Prudential Practice Guide

SPG 220 – Risk Management

July 2013

www.apra.gov.au

Australian Prudential Regulation Authority

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 prudential 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.

About this guide

Prudential practice guides (PPGs) provide guidance on APRA's view of sound practice in particular areas. PPGs frequently discuss legal requirements from legislation, regulations or APRA's prudential standards, but do not themselves create enforceable requirements.

Prudential Standard SPS 220 Risk Management (SPS 220) sets out APRA's requirements for an RSE licensee to have systems for identifying, assessing, managing, mitigating and monitoring material risks that may affect its ability to meet its obligations to beneficiaries. This PPG aims to assist an RSE licensee in complying with those requirements and, more generally, to outline prudent practices in relation to risk management.

This PPG is to be read with other PPGs related to risk management, including: *Prudential Practice Guide SPG 114 Operational Risk Financial Requirement*, *Prudential Practice Guide SPG 231 Outsourcing* (SPG 231) and *Prudential Practice Guide SPG 232 Business Continuity Management*.

For the purposes of this guide, and consistent with the application of SPS 220, 'RSE licensee' and 'registrable superannuation entity (RSE)' have the meaning given in the *Superannuation Industry (Supervision) Act 1993* (SIS Act).

Subject to the requirements of SPS 220, an RSE licensee has the flexibility to structure its business operations in the way most suited to achieving its business objectives. Not all practices outlined in this PPG will be relevant for every RSE licensee and some aspects may vary depending upon the size, business mix and complexity of the RSE licensee's business operations.

Introduction

1. An effective risk management framework includes appropriate levels of risk governance (oversight, monitoring and control) to enable an RSE licensee to manage the material risks of its business operations.
2. This PPG provides guidance on APRA's expectations with regard to an RSE licensee's risk management framework and outlines sound practices in relation to the management of risk throughout an RSE licensee's business operations.
3. The definition of an RSE licensee's business operations is sufficiently broad to include risks arising from not only RSEs within those business operations but also other non-superannuation activities of the licensee, such as the operation of a managed investment scheme, to the extent that these activities may pose a material risk to its activities as an RSE licensee.

Risk culture

4. APRA's view is that a strong risk culture is a core element of an effective risk management framework. An RSE licensee's risk culture generally reflects the RSE licensee's corporate values as well as attitudes and behaviours of individuals within its business operations.
5. An RSE licensee's risk culture is strongly influenced by the 'tone at the top'. APRA expects the Board of an RSE licensee (the Board) to demonstrate its commitment to risk management and foster an environment of active engagement with risk management processes and outcomes, and in which the risk management function is influential and respected.[1]
6. It is APRA's view that an RSE licensee with a strong risk culture would ordinarily exhibit a number of organisational attributes and behaviors. These include transparency, active engagement and risk awareness, objective review and challenge and, importantly, a focus on honesty and integrity. A strong risk culture will generally result in all staff members having a clear understanding of their responsibilities and accountability for managing risk. A strong risk culture will also openly encourage escalation of matters of concern.
7. APRA considers that the development of a strong risk culture will be assisted by an ongoing risk education and awareness training program, processes to ensure behaviour is monitored and managed within risk appetite, and robust and prudent policies for responding to potentially damaging incidents.
8. Remuneration policies can also contribute to a strong risk culture if they are designed to encourage and incentivise employees to act responsibly and with integrity in a manner consistent with the RSE licensee's risk management framework.[2]
9. In APRA's experience, a strong risk culture will be evidenced by high levels of risk awareness across an RSE licensee's business operations, supported by proactive, timely and complete risk reporting with adherence to approved risk management procedures and appropriate action taken when issues are identified.

1 For the purposes of this PPG, a reference to 'the Board' is a reference to the Board of directors or group of individual trustees of an RSE licensee and 'group of individual trustees' has the meaning given in s. 10(1) of the SIS Act.

