



**CHARTERED SECRETARIES
AUSTRALIA**

Leaders in governance

4 July 2013

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

Email: riskmanagement@apra.gov.au

Dear Mr Grummitt

***Harmonising cross-industry risk management requirements:
Discussion paper***

Chartered Secretaries Australia (CSA) is the peak body for over 7,000 governance and risk professionals in Australia. It is the leading independent authority on best practice in board and organisational governance and risk management. Our accredited and internationally recognised education and training offerings are focused on giving governance and risk practitioners the skills they need to improve their organisations' performance.

Members of CSA are all involved in governance, corporate administration, legal practice and regulatory compliance and have a thorough working knowledge of applied governance and risk management frameworks. Our Members are frequently charged with the responsibility of advising boards on these matters, and the amendments to the prudential standards will therefore affect directly those CSA Members who are involved with providing such advice as well as implementing the regulatory and governance frameworks in their organisations.

CSA welcomes, therefore, the opportunity to comment on the Discussion paper: *Harmonising cross-industry risk management requirements* (the discussion paper).

General comments

CSA supports the harmonisation process across APRA-regulated industries to enhance risk management prudential requirements. The consolidation of a cross-industry prudential standard on risk management (CPS 220) that would apply to authorised deposit-taking institutions (ADIs), general insurers and life insurers, and Level 2 and Level 3 groups will strengthen the governance and risk management frameworks for these organisations.

CSA is cognisant that the two key harmonisation and consolidation measures proposed for the prudential standard on risk management and the prudential standard on governance (CPS 510) include:

- amending prudential standard CPS 510 to require institutions regulated by APRA to have a separate board risk committee that provides the board with oversight of the risk management framework, and

- including a requirement in prudential standard CPS 220 that institutions must designate an independent Chief Risk Officer (CRO) position within their organisations, who provides effective challenge to activities and decisions that materially affect the risk profile of the institution.

While CSA supports both of these measures in principle, we stress that there is no one-size-fits-all approach to risk management. We encourage APRA to ensure that the prudential standards for regulated entities are clear on the principles underlying the requirements, while also allowing sufficient flexibility for different types of entities to be able to comply with the prudential standards.

Ensuring flexibility in the prudential standards

CSA supports the mandating of separate board risk committee in CPS 510, but stresses that this view is tied to the financial services sector, which APRA regulates. CSA believes further that due regard must also be given to the existing risk management frameworks that may currently be in place. Sufficient allowance will need to be made to ensure that the sizes and complexities of entities in the financial sector are acknowledged, providing flexibility for organisations to comply with the spirit and intent of the prudential standard rather than 'mandating' compliance.

CSA emphasises, however, that our view should not be extrapolated as our view on the mandating of risk committees more broadly. CSA notes that this condition is not applicable for all entities, but rather limited to the financial services industry. CSA has undertaken research showing that there is no consensus as to whether it is preferable to have a stand-alone risk committee, a combined risk and audit committee or no dedicated committee on the basis that risk management is the responsibility of every board committee.¹

It has been argued that combining audit and risk on the one committee can lead to a backward-looking focus, given that the audit focus is on the oversight of and reporting to the board on the financial accounts and adoption of appropriate accounting policies, internal control, compliance and other matters. The argument for a separate risk committee points to the need for the risk focus to be forward-looking, with a consideration of opportunities and uncertainties with respect to those opportunities. These arguments, however, overlook prospective aspects of financial reporting (the emergence of new risks and changes in existing ones) and the need for risk committees to monitor and review the effectiveness of the controls that a financial services sector entity has put in place.

While there is no one model that is suitable for all organisations, CSA believes that for ADIs, general insurers and life insurers, it is important that the risk management of an entity be dealt with separately from audit, even where both committees may comprise the same membership. Mandating a separate risk committee with a separate agenda, minutes, and action items encourages members of the committee to turn their mind towards specific issues related to both financial and other material business risks, which can be discussed independently from other aspects of board oversight.

Changes to the risk management framework, however, also challenge the current practices and processes of organisations currently regulated by APRA. CSA notes that many APRA-regulated organisations will have already developed significant and complex risk management frameworks which take into account ISO31000/2009: *Risk Management Principles and Guidelines*, and Principle 7 of the Australian Securities Exchange (ASX) Corporate Governance Council's *Corporate Governance Principles and Recommendations* (the Principles and Recommendations) on recognising and managing risk for listed entities.

¹ *Governance and Risk Management Maturity: Indicators and Performance*, Chartered Secretaries Australia and SAI Global, 2010

The requirement for a separate board risk committee proposed by APRA is one which is more prescriptive than the requirements of both the Principles and Recommendations and the prudential standard on governance (SPS 510) for registrable superannuation entities (RSEs).

CSA is cognisant, therefore, that it may not be possible for all regulated entities to set up a separate risk committee comprised of different directors than those sitting on the audit committee. However, as noted above, a separate agenda, minutes and action item will focus the minds of the two committees, even if comprised of the same directors.

In a similar manner, CSA supports, in principle, the requirement for the risk management function of an APRA-regulated institution to be undertaken by a designated Chief Risk Officer (CRO). The appointment of an independent position to provide effective challenge to the activities and decisions of the organisation will strengthen the risk management framework.

CSA is concerned, however, that there is some lack of clarity around how the CRO position will operate in practice. While the importance of the CRO position is recognised, the mandating of a CRO may be problematic for smaller entities that may not have the resources to employ another, senior, independent officer to perform the role. CSA notes that the 'chief' designation implies a senior level of responsibility within an organisation, which may not be consistent with an organisation's structure, pay or business unit separation.

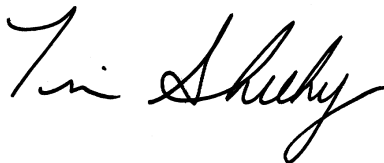
While CSA recognises that APRA will maintain a principles-based approach to the application of its risk management requirements and will, where appropriate, consider exemptions for smaller institutions that can demonstrate they meet, in substance, the principles underlying the requirements; it is important that sufficient flexibility be written into the standards to allow this to occur.

CSA notes that the prudential standards must be worded in a way which ensures that there are no unintended consequences for organisations at the smaller end of the financial services industry. CSA recognises that a majority of APRA-regulated entities will be able to comply with the requirements; however, it is the less resourced organisations that will need flexibility in carrying out the requirements.

CSA reiterates our support for the strengthening of the risk management framework and our support for the initiatives put forward. However, CSA also asks APRA to carefully review and ensure that the prudential standards incorporate sufficient flexibility to enable regulated entities of all sizes to be able to comply with the requirements.

We would welcome the opportunity to discuss any of our views in greater detail.

Yours sincerely

A handwritten signature in black ink, reading "Tim Sheehy". The signature is written in a cursive, flowing style.

Tim Sheehy
CHIEF EXECUTIVE