ASIC
Australian Securities & Investments Commission

CONSULTATION PAPER 204

Risk management systems of responsible entities

March 2013

About this paper

This paper sets out our proposals for regulatory requirements and guidance relating to the risk management systems of Australian financial services (AFS) licensees that are responsible entities and are not regulated by the Australian Prudential Regulation Authority (APRA).

> Note: Subject to the passage of the Superannuation Legislation Amendment (Service Providers and other Governance Measures) Bill 2012 (Superannuation Bill), the proposed requirements and guidance will also apply to APRA-regulated registrable superannuation entity licensees (RSEs) that manage non-superannuation registered managed investment schemes (dual-regulated entities). From the commencement date of the legislation, the obligation to have adequate risk management systems for these entities will exclude risks that relate solely to the operation of the RSE.

These proposals follow our recent review of risk management systems of selected responsible entities, the findings of which are discussed in Report 298 *Adequacy of risk management systems of responsible entities* (REP 298) published in September 2012.

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents.

Consultation papers: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

Regulatory guides: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

Information sheets: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

Reports: describe ASIC compliance or relief activity or the results of a research project.

Document history

This paper was issued on 21 March 2013 and is based on the Corporations Act as at the date of issue.

Disclaimer

The proposals, explanations and examples in this paper do not constitute legal advice. They are also at a preliminary stage only. Our conclusions and views may change as a result of the comments we receive or as other circumstances change.

Contents

The consultation process

You are invited to comment on the proposals in this paper, which are only an indication of the approach we may take and are not our final policy.

As well as responding to the specific proposals and questions, we also ask you to describe any alternative approaches you think would achieve our objectives.

We are keen to fully understand and assess the financial and other impacts of our proposals and any alternative approaches. Therefore, we ask you to comment on:

- the likely compliance costs;
- the likely effect on competition; and
- other impacts, costs and benefits.

Where possible, we are seeking both quantitative and qualitative information. We are also keen to hear from you on any other issues you consider important.

Your comments will help us develop our policy on risk management systems of responsible entities. In particular, of any information about compliance costs, impacts on competition and other impacts, costs and benefits will be taken into account if we prepare a Regulation Impact Statement: see Section E, 'Regulatory and financial impact'.

Making a submission

We will not treat your submission as confidential unless you specifically request that we treat the whole or part of it (such as any financial information) as confidential.

Comments should be sent by 3 May 2013 to:

Violet Wong
Senior Lawyer, Investment Managers & Superannuation
Australian Securities and Investments Commission
Level 5, 100 Market Street
Sydney NSW 2000
facsimile: 02 9911 2414
email: reriskmanagement@asic.gov.au

What will happen next?

Stage 1	21 March 2013	ASIC consultation paper released
Stage 2	3 May 2013	Comments due on the consultation paper
	Mid-2013	Drafting of regulatory guide and accompanying regulatory documents
Stage 3	August 2013	Regulatory guide and accompanying regulatory documents released

A Background to the proposals

Key points

The Australian managed funds sector is one of the largest in the world, managing significant non-superannuation assets.

Risk management systems play an important role in building retail investor and financial consumer confidence by mitigating exposure to relevant risks. They also build confidence in the integrity of Australia's capital markets by better safeguarding the financial services industry from systemic risk.

However, there is no industry-specific guidance available to responsible entities on risk management systems to help them better manage the risks they face both as responsible entities and for the scheme(s) they operate.

This consultation paper sets out our proposals for more targeted requirements and guidance for responsible entities in complying with their risk management obligations as AFS licensees. The proposed requirements can be applied by responsible entities according to the nature, scale and complexity of their operations.

The managed funds sector

1 Australia's managed funds sector is one of the largest in the world, managing significant non-superannuation assets for retail investors.

2 The managed funds sector in Australia is sizable and diverse. As at February 2013, over 500 responsible entities operated about 4,000 registered managed investment schemes (schemes). The largest ten investment management groups collectively managed $531 billion for numerous schemes in the September 2012 quarter, amounting to roughly one quarter of the funds under management in Australia. In contrast, smaller investment managers in the sector may only operate one scheme with a relatively small asset value.

3 The managed funds sector also invests in a variety of assets, including infrastructure, fixed interest products, mortgages, real property, cash and private equity.

Risk management in the managed funds sector

4 Every business takes risks to operate and grow, and needs to manage those risks to do so. Risk management is not about eliminating risk. It is about controlling risks to increase the likelihood of meeting business objectives.

5 Adequate risk management systems and controls in businesses therefore play an important role in building investor and consumer confidence by mitigating exposure to relevant risks. They also build confidence in the integrity of Australia's capital markets by providing measures that will better safeguard the financial services industry from systemic risk.

6 Adequate risk management is critical for an industry which has the size of the managed funds sector in Australia, and has been the focus of regulators across the globe following the global financial crisis. For example, the Monetary Authority of Singapore (MAS) and the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in Germany have introduced new guidance on risk management for investment management companies. The International Organization of Securities Commissions (IOSCO) has also published new principles of liquidity risk management for collective investment schemes.

> Note: See 'MAS Implements Enhanced Regulatory Regime for Fund Management Companies', MAS media release, 6 August 2012; BaFin's Circular 4/2010 (WA) *Minimum requirements for the compliance function and additional requirements governing rules of conduct, organisation and transparency pursuant to sections 31 et seq. of the Securities Trading Act (Wertpapierhandelsgesetz—WpHG) for Investment Services Enterprises*, 14 June 2011; and FR 03/13 *Principles of liquidity risk management for collective investment schemes*, Final report, Report of the Board of IOSCO, March 2013, available at www.iosco.org.

Regulatory framework in Australia

7 As AFS licensees, responsible entities have an ongoing legal obligation under s912A(1)(h) of the *Corporations Act 2001* (Corporations Act) to have adequate risk management systems (risk management obligations), unless they are regulated by APRA. Bodies regulated by APRA need to meet requirements for risk management set out in legislation and prudential standards.

> Note: The relevant legislation for these requirements for RSEs includes the *Superannuation Industry Supervision Act 1993* (SIS Act) and Superannuation Industry Supervision Regulations 1994 (SIS Regulations).

8 In Regulatory Guide 104 *Licensing: Meeting the general obligations* (RG 104), we provide guidance for all AFS licensees (including responsible entities) about what we expect of them in meeting their risk management obligations. This includes guidance that what is 'adequate' for each licensee depends on the nature, scale and complexity of their business and their risk profile.

9 Specifically, in RG 104, we state that an AFS licensee's risk management systems should:

(a) be based on a structured and systematic process that takes into account the licensee's obligations under the Corporations Act;

(b) identify and evaluate risks faced by the licensee's business, focusing on risks that adversely affect consumers or market integrity and including risks of non-compliance with financial services laws;

(c) establish and maintain controls designed to manage or mitigate those risks; and

(d) fully implement and monitor those controls to ensure they are effective.

10 There is also other guidance on risk management that is available to AFS licensees (including responsible entities), such as the international standard for risk management, ISO 31000:2009 *Risk management: Principles and guidelines*. The standard is not specific to the managed funds sector.

Current industry practice

11 In 2011–12, we reviewed selected responsible entities ranging in size and complexity to assess the adequacy, and strategic and operational effectiveness, of their risk management systems, and how they specifically manage financial, investment and liquidity risks. The review sought to:

(a) determine the ability of these AFS licensees to comply with their risk management obligations;

(b) consider whether risk management systems had changed in light of the global financial crisis or other external or internal factors; and

(c) encourage better preparedness for market volatility in the future.

12 Among other observations, we found that:

(a) the selected responsible entities generally appeared to demonstrate compliance with their risk management obligations, although improvements to risk management systems could be made—in particular, for those selected responsible entities that were not part of an APRA-regulated group;

(b) the selected responsible entities each had a unique risk management system, which reflected the nature, scale and complexity of their financial services business;

(c) the selected responsible entities that were part of an APRA-regulated group had more sophisticated risk management systems than those that were not part of an APRA-regulated group; and

(d) generally, the selected responsible entities indicated that their risk management system itself did not change as a result of the global financial crisis.

13 The complete findings of our review were published in Report 298 *Adequacy of risk management systems of responsible entities* (REP 298) in September 2012.

Improving risk management practices across the sector

14 Given the fundamental importance of risk management systems to businesses, the amount of funds under management in this sector, and the findings of our review in REP 298 (especially as they apply to smaller responsible entities), we think that there is a need for more targeted requirements and guidance on risk management for responsible entities that are not APRA-regulated (including by reference to good industry practices).

15 The proposals in this consultation paper aim to help responsible entities to better manage the risks they face as responsible entities, especially in relation to operating scheme(s).

16 The proposals are consistent with the recommendations of the Parliamentary Joint Committee on Corporations and Financial Services (PJC) in its report on the Inquiry into the collapse of Trio Capital (Trio report). Specifically, the PJC recommended that 'further efforts be made to investigate avenues to protect investors in the case of theft and fraud by a managed investment scheme': see Recommendation 1(a).

17 The PJC also noted the need to strengthen the regulatory regime for managed investment schemes in the context of the possibility of higher standards of risk management systems for them as envisaged by the St John inquiry into compensation for consumers of financial services: see paragraph 3.68 in the Trio report.

B Proposed requirements for responsible entities

Key points

We propose to set more targeted requirements for the risk management systems of responsible entities that are not regulated by APRA.

The proposed requirements are fundamental risk management practices that can be applied according to the nature, scale and complexity of the responsible entity and scheme(s).

Subject to the passage of the Superannuation Bill, the proposed requirements would also apply to dual-regulated entities. This is because from the commencement date of the legislation, the obligation to have adequate risk management systems would apply to these entities, excluding risks that relate solely to the operation of the RSE.

Fundamental risk management practices

Proposal

B1 We propose to modify s912A(1)(h) of the Corporations Act by class order to include more targeted requirements for risk management systems of responsible entities: see Table 1 in the attached draft regulatory guide.

Note: The proposed requirements would only apply to responsible entities that are not regulated by APRA. However, subject to the passage of the Superannuation Bill, the proposed requirements and guidance will also apply to dual-regulated entities. From the commencement date of the legislation, the obligation to have adequate risk management systems for these entities will exclude risks that relate solely to the operation of the RSE.

Your feedback

B1Q1 Do you agree with our proposed regulatory approach of modifying s912A(1)(h) of the Corporations Act by class order? If not, why not?

B1Q2 To what extent do you already implement these requirements? Please specify which requirements.

B1Q3 Are stronger, more prescriptive risk management requirements (beyond those proposed) necessary for the managed funds sector and should they be introduced through law reform? If so, please specify the issues that the more prescriptive requirements should address.

B1Q4 Would the proposed requirements be better positioned as good practice guidance? If so, please explain why (including how the good practice guidance can improve risk management standards for responsible entities and why you consider that such good practice guidance will be adopted by the industry) and provide detailed suggestions on how we can encourage the adoption of fundamental risk management practices across the managed funds sector.

