

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

26 June 2013

**Discussion Paper: Harmonising cross-industry risk management requirements, dated 9 May 2013**

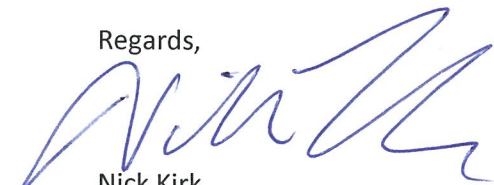
Calliden has reviewed APRA's discussion paper and has a number of comments on the proposed changes. Calliden is supportive of the move to harmonise requirements, but is especially concerned with APRA's apparent intention to:

- begin to mandate executive team structures via the requirement for a Chief Risk Officer ("CRO");
- impose additional financial burden on small regulated entities for little demonstrable benefit with regard to the CRO and the prevention of 'dual-hatting' (APRA's term);
- force quantifiable tolerances on all material risks without regard for whether this would lead to a narrowing of an entity's Risk Appetite Statement ("RAS"), thereby reducing its usefulness as a business tool; and
- reduce the effectiveness of the board risk committee via the proposed restrictions on its membership.

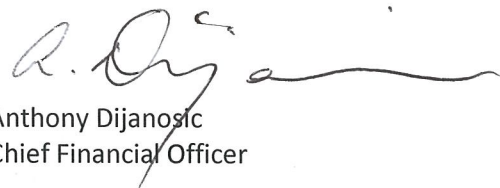
Specific concerns are detailed in the below. All references are to the draft standards unless otherwise specified.

Should you wish to discuss this submission further in any way, please contact Anthony Dijanosic on 02 9551 1145, or via email at [anthony.dijanosic@calliden.com.au](mailto:anthony.dijanosic@calliden.com.au).

Regards,



Nick Kirk  
Chief Executive Officer  
Encl.



Anthony Dijanosic  
Chief Financial Officer



## Discussion Paper: Harmonising cross-industry risk management requirements, dated 9 May 2013

### ***CPS 220 Risk Management***

Prudential Standard content: 24. 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.

Calliden response: Both this, and paragraph 26 dealing with related data quality, are undoubtedly appropriate for material risks that are readily quantifiable. Calliden is concerned, however, that unless the broadest possible interpretation of 'management information system' and 'data' is used, these requirements may not be appropriate for risks that are less easily quantified – reputational risk, or people-related risks for example. As such, the requirement to maintain these systems to cover 'all material risks' (our underline), is unlikely to be satisfied in practical terms.

---

Prudential standard content: 29. An APRA-regulated institution's risk appetite statement must, at a minimum, convey: (b) for each material risk, the maximum level of risk that the institution is willing to operate within, expressed as a risk limit and based on its risk appetite, risk profile and capital strength (risk tolerance); and (c) the process for ensuring that risk tolerances are set at an appropriate level, based on an estimate of the impact in the event that a risk tolerance is breached, and the likelihood that each material risk is realised.

Calliden response: Calliden is of the opinion that compliance with these requirements will detract from the ability to use the RAS as a decision making tool, and as a mechanism to guide organisational behaviour. Risk limits are of value where there is, or could be, a commonly understood calculation method or reference point. Unfortunately, with a number of Calliden's material risks, e.g. employee succession risk, there is no such common calculation method or reference point. One meaningful way to convey the nature of these risks, and to monitor and manage them, is via qualitative reporting that is not unnecessarily narrowed by a pre-defined risk limit calculation methodology.

Calliden's RAS was implemented in mid-2012, and since that time has been used heavily to inform business decisions, including the setting of the reinsurance programme and the investment strategy. Calliden's RAS provides quantitative measures for capital erosion risks only, with all other risk tolerances providing qualitative, relative measures. Structuring the RAS in this way has enabled Calliden to communicate the relative importance of each of the risk tolerances to all employees in language that is easily understood and so acted on. Specifically for Calliden, it communicates that most other risk tolerances are subservient to the capital risk tolerance. Calliden has significant concerns that the implementation of the draft standard requirements would necessitate adding complexity to the RAS, and turn what is an extremely robust and useful document into one that is far too narrow in its focus and application.

---

Prudential Standard content: 38. An APRA-regulated institution's risk management function must be headed by a designated Chief Risk Officer (CRO). The CRO must be involved in, and have the authority to provide effective challenge to, activities and decisions that may materially affect the institution's risk profile.

Calliden response: Calliden has significant concerns with APRA's apparent intention to effectively impose an executive team structure on regulated entities via the requirement for a CRO, especially for smaller regulated entities for whom a role carrying this title would significantly increase expense levels. Paragraph 37 of the draft standard, and its equivalent in the current GPS 220 (paragraph 16), ensures that the risk management function of a regulated institution has the necessary authority and access to perform its activities. Calliden sees this requirement as providing more than enough guidance for regulated entities, and authority APRA, to ensure that risk management is given appropriate focus. Calliden does not consider that APRA's mandating of executive team roles will lead to significantly improved outcomes, nor does it consider organisational and executive team design to be APRA's responsibility, nor key skill.

