



Prudential Practice Guide Draft

SPG 200 – Risk Management

14 August 2009

Disclaimer and copyright

This prudential practice guide is not legal advice and users are encouraged to obtain professional advice about the application of any legislation or operating standard relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in this guide.

APRA disclaims any liability for any loss or damage arising out of any use of this prudential practice guide.

© Commonwealth of Australia

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. All other rights are reserved.

Requests and inquiries concerning reproduction and rights should be addressed to:

Commonwealth Copyright Administration
Copyright Law Branch
Attorney-General's Department
Robert Garran Offices
National Circuit
Barton ACT 2600
Fax: (02) 6250 5989

or submitted via the copyright request form on the website <http://www.ag.gov.au/cca>

About this guide

The *Superannuation Industry Supervision Act 1993* (SIS Act) was amended by the *Superannuation Safety Amendment Act 2004* (SSA Act) to require all trustees operating an APRA regulated superannuation entity to be licensed by APRA and to register the entities for which they are trustee.

This Prudential Practice Guide (PPG) replaces Superannuation Guidance Note 120.1 (Risk Management), and Circular II.D.7 (Derivatives) and information previously contained in the frequently asked questions section on APRA's website. It consolidates existing material, removes duplication and reflects the Registrable Superannuation Entity (RSE) licensing framework.

The PPG aims to assist RSE licensees and their directors in complying with provisions related to risk management frameworks and, more generally, to outline sound practices in relation to this particular area of a licensee's superannuation operations.

It is not the purpose of this guide to provide a restatement of the content of the law.

Not all the practices outlined in this PPG will be relevant for every RSE licensee and some aspects may vary depending upon the size, complexity and risk profile of the licensee.

A reference to a trustee in this guide should be taken as a reference to the RSE licensee of an APRA regulated superannuation fund, approved deposit fund (ADF) or pooled superannuation trust (PST).

Depending on the context, the reference will also be applicable to a director of the RSE licensee if the licensee is a corporation or to an individual trustee if the licensee is a group of individual trustees. Also depending on the context, a reference to a fund or to fund members or beneficiaries will be applicable to ADFs and their members or to PSTs and unit holders of those trusts.

Contents

Introduction	5
Legislative requirements	5
Risk management and licence class	5
Risk management framework and trustee operations	6
Trustee operations: Risk Management Strategy (RMS)	6
RMP – fund (or ADF or PST) Risk Management Plan	6
Derivatives	6
Considerations relevant to both RMS and RMP	7
Risk framework and business plan	7
Risk identification and assessment	7
Risk mitigation and control	11
Monitoring	13
Information systems	13
Escalation and communication	13
Considerations particularly relevant to RMS	14
Considerations particularly relevant to RMP	14
Derivatives	16
Fraud	17
Audit of the risk management framework	18
Internal audit	18
The role of the approved auditor	18
Trustee attestation	19
Conclusion	20
Further resources	21

Introduction

1. A continuous process of effective risk management is critical to the safety and soundness of the operations of each trustee. For all superannuation entities where the trustee holds or applies for an RSE licence, the SIS legislation requires that the trustee must develop, implement and maintain a sound and prudent risk management framework. This framework should provide for the proactive identification, assessment, mitigation, management, monitoring and reporting of risks. It comprises the trustee's policies and procedures, risk management methodology and processes, system of internal controls, formal reporting structure with appropriate governance and oversight and independent review process. Sound practice suggests that these should be appropriate to the nature, scale and complexity of the trustee's operations in the light of changing external conditions and address the material risks, financial and non-financial, as determined by the trustee.
2. The trustee is responsible for the risk management framework, including methodology and governance, and for instilling a strong culture of risk identification and management throughout the entity. In this way material risks can be identified and either be managed before they result in adverse experience for the trustee, or at worst be promptly resolved in the normal course of business operations and in the best interest of fund beneficiaries. In this context, trustees may also wish to give consideration to issues of business resilience; that is, the capacity of the organisation to adapt to and conceivably benefit from significant events which materially change the business operating environment.