2 Refer to *Prudential Practice Guide SPG 510 Governance* (SPG 510) and *Prudential Practice Guide PPG 511 Remuneration* for guidance on the design of remuneration policies.

Material risks

10. Under SPS 220, an RSE licensee is responsible for ensuring that it identifies, assesses, manages and regularly reviews all material risks to its business operations.

11. SPS 220 identifies categories of risk that the risk management framework must, at a minimum, cover. APRA expects an RSE licensee would be able to demonstrate how it determines and communicates 'materiality' of risks within each category and ensure that its approach is understood and consistently applied across its business operations.

12. When considering material risks, APRA expects an RSE licensee would consider contagion risk arising from any non-superannuation activities within its business operations. An RSE licensee may also consider the impact a particular risk event may have on other risks, e.g. a major disruption or prolonged business process failure event (operational risk) during a time of economic downturn may have an impact on liquidity or fund solvency.

13. An RSE licensee would also ensure that risks that may not be unambiguously attributed to a particular category of risk are not overlooked. For example, a risk broadly categorised as a governance risk may include elements that relate to, and should be managed as, another category of risk e.g. operational risk.

14. Attachment A provides examples of the risks that an RSE licensee might identify within each of the categories of material risk set out in SPS 220.

Risk management framework

15. A risk management framework enables an RSE licensee to implement a holistic and forward-looking approach to risk management throughout the entirety of its business operations to support sound risk-based decision-making. This is achieved, in part, through a clearly articulated risk appetite statement that outlines the RSE licensee's risk appetite and risk tolerances within its risk capacity.[3]

16. APRA expects that the primary focus of an RSE licensee's risk management framework would ordinarily be the management of risks in a way that is consistent both with the best interests of beneficiaries and the maintenance of the sound financial position of the RSE licensee's business operations.

17. APRA expects that an RSE licensee would appoint risk owners who are responsible and accountable for identifying, assessing and managing material risks, including ensuring that the mitigants and controls are effective and consistently implemented. This would ordinarily include appropriate consideration of end-to-end risk management processes.

18. An RSE licensee might also consider establishing a Board Risk Committee with delegated authority for risk governance to review and challenge the implementation and oversight of the risk management framework and the RSE licensee's risk profile.

3 Refer to SPS 220 for the definition of risk appetite and risk tolerance. Risk capacity is the maximum risk an RSE licensee can bear.

Strategic and business planning

19. The business plan required by SPS 220 is an important management and control tool that enables an RSE licensee to document and communicate its strategic direction and objectives, identify opportunities in the market place, forecast results, allocate resources and establish appropriate review criteria.

20. APRA's view is that having a risk management strategy and a risk appetite statement that are consistent with a sound business plan is fundamental to an effective risk management framework. As such, APRA expects that the risk management framework would be developed and reviewed in the context of an RSE licensee's strategic and business planning processes.

21. APRA expects the business plan review process would usually consider the impact on the risk profile of the RSE licensee's business operations and identify the potential emergence of any new material risks. This might include formal consideration of issues arising from planned material changes to the RSE licensee's business operations and risks.

Risk appetite statement

22. APRA expects that an RSE licensee's risk appetite statement would identify the strategic and business risks of its business operations and clearly communicate its boundaries and expectations of how much risk it is willing to accept. APRA's view is that a reasonable and easily understood risk appetite statement is a fundamental element of a risk management framework.

23. The articulation of risk appetite and risk tolerances is central to a risk appetite statement. Risk appetite is the degree of risk an RSE licensee is prepared to accept in pursuit of its strategic objectives. Risk tolerances translate risk appetite into operational limits for the day-to-day management of material risks.

24. The development of an RSE licensee's risk appetite statement may be informed by and, in turn, inform the strategic planning process by focusing on the acceptability of risks associated with new business initiatives and planned business activities.

