Harmonising Cross-Industry Risk Management Requirements

Submission to APRA

July 2013

finity

5 July 2013

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

Dear Neil

Harmonising Cross-Industry Risk Management Requirements

This submission sets out Finity's comments on APRA's proposed changes to risk management, as set out in the discussion paper 'Harmonising cross-industry risk management requirements' dated 9 May 2013, and associated draft prudential standards CPS 220 and CPS 510. We thank APRA for the opportunity to make a submission on this important topic.

We would be pleased to answer any questions you may have on this submission; Geoff can be contacted on 02 8252 3337 and Steve on 02 8252 3326. We are also available to meet informally with APRA staff to discuss our feedback.

Yours sincerely

Geoff Atkins

Steve Curley

Finity Consulting Pty Limited
ABN 89 111 470 270
www.finity.com.au
www.finityconsulting.co.nz

Sydney
Level 7, 155 George Street
The Rocks NSW 2000
Ph: +61 2 8252 3300
Fax: +61 2 8252 3399

Melbourne
Level 3, 30 Collins Street
Melbourne VIC 3000
Ph: +61 3 8080 0900
Fax: +61 3 8080 0999

Auckland
Level 27, 188 Quay St
Auckland 1010
Ph: +64 9 363 2894
Fax: +64 9 363 2895

Harmonising Cross-Industry Risk Management Requirements

Part I Summary

We support APRA's goal of promoting sound risk management in regulated institutions. The proposed initiatives reinforce this objective, although we have significant concerns about the cost and effectiveness for general insurers.

We have prepared our submission on an exceptions basis, focusing on areas where we consider improvements could be made to the proposed reforms set out in draft CPS 220 and CPS 510. These areas, not necessarily mutually exclusive, are:

1. Some useful industry specific material has been removed from the existing standard for general insurers (GPS 220)
2. The standards are too prescriptive, moving away from APRA's existing principles-based approach
3. The proposed requirement for a CRO creates problems for many general insurers
4. The reforms represent a prohibitive cost for small to medium-sized regulated institutions, often with little expected benefit.

We elaborate on our concerns in each area, and suggest possible solutions, in the detail of our submission (Part II).

Finity specialises in general insurance, so our comments come from this perspective. We have not commented on the suitability of the reforms for life insurers or authorised deposit-taking institutions (ADIs).

In our view many of the areas APRA wishes to focus on can be better addressed through well designed supervision applied to more principles-based standards.

Part II Detailed Submission

We support APRA's goal of promoting sound risk management in regulated institutions. In our view the proposed initiatives reinforce this objective.

Our submission focuses on areas where we consider improvements could be made to the proposed reforms. Finity operates in the general insurance (GI) sector; our comments draw on this experience and naturally focus on the impacts on general insurers. We have not commented on the suitability of the reforms for life insurers or authorised deposit-taking institutions (ADIs).

Each section of the submission introduces one key issue, and includes suggested solutions.

1 Loss of Useful GI Specific Material

One of the disadvantages of harmonisation of risk management requirements is that it can reduce the focus on issues specific to one regulated industry. This is likely to have a negative impact on the effectiveness of risk management in that industry, thus increasing risk to stakeholders (particularly policyholders).

We believe that in the draft CPS 220 there are several aspects of the current general insurance standard GPS 220 that are lost, to the detriment of the standard's effectiveness. Alongside this is the inclusion of areas of focus which are more significant for authorised deposit-taking institutions (ADI) and life insurers.

The GI-specific elements which are lost (and only implied by the catch all 'other risks' in CPS 220 paragraph 27(g)) are:

- Insurance concentration risk (GPS 220 paragraph 13(e))
- Specific reference to asset and liability mismatch risk (GPS 220 paragraph 13(a))
- Some GI specifics in GPS 220 paragraph 34(j)
- The financial information declaration; it is unclear where this will be covered in future material (GPS 220 paragraphs 41-43).