1 See the SIS Act Part 2A Division 8 and Part 2B, Division 5

2 See the SIS Act s. 29HD and s. 29PC.

3 See the SIS Act s. 29M

4 See the SIS Act s. 29JC and s. 29Q.

Legislative requirements

3. The SIS Act requires trustees to establish a two-tier risk management framework¹. The Risk Management Strategy (RMS) primarily relates to trustee-specific risks, while the Risk Management Plan (RMP) relates to RSE-specific risks.
4. It is a licence condition for all trustees that their RMS satisfies the legislated requirements and that they comply with its terms. Further, they must comply with each measure and procedure set out in the RMP for each registrable superannuation entity for which they are trustee. A range of consequences can flow from a breach of a licence condition.
5. Trustees are obliged to provide a signed copy of any modified or replacement RMS or RMP within 14 days of the change. Failure to do so constitutes an offence under the SIS Act². The RMP must be submitted to APRA upon application to register a new entity³.
6. APRA may give a notice to a trustee requiring it to amend its RMS in order to comply with s. 29H of the SIS Act, or to amend an RMP to comply with s. 29P. It is an offence for a trustee to fail to comply with such a direction within the time specified in the notice.⁴

Risk management and licence class

7. The risk management requirements set out in the legislation do not vary according to the class of licence held by the trustee. While APRA expects that the risk management framework developed by an RSE licensee will reflect the nature, scale and complexity of the trustee's business model and operations, licence class should not be a determinative 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, even though both trustees hold the same class of licence.

Risk management framework and trustee operations

8. Some flexibility is available to cater for varying circumstances of trustee operations. For example, a trustee of a public offer licence class may be the trustee of multiple funds with a similar risk profile. In this case, it is possible for the trustee to determine that an identical RMP is appropriate for a number of its funds that it considers to have the same risk profile⁵. 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.
9. Trustees may wish to consider whether security considerations may preclude some components of the RMS, such as the fraud control plan, being included in the RMP and therefore available to members.

Trustee operations: Risk Management Strategy (RMS)

10. Section 29H of the SIS Act sets out certain categories of risk to be covered by the RMS and also requires it to incorporate various management measures and procedures.⁶
11. While those provisions 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.⁷

RMP – fund (or ADF or PST) Risk Management Plan

12. Under s. 29P of the SIS Act, an RMP is required for each RSE; each RMP is to address the material risks⁸ specific to the individual fund(s) operated by the trustee (including risks to each fund's investment strategy and financial position), the circumstances in which an audit of the risks is to be undertaken and such other matters as are prescribed in regulations.
13. 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 s. 29PA of the SIS Act⁹.

Derivatives

14. Derivative transactions are financial contracts in instruments that derive their value from another underlying security. Examples include swaps, options forwards, futures, contracts for difference (CFDs) and other similar transactions.
15. SIS Regulation 13.15A specifies that a trustee may give a charge over fund assets if required in relation to certain derivatives contracts if the investment is made in accordance with the derivatives risk statement (DRS). APRA expects that the RMP would detail the trustee's requirements in relation to the use of derivatives, whether directly or in pooled investments, and management of derivative risk. It is open to the trustee to determine whether a DRS is required and if so whether it should be prepared separately from the RMP, or whether it could be incorporated within the RMP. It would be sound practice for such a decision to be formally considered and documented by the trustee.

⁵ See the SIS Act ss. 29P(5)

⁶ See the SIS Act s. 29H

⁷ See the SIS r. 4.07A

⁸ See s. 29P of the SIS Act and SIS r. 4.07B

⁹ See in particular SIS Act s. 29PA(1)

Considerations relevant to both RMS and RMP

16. It is APRA's expectation that the RMS and RMP would contain sufficient information to enable the reader to understand in general terms how the trustee identifies, mitigates, manages, monitors and regularly reports on the risks to its own operations and those of the entities for which it is trustee, respectively. Trustees should also have regard to the fact that the documents must have sufficient specificity to be capable of being audited¹⁰. At the same time, trustees need to remain alert to the fact that the RMP is to be made available on request to fund members and unitholders and, in the case of a defined benefit RSE, to employer sponsors. It is therefore not expected that the internal control risk mitigation processes described within the respective documents are so detailed as to facilitate their circumvention by a person who had access to the RMP.

Risk framework and business plan

17. It is APRA's view that the risk management framework would generally be developed and reviewed within the context of the trustee's business planning processes. 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.
18. 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 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.

19. Risks identified in the course of the business planning cycle that are relevant to the trustee achieving its strategic objectives or to the operations of the trustee or fund should be included with the other risks identified in the RMS or RMP and managed accordingly.
20. 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 framework.

