Draft APRA *Prudential Practice Guide PPG 235 Managing Data Risk*

29 March 2013

AIST Submission

AIST

The Australian Institute of Superannuation Trustees (AIST) is an independent, not-for-profit professional body whose mission is to protect the interests of Australia's $500 billion not-for-profit superannuation sector. AIST's members are the trustee directors and staff of industry, corporate and public-sector superannuation funds, who manage the superannuation accounts of two-thirds of the Australian workforce.

AIST is a registered training organisation and has recently expanded its education program to encompass the growing and changing needs of all members of the not-for-profit superannuation sector.

AIST offers a range of services including compliance and consulting services, events - both national and international - as well as member support. AIST also advocates on behalf of its members to relevant stakeholders.

AIST's services are designed to support members in their endeavour to improve the superannuation system and build a better retirement for all Australians.

Contact

Tom Garcia, CEO	tgarcia@aist.asn.au	03 8677 3800
David Haynes, Project Director	dhaynes@aist.asn.au	03 8677 3800

AIST
Australian Institute of Superannuation Trustees
Ground floor 215 Spring St
Melbourne VIC 3000

T 61 3 8677 3800
F 61 3 8677 3801
E info@aist.asn.au
www.aist.asn.au

Executive summary

AIST welcomes PPG 235 as a useful tool in assisting regulated superannuation funds and other regulated entities in managing data risk.

AIST makes some minor but important suggestions:

- Overall, the PPG should use more language and examples that are relevant to the superannuation industry.
- The PPG should be more closely aligned with the Prudential Standard SPS 220 "*Risk Management*", and visa versa.
- There should be a requirement for the management of data risk to be explicitly addressed in a fund's risk appetite statement.
- PPG 235 should be amended to identify data risk as a material risk.
- The PPG should provide additional guidance both to the superannuation industry and to individual funds about the minimum data risk controls required by APRA.
- The PPG should more clearly identify the need to prioritise a hierarchy of data management issues within a fund's data risk management framework.
- The PPG should be more closely aligned with the Prudential Standard SPS 231"*Outsourcing*", and visa versa.
- The data risk management responsibilities of super funds at a fund member and beneficiary level should be more clearly identified and articulated.

ABN 19 123 284 275

AIST
Australian Institute of Superannuation Trustees
Ground floor 215 Spring St
Melbourne VIC 3000

T 61 3 8677 3800
F 61 3 8677 3801
E info@aist.asn.au
www.aist.asn.au

General commentary

AIST welcomes the opportunity to comment on the Draft APRA Prudential Practice Guide PPG 235 "*Managing Data Risk*".

AIST also recognises the critical importance of managing data risk, and agrees that further APRA guidance in this area strengthens the prudential framework.

AIST understands and supports the alignment of the superannuation prudential framework with banking and insurance, and notes that PPG 235 will be applied across APRA's areas of responsibility.

However, this needs to be balanced and expanded by the need to ensure that the document is also appropriately referenced to superannuation structures and the priority superannuation data management issues, and to other APRA documentation and requirements. Relating to superannuation

Similarly, the PPG should be more closely aligned with the Prudential Standard SPS 220 "*Risk Management*", and visa versa. Curiously, and by example, there is no explicit requirement in SPS 220 for a fund's risk management framework to cover data risk.

While it is self-evident that data risk is an "*other risk that may have a material impact on the RSE licensee's business operations*." (SPS 220, 12(g)), its invisibility in SPS 220 suggests that it is a lower priority risk. SPS 220 should be amended to explicitly list data risk as a minimum requirement in a fund's risk management framework.

SPS 220 also requires funds to maintain a risk appetite statement that covers a fund's business operations and each category of material risk. While data risk is not identified by SPS 220 as a material risk, it should be. PPG 235 should also be amended to identify data risk as a material risk.

The inclusion of data risk in a risk appetite statement is appropriate but PPG 235 makes no reference to a fund's risk appetite. In managing data, fund's and there service providers regularly manipulate data. Data can be moved from one organisation to another; it can be moved from one IT system to another; it can be analysed, aggregated and reported upon; it can be used for purposes other than the primary or initial reason for which it was collected or obtained; it can be modified, updated and corrected.

ABN 19 123 284 275

AIST
Australian Institute of Superannuation Trustees
Ground floor 215 Spring St
Melbourne VIC 3000

T 61 3 8677 3800
F 61 3 8677 3801
E info@aist.asn.au
www.aist.asn.au

There are risks associated with the collection, storage, movement and manipulation of data, and at each stage there is the prospect of error, lack of reconciliation, estimation and approximation. On the one hand, funds have a zero tolerance (or appetite) for data errors, on the other hand, there is a recognition that some errors will occur. The issue for funds – and APRA – is what levels of data issues are tolerable, and what is not?

Different data items will have different levels of importance, criticality and relative importance that should be identified and agreed to. For example, a fund may be missing the title of some of its members, and may be aware that the titles of some other members may be incomplete or out of date. While this should be identified at the member level and corrected, it is a much lower priority than, say, a unit-pricing error. A fund's risk appetite statement could identify a fund's tolerance for different types of data issues and the priority of each.

ABN 19 123 284 275

AIST
Australian Institute of Superannuation Trustees
Ground floor 215 Spring St
Melbourne VIC 3000

T 61 3 8677 3800
F 61 3 8677 3801
E info@aist.asn.au
www.aist.asn.au

Comments

Paragraph 1.

