

26 February 2016

Mr. Tim Walker  
Senior Manager  
Investment Managers & Superannuation  
ASIC  
GPO Box 9827  
Sydney  
NSW 2001

**By email only:** [tim.walker@asic.gov.au](mailto:tim.walker@asic.gov.au)

Dear Mr. Walker

### **Risk Management Arrangements for Responsible Entities**

We refer to your email of 22 January 2016 and note your advice that ASIC is currently developing a new regulatory guide to help responsible entities comply with their risk management obligations under Section 912A(1)(h) of the *Corporations Act*. For the purposes of developing this guidance you are consulting with relevant stakeholders and have asked us for our comments.

### **The Financial Services Council (FSC)**

The FSC has over 115 members representing Australia's retail and wholesale funds management businesses, superannuation funds, life insurers, financial advisory networks, licensed trustee companies and public trustees. The industry is responsible for investing more than \$2.6 trillion on behalf of 11.5 million Australians. The pool of funds under management is larger than Australia's GDP and the capitalisation of the Australian Securities Exchange and is the third largest pool of managed funds in the world. The FSC promotes best practice for the financial services industry by setting mandatory Standards for its members and providing Guidance Notes to assist in operational efficiency.

### **Our Comments**

Thank you for asking us to provide our comments. We have sought input from our members and have divided our comments into two parts -in the first part we provide some general comments and in the second part, we respond, on behalf of our members, to your specific request for feedback.

#### **General Comments**

1. A common theme or issue for our membership is that there be no duplication of existing obligations for financial resources or capital requirements. This is particularly relevant for dual APRA-ASIC regulated entities. In this regard, you will see that this was raised by us in paragraph 5 of our submission of 17 May 2013. We also canvassed this issue in some detail in our submission of 17 January 2013 concerning Stronger Super Tranche IV; please refer to pages 4 and 5, sourced at the below link-  
<http://fsc.org.au/downloads/file/SubmissionsFile/130117FSC-FINALMySuperTrancheIV.pdf>

2. Another theme which our membership has raised is that the proposed Regulatory Guide will contain no more onerous obligations than currently exist (noting that you have stated that the proposed Regulatory Guide will not impose new obligations but rather explain ASIC's view of current obligations);
3. In a similar vein, members have stressed that it is important that the proposed Guide does not give rise to inconsistencies with other reporting requirements or frequency of those requirements;
4. In our view, elements of the proposed "Good Practice Guidance" in table 1 of the proposed Regulatory Guide, potentially add regulatory burdens, without commensurate benefits. We expand on this comment further below and in the attachment. However, by way of example, the requirement for an annual independent assurance that a responsible entity's (RE) risk management systems have been complied with and are operating effectively is an unnecessary imposition in regulatory burden and cost. We say this as a mature RE should already be compliant and have in place an appropriate risk management process developed by the risk function which is subject to oversight by the compliance function and also subject to internal audit review testing. The process also is subject to scrutiny by external auditors. There seems little practical benefit in adding this requirement which will ultimately increase costs to consumers.
5. It may also be useful were ASIC to provide some clarification on what it considers to be a "risk management system" given that all the systems within a firm could arguably, among other things, be considered to be managing some form of risk. Existing external audits focus on the internal control environment. Accordingly, industry would value further engagement with ASIC on this point.

### ***Responses to specific requests for feedback***

#### **(a) Will a new regulatory guide help responsible entities comply with their current risk management obligations?**

We support ASIC issuing guidance to describe the elements of a responsible entity's (RE) risk management arrangements. As the proposed Regulatory Guide will clarify ASICs expectations, REs will be able to readily measure whether their existing arrangements are appropriate, noting some REs may be at different stages of maturity on their risk management practices. However ASIC guidance should not be overly prescriptive given risk management arrangements evolve in line with prevailing market conditions, industry best practice, ASIC and other guidance and the RE should determine at its discretion, the appropriate tools and strategies to use in managing all elements of risk.

We assume this guidance will complement existing general guidance for AFS licensees relating to risk management systems contained in Regulatory Guide 104: *Licensing: Meeting the general obligations* (RG 104).