Risk identification and assessment

21. The risk management framework should be comprehensive, systematic and appropriate for the nature of the trustee's business. 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. The framework should both clearly specify the risks to be addressed, and define the criteria applied by the trustee in determining what it would consider to be material in the context of the risk management framework. It should always include a process for updating and re-assessing risks and/or identifying new risks.
22. It would be sound practice for trustees to 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, with the increasing sophistication of the industry, the use of more advanced techniques is recommended. A significant shortcoming of the checklist approach is that it may inhibit the trustee from identifying new or emerging risks. The RMS and RMP should always include a description of the processes used by the trustee in risk identification and assessment.¹¹

¹⁰ See para. 35C(5)(d) of the SIS Act

¹¹ See para. 29H((2)(a) of the SIS Act

23. APRA cautions trustees against adopting a generic risk management framework and documentation that does not take into account the particular nature of each trustee's business and the specific risks facing both the trustee and its fund(s).
24. There are a number of techniques available to a trustee to enable the identification, assessment and quantification of risks and their impact on its operations. Where appropriate, the trustee may consider using such techniques as:
- (a) self assessment – the trustee assesses its operations and activities against a menu of potential risk vulnerabilities. This process can be facilitated through a workshop conducted by internal or external risk management experts and may incorporate checklists or the use of other risk identification tools to identify the strengths and weaknesses of the risk environment. Scenario analyses and stress testing may also be used. Where relevant, trustees may be expected to use more complex risk-rating systems;
 - (b) risk mapping – during this process, various business units, organisational functions, process flows and interdependencies are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action. This process should explicitly give consideration to risks associated with outsourced functions¹²; and
 - (c) risk indicators – risk indicators are statistics and/or metrics, both financial and non-financial, which can provide insight into the trustee's risk position. It would be sound practice for any likelihood/consequence tables used to quantify the thresholds used. For example, the number of IT security breaches could be an indicator for potential business disruption. In respect of consequence, the threshold may be defined as a loss exceeding a specified dollar figure or percentage of members' (or a defined sub-set of members') assets. Similarly, the likelihood table would often have some linkage to quantified probability e.g. a 25% probability of occurrence. Regular reporting of these risk indicators to senior management and the board would provide visibility for the changing state of the organisation's risk landscape, and assist the board and management in ensuring that risk levels are managed within defined tolerances.
25. It would be sound practice for the RMS and RMP to explicitly indicate the trustee's risk appetite both in the aggregate, and at the individual risk level. Risk tolerance objectives/thresholds need to be determined regarding the overall risk posed to the trustee's business. Where residual risks fall outside the trustee's risk appetite, it is expected that the trustee would either identify other mitigants (possibly including risk transfer to a third party via insurance) which would reduce the residual risk to a point within the trustee's tolerance, or else vacate the particular element of the business which gave rise to the risk.
26. As a guide, for each identified risk, APRA envisages that the trustee would record in a risk register or data base its:
- (a) assessment of the inherent impact and likelihood;
 - (b) identified risk mitigation and control strategies;

¹² See SIS r. 29H2(a)(ii)

- (c) assessment of the effectiveness of the control strategies in place;
 - (d) assessment of the residual risk; and
 - (e) decision as to whether or not to accept that risk.
27. In the assessment of risks, the trustee would typically indicate the assumptions made as part of the assessment and analysis of risks. The trustee would also usefully disclose the basis of its estimations as to the levels of risk and hence the level of confidence it places on them. For fully quantified estimates of probability and impact, this could, for example, be a statistical measure such as standard deviation and/or the associated statistical confidence levels.
28. A trustee adopting prudent practices would identify material events which may change its risk environment and hence affect its business. Examples of material events include:
- (a) proposals relating to major modifications to, or the re-organisation of, the functions of the trustee or fund;
 - (b) any changes to a group of which the trustee may be a part;
 - (c) changes to new business lines;
 - (d) appointment as trustee of other superannuation entities;
 - (e) changes in entity administration; or
 - (f) the outsourcing of any material business activity.
29. APRA recognises that the risk environment, and hence the risk management framework, is likely to be less complex for equal representation trustees responsible for a single fund to which a single standard employer sponsor contributes.
30. A non-exhaustive list of the areas of risk that would be considered in developing a sound risk management framework includes:
- (a) specific governance risks – these include:
 - (i) risks associated with a lack of transparency of decision-making processes;
 - (ii) conflicts of interest, for example where trustees or responsible officers have another business relationship with a major service provider;
 - (iii) risks associated with remuneration structures, both for executives and for investment managers, which may skew their risk appetite towards higher but unsustainable short term outcomes which may be inimical to the interests of long term fund members;
 - (iv) fitness and propriety issues¹³;
 - (v) delegations of roles and responsibilities;
 - (vi) processes for project management including transitions when functions are moved between in-sourced and outsourced arrangements, or between outsourced service providers; and
 - (vii) 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:
 - (i) risks in relation to market, counterparty and concentration risk associated with failure to achieve investment objectives. Stock lending provides a particular example of market risk which may be exacerbated by the trustee's decisions; failure to ensure the investment plan remains appropriate as circumstances change; and

¹³ See the SIS r. 4.14 and SPG 520 Fitness and Propriety.

