enhancements made in response to lessons learned during the Global Financial Crisis. The Insurance Council is unaware from comments that APRA made during the crisis, or subsequently, of significant weaknesses being identified in the risk management framework of Australian general insurers which would justify the heavily prescriptive measures proposed.

Prudential Standards should be principles based.

The Insurance Council and its members are concerned with the heavily prescriptive nature of the draft Prudential Standards. In the Executive Summary (page 6) of the Discussion Paper, APRA states that it will "maintain its principles-based approach to the application of its risk management requirements". The Insurance Council strongly endorses this intention.

The proposed standard contains a great deal of detail that gives little flexibility to optimise risk management practices. The unnecessarily prescriptive requirements include:

- the detailing of business structures, roles and/or reporting lines (discussed in more detail below);
- the excessive level of detail prescribed for the risk systems (MIS), Risk Appetite requirement and frequency of independent reviews for the Risk Management Framework;
- no compelling rationale for the separation of Board Audit and Risk Committees; and
- the excessive detail specified in the Policy and Procedure requirement.

Need to recognise sectoral differences between Insurance and Banking

The Insurance Council understands the advantages that may flow from consolidated prudential standards which apply across financial services sectors. However, the Insurance Council considers that APRA, in relation to CPS 220, has underestimated the differences in the risks faced by banks and general insurers. This manifests itself in requirements to consider and manage particular risks that are excessive and unnecessary for a general insurer.

For example, while liquidity risk may be a key risk for an ADI, the equivalent for a general insurer would be asset and liability matching. Similarly, the focus on the risk function, in particular the requirement for a stand-alone Chief Risk Officer (CRO), does not take into account that risk management is core to the business of a general insurer, and therefore the responsibility of a range of executive positions. Furthermore, whereas depositor security in banking is tied to the strength of the ADI, the ability to pay policyholder claims is not necessarily determined by the commercial viability of the insurer.

The Insurance Council recognises that APRA understands that, unlike banks, insurer liabilities cannot be called upon rapidly due to a lack of confidence to result in a "run on the insurers". Moreover, insurers take additional first line measures to mitigate risk, in particular through reinsurance. This leads to insurers' risks being spread more widely, often to global capital markets. As is well understood, bank failures occur much faster and have the scope to be more disorderly than insurance failures.[1]

In view of these sectoral differences, the Insurance Council submits that while it is appropriate for a Prudential Standard to set out principles for effective risk management across financial services, we strongly believe that detailed guidance as to how APRA sees those principles best applied to the general insurance industry should be provided in a sector specific Prudential Guide**.**

Attachment A gives a small sample of the issues raised by Insurance Council members as needing clarification. If APRA persists in setting out detailed obligations in the prudential standard, thorough vetting of its provisions in co-operation with industry will be essential in order to avoid unintended consequences.

Concerns with the mandatory CRO position and related provisions

As explained above, the Insurance Council and its members recognise the importance of sound risk governance. However, we urge APRA to consider that imposing the proposed mandatory CRO structure and related provisions regardless of the circumstances of individual insurers could in fact harm an organisation's ability to mitigate risk, rather than improve it. (See following paragraphs for specific examples.) The ICA considers that it should be left to the Board to decide on the need for a dedicated CRO (and if so, the appropriate reporting lines) in light of the organisation's circumstances. If APRA wishes to advocate the advantages of particular structures, it should be done through the relevant Prudential Guide.

[1] IFF, "The Implications of Financial Regulatory Reform for the Insurance Industry" p 6 , 2011

Lack of additional benefit from a CRO

There is general industry scepticism about the additional benefit from the establishment of a stand-alone CRO position, in light of the widespread emphasis that the senior management of a general insurer gives to risk management as explained above. The addition of a CRO may merely result in a doubling up of roles, increasing staffing overheads while creating overlapping responsibilities and confusion that may actually hinder an organisation's effectiveness in addressing risk.

CRO prohibition on 'dual-hatting'

The prohibition on 'dual-hatting' imposes a cost for all general insurers, and many would find the burden of maintaining a stand-alone CRO position particularly difficult. It is important to keep in mind that some insurers may only have a handful of staff, and an additional FTE at a senior level would add a considerable cost to staff overheads.

The Insurance Council considers that there are a number of advantages from permitting the CRO to also hold the position of CFO or Appointed Actuary (AA) that have not been acknowledged in the discussion paper. The combination of a CRO and CFO (or AA) can complement the risk culture of an organisation rather than lead to a conflict of interest.