---

Prudential Standard content: 39. The CRO must be independent from business lines, the finance function and other revenue-generating responsibilities. The CRO must not be the Chief Executive Officer (CEO), Chief Financial Officer, Appointed Actuary or Head of Internal Audit.

Calliden response: Whilst acknowledging the ideal state of the most senior risk role in an organisation having no other responsibilities, Calliden is concerned with the comparatively higher financial burden that this places on smaller regulated entities with no demonstrable practical benefit. We agree that 'dual-hatting' is not appropriate for most roles including those specifically listed in the draft standard, though do not believe that there is any demonstrable detriment to having the most senior risk role also having oversight of the compliance function, for instance. Calliden does actually comply with the draft standard, with the most senior risk role having no other operational responsibilities, but is concerned with additional restrictions that do not add to risk management quality, and are an unfair burden on smaller regulated entities.

---

Prudential Standard content: 40. The CRO must have a direct reporting line to the CEO, and have regular and unfettered access to the Board and the Board Risk Committee.

Calliden response: Calliden considers that there is little benefit in enforcing a reporting line of the CRO to the CEO, and that this move is misguided. Many organisations would no doubt currently have the most senior risk role reporting through the CFO, as Calliden does from an administrative perspective, and directly to the board risk committee from a risk perspective. The CFO, like the most senior risk role, is a gatekeeper role with little in the way of performance incentives linked to company performance. The proposed standard changes this to a situation where the most senior risk role reports to the CEO, a non-gatekeeper role. Calliden considers that demonstrable, unfettered access to the board risk committee and the Board should be a key aspect of the most senior risk role, and does not believe that the proposed change in reporting line adds in any way to the risk management maturity of a regulated institution.

---

### ***CPS 510 Governance***

Prudential Standard content: 79. The Board Audit Committee is required to provide prior endorsement for the appointment or removal of the APRA-regulated institution's auditor and Head of Internal Audit. If the auditor or Head of Internal Audit is removed from their position, the reasons for removal must be discussed with APRA as soon as practicable, and no more than 10 business days, after the Committee's endorsement is agreed upon.

Calliden response: Calliden considers that such tight time frames are appropriate where there has been no formal, structured tender process involving prior Board Audit Committee approval. It is, however, Calliden's contention that it is good governance to put both internal and external audit services out to tender periodically. Where such appointments occur in an open, structured manner, it is unclear as to why APRA need be informed within such time frames. This is especially the case in circumstances where APRA is informed in advance of a tender being conducted.

---

Prudential Standard content: 105. The Board Risk Committee must have at least three members. All members of the Committee must be non-executive directors of the APRA-regulated institution. A majority of the members of the Committee must be independent.

Calliden response: While the importance of a majority of independent, non-executive directors on the board risk committee is not in question, Calliden considers it counter-productive to prevent the CEO, potentially in the capacity of executive director, to sit on this committee. Especially in smaller regulated institutions, the CEO is likely to be extremely familiar with the detail of most risks, and can provide valuable further insight into the narrative expressed by the reporting of most senior risk role. Calliden's experience is that the CEO sitting on the board risk committee provides the other committee members with increased opportunities to challenge management, and to explore risks in far more detail than they would be able to solely through interaction with the regulated institution's most senior risk role.

---

Prudential Standard content: 106. The Board Risk Committee must have a written charter and terms of reference that outline its roles, responsibilities and terms of operation. The responsibilities of the Committee must include: (e) reviewing the performance and setting the objectives of the Chief Risk Officer (CRO), and ensuring the CRO has unfettered access to the Board and the Committee.

Calliden response: Calliden considers the standard to be inconsistent in that it mandates that the CRO reports to the CEO, yet the CEO cannot set the CRO's objectives nor review the CRO's performance. Further, the standard does not allow for the CEO, if an executive director, to sit on the board risk committee.

---

Prudential standard content: 107. The Board Risk Committee is required to provide prior endorsement for the appointment or removal of the CRO. If the CRO is removed from their position, the reasons for removal must be discussed with APRA as soon as practicable, and no more than 10 business days, after the Committee's endorsement is agreed upon.

Calliden response: While Calliden considers that the requirement for the board risk committee to endorse the removal of the CRO is achievable, full committee endorsement prior to appointment is impractical. It is impractical to wait for the board risk committee to sit before such endorsement occurs, unreasonable to expect a special sitting of the committee to be organised do so, and unreasonable in employment market terms to expect a candidate to wait for such endorsement if other offers are on the table. A far more practical and achievable process would be for the Chair of the risk committee, or a delegated member of the risk committee, to play an active part in the candidate assessment process, with the authority to approve or veto any such appointment on behalf of the committee.