Also, the strong linkages to ICAAP (GPS 220 paragraphs 35 and 36) have been removed and replaced with one reference to ICAAP in CPS 220 (paragraph 24(f)). The paragraphs in GPS 220 provided a strong connection between risk and capital management; the link is weaker in CPS 220. This change affects other industries as well as GI.

Other areas where the proposed standards do not deal well with the GI situation are:

- There is no preamble to paragraph 27 stating that each of the risk areas listed may receive different emphasis from each institution depending on its business model and risk profile. Such a reference could assist in resolving some of the points below.
- Credit risk is separated from market and investment risk (CPS 220 paragraph 27(a)). For general insurers this separation gives the impression that credit risk, market risk and insurance risk have equivalent importance.
- Inclusion of liquidity risk (CPS 220 paragraph 27(c)). This is a minor risk for most general insurers, yet in the standard it is listed as an equivalent risk class as insurance risk.

- The necessity to make reference to another standard (not yet proposed) for run-off insurers (CPS 220 paragraph 14); in GPS 220 paragraphs 22-28 work well.

1.1 Suggested Approach

Finity suggests that, should APRA determine to proceed with a single cross-industry risk management standard, it deal with industry specific issues as follows:

1. Include in the body of the standard only those principles and requirements that are meaningful and significant to all sectors covered by the standard and be clear that emphasis is different between industries.
2. Create an appendix for each regulated industry sector with requirements or elaboration specific to that sector.

For the GI sector the appendix could include the following:

- The primacy of insurance risks
- Specific mention of premium adequacy, reserve adequacy and insurance concentration (catastrophe) as key aspects of insurance risk usually requiring separate treatment
- Identification of liquidity, asset/liability mismatch and credit as risk areas that may require fairly basic treatment
- Specific requirements for run-off insurers
- Specific requirements for branches and the overseas operations of Australian insurers and groups
- Requirement for linkages with ReMS and ICAAP
- Acknowledgement of the place of GPS 320 Actuarial and Related Matters in contributing to risk management for general insurers that have an Appointed Actuary (AA), due to the primacy of insurance risk for general insurers.
- The requirement to mitigate conflict of duties if existing members of staff are also allowed to be the CRO (see later).

2 Prescriptive Nature of Standards

Since APRA's reforms in 2002 its prudential standards have been intended to be principles-based. Each regulated institution can meet the regulations in a manner appropriate to the organisation, given the size, business mix and complexity of its operations. The last 11 years' experience suggests that this is an effective approach.

Our concern is that the proposed standards are more prescriptive in nature, and this may lead to a compliance focus among regulated institutions and a move away from risk management as a business enabler and legitimate control function. In our opinion good risk management requires thinking (and then action if required). It is difficult to make regulations to require thinking, but APRA can make regulations which encourage managers to think about and analyse pertinent issues. APRA can then review the evidence that this thinking and analysis has taken place (as opposed to compliance focused form filling), and intervene as appropriate.

In the remainder of this section we discuss specific areas where we believe the proposed standards are unnecessarily prescriptive.

2.1 Requirement for CRO

The recent global financial crisis (GFC) demonstrated that a skilled and well-resourced central risk function can be effective in mitigating risk and improving business performance. This is particularly true if the risk function is supported by suitable governance and reporting structures. Those most at risk – and most in need of a CRO and associated structures – are complex businesses, usually large and spanning several industries, products, distribution channels and/or regions. Furthermore, it can be argued that the need is generally greater in some industries (ADIs) than others (general insurance), given the operations and nature of risks in each case. Experience during the GFC supports this argument.