25. APRA expects that the Board would be actively engaged in the development, and be able to demonstrate ownership, of the risk appetite statement. APRA considers that this might be achieved, in part, through reporting and communication processes and structures that enable the Board and Board Risk Committee (as appropriate) to:

    (a) understand how senior management interprets and applies risk tolerances;

    (b) be satisfied that senior management interpretation and application of the risk appetite is appropriate; and

    (c) take factors (a) and (b) into account when reviewing the risk appetite statement.

26. A prudent RSE licensee would communicate its risk appetite statement, or pertinent parts of its risk appetite statement, throughout its business operations and to its outsourced service providers to ensure that the risk appetite statement is consistently implemented and understood as appropriate. An appropriate summary of the risk appetite statement would reflect the intended audience and any confidential or commercially sensitive information. It may exclude information on the management of certain risks where the communication of this information may be counter-productive to the risk management objective (e.g. tolerance of fraud risk).

27. A prudent RSE licensee would consider a variety of processes to assess risks. Where an RSE licensee has the capability to use risk quantification techniques, such techniques may form part of setting and monitoring the risk appetite statement. Risk quantification techniques may provide an RSE licensee with assurance that the risk does not exceed an RSE licensee's risk tolerance and also its risk capacity. These techniques may not be appropriate for all types of risk. APRA expects the results of such analysis and testing would be reported to the Board, or Board Risk Committee, and may be considered when establishing or reviewing the risk appetite statement.

Risk appetite

28. Risk appetite is distinct from risk tolerance as it focuses on broader, strategic direction about how much risk is acceptable in relation to an RSE licensee's business operations overall, and for each category of material risk.

29. In APRA's experience, risk appetite can be expressed in a number of ways to ensure that it is commonly understood and consistently applied across an RSE licensee's business operations. Risk appetite may be expressed in the form of high-level qualitative statements that clearly capture the RSE licensee's attitude and level of acceptance of different risk types, or it may be detailed and include quantitative measures, or a mixture of both.

Risk tolerance

30. Risk tolerances for each material risk are based on the maximum level of acceptable risk after taking into account appropriate mitigants and controls to reduce the risk. To facilitate implementation and monitoring of the risk appetite in day-to-day business activities, an RSE licensee may also decide to set risk limits for more granular risks within each material risk.

31. Risk tolerances can be expressed in a number of different forms depending on the nature of the risk being managed. The risk tolerances can act as triggers for consideration of whether any action is necessary in relation to the risk. Where possible, risk tolerance would be expressed as a measurable limit to enable a clear and transparent monitoring process that ensures the RSE licensee remains within the determined risk tolerance. An RSE licensee may also define key indicators with thresholds around the risk tolerance.

32. APRA recognises that for some risks a qualitative risk tolerance may be appropriate. In these circumstances, the RSE licensee would be expected to ensure the tolerance is well-articulated to enable consistent implementation across the RSE licensee's business operations and for determining when the risk tolerance has been exceeded.

33. Sample risk tolerance statements might be structured along the following lines:

    (a) 'an RSE experiences a loss of more than x per cent of members in a rolling month period';

    (b) 'a MySuper product delivers net investment returns (post-tax) in the bottom x per cent of all MySuper products more than x times over a period of x years'; and

    (c) 'a material outsourced provider fails to meet agreed performance standards for x consecutive months'.

34. Where a risk exposure falls outside the RSE licensee's risk tolerance, APRA expects that the RSE licensee would develop and implement a plan of action to review the risk and reduce it to a level that is within its acceptable tolerance.

Risk management strategy

35. The SIS Act requires an RSE licensee to formulate, review regularly and give effect to a risk management strategy.[4]

36. APRA expects that a risk management strategy would contain sufficient information to communicate in general terms the RSE licensee's approach to risk management. This includes how it identifies, assesses, mitigates, manages, monitors and regularly reports on the risks of its operations and those of the RSEs within its business operations. A risk management strategy may include other documents by reference including, for example, relevant policies, standards (or frameworks) and guidelines that describe an RSE licensee's approaches to managing its material risks.