Our members have identified that linking capital management responsibilities (the AA and CFO) with the risk management responsibilities (CRO), can lead to a stronger risk culture and deeper risk management capability. However, due to the need for audit independence, the Insurance Council would agree that the CRO should not also be the Head of Internal Audit.

CRO should be required to be "objective" rather than "independent"

In light of their commercial experience, Insurance Council members consider that it is undesirable for a CRO to have complete independence from business lines, financial function and other revenue generating responsibilities (Paragraph 39). CROs need to have some integration into the business in order to understand key issues.

The requirement of independence through structures and reporting lines can also inhibit the influence or sharing a stake in the organisation that is an enabler of current successful Head of Risk roles. Many Head of Risk roles also have compliance framework responsibilities. These require closer interaction with the operational managers than the oversight role implied by the independence requirement in the draft CPS.

Accordingly, the Insurance Council proposes that "independent" be changed to "objective" in Paragraph 39.

Challenge to find a CRO with the appropriate skill set and qualifications

Insurers are likely to face difficulty in finding appropriate candidates with the required experience, skill set and qualifications. For many insurers, a CRO position would not be a full-time role, and for smaller insurers, may not even have the work to form an acceptable part-time position. The attraction for many managers in working with a small insurer is the range of responsibilities they have. The requirement for a stand-alone CRO position coupled with the restriction on dual hatting may lead to insurers being forced to recruit sub-standard personnel for the CRO role, which would obviously be a poor outcome.

CRO should not be required to have a direct reporting line to the CEO

We consider that this rigid requirement may be incompatible for the optimal risk management function for some insurers. It may suit some insurers for the CRO to have a direct report to the CEO but the mandatory nature of this proposal could lead to a cluttering of reporting lines, where the Head of Risk (or equivalent) does not currently report to the CEO. However, members support the CRO having "unfettered access" to the CEO which would enable the CRO to carry an acceptable degree of authority, without the complexity of a direct reporting line.

The Board Risk Committee should not be required to be separate from the Board Audit Committee

The Insurance Council strongly opposes the proposal to have separate Board Audit and Risk Committees as it would only create unnecessary additional administration and costs without any advantage to the organisation. This proposed position is also inconsistent with existing practices that have been subject to previous APRA approval. We are sceptical that any benefits would be gained from separation, particularly given that APRA is proposing that the composition of the two could be the same. As long as the functions of the Board Risk Committee are fulfilled, it does not matter whether or not they are performed by a separate committee.

The proposed changes are unlikely to improve risk governance and could result in the contrary:

- The enforced separation would inhibit a holistic view of the entire risk landscape faced by a regulated institution unless there is a high level of duplication between the work of the two committees;
- Excluding the discussion of audit and financial issues from a Board Risk Committee would:
    - provide them with an incomplete oversight of all types of risk:
    - cause practical issues for the chair of the Board Risk Committee who has to be one of the signatories to the Risk Management Declaration;
- It is proposed that the Audit Committee retain the responsibility to assist *"…the Board by providing an objective non-executive review of the effectiveness of the institution's or group's financial reporting and risk management framework"* even though there would be a dedicated Board Risk Committee and the chair of the Board Risk Committee must be one of the signatories to the Risk Management Declaration;
- Similarly, the proposal is for the annual independent reviews of the Risk Management Framework to be reported to the Board Audit Committee whilst the three yearly comprehensive independent reviews must be reported to the Board Risk Committee.

The Insurance Council therefore submits that it should be left to the judgement of the Board whether separate Risk and Audit Committees are appropriate for that particular general insurer.

The prudential standard should use "reasonable steps" instead of "ensure"

The Insurance Council supports the need for Boards of regulated entities to have ownership and oversight of risk appetite. However, as raised in the Insurance Council's previous submission of 20 May 2013, members remain concerned about APRA's requirement for Boards to "ensure" a range of outcomes. This sets a high, and largely unattainable, threshold for Boards as the word "ensure" is uniformly taken to mean "to make sure or to make certain".

The Board of an insurer is not in a position to make sure or certain that the requirements set out in paragraph 12 (a)-(h) are satisfied. While Boards can be required to take all reasonable steps to facilitate a particular outcome, even the most expert Board could not "**ensure**", a specific result, such as a "risk culture" as specified in 12(b). The Insurance Council therefore considers that to place such a requirement on a Board is unrealistic and should be reconsidered.