We identify the following problems in requiring a CRO as specified in the draft CPS 220:

- The substantial additional cost – for limited benefit in many cases. We elaborate on this point in Section 3.
- The potential to diminish the important role played by general insurance AAs. Specifically:
  - Actuaries understand insurance risk better than most non-actuarial CROs. Insurance risks are the key risks facing general insurers, and the proposed changes risk moving AAs further into a compliance role and downplaying insurance risks.
  - CROs are not part of a defined professional framework. Actuaries are members of an established and recognised profession, with the Actuaries Institute providing high level oversight of members' activity. This provides useful quality control for APRA.
- The potential for conflicting advice to the Board from the CRO and the AA. There is a risk that they will work in silos, possibly duplicating effort. Alternatively some risks may be missed if the role of each is not clearly defined. Reporting and communication to the CEO and Board may suffer as a result.
- The availability of suitably qualified and experienced CROs for all regulated institutions. If the current proposal is implemented, we are concerned that there will be a shortage of candidates with the appropriate mix of industry and risk management experience and risk management qualifications. If CRO positions are filled with unsuitable candidates this could be counterproductive to APRA's reform objectives and impair the risk management frameworks of the affected institutions.

2.1.1 Three Lines of Defence

We understand that APRA's proposals about who would be ineligible to be the CRO are based in part on the 'three lines of defence' (3LOD) risk management model. APRA proposes that the CRO is an internal control function (2nd line) and should have no 1st line business responsibilities, and should be separate from internal audit (3rd line). Appendix A summarises our understanding of the 3LOD model, with specific observations on its application in the general insurance sector.

While we accept the general direction of this argument, we disagree with the 'blanket ban' on specified personnel also being the CRO. In our view any manager should be permitted to be the CRO **if there is no conflict of duties** and they hold suitable qualifications and/or experience for the role.

2.1.2 Suggested Solutions

If APRA is prepared to consider moving to a more principles-based standard, then suggested principles that relate to the CRO are as follows:

1. Each regulated entity or group must nominate an individual person as responsible for the risk management function (the CRO however named)
2. The CRO must be a Responsible Person and satisfy Fit and Proper requirements set out in the institution's Fit and Proper Policy
3. The CRO must not be the CEO or a member of the Board
4. The CRO must not be part of a business division that is responsible for decisions directly influencing the risk profile of the entity
5. The CRO must identify any potential conflict of duties and put in place suitable mitigants
6. The CRO must have direct access to the CEO, relevant Board Committees and the Board
7. The role description of the CRO must acknowledge the independence of thought required in order to comply with the standard and the possibility of whistle blowing.

Other suggested approaches that APRA could consider are as follows:

- APRA could introduce a size 'threshold' above which companies are required to have an independent CRO. This concept is found in existing regulation, where APRA waives the need for an AA for low-risk small insurers. In a similar vein, smaller institutions with simple business structures and risk profiles would be exempt from the requirement for a stand-alone CRO. The threshold would be higher than that applying for the AA exemption (i.e. would include more insurers); annual GWP of somewhere between $250 million and $500 million might be used as the initial hurdle for consideration. The key issue for securing exemption is complexity; only simple insurers should be exempt, provided they fall below this size threshold. One way to describe a 'simple operation' is that there is only one distinct insurance operating division making independent decisions about accepting insurance risk.
- could be defined so that APRA's proposal applies for larger, riskier, more complex institutions and groups while not imposing unnecessary cost on simpler, smaller insurers.
- We suggest a long transition period to implement the CRO requirements, to allow for the development of a suitable pool of CRO candidates from various backgrounds (including actuaries).

- Any of the insurer's managers should be permitted to be the CRO if they hold no 'first line' or 'third line' responsibilities. CPS 220 (more specifically its general insurance appendix) could provide more general guidance on who may be considered for the role of CRO, subject to recognising and dealing with any conflict of roles.

2.2 Separate Risk and Audit Committees

For many general insurers, especially small to medium insurers, we fail to see the merits of requiring a Board Risk Committee separate from the Audit Committee, as specified in draft CPS 510. For many companies the operation of a combined Audit and Risk Committee (or an Audit, Risk and Compliance Committee) is a very effective approach.

