Australian Institute of Superannuation Trustees

19 January 2015

Mr Pat Brennan
General Manager, Policy Development
Policy, Statistics & International Division
Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001

Email: superannuation.policy@apra.gov.au

Dear Mr Brennan,

Re: Consultation on draft Prudential Practice Guide SPG 223 Fraud Risk Management (SPG 223)

The Australian Institute of Superannuation Trustees is a national not-for-profit organisation whose membership consists of the trustee directors and staff of industry, corporate and public-sector funds.

As the principal advocate and peak representative body for the $600 billion not-for-profit superannuation sector, AIST plays a key role in policy development and is a leading provider of research.

AIST provides professional training, consulting services and support for trustees and fund staff to help them meet the challenges of managing superannuation funds and advancing the interests of their fund members. Each year, AIST hosts the Conference of Major Superannuation Funds (CMSF), in addition to numerous other industry conferences and events.

In brief:
AIST supports practical guidance on fraud risk but this should be consistently provided for banking, insurance and superannuation. The PPG should also address bribery, corruption, IT and outsourcing fraud risk, especially administration-related, in more detail, and provide more clarity about expectations and useful case studies.

AIST welcomes the opportunity to provide comments on this draft Prudential Practice Guide (PPG). As the $1.85 trillion superannuation sector continues to grow, the industry will increasingly be the target of fraud and other criminal activity.

AIST welcomes guidance that better assists trustees to meet their obligations of acting in members' best interests.

Ground Floor
215 Spring St
Melbourne VIC 3000

T +61 3 8677 3800
F +61 3 8677 3801

info@aist.asn.au
www.aist.asn.au

Summary of recommendations

AIST recommends that:

- APRA develops a co-ordinated approach to fraud risk management across the industries it regulates;
- The PPG adopt and incorporate the approach to controlling fraud and corruption in the Fraud and Corruption Control Standard AS 8001-2008;
- The PPG be expanded to include more case studies and examples with associated commentary on APRA's expectations;
- Material outsourced provider fraud be added as a third category of fraud risk and that that the definition more clearly recognises that fraud may involve more than one category of fraud risk;
- APRA provide RSE licensees with best practice guidance on effectively managing bribery and corruption risk, either in this or a separate best practice guide;
- The sentence in paragraph 21 about the disclosure of risk appetite to third parties be deleted, and be replaced by a statement acknowledging that RSE licensees may reasonably keep their risk appetite statement confidential;
- APRA clarify its expectations in respect of a fraud control plan;
- APRA provide additional guidance in the PPG on the provision of independent fraud risk assurance by internal auditors;
- The reference to incentives in paragraph 22(c) be deleted;
- The paragraphs on investment risk be rewritten to more clearly differentiate between investment risk and fraud risk;
- The PPG be amended to provide APRA's view on sound practice on managing fraud risk in outsourced administration; and
- The fraud prevention controls be amended to include more examples of IT-related controls.

Draft Prudential Practice Guide SPG 223 – Fraud Risk Management

As a prudential practice guide, this SPG has the task of assisting RSE licensees to better understand the requirements of Prudential Standard SPS 220 Risk Management, and to outline prudent practices in relation to the management of fraud risk.

The superannuation industry has grown almost fourfold in terms of assets since APRA released its last best practice guide for trustees *How to reduce the risk of fraud*. This, plus the addition of superannuation prudential standard making power by APRA and the release of SPS 220, makes the release of this PPG appropriate.

Ground Floor
215 Spring St
Melbourne VIC 3000

T +61 3 8677 3800
F +61 3 8677 3801

info@aist.asn.au
www.aist.asn.au

Cross-industry approach

AIST notes that Prudential Standard *CPS 220 Risk Management* applying to authorised deposit-taking institutions and life companies does not have a corresponding SPG on fraud risk, and we wonder why this is the case.

We note that APRA has generally sought to apply a cross industry approach to the operation of prudential standards where this is practical and appropriate. In this case, it is suggested that a common approach to fraud risk would also be more efficient for RSE licensees, APRA and the other sectors regulated by APRA.

It would not be efficient for this SPG to be settled for RSE licensees, only to then be revisited after consideration of fraud risk management in other sectors regulated by APRA. Similarly, we do not imagine that regulated entities in other sectors would be pleased if expectations were set in this SPG for the treatment of fraud risk that might impinge on their business operations.

AIST recommends that APRA develops a co-ordinated approach to fraud risk management across the industries it regulates.

Australian Standard AS 8001-2008 – Fraud and corruption control

The Fraud and Corruption Control Standard[1] provides an important outline for controlling fraud and corruption in a wide range of entities, and draws on anti-fraud and anti-corruption initiatives and pronouncements developed in Australia and elsewhere. It should therefore be given greater prominence than just a footnote in the PPG.

