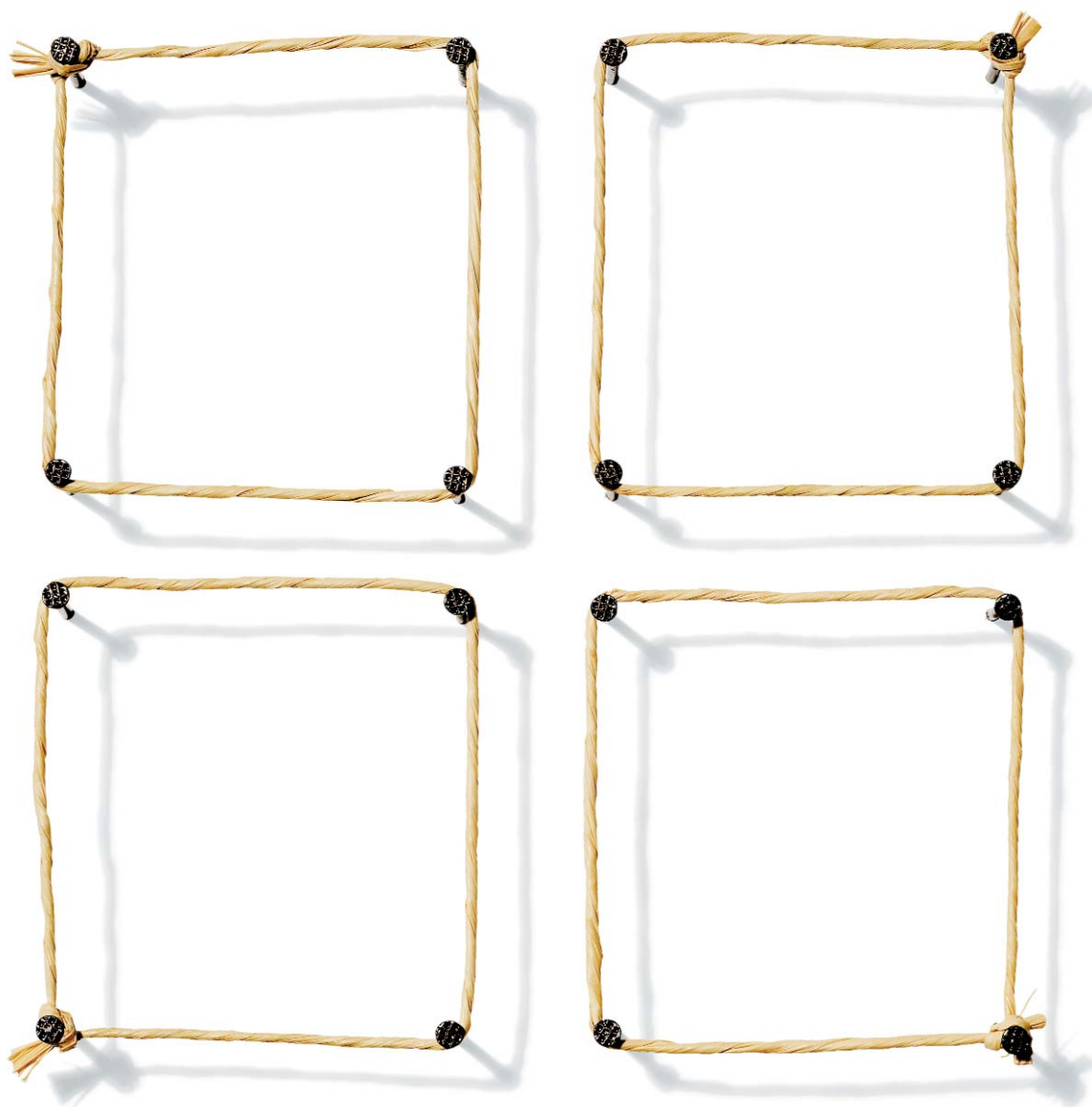




# Guidance Notes and Circulars

## Superannuation guidance note **SGN 120.1** **Risk management**

July 2004



# Disclaimer and copyright notice

1. The purpose of this guidance note is to provide general guidance on issues arising out of the legislation administered by the Australian Prudential Regulation Authority (APRA). It is not exhaustive in its coverage of rights or obligations under any law.

2. This guidance note is based on APRA's interpretation of the relevant legislation and has no legal status or legal effect whatsoever.

3. This guidance note may be affected by changes to legislation. APRA accepts no responsibility for the accuracy, completeness or currency of the material included in this guidance note.

4. Users of this guidance note are encouraged to obtain professional advice on the relevant legislation and to exercise their own skill and care in relation to any material contained in this guidance note.

5. APRA disclaims any and all liability or responsibility for any loss or damages arising out of any use of, or reliance on, this guidance note.