There is no conflict of duties between an Audit Committee and a Risk Committee. We view the duties as entirely compatible, consistent with our preference for a combined approach and can be clearly articulated in a single Committee Charter covering both audit and risk. If APRA wishes to ensure suitable oversight of both audit and risk management issues it can achieve this during its regular on-site supervision activities, ensuring the single Audit and Risk Committee's charter ensures appropriate supervision in each area.

2.2.1 Suggested Solution

We suggest that APRA discard this proposed change.

Alternatively, if the concept is retained, APRA should permit smaller, simpler institutions to have a combined Audit and Risk Committee. Only for larger, more complex organisations can we see that benefits from having separate committees could outweigh the costs.

2.3 Other Prescriptive Elements of Draft CPS 220

The table below identifies the prescriptive requirements of draft CPS 220 that we believe are onerous and disproportionate for many general insurers, particularly small to medium sized companies. It also suggests an alternative approach to dealing with each issue.

Paragraph in CPS 220	Requirement *Commentary*	Suggested Approach
12(g)	Uncertainties relating to models are well understood. *Apart from catastrophe models, the use of risk measurement models to drive key business decisions is very rare in general insurance.*	Omit the requirement, noting that catastrophe model uncertainty is dealt with in GPS 230.
15	Specific requirements for group risk management	Leave as a principle in CPS 220. Include Level 2 requirements in general insurance appendix.
18	Group liquidity policy *This is a low priority for most general insurers.*	Include in the ADI and life insurance appendices as required.
24(g)	Creation of a Risk MIS *The focus on the 'system' rather than a 'process' for managing and reporting material risks will be difficult to implement for risks which are obscure and difficult to quantify.*	If required for ADIs to deal with rapidly changing exposure profiles (e.g. trading), include this in the ADI appendix. Omit for general insurers.
25	Scenario and stress testing analysis	Omit. Already included in ICAAP. Should already be used in setting risk register as well.
26	Risk MIS and robust data framework	Omit. Include any ADI requirements in appendix.
27	Separate specification of credit and liquidity risk	Clarify in a GI appendix.
29	Risk tolerances in the risk appetite. *Risk appetite statements may become documents for micro-managing risks faced by an institution.*	In our view risk appetite and operational risk tolerances should not be merged, but kept as separate (albeit related) components of the risk management framework.
35	List of nine requirements for policies and procedures. *These requirements are implied by the rest of the standard.*	To the extent that any specific policies are required, list them in the appendix for an industry sector or as part of the section on the RMS.
38-41	Designated Chief Risk Officer including direct reporting line to the CEO. *Too onerous for many institutions and already covered by other principles.*	To the extent there are ADI requirements, include in the ADI appendix. Direct ***access*** is the principle, not direct reporting.
42	Separate requirement for a compliance function. *Gives the wrong focus for risk management.*	If the compliance function can be included in the risk management function, this should be clearer. First line compliance should be in the business areas, with second line compliance suitable for inclusion with the risk function.
51-53	Notification to APRA within 10 business days of a series of items. *Difficult to comply with and difficult to define triggers.*	Omit and replace with simpler principles. These requirements detract from the responsibility of the Board and management to manage risk.

3 Smaller Insurers and Branches

3.1 Applicability to Branches

In the draft CPS 220, it is not clear to what extent (and in what way) branches will be expected to satisfy the new requirements. For example, consider the case of a branch with only a small local staff group (or none):

- Would a 'home' insurer CRO satisfy the requirement for an independent CRO?
- What 'modifications' to the proposed framework would apply? (requirement for a Risk Committee etc.)

The current draft standard does not acknowledge the fact that, for a branch, the Senior Officer Outside Australia stands in place of the Board.

3.1.1 Suggested Solution

We suggest the addition of a specific section of the standard (in particular the GI-specific appendix) to establish proportionate requirements for branches. In particular it is often desirable that the risk management function should follow the same framework as, and be integrated with, the home office function.