It is important that ASIC guidance be updated to also reflect changes in industry practices both locally and internationally. In this regard, we note the other guidance ASIC has provided to REs and AFS Licensees since 2004 regarding their obligations, ie. RG78 Breach reporting by AFS licensees, RG94 Unit Pricing: Guide to good practice (jointly with APRA), and the proposed Regulatory Guide on Risk Management Arrangements would complement such guidance to REs.

In summary, we confirm our previous comments and submissions that a Class Order is not required. The Corporations Act is sufficiently concise to hold REs to account. However, for the reasons we have mentioned a proposed Regulatory Guide would be useful.

**(b) Will you need to change your current risk management arrangements in order to comply with the obligatory requirements within the first column of the table? If so, please provide details.**

As a broad proposition, it appears that REs are complying with most if not all of the requirements set out in the first column of the table. However, in relation to the “best practice” guidance in the second column, we seek clarity around a number of the suggested measures (please see below).

With respect to the best practice guidance in the second column, we would like to make some additional observations. For convenience, we have set out some further observations concerning **both** the obligatory and best practice comments in the attached table. For convenience, the table adopts your points in numerical form.

The outcomes *may* be different however for some of our members who form part of global groups or are regulated by APRA or form part of an APRA level 1, 2, or 3 Group for CPS220 Risk Management and CPG220 Risk Management. This is because such groups commonly employ a comprehensive global risk management framework. Some of our members in such a position have indicated that it is likely that it will be necessary to enhance current risk management programs to:

- expand their scope to include the performance of stress testing and/or scenario analysis of market, investment and liquidity risk of relevant RE businesses;
- broaden the scope of information and reporting to the board, compliance committee and senior management in order to provide a comprehensive and regular view of all different types of material risks associated with our business, including stress testing results;
- review and, if necessary, revise policies and procedures to ensure the processes, controls and roles and responsibilities relevant to the Australian business meet the specific guidance objectives- as a number of existing risk management policies are global in nature.

However for other FSC members, they may rely on existing global risk management frameworks and will not be creating bespoke processes for their REs.

**(c) Will complying with these requirements have any cost implications for your business? eg reduce costs, no impact, negligible cost impact, additional costs (if possible please provide an estimate of any reduction or increase in costs)**

We do not expect there to be significant additional costs associated with continuing to comply with the obligatory requirements in the first column (this is subject to the comments made in (b) above).

The additional "independent" annual review processes suggested in the best practice column would add costs if external parties are required to be appointed to undertake these assessments. Further comments in this regard are set out in the attachment. For example, one of our members has estimated the following increases in cost in respect of the “best practice” elements-

- in the order of \$20,000 to \$75,000 per annum for smaller REs and in the order of \$75,000 to \$200,000 for larger entities;
- triennial reviews may cost in the order of 150% of these annual costs;
- management time in the order of between \$100, 000 and \$300,000 will be expended depending on the size and complexity of the schemes managed by the RE.

There may also be some REs who undertake internal controls reporting in accordance with GS007, SSAE No. 16).

For some FSC members, they will be relying on independent assurance performed on the global or group risk management framework.

**(d) Is there any other guidance that would help responsible entities to better manage risks on an ongoing basis?**

In our view, a well-drafted regulatory guide should be adequate in terms of communicating your expectations of an RE's risk management arrangements that satisfies its ongoing legal obligations under section 912A(1)(h) of the Corporations Act. The guidance should not be overly prescriptive given the RE's risk management arrangements should contain controls commensurate with the level of risk presented by the scale, nature and complexity of its business/operations for running registered MISs.


Other guidance which may prove useful is the provision of comments on the observations ASIC has made in performing its regulatory supervision function. We note that ASIC has previously provided overviews, via its media releases, of compliance issues identified during its proactive surveillance of REs. These are a useful insight into what ASIC expects of REs and areas of deficiency it has identified.

We also note that it would be useful and beneficial if there were more ASIC focus on the investment risk component rather than the risk management framework design elements and the leveraging of the SPS530 type regimes – we propose that ASIC undertake further consultation on these points.