6. This guidance note is copyright. You may use and reproduce this material in an unaltered form only for your personal non-commercial use or non-commercial use within your organisation. Apart from any use permitted under the *Copyright Act 1968*, all other rights are reserved. Requests for other types of use should be directed to APRA.

# Contents

<b>Objective</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>Legislative requirements</b>	<b>5</b>
Trustee operations – Risk Management Strategy (RMS)	5
Fund (or ADF or PST) operations – Risk Management Plan (RMP)	6
<b>Format and content of RMS and RMP</b>	<b>8</b>
Risk management and licence class	8
Risk management framework and trustee operations	8
RMS and business plan	9
RMS – risk identification, assessment and management	9
Risk identification and assessment	9
Risk treatment (including residual risk assessment)	11
Internal oversight, implementation and reporting	11
RMP – fund (or ADF or PST) risk management plan	12
<b>Compliance with the RMS and RMP and reporting to APRA</b>	<b>14</b>
<b>Audit of the risk management framework</b>	<b>14</b>
<b>Trustee attestation</b>	<b>15</b>
<b>Conclusion</b>	<b>15</b>
<b>Further resources</b>	<b>16</b>

# Objective

1. The purpose of this guidance note is to provide advice to trustees of Australian Prudential Regulation Authority (APRA)-regulated superannuation funds, approved deposit funds (ADFs) and pooled superannuation trusts (PSTs)<sup>1</sup> about risk management requirements inserted into the *Superannuation Industry (Supervision) Act 1993* (the SIS Act) and the *Superannuation Industry (Supervision) Regulations 1994* (SIS Regulations) by the *Superannuation Safety Amendment Act 2004* (SSAA) and supporting regulations. The requirements apply to trustees who apply for and are granted an RSE licence and to the subsequent registration of the superannuation entities.
2. This document should be read together with the other guidance material prepared by APRA for trustees of APRA-regulated superannuation entities as well as the relevant provisions in the SIS Act and SIS Regulations.

<sup>1</sup> These entities are described as registrable superannuation entities (RSEs) - see definition of 'registrable superannuation entity' inserted into section 10(1) of the SIS Act.

## Introduction

3. A continuous process of effective risk management is critical to the safety and soundness of the operations of a trustee. For all superannuation entities where the trustee applies for an RSE licence, the trustee must develop, implement and maintain a sound and prudent risk management framework that comprises the trustee's policies and procedures, risk management processes, internal controls and independent review process. These should be appropriate to the nature, scale and complexity of the trustee's operations and address the material risks, financial and non-financial, as determined by the trustee.

4. The governance structure of the trustee is critical to ensuring that the interests of fund members are protected. To be effective, the trustee board, trustee committees, senior management and external experts must have the probity, commitment and competence necessary to develop, monitor and review sound practices for managing risk.

5. The trustee is responsible for instilling a strong risk control culture throughout the entity, so that material risks and conflicts of interest that emerge can be identified, managed and promptly resolved in the normal course of business operations and in the best interest of fund beneficiaries.

## Legislative requirements

6. Requirements for a two-tier risk management framework have been established in the SIS Act. The Risk Management Strategy (RMS) primarily relates to trustee-specific risks, while the Risk Management Plan (RMP) relates to RSE-specific risks. A certain amount of flexibility is provided to cater for varying trustee operations, from a public offer trustee with

many funds of a similar risk profile to the single corporate fund where the equal representation trustee entity has no other function than to be trustee of that one fund.

## Trustee operations: Risk Management Strategy (RMS)

7. As a pre-requisite to granting an RSE licence, APRA must be satisfied, among other things, that the RMS of the applicant meets the formal requirements outlined in section 29H of the SIS Act<sup>2</sup>. A condition of the licence is that the licensee must have an RMS that complies with the requirements, and the RSE licensee must comply with the RMS<sup>3</sup>. Applicants for an RSE licence are required to provide a signed copy of the RMS (see section B.4 of the application form) and certify that it complies with section 29H.

8. The RMS must cover certain categories of risk and set out management measures and procedures, as follows:

- the RMS must set out the reasonable measures and procedures the trustee is to apply to identify, monitor and manage risks that arise in relation to:
  - (a) its activities or proposed activities as an RSE licensee; and
  - (b) all its other activities, or proposed activities, to the extent that they are relevant to its activities, or proposed activities as an RSE licensee<sup>4</sup>;
- without limiting these general requirements, the RMS must set out reasonable measures and procedures that the trustee is to apply to identify, monitor and manage:
  - (a) the risks associated with governance and decision-making processes;

<sup>2</sup> See the SIS Act section 29D(1)(e).

<sup>3</sup> See the SIS Act section 29E(1)(c).

<sup>4</sup> See the SIS Act section 29H(1).