- (ii) a lack of timeliness of remedial action in relation to market and counterparty risk;
- (c) solvency risk at the trustee and RSE levels respectively – especially for those trustees not required to hold capital, this includes the risk that the assets of the trustee may fall below those required for it to remain a going concern.¹⁴ The RMP would address the risk of an RSE being placed in an unsatisfactory financial position.
- (d) liquidity risk – this includes:
 - (i) risks associated with insufficient cash flow to meet benefit transfers/ cash payments or investment settlements on a timely basis,
 - (ii) trustee expense payment needs and
 - (iii) the risk that realised income will be inadequate to meet costs;
- (e) operational risks – these include:
 - (i) risks associated with the security and accuracy of management information systems (including but not restricted to IT systems, and including disaster recovery arrangements);
 - (ii) risks relating to the management of beneficiary records, interests and entitlements;
 - (iii) financial management risks;
 - (iv) resource management risks;
 - (v) changes in trustee operations and service providers; and
 - (vi) business disruption due to such events as IT failure, power failure, flood, fire, terror attack or pandemic which APRA would normally expect to see addressed in a Business Continuity Plan;
- (f) outsourcing risk¹⁵, including:
 - (i) risks associated with the due diligence process in selecting an outsourced service provider
 - (ii) legal risk including the precision and enforceability of the contract between the trustee and the service provider, especially where foreign jurisdictions are involved. Issues of preservation of member interests in the event of a contractual dispute with the service provider are paramount in this context;
 - (iii) risks associated with the adequacy of ongoing monitoring of and information flow from the service provider; and
 - (iv) risks associated with the business continuity of the service provider, including its ongoing solvency, insurance arrangements and disaster recovery arrangements.
- (g) agency risk – the risks associated with improper practices by agents and/or advisors in the provision of services to the trustee, or the misalignment of incentives for employees or service providers with the stated risk appetite of the trustee. In this respect, the structuring of executive remuneration is particularly important;
- (h) fraud risk – this includes:
 - (i) 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
 - (ii) external fraud risks such as computer hacking and information theft;

¹⁴ See also SPG 230 Adequacy of Resources

¹⁵ See SPG 231 Outsourcing

- (i) external risks – these include:
 - (i) competition, market changes;
 - (ii) legislative changes including in particular change to the RSE law; and
 - (iii) changes in employer-sponsor circumstances and policies; and
- (j) any other risks – relevant to the operations of the trustee and its compliance with relevant legislation.

Risk mitigation and control

31. As part of a risk management framework, various control mechanisms would typically be in place to mitigate identified risks and to ensure compliance with the risk management framework. Subject to the size and nature of the trustee's operation, principal elements of this may include:
- (a) top-level reviews of the trustee's progress towards stated risk management objectives (including identifying apparently anomalous member take-up of certain investment options which may indicate risks within the distribution channels);
 - (b) a system of clearly defined management responsibilities and accountabilities including documentation for approvals, delegated authorities, setting of limits and authorisations;
 - (c) activity and procedural controls including performance standards and business metrics for each business arm of the trustee and for the interactions between each outsourced service provider (e.g. segregation of duties);
 - (d) policies to document such controls;
 - (e) a system for monitoring compliance with controls, including reporting of compliance and exceptions to senior management and the board;
 - (f) policies and procedures for the treatment and resolution of non-compliance issues, including documented escalation procedures for the accelerated reporting to relevant levels of management of instances of legislative non-compliance, fraud, breaches of corporate policies and instances of material failures in business processes or systems;
 - (g) documented arrangements for the receipt and treatment of information from whistleblowers;
 - (h) mechanisms to ensure that all personnel have appropriate performance objectives, expertise and training with regard to relevant risks;
 - (i) mechanisms to ensure that adequate financial, human and technical resources are available at all times to satisfactorily implement the trustee's business requirements, including its risk mitigation activities¹⁶;
 - (j) regular verification and reconciliation of transactions and accounts; and
 - (k) safeguards for access to, and use of, the trustee's assets and records (physical and electronic controls).