Finally, we ask the following of ASIC:

- That ASIC consult with APRA and provide a joint regulatory approach to Risk Management – a similar exercise conducted in July – December 2004 prior to issuance of RG94 Unit Pricing: Guide to good practice;
- A reasonable transition period to comply/adopt the requirements of the proposed Regulatory Guide;
- REs/industry to be invited to provide further feedback prior to ASIC finalization of the proposed Regulatory Guide

**Yours Sincerely**



**Paul Callaghan**  
General Counsel

cc: [Sarah.Simmons@asic.gov.au](mailto:Sarah.Simmons@asic.gov.au)  
[Leanne.Damary@asic.gov.au](mailto:Leanne.Damary@asic.gov.au)  
[Leah.Quach@asic.gov.au](mailto:Leah.Quach@asic.gov.au)

**ATTACHMENT**

<p><b>Reference- (b) Will responsible entities need to change current risk management arrangements in order to comply with the obligatory requirements within the first column of the table (see attached)? If so, please provide details.</b></p> <p><b>Responsible entities should: maintain documented risk management systems that support:</b></p>	
<p><b>1. a risk governance structure</b></p>	<p>Entities that hold an AFSL should already be compliant; however, some of the smaller, less sophisticated REs may have simpler governance structures. Accordingly, ASIC should clarify its expectations, recognising different levels of sophistication/maturity within the industry and exercising caution not to introduce requirements that would unnecessarily detrimentally impact on costs and fees.</p>
<p><b>2. clearly defined roles and responsibilities</b></p>	<p>As above.</p>
<p><b>3. policies and procedures for identifying, assessing and understanding each of the material risks of the responsible entity's business and schemes it operates</b></p>	<p>As above</p>
<p><b>4. policies and procedures for ensuring that there is adequate controls in place to manage the risks identified</b></p>	<p>As above.</p>
<p><b>5. policies and procedures for ensuring there is adequate oversight of the risk management systems by both the party responsible for ownership of the risk and the compliance function including appropriate reporting</b></p>	<p>This will present a shift for many REs. It will introduce additional cost and present risk in respect in that there is the potential for blurring of responsibilities. Furthermore, it is not clear as to what risk this is addressing as risk management and compliance are distinct disciplines. Larger REs, as pointed out in REP298, already benefit from sufficient segregation. Introducing similar structures and overheads for smaller REs may not be fit for purpose and could detrimentally impact fees charged to investors in the longer term.</p>
<p><b>6. a policy or statement on its risk appetite and the risk tolerance for each material risk identified</b></p>	<p>Dual Regulated organisations are likely to have existing Risk Appetite Statements (<b>RAS</b>). We would be grateful if ASIC could clarify whether an RE which already has a comprehensive RAS due to it being prudentially regulated by APRA will meet your expectations.</p>
<p><b>7. foster a strong risk management culture</b></p>	<p>As above for questions 1-4.</p>
<p><b>8. have regard to relevant industry and International standards</b></p>	<p>Some REs do consider international standards; however, an RE should be responsible for ensuring its risk management system incorporates and meets relevant <u>local</u> industry standards (and regulations). It should not be expected to be fully abreast of and compliant with international standards, i.e Australian &amp; New Zealand Standard AS/NZS ISO</p>

