CUSTOMER OWNED BANKING ASSOCIATION

www.customerownedbanking.asn.au

LEVEL 11, 35 CLARENCE STREET, SYDNEY NSW 2000 GPO BOX 4686, SYDNEY NSW 2001

10 July 2013

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

Dear Mr Grummitt

Harmonising cross-industry risk management requirements

Friendly Societies of Australia (FSA) welcomes the opportunity to comment on APRA's *Harmonising cross-industry risk management requirements* discussion paper released on 9 May. We appreciate the extension of time provided to us to lodge this submission.

The Customer Owned Banking Association is the industry body for Australia's credit unions, building societies, and mutual banks, and through an agreement with the FSA, also represents 12 of Australia's 13 APRA-regulated friendly societies.

Friendly societies are smaller and less complex regulated institutions that have strong risk-management cultures. This is reflected by the fact that APRA proposed to extend the application of the current risk management prudential requirements of the general and life insurance industries to ADIs and Level 2 and Level 3 groups, as reflected in draft *Prudential Standard CPS 220 Risk Management* (CPS 220).[1]

The FSA contends that the current risk management prudential requirements have established a robust, functional and effective risk management framework for its members. In this context, the FSA does not support APRA's proposals for friendly societies to establish a Board Risk Committee and designate a Chief Risk Officer. [2]

In its current form, APRA's proposals will not improve the financial stability of Australia's friendly societies. The cost burden however, imposed by these additional regulations, will undermine the competitive position of our members.

Recommendations

We recognise APRA's broader policy approach of having a single set of prudential standards for all regulated institutions however the standards need to be practical and must be able to accommodate diversity.

The FSA recommends:

- the requirement to designate a Chief Risk Officer (CRO) should not apply to smaller, less complex regulated institutions such as friendly societies; and

[1] APRA, *Harmonising cross-industry risk management requirements,* May 2013, p.3.
[2] *Ibid*

- that APRA removes the prescriptive requirement for the establishment of a separate Board Risk Committee and instead maintain the current flexibility for friendly societies to meet the broader risk management objective within their existing Board Committee frameworks where appropriate.

The prescriptive nature of these obligations is inconsistent with the key requirement set out in the standard that "…an APRA-regulated institution must have a risk management framework that is *appropriate to its size, business mix and complexity,"*[3] (emphasis added).

As currently drafted, the prudential standard presupposes that there is one business model which would be best practice for all friendly societies, and is strongly contrasted with the "principles-based approach" which is evident in most parts of the current prudential regime.

We submit that the current risk management framework provides the flexibility to enable our members to achieve these outcomes in a manner tailored to their size, business mix and complexity.

The FSA believes the current risk management framework will not be enhanced, and that risks will not be mitigated, by compelling friendly societies to designate a CRO and Board Risk Committee.

The rationale for the additional risk management obligations proposed by APRA is unclear. The discussion paper simply states that the new requirements reflect APRA's heightened expectations and "in some respects … underpin the improvements that have been made … in response to lessons learned in the global financial crisis." The discussion paper goes on to state that prudential supervisors are working to address the "serious shortcomings in the governance and risk management of *major global financial institutions*…" (emphasis added). In supporting the need for enhancements in this area, APRA's Chair has also cited[4] the Financial Stability Board's (FSB) observation that "… weak risk controls at financial institutions are still being witnessed and there remains room for improvement in supervision to ensure that it is effective, proactive and outcomes-focussed."[5] However, we note that the FSB made this observation in relation to systemically important financial institutions.

None of this explains why these additional obligations are appropriate in an Australian context, nor does it provide any detail of the types of problems these new obligations would address. Certainly, there has been no context provided on why blanket application of these requirements to friendly societies is appropriate.

While we note that the prudential standard currently provides some supervisory discretion in the application of the new requirements, an explicit carve-out from the draft standard which recognises the existing differentiation of friendly societies would provide our members with greater certainty.

The Chief Risk Officer

Paragraph 38 of the draft standard states that, "an APRA-regulated institution's risk management function must be headed by a designated Chief Risk Officer (CRO)."