- (b) the risks that arise as a result of entering into outsourcing arrangements (other than arrangements that relate only to a particular RSE);
- (c) the risks arising from any changes to the RSE licensee law; and
- (d) the risks of potential fraud and theft.<sup>5</sup>

- the RMS must outline the circumstances in which an audit of the risks listed in section 29H is to be undertaken<sup>6</sup> and set out any other matters prescribed by regulations<sup>7</sup>;
- the RMS must be signed; where the trustee is a body corporate, the RMS is to be signed by the body corporate; in the case of a trustee that is a group of individuals, by every member of that group<sup>8</sup>;
- there are restrictions on what may be incorporated in the RMS by reference; this is to ensure that APRA is able to access all the provisions in the RMS, whether included explicitly or by reference<sup>9</sup>;
- an RMS may reproduce information contained in the RMP of an entity for which the RSE licence applicant is the trustee<sup>10</sup>;
- the RSE licensee must ensure that its RMS is up-to-date at all times and that it is reviewed at least once each year to ensure that it complies with section 29H<sup>11</sup> and must modify or replace the RMS at any time it becomes aware that the RMS no longer complies with section 29H<sup>12</sup>; an RSE licensee must also review its RMS if it becomes a licensee for another RSE or becomes an acting trustee of a superannuation entity<sup>13</sup>.

9. While the provisions outlined above provide a broad indication of the types of risk management measures that should be covered in the RMS, the SIS Regulations clarify the processes expected to be set

out in respect of the material risks that are relevant to the trustee<sup>14</sup>. Under the regulations:

- the RMS must address any 'material risk' that is relevant to the trustee;
- material risks are defined as those that have the potential, should they be realised, to adversely affect the interests of members or beneficiaries of the RSE operated by the trustee or have a significant impact on the business operations, reputation, rate of return, profitability, or net assets of the trustee;
- the RMS must cover assessment of the likelihood and consequences of each relevant material risk being realised; outline the proposed treatment of those risks, and, in consideration of the effectiveness of the proposed risk treatment, assess each of the residual risks; and
- the RMS must set out the proposed arrangements for internal oversight, implementation and reporting in relation to the management of the relevant material risks.

### **Fund (or ADF or PST) operations: Risk Management Plan (RMP)**

10. A condition of the RSE licence is that the licensee must register each of its RSEs under Part 2B of the SIS Act<sup>15</sup>. As part of the registration process, an up-to-date, signed, copy of the RMP for the entity must be provided to APRA<sup>16</sup> and the RSE licensee must attest that the plan complies with section 29P<sup>17</sup>. Where an application for an RSE licence is made during the period 1 July 2004 to 30 June 2006 by an existing trustee<sup>18</sup>, the applicant is also requested to lodge with the licence application a draft copy of the RMP of any

<sup>5</sup> See the SIS Act section 29H(2)(a).

<sup>6</sup> See the SIS Act section 29H(2)(b).

<sup>7</sup> See the SIS Act section 29H(2)(c).

<sup>8</sup> See the SIS Act section 29H(3).

<sup>9</sup> See the SIS Act section 29H(4).

<sup>10</sup> See the SIS Act section 29H(5).

<sup>11</sup> See the SIS Act section 29HA(1).

<sup>12</sup> See the SIS Act section 29HA(1).

<sup>13</sup> See the SIS Act section 29HA(2).

<sup>14</sup> See the SIS Regulation 4.07A.

<sup>15</sup> See the SIS Act section 29E(1)(d).

<sup>16</sup> See the SIS Act section 29L(2)(e).

<sup>17</sup> See the SIS Act section 29L(2)(f).

<sup>18</sup> An existing trustee will be a trustee of an APRA regulated superannuation fund, ADF or PST prior to 1 July 2004.

entities of which it is trustee. A pre-requisite to registration of the entity is that APRA must be satisfied that the RMP for the entity to be registered meets the formal requirements set out in section 29P<sup>19</sup>.

11. An RMP must set out the reasonable measures and procedures the licensee is to apply to identify, monitor and manage risks that arise in operating the RSE<sup>20</sup>. Without limiting the general requirement, the RMP must:

- identify the following categories of risk<sup>21</sup>:
  - (a) the risks to the investment strategy relevant to the entity;
  - (b) the risks to the entity's financial position; and
  - (c) the risks from entering into outsourcing arrangements relating to the entity.
- set out the circumstances in which an audit of these classes of risk is to be undertaken<sup>22</sup>;
- set out any other matters prescribed by regulations<sup>23</sup>.