	31000:2009, Risk Management – Principles and Guidelines, that are not enforced locally. It is the local regulators’ responsibility to encourage (e.g. prudential practice guides) or implement international standards and regulations as appropriate through the local regulatory framework.
9. include as a component of the risk management systems, a liquidity risk management process to ensure the scheme has adequate financial resources to meet its redemption obligations and other financial obligations as and when they fall due	<p>We agree with the sentiment of this requirement, particularly in the context of REs appointing third party managers (noting there is precedent for this specific requirement for APRA regulated entities as part of their Investment Governance arrangements –where a liquidity management plan is required).</p> <p>ASIC should bear in mind that the Corporations Act already requires PDSs to disclose investments risks.</p>
10. Ensure the board or its delegate reviews that the risk management systems have been complied with, are operating effectively and remain current on at least an annual basis and more frequently as required having regard to the nature, scale and complexity of the business; and	<p>This should be happening already through the required statutory audits (FS70 and Compliance Plans), which should highlight if risk systems are degrading. Thus, we suggest this should be considered in conjunction with the Compliance Plan RGs to ensure there is no duplication.</p> <p>In respect of larger REs who benefit from a more mature enterprise risk management framework, the RE Board or Compliance Committee through its reporting from Line 2 risk functions should already be receiving ongoing updates with regards to the operation of the risk management framework. An annual process is too frequent for a complete formalised framework review, a three year stock take is more beneficial and more in keeping with the pace of change in the external context.</p> <p>Evidence of regular review of component parts of risk and compliance arrangements and reporting on such should be sufficient in conjunction with a three year review. REs that form part of a larger group and leverage an enterprise management framework should be able to rely on company-wide risk reviews along the lines of those required by APRA Prudential Standard CPS220 Risk Management.</p>
11. if relying on external service providers for risk management functions maintain a strong understanding of risk management and sufficient skills to independently monitor and assess the performance of the service provider.	As above
Responsible entities should:	
12. keep a risk register as part of their risk identification and	This should already be common practice.

assessment process	
<b>13.</b> ensure that its risk management systems address all material risks, including (but not limited to) credit risk, market and investment risk, liquidity risk, insurance risk, operational risk and strategic risk at both the responsible entity and scheme level;	<p>While it is important to consider risks at an RE and scheme level, existing risk management systems may consider these risks more holistically. A requirement imposing risk registers at RE and scheme level may impose duplication of risk assessment approaches and it is more important to ensure that the relevant risks have been considered, rather than specifying at what level these are to be considered.</p> <p>Creating layers of risk registers (at organisational, RE and scheme level) may in fact lead to over complication and result in risk registers being less effective.</p>
<b>14.</b> when choosing methodologies for identifying and assessing risks to have regard to the nature, scale and complexity of the business; processes based on forward looking analysis; ensuring an appropriate level of human input; ensuring board involvement in the process; and whether different processes should be used for different schemes; and	As above; this should not be presenting a seismic shift in processes.
<b>15.</b> adopt appropriate methods to assess risks which may include: Self - assessment; Risk - mapping; Information technology; and	As above. In addition, as mentioned in our response to question 1, we would be grateful if ASIC could clarify its expectations in this regard.
Responsible entities should:	
<b>16.</b> implement appropriate strategies for managing each of the risks identified, including; conducting stress testing and/or scenario analysis of market and investment risk and liquidity risk of the business and the schemes they operate as part of their risk management systems on at least an annual basis and more frequently as required having regard to the nature, scale and complexity of the business	<p>The concept of stress testing or sensitivity analysis is certainly a step forward in risk management practices and is worthy of being considered more fully. REs however, will need to be efficient in this practice as existing stress testing may be sufficient, i.e. tracking error processes and portfolio stresses in respect of liquidity. This would require a step forward in risk maturity across the industry should it extend to the gambit of risks presented to REs.</p> <p>While the market needs to move to this level of sophistication there will be costs for smaller REs to implement this and therefore ASIC should consider appropriate timing and transitional measures.</p>
<b>17.</b> reviewing their framework for stress testing and/or scenario analysis on at least an annual basis and more frequently as required having	As per above comments with regards to independent reviews – in terms of scenario frequency REs would benefit from selecting a single scenario and then testing it across the RAS against tolerances and the risk register itself to confirm that a) the risk is documented and