B1Q5 Entities that operate managed investment schemes that are not required to be registered under the Corporations Act may also choose to meet these requirements, although we do not propose to make them mandatory for these types of schemes. Should the requirements also apply to unregistered managed investment schemes? If so, why?

B1Q6 Our regulatory experience indicates that most of the proposed requirements are already part of the existing risk management systems of many responsible entities. Therefore, we do not expect prospective compliance costs across all responsible entities to be unreasonably burdensome or prohibitive. Do you agree? If not, please explain why, quantifying costs wherever possible.

B1Q7 What are the potential costs or impacts of this proposal on the managed funds sector? Please quantify where possible.

B1Q8 We consider that responsible entities are well placed to identify those risks that are 'material' to the operation of their businesses, given their diverse nature, scale and complexity. Do you agree? If not, should we provide guidance on what amounts to 'material risks'?

B1Q9 Are there any other requirements that would help responsible entities better manage the risks that face their businesses in operating schemes? If so, what are they and why would they be helpful?

B1Q10 APRA-regulated RSEs must submit to APRA a signed declaration on their risk management strategy. Should we include a similar requirement for responsible entities?

B1Q11 Should similar requirements and targeted guidance (see Sections C–D of this paper) be developed for other particular AFS licensees? If so, why? If not, why not?

Rationale

18 Our guidance in RG 104 recognises that risk management systems will depend on the nature, scale and complexity of the particular business of an AFS licensee and their risk profile. It also acknowledges that risk management systems should adapt as businesses develop and risk profiles change over time.

19 Our findings in REP 298 indicate that general compliance with risk management obligations is evident in the managed funds sector. However, while most responsible entities generally have adequate risk management systems in place, adapted to the nature, scale and complexity of their businesses, we observed that improvements could be made, especially for those responsible entities that are not part of an APRA-regulated group. The lack of industry-specific guidance on risk management does not help to improve risk management systems of responsible entities across the managed funds sector.

20 In addition, our review of selected responsible entities in 2011–12 and our broader regulatory experience highlight a range of risks that responsible entities should consider as part of their business of operating a scheme or schemes and the diverse practices used by responsible entities in managing these risks.

21 We think that the requirements in proposal B1 are consistent with our existing guidance in RG 104 and apply to the business of all responsible entities, regardless of the nature, scale or complexity of their operations, even though these requirements are more targeted, especially towards the types of risks material to a responsible entity's business. The proposed requirements are sufficiently flexible to allow each responsible entity to tailor the requirements to their individual business and strategic and business objectives.

22 Our review and broader regulatory experience suggest that most of the practices covered by the proposed requirements (e.g. documented processes) are already included in the existing risk management systems of most responsible entities, with varying degrees of sophistication. Given the fundamental nature of each of these practices in helping responsible entities to manage risk, we consider that it is important to require them for all responsible entities that are not APRA-regulated. In doing so, we expect these requirements will improve risk management standards across the managed funds sector as a whole.

23 We also consider that the absence of these practices in a responsible entity's risk management systems may indicate certain inadequacies that may warrant further regulatory action by ASIC.

C Proposed guidance on expectations

Key points

As AFS licensees, responsible entities must meet their risk management obligations—that is, to have adequate risk management systems, unless they are regulated by APRA (in which case they need to meet requirements for risk management set out in legislation and prudential standards).

While RG 104 provides limited general guidance to all AFS licensees, we propose to issue guidance stating our more targeted expectations for responsible entities on meeting these obligations, including the proposed class order requirements in proposal B1: see the draft regulatory guide attached to this paper.

These expectations cover:

- relying on key employees or external service providers;
- fostering a risk management culture;
- choosing processes for identifying and assessing risks;
- monitoring compliance with risk management systems;
- reviewing the effectiveness of risk management systems; and
- using stress testing or scenario analysis.

Subject to the passage of the Superannuation Bill, these expectations would also apply to dual-regulated entities. This is because, from the commencement date of the legislation, the obligation to have adequate risk management systems would apply to these entities, excluding risks that relate solely to the operation of the RSE.

Relying on key employees or external service providers

Proposal

C1 If responsible entities rely on key employees or external service providers to establish and monitor their risk management systems in meeting the risk management obligations, including the proposed class order requirements in proposal B1, we expect responsible entities to:

(a) maintain a strong understanding of risk management in the context of their business; and

(b) have sufficient skills to independently monitor and assess the performance of key persons or external service providers.

See draft RG 000.19.

Your feedback

C1Q1 Do you agree with our proposed expectations? If not, why not?

C1Q2 We consider that these expectations are consistent with our guidance in RG 104, so responsible entities should already have existing measures in place. To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible.

Rationale

24 One of the key findings discussed in REP 298 reflected an overreliance on specific individuals to perform risk management functions, or a high level of reliance on external compliance and risk management consultants to meet the risk management obligations. This was especially so in smaller responsible entities.

25 Given this finding, we consider it important to emphasise that AFS licensees remain responsible for compliance with s912A(1)(h) of the Corporations Act. This means that a licensee should maintain a strong understanding of risk management systems and practices, and have sufficient skills to independently monitor and assess the provision of services by key employees or external service providers, to ensure that there is adequate oversight.

26 While outsourcing is not prohibited, the outsourcing of the establishment and monitoring of risk management systems can raise regulatory concerns about the adequacy of risk management systems of a responsible entity and its ability to comply with its risk management obligations.

27 Where functions (including risk management) are outsourced, we expect that AFS licensees, including responsible entities:

(a) will have measures in place to ensure that due skill and care is taken in choosing suitable service providers;

(b) can and will monitor the ongoing performance of service providers; and

(c) will appropriately deal with any actions by service providers that breach service level agreements or their general obligations: see RG 104.36.

28 Consistent with this existing guidance, we expect responsible entities that outsource the functions of establishing and monitoring their risk management systems to be able to exercise effective and robust oversight of the outsourced functions and the performance of external service providers.

Fostering a risk management culture

Proposal

C2 In meeting the risk management obligations, we expect responsible entities to:

(a) foster a strong risk management culture throughout the organisation, including that risk management is well supported by everyone in the organisation;

(b) ensure all staff understand the purposes of risk management and its value; and

(c) require all staff members to report internally, breaches of risk management processes and procedures of which they are aware.

See draft RG 000.30–RG 000.34 and RG 000.37.

Your feedback

C2Q1 Do you agree with our proposed expectations? If not, why not?

C2Q2 We consider that these expectations are consistent with our guidance in RG 104, so responsible entities should already have existing measures in place. To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible.

C2Q3 Are there any specific elements of risk management culture that we should expand on? If so, please provide detailed suggestions.

Rationale

29 The risk management culture of a responsible entity fundamentally affects the effectiveness of its risk management systems. This is because the responsible entity's risk management culture directly impacts on how its staff will implement its systems. Generally, staff members are not directly involved in the establishment of risk management systems so they will require support to understand and apply it as part of their operational decision-making process. A strong risk management culture will encourage a responsible entity's staff to understand and comply with its risk management systems and obligations.

30 Risk management should be the responsibility of everyone in an organisation and not just staff who have specific risk management duties. All staff members may become aware of breaches of a responsible entity's risk management systems and should be encouraged and supported to provide this important feedback to responsible entities to improve compliance. All staff members should report non-compliance with an entity's risk management systems through internal escalation points identified by the responsible entity in its risk management systems.

Choosing processes for identifying and assessing risks

Proposal

C3 In meeting the risk management obligations, including the proposed class order requirements to have processes in place to identify and assess risks, we expect responsible entities to:

(a) maintain a risk register as part of their risk identification process; and

(b) take into account the factors set out in draft RG 000.52 and RG 000.60 when choosing processes for identifying and assessing risks.

See draft RG 000.51–RG 000.52 and RG 000.60.

Your feedback

C3Q1 Do you agree with our proposed expectations? If not, why not?

C3Q2 To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible.

C3Q3 Is it appropriate to expect responsible entities to take into account the factors in draft RG 000.52 and RG 000.60 when choosing processes for identifying and assessing risks? If not, why not?

C3Q4 Should any other factors be included? If so, please state the relevant factors and why they should be included.

Rationale

31 We consider it is essential for responsible entities to keep proper records of risks identified, while choosing a format for the risk register that is most suitable to them and appropriate for their business operations.

32 Given the diverse nature, scale and complexity of responsible entities' operations, we do not consider it practical or possible to prescribe what risk identification and assessment methods should be used. Instead, we expect responsible entities to have regard to a range of factors when considering which approach or combination of approaches to adopt for identifying and assessing risks.

33 We consider the proposed list of factors to be the minimum factors that responsible entities should have regard to when ensuring the approach or combination of approaches they adopt for identifying and assessing risks is suitable for their business operations and objectives.

34 We also think it is important for the board to be involved in the risk assessment process. This is because the process of assessing the likelihood of risks eventuating and their potential impact is directly connected to determining whether an identified risk is at an acceptable level in light of the responsible entity's statement or policy on risk appetite and, therefore, whether it will need to be treated.

Monitoring compliance with risk management systems

Proposal

C4 In meeting the risk management obligations, including the proposed class order requirements for monitoring compliance, we expect responsible entities to ensure there are:

(a) effective information systems and appropriate record keeping policies about risk management systems;

(b) appropriate policies for reporting on risk management activities, including that persons who have ownership of risks within the structure of the risk management systems (risk owners) must report regularly and on an exception basis; and

(c) clear escalation policies, processes and procedures for exception reporting on breaches of the risk management systems.

See draft RG 000.70–RG 000.77.

Your feedback

C4Q1 Do you agree with our proposed expectations? If not, why not?

C4Q2 We consider that these expectations are consistent with our guidance in RG 104, so responsible entities should already have existing measures in place. To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible.

Rationale

35 Effective information systems and appropriate record keeping policies can help capture relevant information to manage risk. They can ensure that staff members responsible for particular risk management functions keep a record of their activities in accordance with risk management systems.

36 Reporting on risk management activities is essential for monitoring compliance and these reports can draw on the information captured by the responsible entity's information systems. Reporting policies ensure that the records and/or reports are provided to the responsible entity and are escalated as appropriate on an exception basis (including to any relevant compliance or risk management function). The responsible entities can then review these records and/or reports to determine whether the risk management systems have been implemented as intended and relevant policies, processes and procedures complied with.

37 We envisage that what is appropriate for any given responsible entity will depend on the size, nature and complexity of its business and operations.

Reviewing the effectiveness of risk management systems

Proposal

C5 In complying with the risk management obligations, including the proposed class order requirement to review risk management systems, we expect responsible entities to carry out such reviews when there have been material changes to the context in which they operate their risk management systems.

See draft RG 000.79–RG 000.80.

Your feedback

C5Q1 Do you agree with our proposed expectations? If not, why not?

C5Q2 We consider that these expectations are consistent with our guidance in RG 104, so responsible entities should already have existing measures in place. To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible.

C5Q3 Are there any other circumstances that should trigger a review of risk management systems? If so, what are these circumstances? Please provide details.

