



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

4 June 2013

Via email: riskmanagement@apra.gov.au

PRINCIPAL MEMBERS



CommonwealthBank



Dear Neil,

ACI would like to take the opportunity to thank you and APRA for providing an opportunity for us to comment upon APRA's proposal to harmonise its cross-industry risk management requirements.

ACI is the peak industry body for the practice of compliance, risk and governance in the Asia Pacific region. Our members are compliance, risk and governance professionals who are actively engaged in the private, professional services and Government sectors.

Generally, ACI supports the concept of harmonisation of the risk management requirements that have been established across the industries regulated by APRA. Specifically we support;

- APRA regulated boards being charged with the ultimate responsibility for overseeing the regulated entities risk management framework and ensuring that a strong risk management culture is established and maintained;
- That adequate risk management measurement, assessment and reporting systems are in place;
- The Chief Risk Officer is an independent standalone responsibility within the organisation.
- Alignment between the organisation's risk management strategy and the overall business strategy;
- The creation of an independent board risk committee and;

Level 1, 50 Clarence Street
Sydney, NSW, Australia 2000
ABN 42 862 119 377
www.acigrc.com

Australia	+612 9290 1788	+613 9229 3871
Hong Kong	+852 3125 7665	
New Zealand	+64 9 363 2749	
Singapore	+65 6322 1463	

- The continuation of the audit committee in having responsibility to review the effectiveness of risk management framework.

Having said this, we note the recent consultation paper issued by ASIC (CP 204) entitled "Risk Management Systems of Responsible Entities", we note that many of this issue raised by APRA have also been raised by ASIC in this CP. We would therefore request that in implementing this program of reform, that APRA work closely with ASIC to insure that there is not only a consistency in approach, but any risk of duplication or conflicting requirements is avoided.

A copy of our submission to ASIC on CP 204 has been attached.

We also note that it is APRA's intention to have its proposed harmonisation reforms take effect on January 1st 2014. In contrast the reforms in CP 204 are currently set down to come into effect during August 2013. Again for the purpose of consistency we request that APRA and ASIC work together to develop a single date when these reforms will come into effect.

Once again ACI would like to thank APRA for providing an opportunity for ACI to make comment on the proposed reforms to its cross-industry risk management requirements. Should you require any additional information or require clarification on the comments that appear in this submission please do not hesitate to contact ACI on +612 9290 1788.

Yours sincerely,

A handwritten signature in dark ink, appearing to read 'M. Tolar', with a stylized flourish at the end.

Martin Tolar CCP

Managing Director

Please note that the views expressed in this submission represent those of the collective ACI membership. Consequently, individual members and organisations may hold a different perspective on some of the points raised and therefore reserve the right to make comment in their own right.



Violet Wong
Senior Lawyer
Investment Managers & Superannuation
Australian Securities and Investments Commission
Level 5, 100 Market Street
SYDNEY NSW 2000

1 May 2013

Via email: reriskmanagement@asic.gov.au

PRINCIPAL MEMBERS



CommonwealthBank



Dear Violet,

ACI would like to take the opportunity to thank you and ASIC for providing an opportunity for us to comment upon Consultation Paper 204: Risk Management Systems of Responsible Entities (CP 204).

ACI is the peak industry body for the practice of compliance, risk and governance in the Asia Pacific region. Our members are compliance, risk and governance professionals who are actively engaged in the private, professional services and Government sectors.

Generally, ACI supports the issuing of the Regulatory Guide as many of the issues covered are similar to those covered in APRA guidance material, both in nature and treatment. However it does remain to be seen how ASIC will approach the implementation of this guidance in respect to style. ACI believes given the similarity of the content covered by APRA guidance material and the proposed content of this Regulatory Guide (RG), there needs to be consistency in approach for not only the treatment of APRA and non-APRA regulated firms but also for businesses that will now have both APRA and ASIC regulation of their risk management framework.

Clarification is also sought from ASIC when it states in RG 000.78 that 'Risk Management Systems' should be subject to at least an annual review. ACI believes that ASIC should actually refer to the annual review of the 'Risk Management Strategy or Framework' in this instance, which would then remove any potential confusion as to whether ASIC is actually referring to the annual review of the operation of risk treatments. ACI believes that the frequency that such risk treatments are reviewed should be dependent upon the nature or level of risk being treated, rather than based upon a prescribed time period. Therefore in practice some risk treatments will be reviewed several times throughout the

Level 1, 50 Clarence Street
Sydney, NSW, Australia 2000
ABN 42 862 119 377
www.acigrc.com

Australia	+612 9290 1788	+613 9229 3871
Hong Kong	+852 3125 7665	
New Zealand	+64 9 363 2749	
Singapore	+65 6322 1463	

course of a year, while others will be subject to longer periods of review that may exceed a year. We note that a review does not necessarily have to result in any modification of treatments or systems.