In addition,

- the RMP must be signed by the RSE licensee of the entity<sup>24</sup>; if the licensee is a group of individual trustees, the RMP must be signed by each of the individuals<sup>25</sup>;
- the RMP must not incorporate provisions of other documents by reference unless those documents are available publicly without charge<sup>26</sup>; this is to ensure that APRA and members and employer-sponsors of defined benefit funds are able to access all the provisions in the RMP, whether included explicitly or by reference;
- an RMP may reproduce information contained in the RMS of the RSE licensee of the entity, or in the RMP of another entity that has the same RSE licensee;<sup>27</sup>

- the RSE licensee must ensure that the RMP of a registered entity is up-to-date at all times and that it is reviewed at least once each year to ensure that it complies with section 29P<sup>28</sup> and must modify or replace the RMP at any time it becomes aware that the RMP no longer complies with section 29P<sup>29</sup>; an RSE licensee must also review the RMP if it becomes the licensee for another RSE or becomes an acting trustee for a superannuation entity<sup>30</sup>.

12. The provisions outlined in the SIS Act provide a broad indication of the risk management measures that should be set out in the RMP and specific areas of risk to be dealt with. The regulations clarify the processes expected to be set out in respect of the material risks that are relevant to the entity<sup>31</sup>. Under the regulations:

- the RMP must address any 'material risks' to the RSE;
- material risks are defined as those that have the potential, should they be realised, to adversely affect the interests of members or beneficiaries of the RSE or have a significant impact on the business operations, reputation, rate of return, profitability, or net assets of the RSE;
- the RMP must cover assessment of the likelihood and consequences of each relevant material risk being realised; outline the proposed treatment of those risks, and, in consideration of the effectiveness of the proposed risk treatment, assess each of the residual risks; and
- the RMP must set out the proposed arrangements for internal oversight, implementation and reporting in relation to the management of the relevant material risks.

<sup>19</sup> See the SIS Act section 29M(1)(d).

<sup>20</sup> See the SIS Act section 29P(1).

<sup>21</sup> See the SIS Act section 29P(2)(a).

<sup>22</sup> See the SIS Act section 29P(2)(b).

<sup>23</sup> See the SIS Act section 29P(2)(c).

<sup>24</sup> See the SIS Act section 29P(3).

<sup>25</sup> See the SIS Act section 13A(6).

<sup>26</sup> See the SIS Act section 29P(4).

<sup>27</sup> See the SIS Act section 29P(5).

<sup>28</sup> See the SIS Act section 29PA(1).

<sup>29</sup> See the SIS Act section 29PA(1).

<sup>30</sup> See the SIS Act section 29PA(2).

<sup>31</sup> See the SIS Regulation 4.07B.

13. Other provisions relating to modification of an RMP and RMS and access to the RMP are discussed at paragraphs 45-49.

14. Some applicants for an RSE licence will have been granted an Australian Financial Services Licence (AFSL) by ASIC. The obligations of financial services licensees are set out in Division 3 of Part 7.6 of the *Corporations Act 2001* (Corporations Act). APRA-regulated AFSL licensees are exempted from the Corporations Act requirement to have adequate risk management systems<sup>32</sup>. ASIC relies on APRA supervision of compliance with this requirement for APRA-regulated entities<sup>33</sup>. Under another Corporations Act requirement, a managed investment scheme must have a compliance plan<sup>34</sup>. To the extent that a compliance plan submitted to ASIC covers part of the risk management framework required under SIS, RSE licence applicants may provide to APRA copies of documents that have been developed for Corporations Act purposes, provided that such documents are up to date and relevant to the information requested in the APRA licence application form. Applicants that hold an AFSL must demonstrate they meet the SIS risk management requirements for the purposes of the RSE licence.

## Format and content of the RMS and RMP

### Risk management and licence class

15. The risk management requirements set out in the legislation do not vary according to the class of licence for which a trustee applies. APRA expects that the risk management framework developed by an applicant for an RSE licence will reflect the nature, scale and complexity of the applicant's

operations and that licence class will not necessarily be an indicator of the complexity of operations. For example, a large multi-employer-sponsored non-public offer industry fund may face a wider range of risks and need more detailed measures to address them than would a small employer-sponsored fund for a family business with, for example, 15 members, even though both trustees apply for the same class of licence.

### Risk management framework and trustee operations

16. Some flexibility is provided in the legislation to cater for varying scenarios of trustee operations. For example, a trustee of a public offer entity class may be the trustee of multiple funds with a similar risk profile. In this case, it is possible for the trustee to have an RMP that applies by reference to other funds operated by the trustee that have the same risk profile<sup>35</sup>. Similarly, where a trustee has no other purpose or function than to operate a single fund in the equal representation context, the trustee RMS and the fund RMP will overlap to a great extent and could conceivably be contained in one document. However, trustees would need to be aware that security considerations would generally preclude some components of the RMS, such as the fraud control plan, being included in the RMP and therefore available to members.