Rationale

38 In developing risk management systems, we expect responsible entities to set out the context in which they operate their business, including the relevant internal and external environments. This is because risk management systems take effect in the context of an organisation striving to achieve its strategic and business objectives in the environment in which it operates.

39 Most of the responsible entities we reviewed indicated that their risk management systems did not change as a result of the global financial crisis: see REP 298.

40 We consider that, if material changes occur in the context in which a responsible entity operates its risk management systems (e.g. severe market disruptions), it should review these systems to ensure they remain current, relevant, effective and appropriate for the business.

Using stress testing or scenario analysis

Proposal

C6 We expect responsible entities to:

(a) conduct stress testing and/or scenario analysis of investment risk and liquidity risk of their business and the schemes they operate as part of their risk management systems;

(b) review their framework for stress testing or scenario analysis at appropriate intervals to ensure the nature, currency and severity of the tested scenarios are relevant and appropriate in light of the responsible entity's business and market conditions; and

(c) if they do not adopt these practices, document why this is the case, keep appropriate internal records of this rationale, and review this decision at appropriate intervals.

See draft RG 000.82–RG 000.87.

Your feedback

C6Q1 Do you agree with our proposed expectations? If not, why not?

C6Q2 To what extent do you currently use stress testing and/or scenario analysis in identifying, assessing and treating liquidity risk and investment risk? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible.

Rationale

41 Our findings in REP 298 indicated that little or no stress testing and/or scenario analysis is undertaken by responsible entities. Nonetheless, we consider it important in identifying, assessing and treating investment risk and liquidity risk. This is because stress testing and/or scenario analysis can allow responsible entities to assess how they will be affected if stressed circumstances emerge 'before the fact'. Responsible entities can then ensure that the measures they have in place to identify, assess and treat investment risk and liquidity risk are appropriate and adequate for addressing stressed circumstances if they arise.

42 Our proposed guidance on stress testing and/or scenario analysis is also consistent with IOSCO's guidance on liquidity risk management as published on 4 March 2013: see FR 03/13 *Principles of liquidity risk management for collective investment schemes*, Final report, Report of the Board of IOSCO, March 2013, available at www.iosco.org.

D Proposed good practice guidance

Key points

We propose to provide good practice guidance on measures responsible entities can adopt in:

- establishing and maintaining risk management systems, including the use of internal and/or external audit to review systems; and
- assessing and managing particular risks by having a written plan for treating risks, which can be implemented through written policies and procedures.

Establishing and maintaining risk management systems

Proposal

D1 We propose to provide guidance that in establishing and maintaining risk management systems, it is good practice for responsible entities to:

(a) separate the responsibility for risk assessment, risk treatment and monitoring compliance with risk management systems to manage conflicts of interest;

(b) establish a designated risk management function and/or risk management committee to ensure that their day-to-day operation is conducted in a way that aligns with their risk management systems (this does not have to be an exclusive function); and

(c) use internal and/or external audits to review compliance with, and the effectiveness of, their risk management systems.

See draft RG 000.36, RG 000.40–RG 000.44, RG 000.81 (and RG 000.20).

Your feedback

D1Q1 Do you agree with our proposed good practice guidance? If not, why not?

D1Q2 Are there any other good practice measures that would help responsible entities in establishing and maintaining risk management systems? Please provide specific details.

D1Q3 To what extent do you currently adopt the proposed good practice measures? Please provide details.

D1Q4 Should the proposed good practice measures be mandated requirements? If so, please explain your reasons and quantify costs of implementation (or additional costs if you already adopt these measures) where possible.

Rationale

43 We consider that the measures in proposal D1 will help responsible entities to establish and maintain their risk management systems. These measures reflect current good practice in the industry to manage conflicts of interest and ensure appropriate oversight of these systems.

44 Regular review and monitoring is a core process through which a responsible entity can ensure the adequacy of its risk management systems. Using internal and/or external audits as part of this process provides independent assurance of the responsible entity's compliance with its risk management systems. It also provides an objective assessment of their effectiveness.

45 We consider such audits can be important in identifying whether:

(a) risk management processes have been followed;

(b) risk identification and assessment processes and procedures that are in place are effective and implemented;

(c) treatment measures and controls to address material risks are in place and effective; and

(d) risk management systems are reviewed regularly with any weaknesses identified for ongoing improvement.

46 We consider that responsible entities are best placed to identify whether these good practice measures are appropriate for their businesses. We expect that industry practice may differ significantly given the significant variance in nature, scale and complexity of responsible entities across the managed funds sector.

47 For example, internal audit may not be adopted in some smaller responsible entities. As such, we do not think it is appropriate to introduce these good practice measures as mandatory requirements at this stage.

Assessing and managing risks

Proposal

D2 We propose to provide guidance that in managing risks, it is good practice for responsible entities to have a written plan for treating risks, which can be implemented through written policies and procedures.

See draft RG 000.64–RG 000.65.

Your feedback

D2Q1 Do you agree with our proposed good practice guidance? If not, please explain why.

D2Q2 Are there any other good practice measures that would help responsible entities to manage risks on an ongoing basis? Please provide specific details.

D2Q3 To what extent do you currently adopt the proposed good practice measures? Please provide details.

D2Q4 Should these good practice measures be mandated requirements? If so, please explain your reasons and quantify costs of implementation (or additional costs if you already adopt these measures) where possible.

Rationale

48 We consider it is good practice for responsible entities to have a written risk treatment plan setting out how each material risk will be treated. We think such a plan informs operational decisions that are made where those risks arise, while providing clarity across all levels of the business about how risks are addressed generally.

E Regulatory and financial impact

49 In developing the proposals in this paper, we have carefully considered their regulatory and financial impact. On the information currently available to us we think they will strike an appropriate balance between:

(a) building retail investor and financial consumer confidence by mitigating exposure to relevant risks that responsible entities and their schemes confront; and

(b) building confidence in the integrity of Australia's capital markets by better safeguarding the financial services industry from systemic risk.

50 Before settling on a final policy, we will comply with the Australian Government's regulatory impact analysis (RIA) requirements by:

(a) considering all feasible options, including examining the likely impacts of the range of alternative options which could meet our policy objectives;

(b) if regulatory options are under consideration, notifying the Office of Best Practice Regulation (OBPR); and

(c) if our proposed option has more than minor or machinery impact on business or the not-for-profit sector, preparing a Regulation Impact Statement (RIS).

51 All RISs are submitted to the OBPR for approval before we make any final decision. Without an approved RIS, ASIC is unable to give relief or make any other form of regulation, including issuing a regulatory guide that contains regulation.

52 To ensure that we are in a position to properly complete any required RIS, please give us as much information as you can about our proposals or any alternative approaches, including:

(a) the likely compliance costs;

(b) the likely effect on competition; and

(c) other impacts, costs and benefits.

See 'The consultation process', p. 4.

List of proposals and questions

Proposal	Your feedback
B1 We propose to modify s912A(1)(h) of the Corporations Act by class order to include more targeted requirements for risk management systems of responsible entities: see Table 1 in the attached draft regulatory guide. Note: The proposed requirements would only apply to responsible entities that are not regulated by APRA. However, subject to the passage of the Superannuation Bill, the proposed requirements and guidance will also apply to dual-regulated entities. From the commencement date of the legislation, the obligation to have adequate risk management systems for these entities will exclude risks that relate solely to the operation of the RSE.	B1Q1 Do you agree with our proposed regulatory approach of modifying s912A(1)(h) of the Corporations Act by class order? If not, why not? B1Q2 To what extent do you already implement these requirements? Please specify which requirements. B1Q3 Are stronger, more prescriptive risk management requirements (beyond those proposed) necessary for the managed funds sector and should they be introduced through law reform? If so, please specify the issues that the more prescriptive requirements should address. B1Q4 Would the proposed requirements be better positioned as good practice guidance? If so, please explain why (including how the good practice guidance can improve risk management standards for responsible entities and why you consider that such good practice guidance will be adopted by the industry) and provide detailed suggestions on how we can encourage the adoption of fundamental risk management practices across the managed funds sector. B1Q5 Entities that operate managed investment schemes that are not required to be registered under the Corporations Act may also choose to meet these requirements, although we do not propose to make them mandatory for these types of schemes. Should the requirements also apply to unregistered managed investment schemes? If so, why? B1Q6 Our regulatory experience indicates that most of the proposed requirements are already part of the existing risk management systems of many responsible entities. Therefore, we do not expect prospective compliance costs across all responsible entities to be unreasonably burdensome or prohibitive. Do you agree? If not, please explain why, quantifying costs wherever possible. B1Q7 What are the potential costs or impacts of this proposal on the managed funds sector? Please quantify where possible. B1Q8 We consider that responsible entities are well placed to identify those risks that are ‘material’

Proposal	Your feedback
	to the operation of their businesses, given their diverse nature, scale and complexity. Do you agree? If not, should we provide guidance on what amounts to 'material risks'? B1Q9 Are there any other requirements that would help responsible entities better manage the risks that face their businesses in operating schemes? If so, what are they and why would they be helpful? B1Q10 APRA-regulated RSEs must submit to APRA a signed declaration on their risk management strategy. Should we include a similar requirement for responsible entities? B1Q11 Should similar requirements and targeted guidance (see Sections C–D of this paper) be developed for other particular AFS licensees? If so, why? If not, why not?
C1 If responsible entities rely on key employees or external service providers to establish and monitor their risk management systems in meeting the risk management obligations, including the proposed class order requirements in proposal B1, we expect responsible entities to: (a) maintain a strong understanding of risk management in the context of their business; and (b) have sufficient skills to independently monitor and assess the performance of key persons or external service providers. See draft RG 000.19.	C1Q1 Do you agree with our proposed expectations? If not, why not? C1Q2 We consider that these expectations are consistent with our guidance in RG 104, so responsible entities should already have existing measures in place. To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible.
C2 In meeting the risk management obligations, we expect responsible entities to: (a) foster a strong risk management culture throughout the organisation, including that risk management is well supported by everyone in the organisation; (b) ensure all staff understand the purposes of risk management and its value; and (c) require all staff members to report internally, breaches of risk management processes and procedures of which they are aware. See draft RG 000.30–RG 000.34 and RG 000.37.	C2Q1 Do you agree with our proposed expectations? If not, why not? C2Q2 We consider that these expectations are consistent with our guidance in RG 104, so responsible entities should already have existing measures in place. To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible. C2Q3 Are there any specific elements of risk management culture that we should expand on? If so, please provide detailed suggestions.