37. APRA envisages that the risk management strategy would also assist the effective review of the risk management framework. An RSE licensee may choose to also develop a separate overarching risk governance document if it decides that this is appropriate to assist clarity and understanding.

Risk management function

38. A key role of an RSE licensee's risk management function is to assist the Board and Board committees by providing independent and objective oversight, monitoring and reporting in relation to risks to the RSE licensee's business operations. An additional responsibility is to assist senior management develop, implement and maintain the risk management framework.

39. APRA expects the risk management function would also ordinarily assist the Board and Board committees by providing support, education and training to directors, senior management and staff of the RSE licensee.[5] It would also typically facilitate and support the development and implementation of a strong risk culture throughout the RSE licensee's business operations.

40. APRA's view is that an effective risk management function would have a clear understanding of the responsibilities and accountabilities associated with the role. APRA expects this would also be evident in documentation relating to the risk management function that is regularly reviewed and updated by the RSE licensee.

41. When determining the appropriateness of the resourcing of the risk management function, APRA expects the function would be able to engage in all major strategic initiatives that are appropriate to enable it to fulfil its risk management role.

42. A risk management function may incorporate different divisions or functions. For example, it may include one or more divisions that focus on a particular type of risk, but who still form part of the overall risk management function to ensure a holistic approach.

43. APRA envisages an appropriate reporting structure for the risk management function would ordinarily include direct access to the Board, Board Risk Committee (as appropriate) or senior management, independent of the business functions. It may also provide direct access to either the Board or Board Risk Committee, where appropriate, whilst maintaining independence from the senior management of the RSE licensee.

44. APRA does not expect that outsourcing the risk management function would be a common practice, but where an RSE licensee considers there is adequate justification for outsourcing this function, APRA will consider it to be a material business activity for the purposes of *Prudential Standard SPS 231 Outsourcing* (SPS 231).[6]

4 Refer to s. 52(8)(a) of the SIS Act.

5 For the purposes of this PPG, a reference to a 'director' is to be read as a reference to an individual trustee in a group of individual trustees within the meaning of s. 10(1) of the SIS Act.

6 Refer to SPG 231.

Risk identification and assessment

45. Risk identification and assessment is an integral part of an RSE licensee's risk management framework. APRA recognises that there are a number of techniques available to an RSE licensee to enable the identification, assessment or quantification of certain types of risks and their potential impact on its operations.

46. Risk and control self-assessment processes are often used as part of the approach for identifying and assessing operational risks and monitoring the control environment. Such self-assessments facilitate a consistent approach that can be independently reviewed and may be a valuable tool for assessing and monitoring the ongoing effectiveness of the internal control environment.

Controls and mitigation

Control approaches

47. Control mechanisms and control assurance are central to the ongoing implementation of an effective risk management framework. APRA expects that control mechanisms would normally operate at every level within an RSE licensee's business operations. Prudent practice suggests that an RSE licensee would consider its risk appetite statement when assessing the adequacy and efficacy of controls in managing and mitigating risks, and ensuring that material risks remain within risk appetite, risk tolerances and other more granular risk limits.

48. APRA's view is that assurance about the design, effectiveness and appropriateness of controls may be achieved through a number of different approaches for different risk types. These may include, but not be limited to:

    (a) ongoing Board and senior management reviews of progress towards stated risk management objectives;

    (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 area of the RSE licensee's business operations and for interactions with outsourced service providers;

    (d) a system for assessing the design and effectiveness of controls and for monitoring compliance with controls, including escalation procedures for accelerated reporting of material control failures and compliance breaches and exceptions to the Board, Board committees and senior management;

    (e) policies and procedures that document controls and treatment plans for the resolution of non-compliance issues including fraud and instances of material failures in business processes or systems;

    (f) documented arrangements for the receipt and treatment of information from whistleblowers;

    (g) mechanisms to ensure that all personnel have appropriate performance objectives, expertise and training with regard to relevant risks;

    (h) mechanisms to ensure that adequate financial, human and technical resources are available at all times to satisfactorily implement the RSE licensee's business requirements and risk management framework, including its risk mitigation activities;

(i) regular verification and reconciliation of transactions, member registers and accounts;

(j) internal assurance programs and external audit; and

(k) safeguards for access to, and use of, the RSE licensee's assets and records, including physical and electronic controls.