The costs of this proposal will fall disproportionately on smaller regulated institutions. For large ADIs which already employ a CRO, the inclusion of this new requirement in the prudential standard will impose no additional cost. In contrast, for friendly

[3] APRA, *Draft Prudential Standard CPS 220 – Risk Management,* May 2013, p. 1.
[4] Laker, *The importance of good governance,* 27 Feb 2013, p. 10.
[5] Financial Stability Board, *Increasing the Intensity and Effectiveness of SIFI Supervision*, Progress Report to the G-20 Ministers and Governors, p. 1.

societies which do not currently engage a CRO, meeting this obligation will be prohibitively expensive.

APRA's proposal states that the CRO cannot be the Chief Executive Officer (CEO), Chief Financial Officer (CFO) or the Head of Internal Audit.[6] This restriction will force our members to engage an additional employee.

Having to employ an additional staff member to meet this prudential requirement would be a significant cost burden. We note that the CROs employed by the largest ADIs attract remuneration packages of more than $2 million. While the costs to our members of filling a similar role would be lower, filling this position would nonetheless represent a sizable financial impost.

In addition to the direct costs of engaging an additional employee, complying with this obligation will impose other related costs on our members, such as restructuring internal reporting lines and putting new procedures and processes in place to integrate with the new position.

For some of our members, absorbing additional costs of this magnitude would have a significant impact on their profitability. This would in turn impact on their financial stability. In addition to the direct cost concerns around the proposal, there are other aspects around its implementation which we believe warrant further consideration:

- We question the degree to which the appointment of a CRO would assist with "instilling an appropriate risk culture across the institution."[7] Creating a dedicated position with responsibility for risk management creates a risk that the rest of the organisation will see risk issues as "someone else's problem". The engagement of a dedicated CRO may compartmentalise risk management, and potentially compromise outcomes, which is completely contrary to the broader policy objective of the draft standard.

- There is a risk that the existence of a CRO could encourage Boards to give less focus to risk issues, by creating a perception that these matters are already being adequately taken care of elsewhere.

- The current system of risk management is based on the primacy of the Board of Directors in setting and monitoring the friendly society's attitude to risk, with input from both internal and external audit. The requirement to engage an independent CRO introduces a "policeman" to sit between the Board and Senior Management. Taking this approach to its logical conclusion, should we also expect ADIs to engage someone to monitor the CRO and ensure that they're doing their job properly?

- There is a risk that the prescriptive nature of the proposal leads to box-ticking to achieve compliance with the standard rather than leading to improved risk management outcomes.

The FSA is concerned about APRA imposing such a significant burden on its members when the risk management benefits such a position would provide are questionable. Given the existing risk management frameworks our members already have in place (including CEO, CFO, Board and internal and external auditors), mandating the appointment of a CRO on top of this would be an unnecessary imposition.
The benefits of such an appointment are questionable. Our members are highly aware of the risks that their businesses currently face, and they have highly experienced Boards and Board Committees who already devote significant time to these issues. We concur with the draft standard's statement that the risk management framework should be appropriate to a regulated institution's size, business mix and complexity.

[6] APRA, *Harmonising cross-industry risk management requirements,* May 2013, p. 11.
[7] APRA, *Draft Prudential Standard CPS 220 – Risk Management,* May 2013, para 31(e).

Friendly societies are smaller and more conservative than ADIs, and provide investment products that are simple to understand and administer compared to more traditional investment products. The sector's business models are generally less complex and risks are relatively static over time. Given these differences, we believe some explicit tailoring within the draft standard to the characteristics of the sector is appropriate.

While paragraph 54 of the draft standard currently provides supervisory flexibility in the practical application of this requirement, this does not provide sufficient assurance to our members. There is no certainty around when and how APRA may or may not choose to grant an exemption, or the factors that they may take into consideration in reaching their decision. There is also a risk that APRA's supervisory application of the exemption could change over time.

As a minimum, APRA should provide greater details in the prudential standard around how this flexibility will be applied. The discussion paper states that "APRA will … consider exemptions for smaller institutions that can demonstrate they meet, in substance, the principles underlying the requirements." Language of this nature should be included in the prudential standard, along with detail around factors that APRA would take into consideration in making their decision.