Proposal	Your feedback
C3 In meeting the risk management obligations, including the proposed class order requirements to have processes in place to identify and assess risks, we expect responsible entities to: (a) maintain a risk register as part of their risk identification process; and (b) take into account the factors set out in draft RG 000.52 and RG 000.60 when choosing processes for identifying and assessing risks. See draft RG 000.51–RG 000.52 and RG 000.60.	C3Q1 Do you agree with our proposed expectations? If not, why not? C3Q2 To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible. C3Q3 Is it appropriate to expect responsible entities to take into account the factors in draft RG 000.52 and RG 000.60 when choosing processes for identifying and assessing risks? If not, why not? C3Q4 Should any other factors be included? If so, please state the relevant factors and why they should be included.
C4 In meeting the risk management obligations, including the proposed class order requirements for monitoring compliance, we expect responsible entities to ensure there are: (a) effective information systems and appropriate record keeping policies about risk management systems; (b) appropriate policies for reporting on risk management activities, including that persons who have ownership of risks within the structure of the risk management systems (risk owners) must report regularly and on an exception basis; and (c) clear escalation policies, processes and procedures for exception reporting on breaches of the risk management systems. See draft RG 000.70–RG 000.77.	C4Q1 Do you agree with our proposed expectations? If not, why not? C4Q2 We consider that these expectations are consistent with our guidance in RG 104, so responsible entities should already have existing measures in place. To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible.
C5 In complying with the risk management obligations, including the proposed class order requirement to review risk management systems, we expect responsible entities to carry out such reviews when there have been material changes to the context in which they operate their risk management systems. See draft RG 000.79–RG 000.80.	C5Q1 Do you agree with our proposed expectations? If not, why not? C5Q2 We consider that these expectations are consistent with our guidance in RG 104, so responsible entities should already have existing measures in place. To what extent do you already meet these expectations? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible. C5Q3 Are there any other circumstances that should trigger a review of risk management systems? If so, what are these circumstances? Please provide details.

Proposal	Your feedback
C6 We expect responsible entities to: (a) conduct stress testing and/or scenario analysis of investment risk and liquidity risk of their business and the schemes they operate as part of their risk management systems; (b) review their framework for stress testing or scenario analysis at appropriate intervals to ensure the nature, currency and severity of the tested scenarios are relevant and appropriate in light of the responsible entity's business and market conditions; and (c) if they do not adopt these practices, document why this is the case, keep appropriate internal records of this rationale, and review this decision at appropriate intervals. See draft RG 000.82–RG 000.87.	C6Q1 Do you agree with our proposed expectations? If not, why not? C6Q2 To what extent do you currently use stress testing and/or scenario analysis in identifying, assessing and treating liquidity risk and investment risk? Please provide details. If you consider that meeting these expectations would involve additional costs, please identify them and quantify where possible.
D1 We propose to provide guidance that in establishing and maintaining risk management systems, it is good practice for responsible entities to: (a) separate the responsibility for risk assessment, risk treatment and monitoring compliance with risk management systems to manage conflicts of interest; (b) establish a designated risk management function and/or risk management committee to ensure that their day-to-day operation is conducted in a way that aligns with their risk management systems (this does not have to be an exclusive function); and (c) use internal and/or external audits to review compliance with, and the effectiveness of, their risk management systems. See draft RG 000.36, RG 000.40–RG 000.44, RG 000.81 (and RG 000.20).	D1Q1 Do you agree with our proposed good practice guidance? If not, why not? D1Q2 Are there any other good practice measures that would help responsible entities in establishing and maintaining risk management systems? Please provide specific details. D1Q3 To what extent do you currently adopt the proposed good practice measures? Please provide details. D1Q4 Should the proposed good practice measures be mandated requirements? If so, please explain your reasons and quantify costs of implementation (or additional costs if you already adopt these measures) where possible.

Proposal	Your feedback
D2 We propose to provide guidance that in managing risks, it is good practice for responsible entities to have a written plan for treating risks, which can be implemented through written policies and procedures. See draft RG 000.64–RG 000.65.	D2Q1 Do you agree with our proposed good practice guidance? If not, please explain why. D2Q2 Are there any other good practice measures that would help responsible entities to manage risks on an ongoing basis? Please provide specific details. D2Q3 To what extent do you currently adopt the proposed good practice measures? Please provide details. D2Q4 Should these good practice measures be mandated requirements? If so, please explain your reasons and quantify costs of implementation (or additional costs if you already adopt these measures) where possible.

ASIC
Australian Securities & Investments Commission

REGULATORY GUIDE 000

Risk management systems of responsible entities

March 2013

About this guide

This guide is for Australian financial services (AFS) licensees that are responsible entities and that are not regulated by the Australian Prudential Regulation Authority (APRA).

It gives specific guidance on how these entities may comply with their obligation under s912A(1)(h) of the *Corporations Act 2001* (Corporations Act) to maintain adequate risk management systems.

> Note: Subject to the passage of the Superannuation Legislation Amendment (Service Providers and other Governance Measures) Bill 2012 (Superannuation Bill), from [date of commencement], this guide will also apply to APRA-regulated registrable superannuation entity licensees (RSEs) that manage non-superannuation registered managed investment schemes (dual-regulated entities). For these entities, the obligation to have adequate risk management systems will exclude risks that relate solely to the operation of the RSE.

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents.

Consultation papers: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

Regulatory guides: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

Information sheets: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

Reports: describe ASIC compliance or relief activity or the results of a research project.

Document history

This draft version was issued in March 2013 and is based on legislation and regulations as at the date of issue.

Disclaimer

This guide does not constitute legal advice. We encourage you to seek your own professional advice to find out how the Corporations Act and other applicable laws apply to you, as it is your responsibility to determine your obligations.

Examples in this guide are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

Contents

A Overview

Key points

As AFS licensees, responsible entities are legally obliged to have adequate risk management systems, unless they are regulated by APRA. These systems are fundamental for mitigating exposure to relevant risks and informing business decision-making.

This guide gives guidance on how responsible entities may comply with this obligation, including:

- establishing and maintaining a risk management system that is suitable for its business (see Section B);
- identifying and assessing risks (see Section C); and
- managing risks (see Section D).

The obligation in s912A(1)(h)

RG 000.1 Under s912A(1)(h) of the *Corporations Act 2001* (Corporations Act), responsible entities that are Australian financial services (AFS) licensees have an ongoing obligation to maintain adequate risk management systems, unless they are regulated by the Australian Prudential Regulation Authority (APRA).

Note: Subject to the passage of the Superannuation Bill, this obligation will also apply to dual-regulated entities: see RG 000.13

RG 000.2 In Regulatory Guide 104 *Licensing: Meeting the general obligations* (RG 104), we set out our expectation that an adequate risk management system for these entities would:

(a) include a structured and systematic process for identifying, assessing and managing risks faced by the business; and

(b) address risks related to both the responsible entity itself and the registered managed investment schemes (schemes) it operates.

RG 000.3 In 2011–12, we reviewed the risk management systems of a selected group of responsible entities ranging in size and complexity to assess their adequacy and strategic and operational effectiveness: see Report 298 *Adequacy of risk management systems of responsible entities* (REP 298).

RG 000.4 We found that the sophistication of risk management systems varied significantly, reflecting the nature, scale and complexity of different responsible entities and their financial services businesses. Generally, we also found that responsible entities that are part of a group regulated by APRA adopted more sophisticated risk management systems than those that are not.

RG 000.5 This guide draws on the findings of our review in providing guidance in specific areas to improve the risk management systems of responsible entities that are not regulated by APRA.

Risk management systems

RG 000.6 Risks are generally described in terms of a combination of the consequences of an event occurring and its likelihood of occurring.

RG 000.7 The international standard for risk management defines risk as 'the chance of something happening that will have an impact on objectives' and risk management as 'the culture, processes and structures that are directed towards realising potential opportunities whilst managing an adverse effect': see International Organization for Standardization ISO 31000:2009 *Risk management: Principles and guidelines*.

RG 000.8 An effective risk management system:

(a) allows for early identification of material risks and assessment of these risks against consistent criteria;

(b) includes cost-effective and efficient ways to reduce risks to acceptable levels;

(c) monitors and manages risks to ensure exposure to the risks is within acceptable levels; and

(d) informs strategic and operational business decisions accordingly with adequate information about risks.

RG 000.9 From [date], AFS licensees that are responsible entities must comply with the requirements for risk management systems in Class Order [CO 13/xxx] *Risk management systems of responsible entities*, unless they are regulated by APRA.

> Note: Subject to the passage of the Superannuation Bill, this requirement will also apply to dual-regulated entities: see RG 000.13

RG 000.10 This guide gives guidance on our expectations of responsible entities in complying with the obligation in s912A(1)(h), including the requirements set out in [CO 13/xxx]. We also include examples of good practice, which we encourage responsible entities to consider when establishing and maintaining their risk management systems.

RG 000.11 Table 1 summarises the requirements, expectations and good practice guidance outlined in this guide. In the appendix to this guide, we give examples of risks and risk treatments that we consider are particularly relevant to responsible entities based on our regulatory experience.

Table 1: Summary of requirements and guidance

	Requirements in [CO 13/xxx]	Expectations for compliance with s912A(1)(h) including [CO 13/xxx]	Good practice guidance
Risk management systems (see Section B)	A responsible entity must: • ensure its risk management systems comprise processes to identify, assess and treat risks; • ensure these processes are suitable for its business' objectives and operations; • review its risk management systems (including the policy or statement on its risk appetite) regularly, but no less than annually, for currency, appropriateness, effectiveness and relevance to the business; • set out in writing: – the context in which the risk management systems are developed; – a policy or statement on its risk appetite; – the risk tolerance for each material risk identified; and – the structure for implementing its risk management systems, including the roles of particular staff responsible for implementation.	If they rely on key employees or external service providers to establish and monitor risk management systems, we expect responsible entities to maintain a strong understanding of risk management and have sufficient skills to independently monitor and assess their performance. We also expect responsible entities to: • foster a strong risk management culture throughout the organisation; • ensure staff understand the purposes of risk management and its value, and that in particular a strong risk management culture, is well supported by everyone in the organisation; and • require staff to report internally breaches of risk management processes and procedures.	Responsible entities should: • separate the responsibility for risk assessment, risk management and compliance with risk management systems to avoid conflicts of interest; and • establish a designated risk management function and/or risk management committee.
Identifying and assessing risks (see Section C)	A responsible entity must: • document the processes used to identify and assess risks; and • ensure that its risk management systems address all material risks, including (but not limited to) the following risks: – strategic risk; – governance risk; – operational risk; – investment risk; and – liquidity risk.	We expect responsible entities to: • keep a risk register as part of their risk identification process; and • take into account certain factors when choosing processes for identifying and assessing risks (see RG 000.50 and RG 000.60).	