Risk transfer

49. Risk transfer involves taking part or all of a risk to which an RSE licensee is exposed and making an arrangement with another party to manage that risk or mitigate that risk, whilst the RSE licensee retains ultimate responsibility for the risk. At times, risk transfer may change the risk profile rather than reduce risk and in some cases it may create new risks. For example, outsourcing the administration function may transfer the risk of processing errors to the provider, but increase other risks such as the risk of reliance on another party, or contractual risk.[7]

50. An RSE licensee may obtain professional indemnity or similar insurance cover with respect to certain material risks indentified within its risk management framework. Whilst such insurance cover may provide for compensation in the event of a claim being made by the RSE licensee, it does not reduce the potential incidence of events leading to a claim. For this reason, APRA expects an RSE licensee would continue to actively manage the risk for which the insurance is purchased and for which an RSE licensee remains ultimately responsible. APRA also expects an RSE licensee would consider uncertainties such as timeliness of claim payments, coverage of the policy, circumstances where the policy may not be effective or triggered, and the risk that the insurer may not be able to meet its obligations to pay under that insurance cover when deciding whether to enter into or continue that cover.

51. When an RSE licensee contracts a third party to provide a material business activity, consistent with the requirements in SPS 231, APRA expects an RSE licensee would assess, as part of its necessary due diligence, what risk mitigants and controls, if any, the service provider has in place. An RSE licensee would then ordinarily determine the extent to which it can reasonably rely upon these measures. As part of this assessment, APRA expects an RSE licensee would consider matters such as contractual arrangements with, and insurance policies held by, the third party. The RSE licensee would also usually instigate an appropriate level of ongoing oversight and reporting to ensure that it is aware of, and in a position to take steps to address, any changes that may impact on its risk exposure to the outsourced activity.

Incident management

52. APRA considers that it would be prudent practice for an RSE licensee to implement processes and systems for the capture, management, reporting and escalation of events that may affect its ability to meet its obligations to beneficiaries (risk incidents). This would involve processes for investigating and analysing the causes of risk incidents to identify the drivers for the incident and areas where the controls and mitigation might be enhanced to prevent similar events from recurring. This information would assist an RSE licensee in reviewing the appropriateness of the risk management framework and, in particular, the application of the risk appetite statement.

53. APRA expects that the depth of investigations and analysis of risk incidents will vary according to the nature, scale and complexity of the risk incident and that the scope of any causal analysis process would be sufficiently broad to allow for the identification of all significant elements of the incident or event.

7 Refer to SPG 231.

54. Key information to facilitate initial and ongoing analysis of risk incidents may include, but is not limited to:

    (a) the occurrence and detection dates;

    (b) identification of the underlying causes and contributing factors;

    (c) direct and indirect financial costs incurred or estimated as the result of the risk incident, including specific documentation of any loss amount and any subsequent recoveries;

    (d) whether the incident was addressed by the operational risk financial requirement (ORFR) and if so, the amount received from the ORFR[8];

    (e) remediation actions;

    (f) changes to controls and risk profile of the RSE licensee's business operations; and

    (g) an assessment of other potential exposures to similar risk incidents.

Monitoring and reporting

Reporting and escalation processes

55. APRA expects an RSE licensee's risk management framework would ensure that the Board receives regular reporting on material risks relative to the RSE licensee's risk appetite statement, assessment of risks and the operation and effectiveness of controls.

56. An RSE licensee's formal escalation procedures would ordinarily cover reporting of exceptions to risk appetite, risk tolerances, and more granular risk limits, key indicators and risk incidents. This reporting would include commentary to facilitate management review and understanding of the report content, where necessary.