¹⁶ See SPG 230 Adequacy of Resources

32. Segregation of duties is an important component of an effective internal control system and ensures that personnel are not assigned responsibilities that may create a conflict of interest.¹⁷ Assigning conflicting duties to individuals or a team may lead to the concealment of losses, errors or inappropriate actions. APRA envisages that any areas of potential conflicts of interest would be identified, minimised and subject to careful independent monitoring and review. Trustees engaging in sound practice would have regard to the risk inherent in moving staff over time from control to operational functions, where they may apply knowledge of control features in order to circumvent them. In limited circumstances, in line with the nature, scale and complexity of operations (e.g. small, simple, low risk activities), adequate segregation may not be achievable. In these circumstances, the frequency of oversight from the board and senior management would typically be increased.
33. Risk mitigation strategies such as insurance arrangements can be used to transfer the risk of 'low frequency, high severity' losses which may occur as a result of events such as third party claims resulting from errors and omissions, physical loss of securities, employee or third party fraud and natural disasters.
34. A trustee would generally, however, view such insurance arrangements as complementary to, rather than a replacement for, sound risk controls. Having mechanisms in place to quickly recognise and rectify risk events can greatly reduce exposure to loss. Careful consideration would normally be given to the extent to which insurance transfers the risk to another business sector or area or even creates a new risk (e.g. legal or counter-party risk).
35. In view of the reliance of many trustees on outsourced service providers for much of their funds' day to day operations, the SIS Act requires that the risk management framework would specifically address risks associated with outsourcing¹⁸, with particular focus on the enforceability of contracts, processes for monitoring the fulfilment of contracts and the insurance coverage provided by the service provider in the event of it failing to meet its contractual obligations, or in the event of its insolvency. When considering the enforcement of such contracts, trustees engaged in sound practice would have regard to the difficulties posed by related party arrangements.
36. Risk treatment strategies would generally 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 risk management framework. Sound practice would dictate that the strategy adopted should be tailored for each identified risk.
37. The risk register would usefully incorporate the risk management controls relevant to each identified risk, including identification of the officer responsible for implementing those controls, an assessment of the control effectiveness and an assessment of the likelihood and impact of the residual risks.
38. A trustee adopting sound practice would make a qualitative assessment of the residual risk remaining after the control is considered. These residual risks would then be ranked in order of criticality. A trustee could consider its residual risks in the context of its risk appetite and, as a result, develop a risk treatment plan to accept, mitigate (e.g. implement additional controls), transfer or avoid the identified risk. The process used to determine and rank residual risks would be outlined in the risk management framework.

¹⁷ See also SPG 521 Conflicts of Interest

¹⁸ See the SIS Act s. 29H(2)(a)(ii) and s. 29P(2)(a)(iii) and also SPG 231 Outsourcing

39. The board and senior management would typically ensure that each element of the risk management framework is operating correctly and in the manner for which it was intended. The tools and indicators used by the board and senior management would typically be identified in the risk management framework.

Monitoring

40. As part of a properly functioning risk management framework, a trustee would typically implement and document a process to regularly monitor risk profiles and material exposures to losses according to the nature, scale and complexity of operations. The frequency of monitoring would reflect the risks involved and the frequency of change, with results reported regularly to the board.

41. A trustee would generally undertake routine monitoring of its position against, and level of compliance with, its mitigation and control activities and record these in the risk register.

42. Where a trustee board has a majority of non-independent directors, it is desirable for initial monitoring of compliance with the RMS and RMP to be through a board committee with a majority of independent members. A trustee adopting sound practice would ensure that particular attention was paid to the monitoring of breaches which, while not significant in themselves, in the aggregate may be symptomatic of systemic weakness in the trustee's risk management processes.

Information systems

43. APRA expects that as part of a trustee's risk management framework, it would establish, maintain and document effective management information systems commensurate with the size and complexity of its operations. These information systems assist in the management, communication and reporting of risk issues and outcomes and assist in informing the trustee so that it is better able to meet its responsibilities.

44. APRA envisages that controls would be in place for ensuring that data in information and reporting systems are timely, accurate and complete. Internal information and reporting systems would be secure and supported by adequate business continuity arrangements.

45. A properly functioning information and reporting system would typically:

- (a) produce detailed financial, operational and compliance data;
- (b) be able to incorporate external market information relating to events and conditions that are relevant to decision-making;
- (c) enable relevant, accurate and timely information to be reported;
- (d) allow the trustee to identify, quantify, assess and monitor business activities, exposure to risk, financial position and performance;
- (e) allow the trustee to monitor the effectiveness of, and compliance with its internal control systems, and report any exceptions that arise; and
- (f) be reviewed regularly to assess the timeliness and relevance of information generated, and the adequacy, quality and accuracy of the system's performance over time.

Escalation and communication

46. The trustee is responsible for ensuring that a strong risk management culture is adopted throughout its operations.

47. Efficient communication and reporting ensures that all staff and other parties 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. APRA envisages that escalation procedures would be established as part of a trustee's risk management framework to facilitate the reporting of risk issues. These may include allocating responsibility for resolution of issues related to unacceptable levels of risk or inadequate or ineffective control measures. A trustee adopting sound practice would implement adequate communication and reporting systems and ensure information flows to and from staff, management, senior management, trustee committees and, ultimately, the trustee.
49. In developing this aspect of the RMS, consideration should be given to:
- (a) 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;
 - (b) the process by which the RMS is to be regularly reviewed and the events that would trigger such a review under s. 29HA of the SIS Act; and
 - (c) compliance with statutory provisions regarding APRA's processes for monitoring institutions and collecting data/information.