	Requirements in [CO 13/xxx]	Expectations for compliance with s912A(1)(h) including [CO 13/xxx]	Good practice guidance
Managing risks (see Section D)	A responsible entity must: • determine appropriate treatment for each identified risk; • document how each risk will be treated; • ensure that the board monitors residual risks to determine whether further treatment is required; • ensure that staff members follow the processes and controls put in place to manage risks; • monitor compliance with the risk management systems and document the processes used to do so; and • regularly review the risk management systems for currency, relevance, effectiveness and appropriateness and document the processes used to do so.	We expect responsible entities to: • conduct stress testing and/or scenario analysis of investment risk and liquidity risk of their business and the schemes they operate as part of their risk management systems; and • review their framework for stress testing and/or scenario analysis at appropriate intervals to ensure the nature, currency and severity of the tested scenarios are relevant and appropriate in light of the business and market conditions. If a responsible entity decides not to conduct stress testing and/or scenario analysis, we expect it to document why this is the case, keep appropriate internal records of this rationale, and review this decision at appropriate intervals. We expect responsible entities to: • maintain: – effective information systems and appropriate record keeping policies about risk management systems; – appropriate policies for reporting on risk management activities, especially that persons who have ownership of risks within the structure of the risk management systems (risk owners) must report regularly and on an exception basis; and – clear escalation policies, processes and procedures for exception reporting; and • review risk management systems where material changes in the risk management context have occurred.	Responsible entities should: • have a written risk treatment plan; and • use internal and/or external audit to review compliance with, and the effectiveness of, their risk management systems.

How this guide applies

RG 000.12 The guide is for AFS licensees that are responsible entities. While RG 104 gives guidance on risk management systems for AFS licensees generally, this guide focuses specifically on the business of responsible entities, the scheme(s) they operate and the particular risks they face.

RG 000.13 This guide focuses on risk management systems for responsible entities that are not regulated by APRA. Bodies regulated by APRA need to meet risk management systems as set out in various legislation and prudential standards.

> Note 1: The Superannuation Bill proposes to amend the Corporations Act so that dual-regulated entities will need to comply with the obligation in s912A(1)(h) to have adequate risk management systems. Subject to passage of this legislation, from [date of commencement], this guide will apply to these entities (in addition to requirements under the *Superannuation Industry (Supervision) Act 1993*). However, the obligation to have adequate risk management systems will exclude risks that relate solely to the operation of the RSE.
>
> Note 2: APRA has issued Prudential Standard SPS 220 *Risk Management* to assist RSEs in developing their risk management systems (www.apra.gov.au).

RG 000.14 The examples of risks in this guide are not intended to be exhaustive. We expect that, through the application of a structured and systematic process, responsible entities will identify, assess and manage risks in an ongoing and dynamic way and in the appropriate context for their own business and scheme(s).

RG 000.15 This guide may not be relevant to entities operating unregistered managed investment schemes in its entirety. However, operators of such schemes may consider our guidance in establishing and maintaining their risk management systems.

B Risk management systems

Key points

A responsible entity must ensure its risk management systems are suitable for its business. This includes:

- setting out in writing the context in which its risk management systems are developed, a policy or statement on its risk appetite, and the risk tolerance for each material risk identified and the structure for implementing its risk management systems; and
- reviewing its risk management systems (including the policy or statement on its risk appetite) regularly, but not less than annually, to ensure they continue to be current, relevant, effective and appropriate to its business.

We also expect responsible entities to:

- maintain a strong understanding of risk management and have sufficient skills to independently monitor and assess the performance of key employees or external service providers if relying on them to establish and monitor the risk management systems;
- foster a strong risk management culture throughout the organisation, including an environment in which risk management is supported by all staff;
- ensure staff members understand the purposes of risk management and its value; and
- require all staff to report internally breaches of risk management processes and procedures.

Depending on the nature, scale and complexity of the business, as a matter of good practice, responsible entities should consider:

- separating the responsibilities for risk assessment, risk management and compliance with risk management systems to manage conflicts of interest; and
- establishing a designated risk management function and/or risk management committee as part of their risk management systems.

Components of a risk management system

RG 000.16 An adequate risk management system enables material risks faced by the business of the responsible entity to be identified, analysed and treated in a comprehensive and systematic manner.

RG 000.17 What is an adequate risk management system for any individual responsible entity depends on the nature, scale and complexity of its business and operations.

RG 000.18 However, we consider the following to be core processes that are essential to an adequate risk management system in any responsible entity's business:

(a) setting out the context in which risk management systems operate, including a policy or statement on the responsible entity's risk appetite (see RG 000.22–RG 000.29);

(b) identifying and assessing risks (see Section C); and

(c) managing risks, including reviewing and monitoring the risk management systems (see Section D).

RG 000.19 A responsible entity must develop these processes to suit the operation of its business. If it relies on key employees or external third party service providers (e.g. compliance and risk management consultants) to establish and monitor its risk management systems, we expect it to maintain a strong understanding of risk management in the context of the business, and have sufficient skills to independently monitor and assess their performance.

RG 000.20 A responsible entity must review its risk management systems regularly (no less than annually).

RG 000.21 We consider that the development of an adequate risk management system is not a 'set and forget' or 'one-off' process. The system should adapt and evolve to take into account internal changes within the responsible entity and scheme(s) it operates, as well as changes in the external environment. To this end, we consider that the responsible entity's board of directors (board) has a specific role in ensuring that risk management systems are current, relevant, effective and appropriate to the business on ongoing basis.

Setting risk management in context

RG 000.22 A responsible entity must consider and document the context in which its risk management system is developed—that is, the internal and external environment in which its business operates, including the objectives of the business. This is because risk management occurs in the context of an organisation striving to achieve its goals and objectives based on its strategic and business plans, and the environment in which it operates.

RG 000.23 An adequate risk management system requires a thorough understanding of the internal and external factors that could affect the responsible entity's ability to achieve its goal and objectives. Table 2 lists some examples of internal and external factors that may affect a responsible entity's business.

Table 2: Examples of internal and external factors

Internal factors	External factors
• Goals and objectives in the strategic and business plans, including the objectives of the relevant scheme(s) (e.g. whether a scheme will be a liquid scheme offering redemptions on demand, or an illiquid scheme). Particular business strategies may create specific risks affecting the business • Capabilities of the organisation (e.g. financial, human and technological resources) • Information flow and decision-making processes • Culture of the responsible entity	• Business, financial, competitive, political, economic, social, cultural, technological and environmental factors the business faces • Expectations of external stakeholders (including shareholders) about the operation of the business • Legal and regulatory changes that affect the operation of the business • New product offerings in the market that compel a responsible entity to compete more effectively

Policy or statement on risk appetite

RG 000.24 A responsible entity must set out in writing its risk appetite. This is a representation of the responsible entity's attitude towards risk taking in carrying out its business plans, including the level of risk (or losses) it is willing to take to pursue its business strategies and achieve its objectives.

RG 000.25 The articulation of risk appetite is a key step in setting the context in which risk management take places in the responsible entity's business, taking into account internal and external factors. The responsible entity may have one such policy or statement setting out its risk appetite in aggregate, or separate policies (e.g. for each business unit).

RG 000.26 A risk appetite policy or statement may be expressed in the form of qualitative and/or quantitative levels of acceptance of different types of risk or risk tolerance.

RG 000.27 A responsible entity must also set out in writing the risk tolerance for each material risk identified.

RG 000.28 A responsible entity must ensure its risk appetite is reviewed at appropriate intervals, but no less than annually, by the board to take into account changes in the internal and external context in which the business operates, including changes to the objectives and strategic direction of the business.

RG 000.29 Depending on the nature, scale and complexity of the business, responsible entities can adopt the following type of approach in setting and applying a policy or statement on risk appetite:

(a) The board sets the policy or statement on risk appetite for the business.

(b) Based on this statement, risk tolerance is set and documented for each material risk, which is broken down into clearly defined limits or thresholds for particular activities of the business to support the decision-making process.

(c) Risk management processes and procedures to implement and monitor the limits and thresholds are developed and communicated to staff at all levels so that they are applied to support day-to-day operational decision-making.

Culture and structure

Risk management culture

RG 000.30 We expect responsible entities to foster a strong risk management culture throughout their organisations because the effectiveness of an adequate risk management system depends on the organisation as a whole understanding the value of managing risks effectively and acting accordingly.

RG 000.31 We expect responsible entities to ensure that staff at all levels understand the purposes of risk management (including ensuring legal and regulatory compliance), as well as its value to the organisation.

RG 000.32 The board has specific responsibility to ensure that a responsible entity as an AFS licensee complies with its obligation to have an adequate risk management system. This means that the board's commitment to fostering a strong risk management culture within the organisation is especially important as the board is in a position to provide leadership.

RG 000.33 For example, the board can ensure that:

(a) communications with staff are focused on managing risks to achieve strategic business objectives;

(b) sufficient resources are provided for all risk management functions;

(c) staff receive ongoing training about risk management to assist them to identify risks and understand how they can be managed;

(d) the organisation's reward and remuneration structure is aligned with and supportive of the responsible entity's risk management systems; and

(e) breaches of any risk management procedures by staff are discouraged through adequate consequence management.

Structure and risk ownership

RG 000.34 We expect responsible entities to foster an environment in which risk management is supported by everyone in the organisation because the system will only be most effective if applied and adhered to in day-to-day decision-making at all levels.

RG 000.35 A responsible entity must set out in writing the structure for implementing its risk management systems, including the roles of particular staff responsible for implementation. The roles of persons responsible for specific risk management activities, if performed by different persons, should be set out in clear terms.

RG 000.36 Depending on the size, nature and complexity of the business, as a matter of good practice, responsibility for assessing and managing risks and monitoring the performance of the risk management functions should be separated so that the same personnel are not assigned to conflicting duties.

RG 000.37 We expect responsible entities' risk management systems to require all staff to report internally to identified escalation points (e.g. the risk management committee, the designated risk management function or the board) breaches of risk management processes and procedures (e.g. exceeding the risk tolerance for particular risk, or a failure to follow the relevant processes) of which they are aware. Such reporting allows information flow to assist decision-making in the organisation and improve risk management systems where systemic issues about their operation are identified.

RG 000.38 We appreciate that the structure of risk management systems varies between responsible entities, depending on the nature, scale and complexity of the business. Nonetheless, we have observed a number of risk management systems based on a 'three lines of defence' model. We encourage responsible entities to consider this approach in developing the structure of their risk management systems.

RG 000.39 The three lines of defence are as follows:

(a) *Management*—The first line of defence comprises controls designed to ensure ongoing compliance is embedded in all relevant decisions and operations.

(b) *Risk management*—The second line of defence follows the risk management controls, develops and implements policies, processes and procedures, monitors the business's compliance with risk management policies, processes and procedures, and ensures staff are well trained on risk management requirements.

(c) *Independent audit*—The third line of defence relies on independent internal and/or external audit and review of compliance with the risk management systems.

Designated risk management function and committee

RG 000.40 Depending on the nature, scale and complexity of the business, we think it is good practice for responsible entities to establish a designated risk management function and/or risk management committee as part of their risk management systems.

RG 000.41 A designated risk management function may not be exclusive and may also perform other roles of the responsible entity (e.g. a compliance role).

RG 000.42 The designated (but not necessarily exclusive) risk management function can have a hands-on role in ensuring the day-to-day operation of a responsible entity is conducted in a way that aligns with its risk management system. To achieve this, the designated risk management function should be

independent from the operating units of the responsible entity's business. It should also have the specific responsibility of monitoring compliance with risk management policies, processes and procedures and report to the board and any risk management committee all significant breaches of these policies, processes and procedures.