ASIC has also suggested in RG 000.79 that a number of investment schemes are riskier than other investment vehicles, and therefore the risk management systems should be reviewed quarterly. ACI believes that this is not practicable and is inconsistent with the current APRA requirements. At present, the current approach employed by APRA regulated entities is for the 'Risk Management Strategy' to be reviewed annually or upon a significant change occurring to the entity's or scheme's business operations or structure.

ACI also believes it would be useful to have some clarification from ASIC as to its expectations around what constitutes an *independent* review of the 'Risk Management System' (RG 000.81). For example, is a review considered *independent* if it is conducted by the risk function and/or the Audit & Risk Committee? Alternatively, should the review be undertaken in a more independent manner by using the entity's compliance function and/or internal audit function (where these functions are separate to the risk function). Alternatively, is independence only achieved through the use of external auditors who have not been involved in setting up the system?

We would also like to see additional guidance around what ASIC believes is good practice in terms of undertaking 'stress testing' of the risk management framework. This includes examples of the factors to be tested, especially in the context of small RE which likely have quite limited resources compared to larger entities.

ACI members have also expressed concern about the suggested implementation timetable. We note that the RG will be released in August this year. Is the expectation that the RG will then be used by ASIC when undertaking a review of a responsible entity ('RE')? If so, this does not allow for the RE to make adjustments to its risk management systems to bring them into line with the RG, therefore creating potential compliance breaches. ACI recommends a 12 month transitional period to phase in and embed appropriate systems.

There are some organisations (who are licensees) that have been registered as RE in the past but at present are not undertaking activities as an RE. Under these circumstances where they do not therefore have any investors on the books (ie do not operate any schemes), it makes sense that the RG does not apply to them. Can you confirm this? It appears that where a licensee no longer acts as an RE of any *registered* scheme, it ceases to be a RE and the RG will not apply (even though it is still licensed to operate a registered

scheme). This results from applying the definitions of 'responsible entity' and 'managed investment scheme' in s 9 and s 601FB Corporations Act which requires a RE to be the only operator of a registered scheme. Therefore a licensee can only be a 'responsible entity' if it operates a scheme registered with ASIC (s 601FB). Please confirm our understanding. This leads onto the another question concerning schemes not required to be registered and so technically do not have a RE – how will they be affected by the RG? (see our response to B1Q5 below).

We will now turn our attention to some of the specific questions ASIC has raised in CP204.

B1Q4 Would the proposed requirements be better positioned as good practice guidance? If so, please explain why (including how the good practice guidance can improve risk management standards for responsible entities and why you consider that such good practice guidance will be adopted by the industry) and provide detailed suggestions on how we can encourage the adoption of fundamental risk management practices across the managed funds sector.

ACI is of the view that the proposed requirements should be made mandatory in nature rather than suggested 'good practice guides'. This will ensure that all requirements are considered and dealt with by the RE. We believe that many if not all of these requirements will have already been established by competent RE. Therefore making these requirements mandatory will have minimal impacts upon most RE. So long as there is flexibility to recognize the risk management framework needs to reflect the size, scale, scope and complexity of the RE, then the only push back will come from those RE that wish to sit outside what is considered to be sound governance, risk and compliance practice.

B1Q5 Entities that operate managed investment schemes that are not required to be registered under the Corporations Act may also choose to meet these requirements, although we do not propose to make them mandatory for these types of schemes. Should the requirements also apply to unregistered managed investment schemes? If so, why?

We believe that the requirements for risk management systems ('RM systems') should also apply to unregistered schemes offered to wholesale investors. As sophisticated and (presumably) prudent investors, we anticipate that they will inquire about the adequacy of the scheme's RM systems before they invest.

B1Q8 We consider that responsible entities are well placed to identify those risks that are 'material' to the operation of their businesses, given their diverse nature, scale and complexity. Do you agree? If not, should we provide guidance on what amounts to 'material risks'?

Small REs would benefit from practical guidance from ASIC in this respect. This could be in the form of a sample RM system including hypothetical material risks, assessment of those risks, possible treatment and monitoring procedures. Presently ASIC provides detailed guidance on risks, treatments and monitoring procedures in RG116 Commentary on compliance plans – Agricultural industry schemes and similarly in other commentaries for several specialised types of schemes. As identified in RG 000.79 some types of schemes (eg agribusiness, hedge funds) face more complex risks and these operators would also benefit from sample RM systems and guidance.

B1Q10 APRA-regulated RSEs must submit to APRA a signed declaration on their risk management strategy. Should we include a similar requirement for responsible entities?

ACI is of the opinion that REs should be required to retain (but not file with ASIC) an annual declaration from its designated authority (eg RM Committee) concerning the adequacy of the RM systems for each scheme and the operator itself. Then at the time of audit, ASIC can ask to see past declarations. If however ASIC is of the view, after this consultation process, that the annual declarations need to be submitted to ASIC, ACI would like to know how these declarations will be treated or used by ASIC.

C2 In meeting the risk management obligations, we expect responsible entities to...