17. APRA does not intend to issue templates for trustees to follow when devising their risk management frameworks. However, in the appropriate context, such as for a non-complex operation, APRA is not averse to trustees using checklists, particularly in the area of risk identification.

<sup>32</sup> See *Corporations Act 2001* section 912A(1)(h).

<sup>33</sup> ASIC PS 164, paragraph PS 164.105.

<sup>34</sup> See *Corporations Act 2001* section 601EA(4)(b) and Part 5C.4.

<sup>35</sup> See the SIS Act section 29P(5).

18. APRA cautions trustees against adopting generic risk management frameworks and documentation that do not take into account the particular nature of each trustee's business and the specific risks facing both the trustee and its RSE.

## RMS and business plan

19. It is APRA's view that the risk management framework should be developed within the context of the trustee's business plan. The business plan is an important management and control tool that enables the trustee to document and communicate its strategic direction and objectives, identify opportunities in the market place, forecast results and establish benchmarks.

20. For a non-public offer fund trustee that deals only with a single standard employer-sponsor or corporate group, it is expected that the business plan would focus on the internal operations of the fund. The business plan for the superannuation operations of a trustee of one or more public offer entities would focus on the trustee operations as well as those of the entities for which it is trustee.

21. Risks identified in the course of the business planning cycle that are relevant to the operations of the trustee or entity should be included with the other risks identified in the RMS or RMP and managed accordingly.

22. APRA requests that the trustee's business plan be submitted with its licence application. Although having a business plan is not a requirement under the legislation, it is APRA's view that having an RMS and RMP that are congruent with a sound business plan is an indication of the appropriateness and rigour of the risk management

structures the trustee has in place and will assist APRA in its assessment of the framework.

23. If a material change that would impact on the trustee's RMS is made to the business plan after it has been submitted to APRA but before the application had been decided, APRA would expect the change to the RMS to be advised to APRA consistent with section 29C(8). In this context, examples of material changes could include proposals relating to acquisitions; major modifications to, or the re-organisation of, the functions of the trustee or RSE, including changes to the governing rules that affect the powers of the trustee; any changes to the corporate group of which the trustee may be a part and which impact on the trustee; new business lines; changes in fund administration; and the outsourcing or bringing back in-house of any material business function.

## RMS - risk identification, assessment and management

### Risk identification and assessment

24. An effective risk management framework requires a continuous process of identification and assessment of all material risks that could adversely affect current and future operations. All material risks should be included and clearly described. Where business activities are outsourced, trustees must consider the risks to the trustee as well as to the RSE that arise as a result of entering into outsourcing arrangements<sup>36</sup>.

25. Where trustees conduct operations other than those relating to trusteeship of a single fund in the equal representation situation, they should identify material events which may affect the trustee's business. Examples of material events include

<sup>36</sup> See the SIS Act section 29H(2)(a)(ii) and section 29P(2)(a)(iii).

proposals relating to major modifications to, or the re-organisation of, the functions of the trustee or fund, any changes to a group of which the trustee may be a part, new business lines, appointment as trustee of other superannuation entities, changes in entity administration or the outsourcing of any material business activity.

26. Trustees should use a well-structured process to identify and assess risks, possibly with the aid of a facilitated risk workshop. A checklist approach may be sufficient in the simplest scenarios, provided the trustee could demonstrate that it had covered the field adequately; however, the use of more advanced techniques is recommended.

27. Risk tolerance objectives/thresholds need to be determined regarding the overall risk posed to the trustee's business.

28. A non-exhaustive list of the areas of risk that should be considered in developing this section of the trustees RMS includes:

- (a) **specific governance risks** - these include risks associated with a lack of transparency of decision-making processes; conflicts of interest, for example where trustees or responsible officers have another business relationship with a major service provider; fitness and propriety issues<sup>37</sup>; delegations of roles and responsibilities; and means for dealing with transitional situations where essential staff are absent or to be replaced;
- (b) **investment risks** - (this is more relevant to the fund RMP although trustees operating other businesses and/or investing on their own behalf, including investment of capital, should include investment risk in their RMS). These include risks associated with failure to achieve investment

objectives; with failure to ensure the investment plan remains appropriate as circumstances change, and lack of timeliness of remedial action in relation to market and counterparty risk;

- (c) **liquidity risk** - this includes risks associated with insufficient cash flow to meet payment needs and the risk that income will be inadequate to meet costs;
- (d) **operational risks** - these include risks associated with the security and accuracy of management information systems (including disaster recovery arrangements); risks relating to the management of beneficiary records, interests and entitlements; financial management risks; resource management risks; changes in trustee operations and service providers; and business disruption due to such events as IT failure, power failure, flood or fire for which APRA would normally expect to see a Business Continuity Plan;
- (e) **outsourcing risk**<sup>38</sup>;
- (f) **agency risk** - the risks associated with improper practices by agents and/or advisors in the provision of services to the trustee;
- (g) **fraud risk** - this includes internal fraud risks such as theft or misappropriation of assets, weakness with segregation of duties, system user access controls, payment and settlement processes, accounting and reconciliation procedures, member identification and verification procedures, and external fraud risks such as computer hacking and information theft;
- (h) **external risks** - these include competition, market changes; legislative changes; and changes in employer-sponsor policies; and

<sup>37</sup> See the SIS Regulation 4.14 and APRA guidance note SGN 110.1.