regard to the nature, scale and complexity of the business to ensure the tested scenarios are relevant and appropriate in light of the business and market conditions; and	b) the controls were sufficient or require improvement.
<b>18.</b> if stress testing and/or scenario analysis is not conducted, document why this is the case, keep appropriate internal records of this rationale, and review this decision at appropriate intervals	Agree.
<b>19.</b> have adequately experienced staff regularly review and monitor the risks identified	This should already be in place.
<b>20.</b> ensure there is regular reporting and escalation of issues to the board, risk committee and compliance committee as appropriate	As above and earlier comments with regard to meeting existing obligations.
<b>21.</b> maintain adequate professional indemnity insurance as required under by the Corporations Act and AFS licence conditions	Already a requirement.
<b>22.</b> keep adequate records relating to the establishment, implementation and review of its risk management systems	Already a requirement.
<b>23.</b> maintain secure information systems; and	Already a requirement.
<b>24.</b> ensure compliance with the financial requirements which apply to responsible entities	Already a requirement.
<p><b>See comments below with respect to each point in the 'Good practice guidance' section of the table.</b></p> <p><b>Responsible Entities may:</b></p>	
<b>25.</b> at least annually obtain an independent assurance that the risk management systems have been complied with and are operating effectively	<p>See comments under paragraph 10 above. In our view, this will lead to higher costs and fees and an annual frequency is arguably too frequent to add real benefit.</p> <p>In any event, clarification is sought as to whether use of an Internal Audit function is an independent assurance. If the requirement is to engage an external party, an "annual review" is certainly very onerous. By utilising internal audit, a regular review becomes more manageable. Nevertheless, as mentioned we do question whether an <b>annual review</b> adds any benefit or value.</p>



<p><b>26.</b> at least every three years have a comprehensive review of the appropriateness, effectiveness and adequacy of the risk management systems by an operationally independent, appropriately trained and competent person</p>	<p>We believe this will benefit the industry and investors.</p> <p>Again, there is an issue as to whether Internal Audit functions would satisfy the tests proposed-certainly, an Internal Audit centre is operationally independent of the risk function. Clarification would be appreciated.</p> <p>A triennial review may be too prescriptive however. In order to cover the multiplicity of situations which can arise, the timing requirement should be along the lines of "Regularly, but no less than every five years". For completeness, we note that this suggestion is similar to an existing Prudential Standard requirement for <b>APRA-regulated</b> institutions such as banks, superannuation fund trustees, insurance companies, and friendly societies, where APRA functions to protect the interests of depositors, policy holders and fund members. The APRA focus however is quite different from that of ASIC and cannot necessarily be transposed to the ASIC regulatory context.</p> <p>Again, for completeness, we assume that this is only intended to be aspirational and not mandatory.</p> <p>We also note that there should be some clarification provided around the distinctions between annual independent assurance above in 25 and the review mentioned here.</p>
<p><b>27.</b> separate the responsibility for risk identification, assessment, risk management and compliance with risk management systems to avoid conflicts of interest</p>	<p>We seek more clarity here. As we understand it, the suggestion is that risk identification, assessment, management, etc. should be independent of each other. Risk identification, assessment and management should be embedded in the business. There should be appropriate oversight of these processes through risk and compliance stakeholders, the Board and/or Compliance Committee, who receive reporting on such matters, and where required, validate that actions plans have been completed. These processes and functions are therefore not necessarily independent of each other. The business functions then of our membership operate in tandem insofar as risk identification, assessment and management are concerned. This requirement appears to be overly restrictive.</p>
<p><b>28.</b> establish a designated risk management function and/or risk management committee; and</p>	<p>We suggest firstly that this is not necessary if the Board and Compliance Committees operate effectively. Secondly, for larger REs, Audit, Risk &amp; Compliance Committees (ARCCs) would already be in place which should provide sufficient comfort.</p>
<p><b>29.</b> publicly disclose appropriate details of its risk management policies.</p>	<p>It is not entirely clear to us what the intention is in this regard. If REs have adequate compliance plans, then documented risk management systems should already be available.</p>

	In addition, the PDSs of an RE's products generally would provide appropriate disclosure about risk management.
<b>30.</b> Have a written risk treatment plan	We would expect that the operating controls for risk and identified compliance plan obligations are documented.
<b>31.</b> Include in the compliance plan for their schemes, procedures for ensuring that the key risks identified for the responsible entity and relevant scheme are managed on an ongoing basis	<p>As noted in 30, we anticipate that the broad parameters for this process would be set out in the compliance plan documentation.</p> <p>However, we do note that the inclusion of detailed procedures in the compliance plan around key risks and their management, and ensuring they remain up to date, would become an onerous task. As key risks are reviewed and managed on an ongoing basis, regularly updating the compliance plans would become costly and inefficient, impacting the cost of products.</p>