The Insurance Council considers that this issue can be resolved through amending the wording in paragraph 12 from the Board being required to take "reasonable steps" to have these things done. This will result in the requirements being more closely aligned to a Board's responsibilities.[2]

Recognition of the Board's role as distinct from management

The references in paragraph 12(e) and (h) to the Board's requirement to ensure "processes" and controls are established that are consistent with the institution's risk appetite, risk profile and capital strength" appear to blur the lines between Board and management. The Board should approve the risk appetite measures and framework but individual controls are a matter for management and are at a level too detailed for extensive review by the Board.

Implementation timeframe is inadequate

Members are concerned that the changes, particularly the CRO proposals if they proceed, are not achievable in the time frame proposed. Many of the requirements such as those relating to recruitment of a new CRO, changes to risk systems and embedding of Risk Appetite and Risk Tolerances are time consuming activities, particularly in large insurance groups. The proposed changes to the Risk Management Prudential Standards are the most significant since their introduction in 2006 as part of the General Insurance Reforms Stage II.

Implementation will require interpretation of the final Standard/Guide, business analysis of current state of compliance and the establishment of new practices. It will also require Board engagement, including training, approval and finalisation. We are concerned that there is insufficient time to undertake these steps and ensure appropriate implementation.

Furthermore, it is not realistic to propose an effective date for CPS 220 of 1 January 2014, when the APRA response to the Prudential Standard feedback is unlikely to be released before late August or September, with release of a draft Prudential Practice Guide presumably even later.

---

[2] There would be considerable merit in the governance responsibilities for a Board being set out in a single prudential standard rather than have some aspects contained in CPS 510 and other aspects in CPS 220.

The Insurance Council recommends that the effective date be set at least 12 months from the release of the final versions of the Prudential Standards and Prudential Practice Guides with the ability to seek transition relief depending on circumstances.

If you require further information in relation to this submission, please contact Mr John Anning, Insurance Council's General Manager Policy – Regulation Directorate at janning@insurancecouncil.com.au.

Yours sincerely

Robert Whelan
Executive Director & CEO

INSURANCE COUNCIL OF AUSTRALIA

ATTACHMENT A

EXAMPLES OF PROPOSED PROVISIONS THAT REQUIRE CLARIFICATION

CPS 220 (24) Risk Management Framework
Paragraph 24(d) states that:

> "an APRA-regulated institution's risk management framework must, at a minimum, include: policies and procedures supporting clearly defined and documented roles, responsibilities and formal reporting structures for the management of material risks throughout the institution;"

This paragraph could be interpreted as requiring formal policies for each material risk identified in a company's risk profile. The Insurance Council considers that this is excessive and suggests rewording this subsection to clarify the intention is to achieve certainty about who has the accountability for managing each material risk.

Paragraph 24(g) states that:

"An APRA-regulated institution's risk management framework must, at a minimum, include:

> (g) a management information system (MIS) that is adequate, both under normal circumstances and in periods of stress, for measuring, assessing and reporting on all material risks across the institution".

This subsection, together with section 26, could be taken to require an IT system capable of covering each risk category or framework. However, this is contrary to a key principle underlying the standard, that "risk frameworks should be designed according to the size, business mix and complexity of its operations".

The requirement for all insurers to invest in expansive IT systems could involve material cost and resources to replace processes that are deemed by management, the Board and independent reviewers (e.g. internal and external audit) as effective and efficient.

CPS 220 (36)
Paragraph 36 has the potential to turn the existence of a dormant or static company policy into a breach of APRA requirements. Companies establish policies to drive significant decisions (for example on Investment Policy, RMS, ReMS, ICAAP) as well as to aid operational clarity (for example mobile phone acquisition policy, travel purchasing policy).

Accordingly, this section should be amended to apply only to Board approved policies.

CPS 220 (48) – Risk Management Declaration - Qualifications
This paragraph effectively extends past APRA's regulatory remit and in some circumstances would be inconsistent with other legislative requirements on general insurers.

An organisation's risk management framework does not exist solely to address the regulatory requirements of the Insurance Act 1973 and APRA Prudential Standards, but rather covers a range of other external requirements (e.g. AFSL obligations *under the Corporations Act 2001*) and internally set requirements. In some circumstances such as Anti-Money Launderings and Sanctioned Parties an organisation is legally bound to not disclose details to any other party.