57. Analysis of the trends of material risks, operation of controls and risk assessments through time can provide valuable information about business activity and changes in the business environment that may alter the risk profile of an RSE licensee.

8 Refer to SPG 114.

Information systems for reporting

58. APRA expects that an RSE licensee would, as part of its risk management framework, ordinarily establish, maintain and document effective management information systems commensurate with the size, business mix and complexity of its business operations. Such information systems assist in the management, communication and reporting of risk issues and outcomes and may assist the RSE licensee to appropriately manage different types of risk that may affect its ability to meet its obligations to beneficiaries.

59. APRA envisages that an RSE licensee would implement controls for ensuring data in information and reporting systems is current, accurate and complete. Internal information and reporting systems would be secure and supported by adequate business continuity and disaster recovery arrangements.[9]

60. A well-functioning information and reporting system would typically:

    (a) produce appropriate financial, investment, operational, risk and compliance data;

    (b) incorporate relevant markets information that is relevant to decision-making;

    (c) report accurate and timely information;

    (d) allow the RSE licensee to identify, assess and monitor business activities, risks, financial position and performance;

    (e) allow the RSE licensee to identify, assess and monitor business activities, existing and emerging risks, financial position and performance;

    (f) allow the RSE licensee to monitor the effectiveness of, and compliance, with, its internal control systems and report any exceptions that arise; and

    (g) 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.

9 Refer to Prudential *Practice Guide PPG 235 Managing Data Risk* for further guidance.

Review of the risk management framework

61. SPS 220 requires an RSE licensee to ensure its risk management framework is comprehensively reviewed by operationally independent, appropriately trained and competent persons at least every three years, and provides details of the scope of this review.

62. A prudent RSE licensee's consideration of whether a person is operationally independent would take into account any role that the person may have in connection with the development or implementation of the framework, or the activities under review, that may impact on their ability to perform an objective review.

63. In some circumstances an internal audit function may be regarded as operationally independent for the purposes of conducting or participating in the comprehensive review of the risk management framework, e.g. where the role of the internal audit function will not limit the robustness of the review.

64. SPS 220 also requires the risk management framework to be subject to a review of its appropriateness, effectiveness and adequacy during interim years. This interim annual review may explore particular elements of the risk management framework in depth on a rotational basis.

65. An RSE licensee may decide that resources from the internal audit or risk management function have the appropriate skills and experience to perform the interim review of the risk management framework. In these circumstances, a prudent RSE licensee would consider appropriate steps to ensure the review is objective.

66. APRA considers that effective reviews of the risk management framework would normally encompass:

    (a) an assessment as to whether the framework remains appropriate for the RSE licensee and the risks being managed;

    (b) whether the framework has been consistently implemented;

    (c) whether lessons have been learnt from risk incidents; and

    (d) consideration as to whether the framework is effective in providing appropriate and timely information to inform the decision-makers.

Audit

67. Internal audit provides independent assurance to an RSE licensee that key controls are in place and operating effectively, and are appropriate for risk mitigation purposes.[10] Where control weaknesses are identified, APRA expects the internal audit function would confirm rectification procedures are in place and are actively monitored to completion and reported to the appropriate levels of senior management and the Board or relevant Board committee.

68. An RSE licensee may also include, as part of the internal audit approach, specific consideration of key aspects of the risk management framework and related implementation. This information may support the annual risk management declaration requirement required by SPS 220.

Risk management declaration

69. SPS 220 requires the Board to provide APRA with a risk management declaration on an annual basis. Whilst this declaration does not have to be audited, APRA expects that the two directors of the RSE licensee who sign the declaration would have obtained reasonable assurance, and if necessary considered independent advice, on the matters upon which they have made a declaration.

APRA notification requirements

70. An RSE licensee is required to notify APRA of material changes to the size, business mix and complexity of the RSE licensee's business operations. APRA expects this would include, but not be limited to, events such as proposals relating to major modifications to, or the re-organisation of, the functions of the RSE licensee or RSE, any changes to a group of which the RSE licensee may be a part, changes to new business lines, successor fund transfers, appointment as RSE licensee of other RSEs and changes in entity administration.