AIST recommends that the PPG adopt and incorporate the approach to controlling fraud and corruption in the Fraud and Corruption Control Standard AS 8001-2008.

Flexibility

While AIST strongly support PPGs allowing RSE licensees to have flexibility to structure their business operations in a way best suited to achieving their business objectives, this would be complemented by this PPG giving clearer and more detailed examples of APRA's expectations. This also aids the consistent application of SPS 220 and provides a 'no surprises' basis for prudential reviews – for both APRA and the RSE licensee.

It does not serve the interests of any party for a PPG to state that an RSE is able to respond flexibly to the requirements of an SPS only to subsequently find that it has a different view about the range of allowable flexibility than APRA.

[1] *AS 8001-2008: Fraud and Corruption Control* (2008) Sydney: Standards Australia.

It is noted that APRA's previous best practice guide for trustees *How to reduce the risk of fraud* included illustrative case studies.

AIST recommends that the PPG be expanded to include more case studies and examples with associated commentary on APRA's expectations.

Paragraph 2 – Types of fraud risk

The use of third-party providers is endemic to the superannuation industry, and Prudential Standard SPS 231 that sets out the requirements relating to outsourcing recognises this. Throughout this submission, AIST identifies the significance of outsourcing in relation to fraud risk management but does not always come to the same conclusion as APRA.

The dichotomy of fraud risk between internal and external fraud is not always as clear-cut as suggested in paragraph 2. Fraud can also involve collaboration between internal and external parties, and between ostensibly separate third parties (e.g., between employees of a custodian and an administrator acting in collusion). The SPG definition of internal fraud includes fraud which involves at least one internal party meaning that a fraud involving largely external parties could be defined as internal fraud.

As an alternative, AIST suggests a third category of fraud, material outsourced-provider fraud and stronger recognition of the possibility that fraud might involve a combination of these categories.

As APRA is well aware, some RSE licensees have outsourced the majority of functions and their associated transactions to third-party administrators, custodians, asset consultants, investment managers and insurers. Many of these functions are covered by the material outsourced provider requirements of SPS 231, and fall in the space between internal and external activities.

AIST recommends that material outsourced provider fraud be added as a third category of fraud risk and that that the definition more clearly recognises that fraud may involve more than one category of fraud risk.

Paragraph 4 – Bribery and corruption

Bribery and corruption are identified in the Introduction as being included in fraud risk, but neither rates a mention again in the PPG until Appendix A. However, other than providing some limited examples of bribery and corruption in Appendix A, the PPG does not provide assistance to RSE licensees about the treatment of bribery and corruption.

As RSE licensees manage larger and larger pools of money on behalf of their members, and as they increasingly have direct investments in areas such as infrastructure and private equity, bribery and corruption risk may increases as well.

Ground Floor
215 Spring St
Melbourne VIC 3000

T +61 3 8677 3800
F +61 3 8677 3801

info@aist.asn.au
www.aist.asn.au

These are important matters, and the PPG should either be expanded to provide assistance and views on sound practice or APRA should provide separate and more detailed guidance on bribery and corruption risk management.

It is noted that neither bribery nor corruption rated a mention in APRA's last best practice guide for trustees *How to reduce the risk of fraud*, and this should now be redressed.

AIST recommends that APRA provide RSE licensees with best practice guidance on effectively managing bribery and corruption risk, either in this or a separate best practice guide.

Paragraphs 7, 8 & 21– Communicating approach to managing fraud risk

AIST agrees that effective communication with staff about policies relevant to managing fraud risk (e.g., whistleblowing policy) is prudent practice. However, this is an area where there should be limits to transparency, as excessive disclosure may increase rather than decrease fraud risk.

For example, knowledge that an institution actively pursues instances of fraud above a disclosed minimum may serve to encourage fraudulent activity below the minimum level. This is an issue both with public disclosure and disclosure to staff and service providers.

Every AIST member involved in this consultation has responded negatively to the statement in paragraph 21 that:

> *A prudent licensee would inform third parties, such as contractors and suppliers, of its risk appetite in respect to fraud to strengthen the overall risk culture of the licensee.*

While having a culture that promotes ethical behaviour clearly mitigates against fraud risk, the communication of fraud appetite does not. The risk appetite statement and the promotion of a risk-averse culture are both important elements in managing fraud risk, but they are separate requirements and should not be conflated.

We note for example that paragraph 11 of the Prudential Practice Guide *SPG 220 Risk Management* states:

> *Trustees may wish to consider whether security considerations preclude some components of the RMS, such as the fraud control plan, being included in the RMP which is available to members.*

We suggest that similar guidance be provided in this PPG.