<sup>38</sup> See APRA guidance note SGN 130.1.

(i) **any other risks** - relevant to the operations of the trustee and its compliance with relevant legislation.

29. After the risks have been identified they may be recorded in a risk register or an appropriate database. The trustee should assess the likelihood of occurrence of each risk and the consequences if it did occur, and then apply a rating to describe the magnitude of potential consequences and the likelihood of occurrence for each risk. Scenario analyses and stress testing may also be used. Where relevant, trustees may be expected to use more complex risk-rating systems.

### **Risk treatment (including residual risk assessment)**

30. The individual controls that mitigate the likelihood and consequence of each risk occurring should be identified and a qualitative assessment made of the residual risk remaining after the control is considered. These residual risks should then be ranked in order of criticality. The process used to determine and rank residual risks should be outlined in the RMS.

31. Risk treatment strategies should reflect the nature, scale and complexity of the operations and have regard to a balance between cost and efficiency. The strategy, policy and procedure for risk treatment, control and mitigation should be clearly documented in the RMS. The strategy adopted should be tailored for each identified risk.

32. Treatment strategies may include:

- (a) acceptance of the risk;
- (b) mitigating controls (either by implementing new controls or strengthening existing controls);

(c) transference (by way of insurance as complementary to, rather than a replacement for, mitigating controls or outsourcing, although full accountability for the outsourced activity remains with the trustee<sup>39</sup>); and/or

(d) avoidance.

33. In proposing appropriate risk treatment, trustees should consider:

- (a) the overall risk management framework being adopted;
- (b) risk tolerance thresholds; and
- (c) compliance with legislative requirements and APRA directives.

### **Internal oversight, implementation and reporting**

34. Efficient communication and reporting ensures that all staff understand and adhere to policies and procedures affecting their duties and responsibilities. Pertinent information should be identified, captured and communicated in a form and timeframe that will enable the responsibilities of the trustee to be met. The trustee should implement adequate communication and reporting systems and ensure information flows to and from staff, management, senior management, trustee committees and, ultimately, the trustee.

35. A process of regular internal risk reporting to the trustee and, where appropriate, trustee committees should be established. The RMS of trustees of public offer entities and of large and complex non-public offer funds would be expected to outline the risk reporting framework including material risks, the status of individual controls, progress on treatment plans, and risk indicators. Trustees of less complex funds should also have clear reporting structures for transfer of information.

<sup>39</sup> See APRA guidance note SGN 130.1.

36. In developing this aspect of the trustee RMS, consideration should be given to: trustee and managerial oversight responsibilities and reporting lines; the processes for ensuring compliance with the SIS Act and Regulations and relevant provisions under the Corporations Act; the process by which the RMS is to be regularly reviewed and the events that would trigger such a review under section 29HA of the SIS Act; and compliance with statutory provisions regarding APRA's processes for monitoring institutions and collecting data/information.

37. The trustee is responsible for ensuring that a strong risk management culture is adopted throughout its operations. Depending on the nature, size and complexity of the trustee's business, the following are some of the means by which the trustee can ensure compliance with risk management policies and procedures:

- (a) clearly defined management responsibilities;
- (b) adequate segregation of duties;
- (c) establishing a risk committee (or similar) to set the strategy for and review the risk management framework;
- (d) instituting risk controls for each department/division, including limits on market and counterparty risk;
- (e) having appropriate selection and security checks for all staff;
- (f) incorporating discussion of risk management policies into staff induction and training; and/or
- (g) use of external consultants to assess risk management frameworks.

### **RMP - fund (or ADF or PST) Risk Management Plan**

38. Under section 29P of the SIS Act, an RMP is required for each RSE; each RMP is to address the material risks specific to the individual fund(s) operated by the trustee.

39. The objectives of the RSE should be clearly articulated in the RMP. The RMP should outline how the trustee is to identify, assess, control and actively review the risks specific to the individual fund/s for which it is trustee. This may primarily be the risks related to the investment strategy and financial position of the RSE, and any risks arising from entering outsourcing arrangements relating to the RSE. However, it may include other relevant material risks, for example, changes in membership profile or changes in membership base and their impact upon liquidity and investment, or matters relating to benefits and reserving requirements in a defined benefit fund.