Considerations particularly relevant to RMS

48. 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 would also have clear reporting structures for transfer of information. Where deficiencies or breaches of controls are identified as part of the monitoring process, periodic review process or internal audit, these would typically be escalated in a timely manner to the appropriate level of management. Furthermore, material deficiencies or breaches would typically be reported promptly to senior management and the board or relevant board committee. For this purpose, a material deficiency or breach can result not only from a single incident, but also from a number of smaller incidents that, when considered together, amount to a material deficiency or breach.

Considerations particularly relevant to RMP

50. Trustees adopting sound practice would ensure that the objectives of the RSE were clearly articulated in the RMP. The RMP would 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.

51. 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 30):
- (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, or by constraining trustee discretion in ways that may inhibit its capacity to act in members’ best interests;
 - (b) risks associated with benefit design, including particularly the investments underpinning any explicit or implied capital guarantee offered to members. In considering risks related with benefit design, trustees adopting sound practice would have regard to the potential for members to benefit from arbitrage opportunities if unit prices or crediting rates for members switching between investment strategies are set using historic rather than forward pricing¹⁹, and, for defined benefit funds, risks to the financial position of the fund, which will include risks associated with the solvency of an employer sponsor as well as those associated with the investments supporting the fund’s defined benefit liabilities;
 - (c) investment risks – these include risks associated with
 - (i) failure to achieve investment objectives;
 - (ii) failure to ensure that investments are maintained within approved asset allocation ranges;
 - (iii) failure to ensure the investment plan remains appropriate as circumstances change;
 - (iv) the risk of financial loss resulting from an adverse movement in the market price of an asset (market risk);
 - (v) the failure of a debtor or trading counterparty to fully honour any financial or contractual obligation (counterparty risk);
 - (vi) lack of timeliness of remedial action in relation to market and counterparty risk;
 - (vii) concentration of assets (lack of diversity); and
 - (viii) derivative investments (see paragraphs 54-61);
 - (d) operational risks – in addition to the operational risks described in paragraph 30(e) above, operational risk in the fund context would include risks that may result in the trustee being 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, insurance or indemnification from a service provider responsible for the liability;
 - (e) liquidity risk – including risks arising from higher than anticipated levels of investment switching or transfers to other funds;
 - (f) valuation risk – in particular, the risks that the frequency of valuation is inconsistent with the frequency of establishing crediting rates or unit prices, giving the opportunity for arbitrage; the risk of incorrect valuation of assets for which there is not a deep or liquid market; and the risk of incorrect assessment of the tax implications associated with particular assets;

19 See Joint APRA/ASIC “Unit Pricing – Guide to Good Practice”

- (g) outsourcing risk – APRA’s guidance note SPG 231 on outsourcing (forthcoming) 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;
 - (h) 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;
 - (i) fraud (see paragraph 30(h) and paragraphs 62-64);
 - (j) 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;
 - (k) any other risk particular to the fund.
52. 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 charge²⁰. The document may be made available electronically or in hard copy. It follows that prudent trustees would be careful how they disclose sensitive information (such as policies for preventing theft and fraud) in these documents.
53. An RSE licensee which acts as trustee for a single non-complex fund may choose to prepare a single document to satisfy the requirements of both the RMS and RMP; however, in such circumstances the whole document must be made available as noted in paragraph 52 above.

Derivatives

54. Irrespective of whether a separate DRS is prepared, the trustee’s risk policies would typically take risks associated with the direct or indirect use of derivatives into account with appropriate risk controls and procedures. The use of derivatives for reasons other than hedging purposes is likely to give rise to unique risks.
55. A trustee’s risk management framework for derivatives would typically incorporate the following elements:
- (a) the trustee’s objectives in using derivatives;
 - (b) the trustee’s risk tolerances and a limit framework consistent with those risk tolerances;
 - (c) appropriate lines of authority and responsibility for transacting derivatives, including trading limits; and
 - (d) consideration of worst case scenarios and sensitivity analysis and reporting of that analysis.
56. APRA considers that trustees should not use derivatives for ‘speculation’, defined for the purposes of this SPG to mean investment activity which results in one or more of the following:
- (a) the net exposure of the fund to an asset class being outside the limits set out in the fund’s investment strategy. (Net exposure is exposure taking account of both physical and derivative exposure);
 - (b) the risk involved for the whole portfolio being outside that which the trustee considered appropriate when it developed and approved the fund’s investment strategy;
 - (c) the fund holding uncovered derivatives;
 - (d) the fund’s total portfolio being ‘geared up’ through derivatives to circumvent the limitations imposed by ss. 67, 95 and 97 of the SIS Act on borrowings.