AIST recommends that the PPG clarify that it is reasonable for RSE licensees not to disclose any information that may assist fraudulent activity.

AIST recommends that the sentence in paragraph 21 about the disclosure of risk appetite to third parties be deleted, and be replaced by a statement acknowledging that RSE licensees may reasonably keep their risk appetite statement confidential.

Paragraph 16 – Fraud control plan

The nature of a fraud control plan and its relationship to the fraud risk management framework is unclear from the PPG. Is this the same fraud control plan that is component of the Risk Management Strategy, or does APRA have expectation of another or an expanded plan?

Similarly, the relation between the fraud risk management framework and the Operational Risk Financial Framework should be clarified.

If APRA have a clear expectation of the structure and content of such a plan this should be articulated in the PPG. If, however, this is an area where APRA accept that there could be a range of sound practices and plans, then this should also be articulated.

AIST recommends that APRA clarify its expectations in respect of a fraud control plan.

Paragraphs 20 & 50 – Internal audit

RSE licensees employ a range of audit functions, including internal audit functions that involve both employees of the RSE licensee and externally-sourced internal auditors.

AIST recommends that APRA provide additional guidance in the PPG on the provision of independent fraud risk assurance by internal auditors.

Paragraph 22 – Incentives

It is understood that performance incentives have to be aligned to the objectives and requirements of the RSE licensee, and its performance. However, the notion of offering incentives to promote a strong risk culture looks at incentives in the wrong way. Incentives should be set in a way that do not encourage or implicitly reward inappropriate, wrong or fraudulent behaviour.

Melbourne media has recently reported on trains intentionally missing stations in order to meet punctuality targets, and so meet standards of service and avoid penalties. Similar behaviour within financial institutions in order to obtain financial reward for meeting performance targets would be just as wrong. The experience of commissions being paid to sell financial products regardless of the best interests of clients is evidence of this.

A strong risk culture should not be an optional extra within a RSE licensee and employees should not be paid incentives for developing such a culture.

Ground Floor
215 Spring St
Melbourne VIC 3000

T +61 3 8677 3800
F +61 3 8677 3801

info@aist.asn.au
www.aist.asn.au

AIST recommends that the reference to incentives in paragraph 22(c) be deleted.

Paragraph 44– Improper registration of an RSE

AIST is surprised to read that it is APRA's experience that a common type of fraud involves the improper registration and use of a RSE's assets.

AIST recommends that APRA provide case studies of common types of fraud, and encourage the superannuation industry to undertake fraud management workshops.

Paragraphs 46 to 49 & Attachment A – Investment risks

Investment risks are not fraud risks. While investing involves risks, and due diligence and management of conflicts of interests are part and parcel of the investment process, care should be taken not to conflate these risks.

In particular, the comments in paragraph 48 about ensuring that the RSE licensee has sufficient expertise or independence to make an objective assessment is relevant to all parts of the investment process, and not just fraud risk.

This conflation is further evidenced in Attachment A where many of the characteristics given of investments that may create potential for fraud are characteristics that are routinely considered in the assessment of investments generally.

AIST recommends that the paragraphs on investment risk be rewritten to more clearly differentiate between investment risk and fraud risk.

Paragraph 50 – Outsourcing risks

In contrast to the attention paid to investment risk, there is no explicit reference made to the risk of outsourcing administration services.

Where administration is outsourced, the provider typically manages members' accounts, allocation of contributions and rollovers to (and from) member accounts, recording and changing member details, merging accounts and arranging benefit payments. Additionally, the administrator may manage fund accounting, accounts payable and other functions. In short, the extent of this outsourcing should be explicitly identified and addressed in the PPG.

AIST recommends that the PPG be amended to provide APRA's view on sound practice on managing fraud risk in outsourced administration.

Ground Floor
215 Spring St
Melbourne VIC 3000

T +61 3 8677 3800
F +61 3 8677 3801

info@aist.asn.au
www.aist.asn.au

Attachment B – Examples of fraud prevention controls

The examples appear to be a reworked version of APRA's *Superannuation Fraud Checklist* but does not seem to have given increased weight to the increased potential for and incidence of internet fraud. For example, there is no reference to the fraud risks of penetration tests, where attacks on the RSE's system are aimed at finding security weaknesses and gaining access to it.

AIST recommends that the fraud prevention controls be amended to include more examples of IT-related controls.

***

If you have any further questions regarding this submission, please contact David Haynes, Executive Manager, Policy & Research on 03 8677 3804 or at dhaynes@aist.asn.au .

Yours sincerely,

Tom Garcia
Chief Executive Officer

Ground Floor
215 Spring St
Melbourne VIC 3000

T +61 3 8677 3800
F +61 3 8677 3801

info@aist.asn.au
www.aist.asn.au