40. The RMP should also detail the processes for determining the investment strategy and include, where relevant, requirements in relation to use of derivatives and management of derivative risk (refer to requirements set out in the SIS Act and APRA Circular II.D.7)<sup>40</sup>.

41. In developing each RMP, trustees should identify the risks specific to each RSE, as well as the risk tolerance objectives/thresholds. The following is a non-exhaustive list of risks that could be included in the RMP (for more details about each type of risk, see paragraph 28):

- (a) **specific fund or trust governance risks** - the governing rules may themselves expose fund or trust operations to additional risks, by giving trustees or others wide powers. This factor must be considered in designing risk management policies and framework;
- (b) **operational risks** - in addition to the operational risks described in paragraph 28(d), operational risk in the fund context would include risks that may result in the trustee being

<sup>40</sup> Note that SIS Regulation 13.15A(1)(c) and (d) have been amended to refer to 'derivative risk statement' rather than 'risk management statement'.

indemnified out of fund assets for liabilities incurred due to a lack of care or diligence that is not negligent or reckless. An example would be a bona fide payment of a benefit to the wrong party where the trustee is unable to recover the amount or make good the loss from its own assets or insurance;

(c) **investment risks** - these include risks associated with failure to achieve investment objectives; with failure to ensure the investment plan remains appropriate as circumstances change; lack of timeliness of remedial action in relation to market and counterparty risk; concentration of assets (lack of diversity);

(d) **liquidity risk** - this includes risks associated with insufficient cashflow to meet benefit payment needs as well as investment settlements;

(e) **outsourcing risk** - APRA's guidance note SGN 130.1 on outsourcing refers to APRA's expectation that trustees fully understand the measures the service provider has in place to limit trustee exposure to the outcome of any adverse event, the extent of any limitation of liability on the part of service providers, and how such limitation would interact with the trustee's ability to meet its obligations to fund members;

(f) **agency risk** - in the fund context, agency risk also includes risk arising from conflict of interest issues where services are provided by parties related to the trustee;

(g) **fraud** (see paragraph 28(g));

(h) **market and counterparty risk** - the risk of financial loss resulting from an adverse movement in the market price of an asset (market risk) or the

failure of a debtor or trading counterparty to fully honour any financial or contractual obligation (counterparty risk);

(i) **insurance risk** - the risk that an insurer of fund benefits or assets may fail or that a claim may be rejected fully or in part due to inadequate coverage or mismatch;

(j) **any other risk particular to the fund.**

42. Similar processes for risk assessment, treatment and oversight and reporting should be followed as set out for the RMS in paragraphs 30-37.

43. All trustees must outline the process by which the RMP is to be regularly reviewed and the events that would trigger such a review under section 29PA of the SIS Act.

44. The RMP must be submitted to APRA upon application to register a new entity<sup>41</sup>. A material revision to an RMP will be required to be advised to APRA within 14 days<sup>42</sup>.

45. Once a superannuation entity has been registered with APRA, a member of a fund, an employer sponsor of a defined benefit fund, or a unit holder in a PST, may request a copy of the fund or trust's RMP from the trustee. The trustee must make the RMP available as soon as practicable and without charge<sup>43</sup>. The document may be made available electronically or in hard copy.

<sup>41</sup> See the SIS Act section 29PA.

<sup>42</sup> See the SIS Act section 29PC.

<sup>43</sup> See the SIS Act section 29PD.

## Compliance with the RMS and RMP and reporting to APRA

46. Each RSE licence will include a condition that the licensee must have an RMS that complies with the relevant requirements of the legislation, and the licensee must comply with that RMS<sup>44</sup>. A further condition requires each RSE licensee to comply with each measure and procedure set out in the RMP for each RSE for which it is the licensee<sup>45</sup>.

47. It is not an offence to breach a licence condition, but it is an offence to fail to report a breach of a condition to APRA<sup>46</sup>. Accordingly, the risk management framework needs to encompass a process for identifying and reporting failures to comply with the RMS and RMP. There is no concession for materiality in the requirement to report a failure to comply with 'each measure and procedure'. APRA's view is that it is unlikely to take action over failure to report a one-off failure to comply with a minor element of a practice that supports a measure or procedure, provided that rectification action was taken and recorded for purposes of the requirement to review and update the risk management strategy or plan. Where the compliance failure leads to a breakdown of a significant control, APRA would expect that to be reported. In APRA's view, RSE licensees should be mindful that a failure to deal effectively with any instance of non-compliance could weaken the risk management process, and frequent instances of minor compliance failures would be an indicator that the system was not as robust as could be expected.