²⁰ See the SIS Act s. 29PD

57. A fund whose only exposure to derivatives is through a collective investment such as a PST, unit trust or life insurance policy will not require a separate Derivative Risk Statement. However, APRA would expect that before investing in a collective investment and during any subsequent review process, the trustee would consider the return likely to be achieved from the collective investment and the risks involved. The risks include those from the use of derivatives. In such cases, the trustee would generally be able to demonstrate that the derivative exposure policies of the collective vehicle have been subject to the trustee's own due diligence.
58. APRA expects that the trustee would carefully assess whether the derivative usage of the collective investment schemes (both individually and in the aggregate) is in accordance with the investment strategy of the fund. APRA would expect to seek evidence of the trustee's consideration of these risks, as well as the manner in which the overall investments of the schemes relate to the investment strategy of the fund, when undertaking prudential reviews.
59. The trustee may consider it appropriate to rule out or restrict the use of derivative products where:
- the potential exposure cannot be reliably measured;
 - closing out of a derivative may be difficult considering the illiquidity of the market;
 - the derivative is not readily marketable (e.g. over-the-counter (OTC) rather than exchange traded derivatives); or
 - the counterparty is not suitably creditworthy.
60. Trustees adopting sound practice would consider setting exposure limits for derivatives taking account of the uncertainty caused by all types of risks such as credit, market, liquidity, counterparty, operational and legal risk. Serious consideration should be given to having quantitative limits for the exposure to any one counterparty (taking account of the credit risk attached to the counterparty) particularly in relation to OTC transactions.
61. To determine the level of those exposure limits the trustee would commonly address the types of risks involved in their investment portfolio and adjust these limits accordingly. For example, the level of uncertainty caused by credit, legal and operational risk (e.g. incorrect calculation of exposure) is significantly less for exchange traded as opposed to OTC derivatives. Therefore, a portfolio trading predominantly in exchange traded derivatives may allow for higher exposure limits than if the portfolio invested predominantly in OTCs.

Fraud

62. The SIS Act requires that the risk management framework would address fraud risk. Fraud risk relates to the risk associated with intentional acts, undertaken with the objective of personal benefit, to tamper with or manipulate the financial or operational aspects of the business.
63. Fraudulent activity can arise from internal sources (e.g. contribution redirection) or external sources (e.g. falsified rollover applications) and exposes the fund to risk of financial loss if not managed appropriately.
64. In relation to fraud, the risk management framework would typically include (but not be limited to) the following elements:
- risk identification and assessment;
 - internal controls and mitigation strategies, including both preventative and detective measures, and a fraud response policy incorporating processes for investigation, prosecution and recovery;
 - segregation of duties at both an operational level and in relation to functional reporting lines;
 - financial accounting controls; and
 - staff training and awareness.

Audit of the risk management framework

65. Both internal audit (assuming that the function exists within the RSE licensee or the group of which the licensee forms a part) and the approved auditor²¹ have a role to play in providing assurance to the RSE licensee and other stakeholders that the risk management framework has been properly developed, implemented and monitored.
66. APRA expects trustees to have due regard to the audit reports and the issues arising so that they are fed back into the review of risks and mitigants on an ongoing basis.

Internal audit

67. APRA envisages that a clear methodology would normally exist for determining the scope and frequency of the internal audit of all elements of the risk management framework.
68. Internal audit provides independent assurance to the trustee that internal control systems are in place and operating effectively, and that senior management are managing identified risks in order to minimise the possibility of unacceptable loss, either financial or non-financial, to the trustee, members or unitholders. Internal audit has a role in providing the trustee with assurance that the systems are effective. Where it does not already do so, the internal audit function would typically seek to expand its purview to also provide the trustee with assurance that the internal control systems are appropriate.
69. Typically, the internal audit function would have unfettered access to the records, personnel and property of the trustee, when and as required. Internal audit staff would be objective and impartial in discharging their duties and not allow themselves to be inappropriately influenced by management. To be fully effective, the internal audit function would have a direct reporting line to the Audit Committee or Board.

70. A trustee could consider setting out coverage of internal audits in a plan determined by the head of internal audit and approved by the trustee's Audit Committee. Whilst management may be consulted as part of the planning process, this would not typically control the outcome.
71. The internal audit function typically ensures that key controls are working and are adequate for risk mitigation purposes. Where control weaknesses are identified, the internal audit function would ensure rectification procedures are in place and actively monitored and reported to the appropriate levels of senior management and the relevant trustee committee.
72. It is typical for the internal auditor to liaise with the external approved auditor(s) on a regular basis. In particular, the approved auditor would ordinarily be made aware of any significant control issues and any other issues that may impact on the assessments undertaken during the financial statement and other statutory audits.