3.2 Prohibitive Costs

Many aspects of APRA's package of reforms are appropriate for large, complex businesses. However, for small and medium insurers (including many branches) some of the requirements of draft CPS 220 are onerous and disproportionate to the nature of the risks faced.

3.2.1 Suggested Solutions

In our view APRA should:

- Be more principles based and exempt smaller institutions with relatively simple operations and risk profiles from the prescribed requirements applying to larger, more complex businesses. The need for an independent CRO and separate audit and risk committees are cases in point.
- Assess smaller, simpler organisations on a case by case basis so that the spirit of the reforms is met in other ways. For instance, the CRO role may be covered by an existing member of the insurer's management team, provided that conflicts of duty are managed appropriately.

3.2.2 Cost-benefit analysis information

As with all consultations on proposed standards, APRA seeks cost-benefit information. While we are not in a position to give specific figures for an individual insurer, we will attempt to give an overview of the likely costs for a small to medium sized insurer incorporated in Australia.

We estimate that the risk management function, in order to meet the requirements of GPS 220 (along with CPS 231 and 232), would currently cost a small to medium-sized insurer $200,000 to $300,000 per annum. This includes the cost of all necessary systems (e.g. maintaining the risk register).

By way of comparison, the cost of the AA function would be in the order of $100,000 to $200,000 per year (outsourced). With an employed AA the cost would be greater, but the company would expect significant contribution to the business outside the AA role.

Estimated cost for CPS 220 as proposed

We estimate that the cost of the risk management function would increase by a further $150,000 to $200,000 per year, with additional costs arising from:

- A more expensive CRO (cost much greater than this if it is an additional role)
- A risk MIS – software, implementation and usage
- Additional Risk Committee of the Board.

Benefits from CPS 220 as proposed

For the general insurance sector (at least for small to medium-sized insurers including branches) we could not identify any benefits in terms of reduced risk to policyholders through more effective risk management from the proposed amendments to GPS 220. To the extent that the risk management function may not be operating to the desired quality under the current standards, there is nothing that APRA cannot identify and require rectification through the current on-site examination program.

4 Other Suggestions

The table below identifies some other small sections and wordings in the draft CPS 220 that we believe could be improved.

Section of CPS 220	Principle (where applicable)	Suggested Edit
List of systems (front page and paragraph 24(h))		*'Identifying, measuring, evaluating, monitoring, reporting and controlling or mitigating'* lists seven different steps for risk management. The four components in GPS 220 of '*identifying, assessing, mitigating and monitoring'* represent a simpler and clearer statement.
Risk Management Framework (front page)		*'These systems, together with the structures, policies, processes and people'* is an inferior description to saying directly that the '*systems, processes, structures, policies and people'* comprise the RMF.
Maintain adequate resources (5th dot point on first page)		Replace with '*maintain adequate resources to execute the risk management strategy and ensure compliance with this Prudential Standard'*
Notify APRA (6th dot point on first page and paragraphs 51-52)	Too prescriptive	Should be to *'submit a Risk Management Declaration to APRA annually and make other required notifications'*
Application (paragraph 3)	Appropriate to size, business mix and complexity	CPS 220 should state that '*the risk management framework must be appropriate to the size, business mix and complexity of the institution. An institution must be in a position to explain to APRA how its application of any section of the Prudential Standard meets this requirement'.* (Note APRA's power in CPS 220 paragraph 54.)

Part III Appendices

Three Lines of Defence

Application to the General Insurance Industry

The concept of ***three lines of defence*** was established by the internal audit profession, and has gained prominence since about the year 2000. It has been adopted by financial regulators around the world, most notably in Europe.

How can this model best be applied in the ***general insurance industry***, as part of a comprehensive ERM framework?