48. RSE licensees must give copies of modifications of the RMS or RMP to APRA within 14 days of making the modification. A similar requirement applies where an RMS or RMP is repealed and replaced. In the latter

case, the licensee must give APRA a signed statement to the effect that the new strategy or plan replaces the old. It is an offence to fail to comply with these requirements<sup>47</sup>. There is no concession for materiality in the requirement to report modifications to APRA. The risk management framework encompasses material risks, therefore at a minimum, any modification in respect of nature, assessment, control, treatment, oversight and reporting of specific risks or processes and controls in general should be reported.

49. APRA may request information from an RSE licensee about its RMS or the RMP of an entity for which it is the licensee<sup>48</sup>. APRA may also direct an RSE licensee to modify its RMS or the RMP of an entity for which it is the licensee<sup>49</sup>.

## Audit of the risk management framework

50. The RMS and RMP must also set out the circumstances in which an audit of the risks specified in subsections 29H(2) and 29P(2) is to be undertaken. An approved auditor<sup>50</sup> must audit the RMS and RMP annually and attest that the framework adopted by the trustee to identify, assess, control, report and review the risks of the RSE licensee and fund or PST has been implemented and is operating effectively<sup>51</sup>.

51. Matters identified with respect to the RMS and RMP by the approved auditor should be reported to the trustee and not excluded by a financial materiality threshold. Amendments to the 'whistleblowing' provisions in section 129 of the SIS Act mean that the approved auditor must report to APRA at the same time as to the trustee if the auditor forms an opinion about a contravention that may affect the interests of members or beneficiaries.

<sup>44</sup> See the SIS Act section 29E(1)(c).

<sup>45</sup> See the SIS Act section 29E(1)(e).

<sup>46</sup> See the SIS Act section 29JA.

<sup>47</sup> See SIS section 29HC and section 29PC.

<sup>48</sup> See the SIS Act section 29HD and section 29PE.

<sup>49</sup> See the SIS Act section 29HB(3) and section 29PB(3).

<sup>50</sup> See definition in SIS section 10(1) and Regulation 1.04(2).

<sup>51</sup> See the SIS Act section 113(3)(c).

52. The risk management framework should include consideration of audit related risks and conflicts of interest. For example, an auditor involved in advising a trustee on the risk management framework to be adopted should be precluded from conducting the audit of the RMP or RMS for the purposes of section 113 of the SIS Act. Similarly, any conflicts of interest arising from using the services of the same approved auditor for the financial and compliance audit and the audit of the RMS and RMP should be identified and appropriately managed. In these examples, another auditor from the same practice is not precluded from providing the services.

53. APRA will be working with the audit profession to develop guidelines for the audit of RMS and RMP.

### **Trustee attestation**

54. It is likely that, in future, RSE licensees will be required to provide APRA with a signed attestation as to the existence and efficacy of the risk management structures in place at the time the trustee lodges its yearly statutory returns.

55. APRA may also request an RSE licensee to provide a copy of its risk report supporting the attestation.

56. If necessary, the trustee may be requested by APRA to provide evidence of the processes undertaken to compile the risk report and support the attestation. Inaccurate attestations would reflect on trustee fitness and propriety.

### **Conclusion**

57. APRA views risk management as a crucial aspect of a trustee's operations. Having an RMS and RMPs that are 'living' documents will ensure that a trustee can more effectively meet the prudential management requirements incumbent upon it.

## Further resources

To assist trustees in the development of their RMPs and RMS, the following resources may be useful. Please note that the content of these documents do not necessarily reflect the views of APRA on risk management. APRA does not bear any responsibility for any person who relies, or partially relies upon the contents of, or anything omitted by, these documents.

ASFA (2003) *A risk management framework for superannuation funds*. Best practice paper 19, June 2003.

ASIC, *Managed investments: compliance plans*. ASIC Policy Statements PS 132.

Bank for International Settlements (2001) *Sound Practices for the Management and Supervision of Operational Risk*. December 2001, revised July 2002, February 2003.

Basel Committee on Banking Supervision (2001) *Working paper on the regulatory treatment of operational risk*. Bank for International Settlements. September 2001.

Centre for Business Performance (1999) *Implementing Turnbull: A boardroom briefing*. The Institute for Chartered Accountants in England and Wales.

Financial Services Commission of Ontario (2003) *Risk-based supervision of pension funding: A report back to the pension industry*.

ISC *Best practice guide to the detection of superannuation fraud*. To be reissued on the APRA website at <http://www.apra.gov.au>

Towers Perrin (2002) 'Risk management' in *FocusOn*. August 2002.

Standards Australia lists a number of publications on risk management on its website at [www.standards.com.au](http://www.standards.com.au)



Telephone  
1300 13 10 60

Website  
[www.apra.gov.au](http://www.apra.gov.au)

Mail  
GPO Box 9836  
SYDNEY NSW 2001