(b) ensure all staff understand the purposes of risk management and its value;

ACI seeks clarity on this point as we do not believe that this necessarily means that formal risk management training should be provided for all staff. ACI believes that the amount of risk training that is delivered to staff should be appropriate for their role within the organisation. Some front line staff, for example, may only need to ensure they perform their tasks as per mandated procedures and the focus of their training should be on the established procedures. This then mitigates these risks from eventuating. From there, more detailed, personal training on risk management can be provided to managers and other decision-making staff to set them on the right course when making decisions to ensure it is in keeping with the RE's risk appetite.

D1 We propose to provide guidance that in establishing and maintaining risk management systems, it is good practice for responsible entities to:

(a) Separate the responsibility for risk assessment, risk treatment and monitoring compliance with risk management systems to manage conflict of interests.

ACI does not support the suggestion that it is good practice to separate (i) the identification/assessment and (ii) treatment of risk from (iii) the monitoring of the risk controls against the risk framework. This approach not only has the potential to increase the cost of an entities risk management and compliance program, but also does not recognize industry practice and developments that have seen the first two functions becoming increasingly intertwined over time as business units work closely together with compliance and risk officers. In fact ACI believes that this does not represent a conflict of interest but rather an effective and efficient program that reflects the growing adoption of broader GRC frameworks which are integrated into business units and operations thus promoting a compliance culture.

Alternatively is ASIC suggesting that it would like to see Risk as a separate function from the business? Our concern here is that in practice most risks are identified and assessed by the business unit with some help from the risk/ compliance officer(s). Treatment is devised by the risk/compliance officer(s) with help from the business unit whilst monitoring is exclusively carried out by compliance. In practice, the identification/assessment and treatment functions cannot exclusively be given to either the business unit or the risk/compliance officer(s); these are shared functions.

Another consequence of this suggestion is that the separation of these functions will require that all staff need to undertake risk training. As stated above, ACI believes risk training should be targeted to ensure it remains appropriate for personnel. Therefore some staff require very limited risk management training, whereas others require more sophisticated training. The separation of these functions has the potential to create a risk management training need that is both uniform, costly and maybe ineffective in the long term as business units often focus on profit making.

ACI is of the view that rather than trying to separate these functions, ASIC should be looking towards the integration of compliance, risk, audit and governance as suggested by a number of leading models, while at the same time ensuring that responsibility is assigned to the business in the first instance as is in keeping with the widely used 'Three Lines of Defence' model (noted in paragraph 46 of ASIC Report 298). We also believe

that guidance that recommends this approach also clarifies our earlier concerns around what constitutes an *independent* review of the 'Risk Management System'.

We acknowledge and agree with ASIC's position not to be overly prescriptive and to create some flexibility in this respect to ensure that the risk management framework that is developed is appropriate for the scale, size, scope and complexity of the RE in question (see paragraph 32 of CP204).

D1 We propose to provide guidance that in establishing and maintaining risk management systems, it is good practice for responsible entities to:...

Establish a designated risk management function and/or risk management committee to ensure that their day-to-day operation is conducted in a way that aligns with their risk management systems (this does not have to be an exclusive function).

Under s601JA(1) of the Corporations Act, the RE of a registered scheme may already be required to have a compliance committee. Section 601JC establishes the functions of the compliance committee. It appears that the compliance committee may not be able to undertake the functions of the Risk Management Committee that should be established as a result of this guide. Clarification is sought to determine if this is indeed the case, or can these related functions be undertaken by the compliance committee 'wearing a different hat' but still comprised of the same membership?

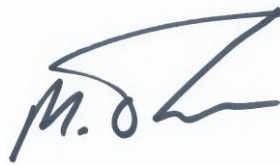
D1 We propose to provide guidance that in establishing and maintaining risk management systems, it is good practice for responsible entities to:...

(b) use internal and/or external audits to review compliance with, and the effectiveness of, their risk management systems.

From the perspective of smaller REs, ACI is concerned that these REs may not have a separate internal audit function and therefore the audit obligation may fall on the risk/compliance officer who authored the RM system. Under these circumstances, it may be difficult for the risk/compliance officer to objectively critique their own work. This would compel the small operator to seek an external audit as an alternate approach and present an additional cost to the smaller RE. In an attempt to address this issue, ACI proposes that, in these circumstances, an external review only be required every three years and that in between, an annual audit undertaken by the author be acceptable practice.

Once again ACI would like to thank ASIC for providing an opportunity for ACI to make comment on CP204. Should you require any additional information or require clarification on the comments that appear in this submission please do not hesitate to contact ACI on +612 9290 1788.

Yours sincerely,

A handwritten signature in dark ink, appearing to read 'M. Tolar', with a stylized flourish extending from the end.

Martin Tolar CCP

Managing Director

Please note that the views expressed in this submission represent those of the collective ACI membership. Consequently, individual members and organisations may hold a different perspective on some of the points raised and therefore reserve the right to make comment in their own right.