RG 000.43 The responsibilities of a risk management committee may generally include:

(a) assisting the board in developing the risk management system;

(b) implementation of the risk management system throughout the organisation;

(c) reviewing the effectiveness of the risk management system;

(d) reporting to the board on breaches of risk tolerance or risk management procedures according to the responsible entity's escalation policy; and

(e) reporting to the board about the risk management system and its effectiveness or otherwise.

RG 000.44 A responsible entity must set up a compliance committee unless half or more of its board are external directors: s601JA. We consider that the responsibilities of a risk management committee and a compliance committee may overlap (e.g. the compliance committee may have the responsibility of compliance with risk management policies, processes and procedures).

RG 000.45 We also expect the board to foster an environment in which the designated risk management function or risk management committee is supported by all staff in the organisation. This would include developing policies ensuring that:

(a) access is provided to all aspects of the responsible entity's business that may be subject to risks, including resourcing constraints (this includes providing adequate training to the designated risk management function and/or risk management committee to enhance understanding of the operation of different business units); and

(b) authority is provided to allow the designated risk management function and/or risk management committee to carry out their duties effectively.

C Identifying and assessing risks

Key points

A responsible entity must have documented processes for identifying and assessing risks, which are suitable for the business's objectives and operations.

It must ensure its risk management systems address all material risks, including (but not limited to) the following risks:

- strategic risk;
- governance risk;
- operational risk;
- investment risk; and
- liquidity risk.

We also expect responsible entities to keep a risk register as part of their risk identification process and to take into account certain factors when choosing processes for identifying and assessing risks.

Identifying risks

RG 000.46 Risk identification is the process used by responsible entities to identify and record risks that will affect their ability to pursue business strategies and achieve the objectives of their business.

RG 000.47 Responsible entities should adapt the processes for risk identification in their risk management systems as the business develops and business risk profiles change over time and in different market conditions. Risks need to be identified at any given point in time to ensure responsible entities can effectively manage them in the operation of their business and day-to-day decision making.

RG 000.48 There are different ways to identify the risks that can affect a responsible entity's business. For example, evidence-based methods that rely on reviewing audit reports, post-event reports, historical data or risk registers can help to identify existing and emerging risks that the responsible entity may face. Observations from our regulatory experience indicate that incorporating this approach to risk identification in strategic and business planning is particularly helpful in identifying risks. Responsible entities may use a systematic team approach that uses focus groups and brainstorming to identify risks. Purpose-built computer software can also be used.

RG 000.49 We do not consider that any one particular method for identifying risks is the most appropriate and applicable for all responsible entities.

RG 000.50 A responsible entity must document the processes and procedures it uses to identify risks.

RG 000.51 We expect responsible entities to maintain a risk register for recording material risks to the business as part of their risk identification process.

RG 000.52 When choosing a risk methodology or combination of methodologies for identifying risks, we also expect responsible entities to consider:

(a) the nature, scale and complexity of the business;

(b) processes based on a forward-looking analysis in accordance with strategic and business plans—for example, when assessing the risk of not having adequate technological or human resources, identification of risks should be based on forward planning;

(c) that there is an appropriate level of human input in the process—sole or disproportionate reliance on electronic systems to identify risks may not be adequate; and

(d) if applicable, whether different processes for identifying risks are appropriate for different schemes, given the operation of a particular scheme and the risks that are specific to it.

Risks relevant to the business

RG 000.53 We appreciate that the risks identified by responsible entities as part of their risk management systems will depend on the nature, scale and complexity of their business and risk profile, and will be different for each responsible entity: see RG 104.59.

RG 000.54 A responsible entity must ensure that its risk management systems address all the material risks faced by its business at both the responsible entity and scheme level, including (but not limited to) the following risks:

(a) *Strategic risk*—This is the risk of a responsible entity not being able to pursue its business strategies or meet its business objectives as a result of inappropriate business model or strategies.

(b) *Governance risk*— This is the risk of a responsible entity not having the appropriate decision-making processes in place to:

(i) support sound and transparent decision making that is not influenced by conflicts of interests, and

(ii) ensure that decisions related to the scheme(s) are in the best interest of members.

(c) *Operational risk*—This is the risk of interruption to the operation or internal processes of a responsible entity's business, including the scheme(s) it operates. Specific operational risks include those relating to legal and compliance requirements, technological resources, human resources (including key persons), outsourcing, transitioning of the business and fraud.

(d) *Investment risk*—This is the risk that a scheme operated by a responsible entity will not meet its objectives due to failure in the performance of the scheme's underlying investments. Specific investment risks include those relating to investment governance and structure, market conditions, counterparty failure, product suitability, and valuation and pricing.

(e) *Liquidity risk*—This is the risk that the responsible entity or the scheme(s) it operates will not have adequate financial resources to meet financial obligations as they fall due.

RG 000.55 For a detailed description of these risks, including examples of specific risks and treatments to manage these risks based on our regulatory experience, see the appendix to this guide.

Assessing risks

RG 000.56 Risk assessment is the process of describing identified risks, including by reference to the inherent risk, and understanding the consequences of the risks eventuating in terms of the likelihood of the risks eventuating and the potential impact of such an occurrence. This process should help a responsible entity in determining whether the identified risks are acceptable or not acceptable in light of its policy or statement on risk appetite as well as its risk management context and therefore assist it in developing the appropriate treatment for those risks.

RG 000.57 Examples of different methods that responsible entities may adopt for assessing risks include the following:

(a) *Self-assessment*—The responsible entity, its board and those in the designated risk management function (if applicable) assess risks through the business (as relevant).

(b) *Risk mapping*—Risks are prioritised according to where they fall in a four-quadrant map based on the significance and likelihood of a risk eventuating.

(c) *Electronic systems*—Purpose-built computer software can be used to assess risks.

(d) *External consultants*—Consultants can assist in the process of assessing the likelihood of a risk eventuating and the significance of its potential impact.

RG 000.58 We do not consider that any one particular approach will be the most appropriate and applicable to the operation of all responsible entities.

RG 000.59 A responsible entity must document its risk assessment processes. This should include the reasons why particular assessments are made, which can give a record of the thinking that led to the decisions about those identified risks and a useful context for future risk assessment.

RG 000.60 We expect that, when considering which approach or combination of approaches to adopt in assessing risks, responsible entities will consider:

(a) the nature, scale and complexity of the business;

(b) the need to ensure there is an appropriate level of human input in the process;

Note: We are unlikely to consider that sole or disproportionate reliance on electronic systems to assess risks is adequate. Our regulatory experience demonstrates that, generally, electronic systems monitor risks the business faces using system-generated questionnaires for relevant staff. Some of these systems appear to require 'box-ticking' or participation in rubber-stamping exercises that in our view is insufficient to demonstrate, on their own, the adequacy of a responsible entity's risk management system.

(c) board involvement in the process—for example, any determination about whether an identified risk is at an acceptable level in light of the policy or statement on risk appetite; and

(d) if applicable, whether different processes should be used to assess identified risks for different schemes in light of the operation of each particular scheme.

D Managing risks

Key points

A responsible entity must:

- determine the appropriate treatment for identified risks and document how each risk will be treated;
- ensure that residual risks are monitored by the board, which can then determine whether further treatment is required;
- monitor compliance with, and regularly review, its risk management systems and document the processes used to do so; and
- ensure staff members follow the processes and controls put in place to manage risks.

We expect responsible entities to:

- have policies in place that require risk owners to report on their risk management related duties;
- maintain effective information systems and appropriate record keeping policies about risk management systems;
- have clear escalation policies, processes and procedures in place for exception reporting; and
- review their risk management systems if material changes occur in the risk management context.

We also expect responsible entities to:

- conduct stress testing and/or scenario analysis of investment risk and liquidity risk to their business and the schemes they operate as part of their risk management systems; and
- review their framework for stress testing and/or scenario analysis at appropriate intervals to ensure the nature, currency and severity of the tested scenarios are relevant and appropriate in light of the business and market conditions.

If a responsible entity decides not to conduct stress testing and/or scenario analysis, we expect it to document why this is the case, keep appropriate internal records of this rationale, and review this decision at appropriate intervals.

As a matter of good practice, responsible entities should:

- have written risk management plans for treating risks, which can be implemented through written policies and procedures; and
- use internal and/or external audit to review compliance with, and the effectiveness of, their risk management systems.

Determining appropriate risk treatments

RG 000.61 There are different ways that responsible entities may manage risks. For example, they may:

(a) do nothing if the identified risk is within acceptable risk tolerance levels;

(b) avoid the risk by not undertaking the relevant activities completely;

(c) prevent the eventuation of the risk through specific action like developing rules and documented policies and procedures;

(d) reduce the consequences or impact of realised risks (e.g. through contingency, emergency or business continuity plans); and/or

(e) transfer the risks to other parties, for example, through insurance or outsourcing.

RG 000.62 Responsible entities should manage the risks faced by the business as a whole given that some risks may be interrelated (e.g. liquidity and valuation risks).

RG 000.63 A responsible entity must determine the appropriate treatment for an identified risk and document how each of the identified risks will be treated.

RG 000.64 We consider it good practice for responsible entities to have written risk treatment plan(s) setting out how each risk will be treated, including:

(a) the intention or objective of the treatment;

(b) the measures that will be applied to manage the risk, including whether a documented risk management plan is required for specific material risks;

(c) how implementation of the measures will be monitored and reviewed, including who is expected to implement the measures and ensure the adequacy of the resources required to implement them; and

(d) whether residual risk exists after the treatment plan has been implemented and whether such risk falls within acceptable risk tolerance levels.

RG 000.65 Regardless of whether the responsible entity has a written risk management plan for treating material risks, risk treatment measures should be implemented through written processes and procedures as a matter of good practice.

Measures to treat risks

RG 000.66 How responsible entities treat identified risks will typically depend on the nature, scale and complexity of their business, and whether the particular risks are material to their operations and the scheme(s) they operate.

RG 000.67 The appendix to this guide includes examples of measures for treating the risks that we consider are most relevant to the business of a responsible entity.

Residual risks

RG 000.68 Residual risks often remain even after measures to treat risks have been applied. Understanding the concept of residual risk is an important consideration when identifying, assessing and managing risks, as it determines whether residual risks are within acceptable risk tolerance levels or require further treatment, and can inform future risk assessments.

RG 000.69 A responsible entity must ensure that any residual risks are monitored by the board in light of its policy or statement on risk appetite to determine if, when and what treatment should be applied to manage the residual risk.

Monitoring and review

RG 000.70 Risk management and the development of a risk management system is not a 'set and forget' or 'one-off' process. A responsible entity must ensure that, at appropriate intervals, it:

(a) monitors compliance with its risk management systems, including the processes and procedures put in place to identify, assess and treat risks;

(b) regularly reviews its risk management systems; and

(c) documents the processes used to monitor compliance with and review its risk management systems.