10 SPG 510 provides further guidance on the role of the internal auditor.

Attachment A

Categories of material risks

1. Strategic and tactical risk is those risks that arise from an RSE licensee's strategic and business plans. Examples may include, but are not limited to, risks:
   (a) from the development of new products or introduction of new systems and processes;
   (b) associated with a change of strategic direction, e.g. developing an in-house business function, or a decision to outsource or offshore an existing business function;
   (c) associated with planned activities such as merger or acquisition;
   (d) associated with the solvency of the RSE licensee or the risk that the value of the assets of at least one of the RSEs may fall below that required for it to remain a going concern or that an RSE may not be able to provide benefits under the governing rules; and
   (e) arising from changes to the external business environment, e.g. competitor and market changes.
2. Governance risk is those risks that threaten the ability of an RSE licensee to make reasonable and impartial business decisions in the best interests of beneficiaries. Governance risks may include, but are not limited to, risks associated with:
   (a) accountability and transparency of decision-making processes;
   (b) delegations of roles and responsibilities;
   (c) remuneration arrangements;
   (d) fitness and propriety; and
   (e) the management of conflicts of interest.[11]
3. Governance risks may also arise in transitional situations where, for example, functions are moved between in-sourced and outsourced arrangements, or when transferring business functions between outsourced service provider; or in situations where essential staff are absent or to be replaced.
4. APRA expects an RSE licensee would ordinarily expressly consider agency risk as part of governance risk. Agency risk relates to the possibility that internal or external service providers, subsidiaries, fund promoters, agents and advisors will not act in the best interests of beneficiaries and/or have misaligned incentives for the provision of service to the RSE licensee.
5. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This includes legal risks, but excludes strategic and reputational risks. Operational risks are often categorised as the risk of loss from:
   (a) internal fraud - losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy (excluding diversity/discrimination events) which involve at least one internal party;
   (b) external fraud - losses due to acts of a third party that are of a type intended to defraud, misappropriate property or circumvent the law;
   (c) employment practices and workplace safety - losses arising from acts that are inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims or from diversity/discrimination events;
   (d) clients, products and business practices - losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients, including fiduciary and suitability requirements, or from the nature or design of a product;

11 Refer to SPG 510, *Prudential Practice Guide SPG 520 Fit and Proper* and *Prudential Practice Guide SPG 521 Conflicts of Interest* for further guidance on governance risk.

(e) damage to physical assets - losses arising from loss or damage to physical assets from natural disaster or other events;

(f) business disruption and systems failure – losses arising from disruption of business or system failures; and

(g) execution, delivery and process management – losses arising from failed transaction processing, process management, relations with trade counterparties and vendors. This category includes administration errors and unit pricing errors.

6. Investment governance risk is the risk that threatens the ability of an RSE licensee to manage its investments to adequately protect the interests, and meet the reasonable expectations, of beneficiaries. Investment governance risks may include, but are not limited to, weaknesses in:

   (a) the investment governance framework;

   (b) delegations and decision-making processes;

   (c) the selection, retention, monitoring and reporting of investments; and

   (d) management of the services provided by investment managers, advisors and other third-party service providers.[12]

7. Liquidity risk is the risk of inability to meet obligations as and when they fall due without incurring unacceptable losses.

8. Insurance risk is the risk of making insured benefits available to beneficiaries including where an RSE licensee self-insures benefits to members.[13]

12 Refer to *Prudential Standard SPS 530 Investment Governance* and associated guidance.

13 Refer to *Prudential Practice Guide SPG 250 Insurance in Superannuation* and *Prudential Standard SPS 160 Defined Benefit Matters.*

Telephone
1300 55 88 49

Email
info@apra.gov.au

Website
www.apra.gov.au

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

APRA_PPG_SPG520_062013_ex