The essence of the three lines of defence model can be captured in the following characteristics:

Line of Defence	Characteristics	Description
First line	***embedded***, part of the business, controls, processes	The 1st LOD covers business areas responsible for decisions which determine the risk profile of the institution. Examples for a general insurer include pricing, underwriting, claims management, investment management, reinsurance and setting strategy.
Second line	***engaged***, monitoring, coaching, assisting, reporting	The 2nd LOD is usually an internal function that is independent of the business units and which routinely (nearly continuously) reviews initiatives and the implications for the firm's risk profile. Examples include many actuarial functions and finance.
Third line	***independent***, reviewing, assurance	The 3rd LOD is strictly independent, not continuous, and often more process oriented. It advises on the effectiveness of the 1st LOD and 2nd LOD.

The risk management strategy, as part of Enterprise Risk Management (ERM), will explicitly recognise the three lines, and the central ***risk management function*** sits in the second line. It:

- Oversees the process of risk identification and measurement
- Guides and assists with development of risk mitigation and management initiatives
- Continuously monitors performance in risk management – updating the risk register, preparing analyses and reports
- Compares the emerging risk profile with the risk appetite
- Is a scrutineer for business initiatives and risk taking
- Reports regularly to senior management and the Board
- Is a 'trusted advisor' to the business on risk issues.

The third line comprises ***internal audit,*** supplemented by external audit and other specialists, providing independent reviews and assurance that what the first and second line say they are doing is actually what they are doing. We comment further on this later.

Application to the main risk types for general insurance

Risk Category	First Line	Second Line	Third Line
Underwriting Risk	Underwriting authorities and controls, peer review, price adequacy reports	Underwriting audits FCR	Independent underwriting reviews by Internal Audit
Claims Risks	Claim authorities Regular file review Estimate change reports Large claim reporting	Claims audits Actuarial valuation	Independent claims reviews by Internal Audit
Catastrophe Risk	Accumulation monitoring Product design Underwriting rules	Exposure modelling Reinsurance broker modelling FCR	Internal audit can possibly check compliance with the ReMS but a substance review is technical and complex
Reinsurance risk	ReMS Placement policies Recovery processes	Reinsurance committees Reinsurance broker advice FCR	As above - technically complex
Investment risks	Investment policies Custody	Finance monitoring and reporting Asset consultants Board reporting FCR	Internal audit review of investment risks and compliance with investment policy
Credit risk (premiums and brokers)	Credit control system	Finance reporting External audit FCR	Internal audit review of credit risks and controls
Capital adequacy	ICAAP Finance function control Reporting Regulatory returns	Risk analysis ICAAP annual report FCR	Independent review of ICAAP
Operational risks	Internal systems such as: - security - fraud investigation - human resource systems - IT recovery Separation of roles	Periodic testing Risk management reviews	Internal audit reviews
Regulatory compliance	Compliance systems	Compliance reviews Breach reporting	Internal audit reviews External audit (in some areas)

This table gives a practical summary of how risk management and the three lines of defence lines up in the context of general insurance.

Risk function supported by the AA in the second line

It can be seen that in the second line the risk management function should have a broad view across all the risk areas. The effectiveness will be increased to the extent that it is engaged with the relevant business area, in developing, monitoring and reporting on the first line activities. From time to time the second line will need to make its own investigations, while in some areas they are supported by other specialist functions in the company such as finance, actuarial and HR.

It is noteworthy the frequent appearance of the Appointed Actuary in the second column – with direct second line control over claims provisions and a window into many other risk areas through the Financial Condition Report. The AA function also benefits from substantial institutional protection through APRA prudential standards, actuarial professional standards, Board appointment, Board access and reports being forwarded to APRA.

Is the AA second line?