RG 000.71 To promote effective monitoring of the process, we expect responsible entities to ensure that there are:

(a) effective information systems and appropriate record keeping policies;

(b) appropriate policies for regular reporting on risk management activities, in particular by the person responsible for the identified risk; and

(c) clear escalation policies and procedures for exception reporting, including the breaches of risk management systems or policies, processes and procedures that must be promptly reported to identified escalation points.

Monitoring compliance with processes and procedures

RG 000.72 A responsible entity must ensure that staff members follow the processes and procedures put in place to manage risks.

RG 000.73 The individuals responsible for identified risks within the structure of the risk management systems (risk owners) should monitor the relevant risks by regularly comparing the actual outcome or performance of the business against the limits or other criteria established through consideration of risk appetite or under a risk management plan (if applicable).

RG 000.74 These comparisons should take place at appropriate intervals so monitoring takes place as close to real time or the point of transaction as possible in order to allow real-time exposure measurement and management.

RG 000.75 We expect responsible entities to require risk owners to regularly report on their risk management related duties in accordance with their policies for reporting. Reporting may be weekly, monthly or quarterly, depending on the nature, scale and complexity of the responsible entity's business.

RG 000.76 We also expect responsible entities to require risk owners to make exception reports (e.g. to the designated risk management function or risk management committee or to the board as appropriate) when there are breaches of the risk management systems or its policies, processes and procedures, in accordance with escalation policies.

RG 000.77 This information can help the board in understanding the effectiveness of, and compliance with, the control measures put in place to manage identified risks and the validity of the acceptable risk tolerance levels in light of the objectives of the business. The information may also help the board to evaluate the effectiveness of the responsible entity's risk management systems as a whole, in particular by identifying systemic issues or trends.

Reviewing the effectiveness of the systems

RG 000.78 A responsible entity must review its risk management systems (including the policy or statement on its risk appetite) regularly (no less than annually) for currency, relevance, effectiveness and appropriateness to its business on an ongoing and dynamic basis: see RG 000.20–RG 000.21.

RG 000.79 Our regulatory experience suggests that certain types of schemes (e.g. unlisted property schemes, mortgage schemes, agribusiness schemes or hedge funds) are subject to more complex risks. Accordingly, we think that the risk management systems for these types of schemes should be reviewed more frequently (e.g. on a quarterly basis).

RG 000.80 In addition, we expect responsible entities to review their systems where material changes to the context in which they operate the business may affect how they manage risks. Examples include changes to laws that affect the business, changes to business plan objectives (including starting any new business), or changes to the structure of the risk management systems (e.g. due to departure of senior staff). This ensures that the risk management systems remain current and relevant and take into account changes in the internal and external environment in which the responsible entity operates and sets strategic business objectives.

RG 000.81 We also consider it good practice for responsible entities to use internal and/or external audit as part of their process for reviewing risk management systems. Audits should seek to provide independent assurance of the

responsible entity's compliance with, and effectiveness of, risk management systems and, specifically, whether:

(a) risk management policies, processes and procedures have been followed;

(b) effective risk identification and assessment processes and procedures are in place and implemented;

(c) treatment measures and controls are in place for the material risks identified, and whether they are effective; and

(d) risk management systems are reviewed regularly with any weaknesses identified for ongoing improvement.

Stress testing or scenario analysis

RG 000.82 While terminology varies, stress testing and/or scenario analysis is generally used to assess how a responsible entity will be affected and respond in different scenarios (e.g. addressing the solvency and liquidity of a responsible entity and the scheme(s) it operates). This is essentially a 'what if' exercise that looks at what may happen to, for example, the cashflow, profit or capital of a responsible entity when subjected to particular circumstances that affect the business.

RG 000.83 There is no common methodology for stress testing or scenario analysis. The range of methods we have observed vary from a balance sheet-based approach or market price-based approach to brainstorming possible scenarios.

> Note: Stress testing can be used for different objectives including stress testing as an internal risk management tool, supervisory stress testing as an assessment tool, surveillance stress testing to identify sources of systemic risk or crisis management and stress testing for business restructuring plans. For further details, see International Monetary Fund, *Macrofinancial stress testing—Principles and practices*, August 2012 and the report of the International Organization of Securities Commission (IOSCO), FR 03/13 *Principles of liquidity risk management for collective investment schemes*, Final report, Report of the Board of IOSCO, March 2013, available at www.iosco.org.

RG 000.84 We expect responsible entities to conduct stress testing and/or scenario analysis of investment risk and liquidity risk of their business and the schemes they operate as part of their risk management systems. If a responsible entity does not adopt these practices, we expect it to document why this is the case, and keep appropriate internal records of this rationale.

RG 000.85 We also expect responsible entities to review their framework for stress testing and/or scenario analysis at appropriate intervals to ensure the nature, currency and severity of the tested scenarios are relevant and appropriate in light of the business and market conditions. If a responsible entity has decided not to conduct stress testing and/or scenario analysis, we expect this decision will also be reviewed at appropriate intervals.

> Note: This is consistent with IOSCO guidance on liquidity risk management as set out in FR 03/13 *Principles of liquidity risk management for collective investment schemes*, Final report, Report of the Board of IOSCO, March 2013, available at www.iosco.org.

RG 000.86 The testing and analysis should include short-term and prolonged adverse environmental impacts, and take into account entity-specific and market-wide 'shocks'. For example, the framework may consider:

(a) the impact of significant market movements;

(b) liquid assets becoming illiquid;

(c) significant reductions in cash inflows through applications or increases in redemption requests; and

(d) asset revaluation.

RG 000.87 The results of any stress testing or scenario analysis will inform future risk identification, assessment, evaluation and management.

Appendix: Examples of risks and risk treatments

This appendix lists the risks that we consider are most relevant to the business of responsible entities and should generally be managed. It gives examples of these risks, including specific risks under each category, and examples of measures that responsible entities can consider in treating these risks. The examples are not intended to be exhaustive and reflect common risks and measures we have observed through our regulatory experience.

Identified risk	Examples of risk based on our regulatory experience	Examples of risk treatments
Strategic risk *This is the risk of a responsible entity not being able to pursue its business strategies or meet its business objectives as a result of inappropriate business model or strategies.*	Market conditions (e.g. instability or volatility) and market sentiment (e.g. uncertainty) can lead to cost pressures and reductions in inflow for many responsible entities in the managed funds sector. This raises risks for the operating model of some responsible entities and may endanger the continuity of particular entities and/or schemes. Changes in the external environment (e.g. the introduction of new financial requirements or tax changes) may affect an entity's business strategies or the investment strategy of the scheme(s) it operates. Similarly, consolidation through merger and acquisition activity can raise risks of unsatisfactory business integration for the merging entities. If the consolidation is not managed appropriately, it could undermine each of the relevant business's risk management systems and lead to practical implementation issues, especially if full integration and consolidation may take long periods of time to complete.	• Regular 'horizon scanning' • Engagement with regulatory bodies • For mergers and acquisitions, policies and processes that ensure consideration is given to: – alignment of systems, processes, procedures and cultures before business integration – appropriate resources and attention for effective implementation under direct supervision of the board during and after business integration • Stress testing of key assumptions or factors that underpin the business model
Governance risk *This is the risk of a responsible entity not having the appropriate decision-making processes in place to support sound and transparent decision making that is not adversely influenced by conflicts of interests, and ensure that decisions related to the scheme(s) are in the best interests of members.*	Observations from our regulatory experience highlight a governance risk that may be particularly relevant to some responsible entities. This is the risk that, when considering whether to enter into a transaction with a related party, the interests of the related party will influence the decision-making of a responsible entity to the detriment of scheme members' interests or the scheme as a whole. Note: For more information on managing related party transactions, see Regulatory Guide 76 *Related party transactions* (RG 76).	• Policies and processes that guide decision making • Regular compliance certifications • Policy and processes that ensure compliance with laws concerning related party transactions

Identified risk	Examples of risk based on our regulatory experience	Examples of risk treatments
Operational risk *This is the risk of interruption to the operation or internal processes of a responsible entity's business, including the scheme(s) it operates.* *Specific operational risks include those relating to:* • *legal and compliance requirements;* • *technological resources;* • *human resources (including key persons);* • *outsourcing;* • *transitioning of the business; and* • *fraud.*	Operational risk includes the risk of a responsible entity having insufficient capacity and/or competency to conduct its financial services business and carry out supervisory arrangements in the best interests of scheme members (e.g. the risk of inadequate financial, technological and human resources). Note: Unless it is regulated by APRA, an AFS licensee must have available adequate resources (including financial, technological and human resources) to provide the financial services covered by its licence and to carry out supervisory arrangements: s912A(1)(d). We expect responsible entities to identify and assess this particular risk regularly, such as by setting and reviewing the context of their risk management systems. This will allow them to address any required changes in resourcing needs as the internal and external environment evolves and business objectives align. *Legal and compliance requirements* There is a risk that a responsible entity may not comply with financial services laws in conducting its financial services business, or be able to enforce certain legal rights that affect its business or the operation of the registered scheme(s) it operates under particular circumstances (e.g. if it is cost prohibitive to enforce those rights). Alternatively, a responsible entity may be the subject of legal action (e.g. a case in contract or tort law) or placed in external administration. *Technological resources* There is a risk that the responsible entity will not have adequate technological resources to conduct its business. This may include a lack of technological resources to recover from disasters or other major disruptions within a reasonable period so that the business can continue to operate. In our regulatory experience, this risk tends to be higher with responsible entities of small scale operations due to resource constraints. It also plays out in larger entities due to a lack of a systematic approach in assessing the adequacy of technological resources, particularly if the entity is part of a corporate group and the group's resources are made available to it.	*Legal and compliance requirements* • Documented compliance plans and arrangements for the responsible entity and the scheme(s) it operates • Breach registers and breach notification protocols *Technological resources* • Disaster recovery and business continuity plans

Identified risk	Examples of risk based on our regulatory experience	Examples of risk treatments
Operational risk (cont.)	*Human resources (including key persons)* There is a risk that the responsible entity will not have adequate human resources or competency to conduct its financial services business. This risk may arise, for example, as a result of resource constraints or a lack of training. Our regulatory experience particularly highlights key persons as an area of risk inherent in responsible entities of small scale operations where reliance on the skills and experience required by a responsible entity to successfully run its business is concentrated in one or two people crucial to its operation, or who have dominance in its culture. The dominance of such key persons can override what could otherwise be adequate risk management systems in a resource constrained environment. Such dominance may also lead to operational decisions being made that would not be considered appropriate within the responsible entity's risk management system.	*Human resources (including key persons)* • Succession planning to address key person risk • Training to promote competency in the provision of financial services • Skill audits • Key person insurance • Recruitment policies • Regular review of resource requirements, particularly during periods of growth or change
	Outsourcing We have observed a particular risk in this area through our regulatory experience. Some responsible entities, particularly those of a smaller scale, outsource some or most of their functions to conduct their financial services business instead of having the required technological or human resources inhouse. This often presents the risk of inadequate supervision of these functions, particularly where these functions are outsourced overseas, which may lead to unsatisfactory quality control over the distribution chain for financial products issued by a responsible entity. For example, if a product distributor enters into an arrangement with a responsible entity, but engages in misconduct, this is likely to result in adverse impacts on the relationship between a responsible entity and scheme members.	*Outsourcing* • Due diligence processes for choosing suitable service providers • Service level agreements • Monitoring processes to address the ongoing performance of service providers • Maintaining adequate staff and skill sets to effectively monitor service providers • Mechanisms for dealing appropriately and swiftly with any actions by service providers that breach service level agreements • Policies and processes to ensure agreements are always formalised and documented