The PPG identifies that weaknesses in data risk management continue to be identified as part of APRA's ongoing supervision activities. In addition to giving generic examples of data risk such as provided in paragraph 11, the PPG should specifically identify both the category and examples of specific superannuation risk so that trustees are better able to identify and respond to superannuation-specific risks. This focus will mean that funds are more likely to act in a pro-active manner, with a corresponding reduction in matters identified in APRA's supervision activities.

Paragraphs 2 and 20 to 30.

Paragraph 2 is somewhat ambiguous. Paragraph 20 calls on funds to adopt a systematic and formalised approach, with paragraphs 20 to 30 identifying the elements that could be encapsulated in a formally approved data risk management framework. In contrast, paragraph 2 states that the PPG does not seek to provide an all-encompassing framework, and tantalisingly notes that there will be additional areas not addressed in the PPG.

If APRA is aware of other areas not specified in the PPG that should be subject to appropriate controls then these should be specified.

If paragraph 2 means that funds have the discretion to adopt an alternative risk-based approach (for example, a fund may consider that a different approach to exemptions management to that specified in paragraph 25 may be appropriate), then this should either be made clear. Alternatively, this paragraph could specify that funds are required to follow the details of the systematic and formalised approach spelt out in paragraph 20 to 30. Either approach seem to be possible under the terms of Prudential Standard SPS 220.

Most funds already have well-developed risk management frameworks that have been developed in consultation with APRA. It would be inappropriate and an inefficient use of fund resources for funds to be required to establish a new data risk frameworks. APRA should provide additional guidance both to the superannuation industry and to individual funds about the minimum data risk controls required by APRA.

Paragraph 7.

The PPG identifies a number of data management organisations by name in Paragraph 7 but states that their documentation can be used for guidance but is not endorsed.

ABN 19 123 284 275

AIST
Australian Institute of Superannuation Trustees
Ground floor 215 Spring St
Melbourne VIC 3000

T 61 3 8677 3800
F 61 3 8677 3801
E info@aist.asn.au
www.aist.asn.au

These references nonetheless provide tacit support for the guidelines and standards issued by these bodies. It would be more useful if this paragraph used the more positive language used in Paragraph 6 of Prudential Practice Guide PPG 234 – "*Management of security risk in information and information technology*", so that the relevant paragraph reads:

> *"A regulated institution would typically use discretion in adopting appropriate industry standards and guidelines in specific control areas. In APRA's view, useful guidance may also be obtained from industry accepted standards such as the International Association for Information and Data Quality, Data Management Association, International Organization for Standardization and Standards Australia in that they provide broad frameworks for establishing and maintaining control environments."*

Paragraphs 8 and 46 to 49.

Outsourcing is an important feature of the Australian superannuation system, the operation of which has generally served funds and their members well. Outsourcing requirements are contained in Prudential Standard SPS 231. The factors used to determine if outsourcing is a material business activity are congruent with many risk factors. A fund's outsourcing policy should including provisions for managing risk.

Paragraphs 46 to 49, and in particular, paragraph 49, should be more closely aligned with SPS 231. For example, the references in SPS 231 about taking into account the changes in the risk profile of the outsourced provider (19(d)), established procedures for monitoring performance on a continuing basis (19(h) and developing contingency plans (19(j)) should be replicated in PPG 235.

Paragraph 23 and 39.

Paragraph 23 addresses the data management responsibilities of staff, but is silent on data management responsibilities to members. Presumably, the reference to "data users" does not include super fund members: if it does, it is too vague. Much fund data is member data, be it account balance, contribution, tax, fee, insurance fees and cover, application of investment returns or demographic information.

The roles and responsibilities should be expanded to explicitly cover data management responsibilities to super fund members. This could include the publication on funds' webpages of their data risk policies, and information to members about the process to

ABN 19 123 284 275

AIST
Australian Institute of Superannuation Trustees
Ground floor 215 Spring St
Melbourne VIC 3000

T 61 3 8677 3800
F 61 3 8677 3801
E info@aist.asn.au
www.aist.asn.au

be followed for the correction of incorrect data. This may be linked with a fund's dispute resolution policy.

It is noteworthy that paragraph 39 does not refer to members or beneficiaries, referring instead to "customers". Superannuation funds operate as trusts with trustees being responsible for the prudent management of members and beneficiaries interests. While the PPG has wider application, this terminology should nonetheless be amended for super funds.

Paragraph 43.

It would be useful if the consistency and replicability of data were included as a subset of auditability (these comments are also relevant to paragraph 18). Consistency of information is important for member confidence in superannuation, and lack of confidence in data quality and consistency is a risk factor.

The PPG should also be amended here to emphasize the importance of managing data risk at a member level. Information is variously provided to members in annual member statements, six-monthly records of contributions, information provided to members by call centres and on fund websites, and on the ATO's SuperSeeker website. That is consistency of a fund's data.

In addition, funds also need to be able to replicate previous account balances at a member level, showing how the receipt of contribution of contributions and rollovers, and the deduction of contributions tax, insurance premiums and fees explain the difference between opening and closing balances. The other key member data includes full name, home address, and Tax File Number.

This is also relevant to the need for consistency between super funds. This has always been important but becomes more so with the introduction of the mandated SuperStream data and payment standards and the ATO's enhanced online SuperSeeker service.

These changes mean that there are minimum data quality standards for rollovers and contributions. This will increase the level of data quality in the superannuation system, and the PPG should be amended to encourage super funds to have the same minimum data quality standards for the data they hold, even if it is not being transferred to a member or another entity.

[end]

ABN 19 123 284 275

AIST
Australian Institute of Superannuation Trustees
Ground floor 215 Spring St
Melbourne VIC 3000

T 61 3 8677 3800
F 61 3 8677 3801
E info@aist.asn.au
www.aist.asn.au