While this would be a step in the right direction, a better solution would be to provide an explicit exemption for friendly societies. This would be a more transparent way of achieving the same outcome while also providing the sector with greater certainty around their prudential obligations. We believe that the current prudential framework is working well, and provides appropriate flexibility for friendly societies to engage a CRO when it makes sense to do so.

The draft prudential standard has created uncertainty, and clarification is required around exactly who can fill the CRO role. The discussion paper, APRA's letter of 9 May, and the APRA Chair's speech on good governance all included statements setting out the ways in which the CRO must be "independent." However, each of these descriptions could be interpreted differently. It would be valuable if APRA could elaborate on the independence requirements and specify exactly what it would see as compromising a CRO's independence. For example:

- Can the CRO be a member of the Executive Management (EM) team? Does APRA see a CRO participating in executive decisions as compromising their independence? Allowing the CRO to be part of the EM team serves a number of useful purposes, such as ensuring that the risk perspective is always brought to executive discussions and enabling effective performance of the challenger role. Being part of the EM team also ensures that the position carries the necessary stature and authority, and is seen that way by the business.

- Where does the operational management of risk blur the lines of independence and potentially provide a conflict of interest? Does APRA see oversight of AML transaction monitoring as a risk management function or a business function? Could the compliance function form a part of the CRO's role or is it intended to be a separate independent unit?

- What does "distinct" and "dual hatting" actually mean to APRA? For many of our members, when a senior executive takes leave, their role will be covered by another senior executive. This type of arrangement is common and necessary. By putting in place appropriate controls, our members are already able to ensure that any potential conflicts are able to be managed effectively. However, is it APRA's intention that the CRO not be able to act in the role of CFO or CEO in this manner?

- Does a friendly society need to explicitly call the position "Chief Risk Officer" to meet the requirements of the draft standard? Where an ADI has an employee that meets the other requirements of the prudential standard, but calls this employee their "Head of Compliance", or something similar, would this be sufficient to meet the CRO obligation?

- While the draft standard prevents the CRO from being the CFO, CEO or Head of Internal Audit, how does this apply to a friendly society which does not use these labels to name the executives who hold these positions? Could the CRO also be the Head of Finance for instance?

- Can the CRO function be undertaken by an individual who also has a similar capacity for other APRA and non-APRA regulated entities e.g. shared by an ADI, Friendly Society and Health Insurer with the same group?

The Board Risk Committee

The discussion paper proposes requiring all friendly societies to establish an independent Board Risk Committee, and states that this is "essential in providing the Board with greater oversight of and advice on the risk management framework."[8] While, "the proposed composition requirements … do not preclude this Committee having the same composition as the Board Audit Committee,"[9] the Risk Committee would be required to operate under a separate charter.

The FSA recognises the importance of a friendly society Board devoting time to risk matters. However, where a member already has a joint Audit and Risk Committee in place, we question what additional prudential benefit is derived from splitting the Committee in two. If the same Board members are able to sit on both Committees, a strong argument can be made that the existing arrangements would be able to achieve the prudential outcomes sought by APRA in an equally effective fashion.

If the same people are meeting at the same time to talk about the same things, the FSA argues that changing the name of the Committee will not improve prudential outcomes. Requiring the Committee to meet under two separate "hats" and two separate charters appears to simply be adding red tape to the operation of a friendly society for no benefit.

The FSA contends that the current risk management prudential requirements have established a robust, functional and effective risk management framework for its members. In its current form, APRA's proposals will not improve the financial stability of Australia's friendly societies. The cost burden however, imposed by these additional regulations, will undermine the competitive position of our members.

If you have any questions regarding this submission, please contact me on 02 8035 8441, or Jim Aliferis, Senior Policy Adviser, on 02 8035 8442.

Yours sincerely

Mark Degotardi
Head of Public Affairs

[8] APRA, *Harmonising cross-industry risk management requirements,* May 2013, p. 12.
[9] *Ibid*