Identified risk	Examples of risk based on our regulatory experience	Examples of risk treatments
Operational risk (cont.)	*Transitioning of the business* A risk may arise if a responsible entity is unable to conduct its business due to a lack of adequate planning and preparation to facilitate the transitioning of the business, resulting in unnecessary loss. Examples include: • appointment of a receiver over assets of the scheme (if a responsible entity becomes subject to external administration); or • a change of responsible entity for the scheme. Our regulatory experience indicates that it may often be difficult for external administrators to acquire sufficient working knowledge of a responsible entity and the scheme(s) it operates in a short period of time. Administrators are also likely to be financially constrained, given that schemes in these circumstances are typically adversely affected by a loss of confidence.	*Transitioning of the business* • Business continuity plans • 'Living wills' • Policies to ensure clear records identifying scheme assets
	Fraud This is the risk of concealment of misconduct within the responsible entity or the scheme(s) it operates (e.g. misappropriation or improper use of assess, as well as failure to manage conflicts of interest)	*Fraud* • Internal controls, including exception reporting of unusual events • Segregation of duties • Peer review
Investment risk *This is the risk that a scheme operated by a responsible entity will not meet its objectives due to failure in the performance of the scheme's underlying investments.* *Specific investment risks include those relating to:* • *investment governance and structure;* • *market conditions;* • *counterparty failure;*	*Investment governance and structure* There is a risk that a scheme operated by a responsible entity may not meet its objectives as a result of, for example, an inadequate framework for the selection and ongoing monitoring of the performance of the underlying investments of the scheme. Note: Where issue and redemption of scheme interests is permitted, valuation policies may be required in a pricing policy: see Regulatory Guide 134 *Managed investments: Constitutions* (RG 134). A risk also arises if a responsible entity's schemes are exposed to a financial product through a multi-layered structure in that the scheme invests in an investment vehicle which in turn invests in another investment vehicle. Such a structure is likely to create difficulties in identifying the scheme's ultimate exposure and the extent of exposure to a particular financial product or the type of financial product that may arise indirectly through the multiple investment vehicles.	*Investment governance and structure* • Establishing and implementing an adequate investment governance framework that takes into account: – whether the scheme will be a liquid scheme and how withdrawal will be made available; – whether the scheme is exposed to counterparty risk and, if so, monitoring the extent of that risk exposure regularly; – due diligence processes for investment selection in giving effect to investment strategies; and – objective measures to monitor the performance of investments at appropriate intervals and provide feedback information to review investments and, if appropriate, update the framework

Identified risk	Examples of risk based on our regulatory experience	Examples of risk treatments
• *product suitability; and* • *valuation and pricing.*	This risk may be exacerbated when one or more of the investment vehicles are not subject to the regulation of Australian laws. *Market conditions* There is a risk that the performance of the underlying assets of a scheme will be adversely impacted as a result of changes in the market conditions. Although our regulatory experience indicates that some responsible entities consider disclosure of this risk to investors alone as sufficient, we do not think that this is the case where responsible entities actively manage schemes. For example, while disclosure of market risk may be appropriate for an index tracking scheme that is not actively managed, we would expect that responsible entities would have processes in place to effectively manage market risk in other circumstances in addition to disclosure. *Counterparty failure* There is a risk that a counterparty will fail to meet its obligations, with the effect that the responsible entity cannot put in place a replacement transaction economically and efficiently to meet any ongoing obligations. Any assessment of counterparty risk should take into account the type and extent of counterparty risk the business or relevant schemes are exposed to. We do not consider, for example, that a generic approach to reviewing the business's counterparty risk exposure once a month is necessarily sufficient. *Product suitability* There is a risk of a product design becoming unsuited to the needs of current and potential scheme members, or the needs of the business. In our regulatory experience, this risk most often arises for some complex structured products offered to retail investors and legacy systems.	• Policies and processes to monitor investment risk in actively managed schemes • Disclosure of investment risk in Product Disclosure Statements (PDSs) for scheme(s) • Consumer research to address any product suitability issues

Identified risk	Examples of risk based on our regulatory experience	Examples of risk treatments
Investment risk (cont.)	*Valuation and pricing* At the scheme level, there is a risk of scheme assets not having a correct valuation on a timely basis. While this risk may not be relevant to some registered schemes (e.g. timeshare schemes, property syndicates or forestry schemes), robust valuation practices are essential for effective liquidity risk management and correct pricing of interests in most registered schemes. This risk generally is higher for schemes that invest in assets that are not traded on a financial market or assets that do not have a liquid market (e.g. mortgage or property schemes) where transparent price setting for scheme assets is more difficult to facilitate. In our regulatory experience, some constitutions or compliance plans only require a responsible entity to value scheme assets at specific intervals or use a qualified independent valuer as required by the Corporations Act. This can present a risk to members of the scheme that valuations are outdated and inappropriate to rely on when assessing their investment.	*Valuation and pricing* • Valuation policies that take into consideration factors like the type of assets a scheme invests in and the operating model of the scheme (e.g. whether it allows off-market issue and redemption of interests) • Regular independent valuations • Rotation of valuers used to value scheme assets
Liquidity risk *This is the risk that the responsible entity will not have adequate financial resources to meet its financial obligations as and when they fall due, either:* • *at the responsible entity level; or* • *at the scheme level (including meeting members' expectations and requests for redemptions).*	*At the responsible entity level* Regulatory Guide 166 *Licensing: Financial requirements* (RG 166) sets out the financial requirements for AFS licensees that are responsible entities. In summary, unless they are bodies regulated by APRA, responsible entities must meet: • the standard solvency and positive net assets requirement; • a tailored cash needs requirement; • a tailored audit requirement; • a net tangible assets (NTA) requirement, including requirements for holding at least 50% of the NTA requirement in liquid assets; and • depending on the financial products and services offered, any other requirements set out in RG 166 that apply. Note: Our general expectation is that risk management systems need to address the risk that an entity's financial resources will not be adequate: see RG 104.62. For more information on the financial requirements for responsible entities, see Appendix 2 of RG 166.	*At the responsible entity level* • Regular monitoring of financial requirements and reporting to the board • Diversification of income sources • Internal audit of high risk areas of the business, including management of liquid assets, pricing of assets and investment

Identified risk	Examples of risk based on our regulatory experience	Examples of risk treatments
	In our regulatory experience, we have seen a number of responsible entities become insolvent and unable to maintain their AFS licences or operate their scheme(s). This could be a result of market conditions putting pressure on less robust business models in the managed funds sector or inadequate fee structures where the entity receives less than expected management fees after the initial phase of scheme's operation (although it is otherwise envisaged that the scheme will operate over decades). Such mismatches in the internal and external context in which risk management systems are developed give rise to risks that a responsible entity will not have sufficient financial resources to operate its business including the relevant scheme(s) in accordance with its strategic and business objectives and those of the scheme(s). If the responsible entity also operates wholesale schemes or superannuation trusts, the operation of these other schemes or trusts may affect its cash flow or liquidity, and should be taken into account in assessing any liquidity risk. *At the scheme level* In our regulatory experience, responsible entities of schemes that invest in assets that are not well traded on a financial market or do not have a liquid market (e.g. mortgage or property schemes) face particular challenges in managing liquidity risk within the schemes they operate. This is evident in the wide-scale suspension of redemptions in the mortgage scheme sector when schemes with limited liquidity experienced increased investor demand for redemptions in 2008 and subsequently. Responsible entities of these schemes need to identify and address the risk of not being able to meet short-term commitments and the risk of misalignment of members' expectations on liquidity with the capacity of the scheme's assets to be realised to meet those expectations: see also RG 000.20.	*At the scheme level* • Policy and processes for assessing the liquidity of the assets of the scheme(s) the responsible entity operates to ensure that these assets are consistent with the scheme's ability to meet member redemption expectations and liabilities, as well as withstand a range of stress-tested events • Disclosure of the time it would generally take to meet redemption requests set out in PDS(s) for scheme(s) • Continuous monitoring of the market for assets the scheme holds to identify emerging liquidity shortages before they occur • Comparison of the performance of schemes to their peer groups (including trends in issue and redemption of interests) to identify emerging liquidity shortages before they occur

Key terms

Term	Meaning in this document
AFS licence	An Australian financial services licence under s913B of the Corporations Act that authorises a person who carries out a financial services business to provide financial services Note: This is a definition contained in s761A of the Corporations Act.
AFS licensee	A person who holds an AFS licence under s913B of the Corporations Act Note: This is a definition contained in s761A.
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
board	A responsible entity's board of directors
[CO 13/xxx] (for example)	An ASIC class order (in this example numbered 13/xxx)
Corporations Act	*Corporations Act 2001*, including regulations made for the purposes of that Act
CP 204 (for example)	An ASIC consultation paper (in this example numbered 204)
IOSCO	International Organization of Securities Commissions
Product Disclosure Statement (PDS)	A document that must be given to a retail client in relation to the offer or issue of a financial product in accordance with Div 2 of Pt 7.9 of the Corporations Act Note: See s761A for the exact definition.
RG 104 (for example)	An ASIC regulatory guide (in this example numbered 104)
REP 298 (for example)	An ASIC report (in this example numbered 298)
RSE	Registrable superannuation entity licensee
s912A (for example)	A section of the Corporations Act (in this example numbered 912A)
scheme	A registered managed investment scheme under Ch 5C of the Corporations Act
Superannuation Bill	Superannuation Legislation Amendment (Service Providers and other Governance Measures) Bill 2012

Related information

Headnotes

AFS licensees, identifying risks, assessing risks, managing risks, responsible entities, risk management systems, risk treatments

Class orders and pro formas

[CO 13/xxx] *Risk management systems of responsible entities*

Regulatory guides

RG 76 *Related party transactions*

RG 104 *Licensing: Meeting the general obligations*

RG 134 *Managed investments: Constitutions*

RG 166 *Licensing: Financial requirements*

Legislation

Corporations Act, Chs 5C, 7, Div 2, s601JA, 761A, 912A(1)(h), 913B

Superannuation Bill

Superannuation Industry (Supervision) Act 1993

Consultation papers and reports

CP 204 *Risk management systems of responsible entities*

REP 298 *Adequacy of risk management systems of responsible entities*

Other documents

APRA, Prudential Standard SPS 220 *Risk Management*

International Monetary Fund, *Macrofinancial stress testing—Principles and practices*

International Organization for Standardization, ISO 31000:2009 *Risk management: Principles and guidelines*

IOSCO, FR 03/13 *Principles of liquidity risk management for collective investment schemes*, Final report