The role of the approved auditor

73. An approved auditor 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. The RMS and RMP must set out the circumstances in which an audit of the risks specified in SIS ss. 29H(2) and 29P(2) is to be undertaken.²² This should include any triggers which would cause the trustee to commission an additional audit outside the annual audit cycle.
74. 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. The 'whistleblowing' provisions in s. 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 that there has been a contravention that may affect the interests of members or beneficiaries.

21 See the SIS Act s. 10 and SIS Regulations Schedule 1AAA

22 See the SIS Act para. 35C(5)(d)

75. A sound risk management framework would 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 may be precluded from conducting the audit of the RMP or RMS for the purposes of s. 35C of the SIS Act. Similarly, a trustee adopting sound practice would ensure that 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 were identified and appropriately managed. In these examples, another auditor from the same practice is not precluded from providing the services. The risk management framework would usefully address the risks inherent in using the firm of the approved auditor for non-audit consultative work.
76. The trustee is required to obtain annual reports from an approved auditor in relation to its risk management framework. Section 35C of the SIS Act requires the auditor's report to address compliance with the trustee's RMS and the RMP in relation to the fund or PST and whether there are adequate systems in place to ensure future compliance. These reports need not be prepared at the same time as the audit reports on the financial statements of the fund and compliance with specified legislative provisions, and on the APRA Annual Return. The auditor's report on the risk management framework may be provided in the form of one document or as two or more separate documents at the request of the trustee. This is a matter for the trustee and the approved auditor to determine.
77. APRA has no objection to the audit of the RMS and RMP being conducted by different approved auditors provided that they each use the relevant parts of the approved form for reporting²³. Where different approved auditors are engaged to audit the RMS and RMP, APRA would expect that the trustee would need to make the RMS available to the approved auditor of the RMP so that the audit of the RMP is not carried out in isolation from the trustee's RMS.
78. Some trustees may have an RMS and RMP that contain identical information. The approved auditor may decide to combine the audit of the RMS and RMP under this scenario. However the auditor must still prepare separate auditor's reports on the RMS and RMP using the approved form.
79. Where the first audit of compliance with an RMP is being conducted, the period to be audited commences from the date the trustee approved the RMP (this date cannot be earlier than the date the RSE licence came into force or later than the date the trustee submitted an application to APRA under s. 29L of the SIS Act for the fund to be registered).
80. As the RMP is available on request to the members of the fund (and to employer sponsors where the fund is a defined benefit fund), approved auditors should assume that the auditor's report related to the RMP may also be provided to members.
81. The trustee is required to keep the RMS and RMP up-to-date and to review them at least annually to ensure that they continue to comply with the legislation. Where positive assurance is being provided on a trustee's compliance during a year of income, the audit should address all RMSs and RMPs in operation during that year of income.
82. It is common for trustees to engage other professional experts (actuaries, lawyers, investment advisers, IT personnel) to advise on issues arising from an audit. The trustee would generally ensure their reports (in addition to assisting in immediate remedial action) are used to update RMS and RMP as warranted.

Trustee attestation

83. RSE licensees are 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.

²³ See Part 3 of the form of audit report approved for the purposes of s. 35C of the SIS Act

84. APRA may also seek a copy of the trustee's risk reporting for the twelve months of the statutory return period, supporting the attestation.
85. The trustee may be requested by APRA to provide evidence of the processes undertaken to compile the risk reporting in support of the attestation. Inaccurate attestations would constitute a breach of the *Financial Sector (Collection of Data) Act 2001* and would also reflect on trustee fitness and propriety.

Conclusion

86. 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.

Australian Standard for Risk Management (AS/NZS/4360:2004)

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

ASFA (2004) *Managing the Risk of Fraud and Theft in Superannuation Funds* Best practice paper 20, January 2004

ASFA (2005) *Risk Treatment Tools and Resources* Best practice paper 23 [July 2005]

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*. February 2003.

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*.

Institute of Internal Auditors, American Institute of Certified Public Accountants and Association of Certified Fraud Examiners (2008), *Managing the Business Risk of Fraud: a Practical Guide*.

Standards Australia lists a number of publications on risk management on its website at www.standards.com.au



Telephone
1300 13 10 60

Email
contactapra@apra.gov.au

Website
www.apra.gov.au

Mail
GPO Box 9836
in all capital cities
(except Hobart and Darwin)