Our interpretation of how general insurance actuaries sit in this model is as follows:

1. The general insurance Appointed Actuary has two main statutory obligations. They are to prepare:
   (a) the Insurance Liability Valuation Report (ILVR), including central estimates and risk margins for outstanding claims and premium liabilities, and
   (b) the Financial Condition Report (FCR), which involves a broad review of many aspects of the insurer's business.
2. For outstanding claims, the 1st LOD is the claims department which assesses reported claims and establishes case estimates. Any deterioration or unexpected claim events should be identified in the claims department as the 1st LOD.
3. The review by the Appointed Actuary establishes an IBNER/IBNR reserve for outstanding claims. This will always incorporate an operationally independent assessment of claims development and is therefore a 2nd LOD review of reserve risk. The IBNER/IBNR reserve is a financial reporting element, and does not create business risk. To the extent that there is risk arising from mis-statement of the financial reports, there is strong review and oversight through the External Peer Review and the external audit.
4. In terms of premium liabilities, the prospective assessment of premium liabilities, along with the Liability Adequacy Test (LAT), is essentially a 2nd LOD review of the adequacy of premium rates. The 1st LOD rests with those who set premiums and monitor achieved premiums (underwriters and management). Thus the Appointed Actuary is a 2nd LOD role in respect of premium adequacy risk.
5. Virtually all aspects of the FCR would be regarded as 2nd LOD. By its nature it is a report to the Board, by an expert and objective party (the Appointed Actuary), giving the actuary's independent perspective on many aspects of the insurer's operations. We note that if the AA had other 1st or 2nd LOD responsibilities, the relevant component of the FCR could not be regarded as 2nd LOD.
6. All of the AA's observations are supported by the Actuaries Institute's professional Code of Conduct and professional standards. More broadly, the actuarial profession brings a tradition of objectivity (or independence of thought), supporting the view that Appointed Actuaries operate in the 2nd LOD.

In conclusion, all of the statutory responsibilities of the AA will generally be 2nd LOD.

Examples where the general insurance AA has 1st LOD responsibilities include:

- The AA having responsibility for the claims department
- The AA being responsible for premium setting or having the primary obligation to monitor achieved premiums or underwriting effectiveness

  The AA being the Chief Reinsurance Officer.

How is the third line constructed?

The very specific prudential (policyholder protection) responsibilities placed on the Board of Directors creates a powerful governance framework for the third line. Board members themselves will provide a degree of oversight and challenge to both first line and second line reports received by the Board.

The internal audit function is at the centre of the third line. In our experience the internal audit function in general insurers is not very visible. In some ways this is quite understandable because of the necessary independence of the function. To some extent it is due to the small size of most insurers, leading to the internal audit function being largely or wholly outsourced to an external provider. In some cases internal audit is provided by the home office (for branches) or parent company (for subsidiaries).

In some ways outsourcing makes more sense for the internal audit function than for say the risk management or compliance function. Outsourced internal audit provides strong independence and access to a range of specialist skills.

A critical component is the management of the internal audit function and work program which, particularly in a smaller company, needs to be directly overseen by the Board audit committee.

Of particular note is that APRA has mandated a series of independent reviews that form a solid part of the third line, including:

- Reporting by the external auditor on compliance with the risk management strategy
- External Peer Review of the AA's insurance liability valuation
- Independent review of the risk management framework
- Independent review of the ICAAP
- Establishment of a Board remuneration committee.

These reviews are supplemented by a range of other assurance functions undertaken by external audit. Given that independence is reasonably assured, the co-operation and limited mutual reliance between internal and external audit is a sound approach.

What does this mean for prudential standards in risk management?

In our view the analysis above leads to the following propositions, which we believe are consistent with the comments and suggestions in our submission:

(a) Several specific aspects of the risk profile of general insurers should be dealt with specifically in the standard (a general insurance appendix would be suitable)

(b) Several of the insurer's managers could also serve as the CRO if an insurer chose, provided that potential role conflicts are identified and mitigated (simplistically, the CRO can't review their own work)

(c) Many of the existing APRA requirements for general insurers, such as reinsurance, actuarial, ICAAP, independent review requirement, contribute substantially to both the 2nd line and 3rd line of defence. It would be more helpful to insurers if this is recognised in the standards.

We would like to reiterate that this commentary relates only to general insurance. We have not considered life insurance or ADI issues, and there may well be differences in circumstances.