ASIC
Australian Securities & Investments Commission

REPORT 298

Adequacy of risk management systems of responsible entities

September 2012

About this report

This report discusses the key findings of a proactive ASIC review of risk management systems of selected responsible entities undertaken in 2011–12.

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.

Disclaimer

This report 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 report are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

Contents

Executive summary

Managing 'risk'

1 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.

2 Adequate risk management systems and controls in businesses, therefore, 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 through providing measures intended to better safeguard the financial services industry from systemic risk.

Current law and guidance

3 Responsible entities, as Australian financial services (AFS) licence holders, have an ongoing legal obligation under s912A(1)(h) of the *Corporations Act 2001* (Corporations Act) to have adequate risk management systems, unless they are regulated by the Australian Prudential Regulation Authority (APRA). Bodies regulated by APRA need to meet requirements for comprehensive risk management systems as set out in various prudential standards.

4 Regulatory Guide 104 *Licensing: Meeting the general obligations* (RG 104) provides guidance to AFS licensees about what ASIC expects in meeting the obligation to have adequate risk management systems.

Scope of our review

5 In 2011–12, we completed a review aimed at assessing the adequacy and strategic and operational effectiveness of the risk management systems of selected responsible entities ranging in size and complexity, and how they specifically managed financial, investment and liquidity risk. This was with a view to:

(a) determining the ability of these AFS licensees to comply with their licence conditions;

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

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

Key findings

6 Table 1 summarises our key findings from our review of selected responsible entities.

Table 1: Key findings from our review of selected responsible entities

Risk management systems	
1	The selected responsible entities generally appear to demonstrate compliance with their obligation as AFS licensees to maintain adequate risk management systems, although improvements to risk management systems could be made—in particular, for those selected responsible entities that are not part of an APRA-regulated group.
2	Each of the selected responsible entities has a unique risk management system, which reflects the nature, scale and complexity of their financial services business. Of the selected responsible entities, those that are part of an APRA-regulated group have more sophisticated risk management systems than those that are not part of an APRA-regulated group. This usually means embedding risk management in strategic and business planning (as well as day-to-day operations), a well-considered risk appetite, and a strong risk management culture. While there are a number of variations, some of the most sophisticated risk management systems observed adopt a 'three lines of defence' risk management model focused on checks and balances for management, compliance and risk management, and independent audit (internal and/or external). A number of the selected responsible entities have implemented electronic compliance and risk management monitoring systems, which track their business's compliance obligations by requiring completion of business managers' attestations.
3	Most of the selected responsible entities indicated that their risk management system itself did not change as a result of the global financial crisis.
4	A number of the selected responsible entities made changes to internal processes and procedures and business operations as a result of the global financial crisis and other internal and external developments.
Adequacy of financial, technological and human resources	
5	Subject to finding 6 below, the selected responsible entities generally appear to have adequate financial, technological and human resources. Adequacy of financial resources is more easily demonstrated than the adequacy of other resources. Each of the selected responsible entities was able to demonstrate compliance with its financial resource requirements as an AFS licensee, and financial risk of the selected responsible entities appears adequately managed and monitored, including through regular reporting to Boards.
6	Of the selected responsible entities, those categorised as 'small' carry the following specific resource adequacy risks: • the risk that the skills and experience required by the responsible entity to successfully run a financial services business are concentrated in one or two people crucial to its operation, or who have dominance in its culture (key person risk); and/or • the risk of overreliance on external compliance and risk management consultants to establish and monitor risk management systems. These risks may be an indicator of inadequacy of the risk management systems in place and/or a lack of adequate skills and/or resources to independently assess the quality of external consultants' contributions and their ability to value-add to a business.

Investment and liquidity risks within responsible entities	
7	Investment and liquidity risks at the fund level are generally considered by the selected responsible entities to be owned by the investors in the managed investment schemes. There appears to be significant reliance by the selected responsible entities on disclosure of these risks.
8	Of the selected responsible entities, there are generally different approaches to managing investment and liquidity risks at the fund level. There is little or no stress testing conducted by most of the selected responsible entities that are not part of an APRA-regulated group. Where stress testing practices are adopted, there appears to be a diversity of approach, which may be explained by the nature, scale and complexity of a responsible entity's business.
Business integration risks in the managed funds sector	
9	The managed funds industry is undergoing significant transformation as a result of the global financial crisis and continuing market instability, volatility and uncertain market sentiment. This environment is exacerbating risk aversion and creating higher expectations from retail investors, as well as increasing cost pressures and reducing inflows; these factors are driving responsible entities to integrate and consolidate. Business integration poses new and emerging risks that need to be managed by a number of the selected responsible entities.

A Background

Key points

Every business takes risks to operate and grow, and needs to manage those risks to do so.

Risk management is not about eliminating risk, but instead is about helping an organisation increase the likelihood of achieving its objectives and reducing the likelihood of not doing so, or failing.

Responsible entities, as AFS licensees, have an ongoing general obligation to have adequate risk management systems, unless they are regulated by APRA. Bodies regulated by APRA need to meet prudential requirements for comprehensive risk management systems.

What is 'adequate' will vary between licensed responsible entities, having regard to the nature, scale and complexity of their businesses.

Managing 'risk'

7 All activities of an organisation involve 'risk'. Risk is defined by the International Organization for Standardization as 'the effect of uncertainty on objectives': International Organization for Standardization ISO 31000:2009 *Risk management: Principles and guidelines* (ISO 31000:2009). It is usually described in terms of a combination of the consequences of an event occurring and its likelihood of occurring.

8 For responsible entities, we consider that adequate risk management systems will help them to deliver their objectives to retail investors and financial consumers by mitigating the risk of investors and consumers losing their investment or not being able to access it. Risk management is not about eliminating risk. Instead, robust risk management systems that work in practice strengthen the operations of responsible entities charged with managing investments of retail investors and financial consumers, and address and manage risks arising in the operation of such a business.

9 Ensuring the adequacy of risk management systems of responsible entities, therefore, has a direct bearing on achieving two of ASIC's strategic priorities, the key outcomes of:

(a) confident and informed investors and financial consumers; and

(b) fair and efficient financial markets.

Current law and guidance

10 Responsible entities, as AFS licensees, have an ongoing legal obligation under s912A(1)(h) of the Corporations Act to have adequate risk management systems, unless they are regulated by APRA.

11 Bodies regulated by APRA need to meet principles-based prudential standards for comprehensive risk management systems. APRA does not endorse any particular methodology and expects the bodies it regulates to implement approaches that will appropriately manage different types of material risk to ensure that decision making is supported with effective information and oversight.

> Note: Risk management requirements for bodies regulated by APRA are set out in APRA's Prudential Standard APS 310 *Audit and related matters*, Prudential Standard LPS 220 *Risk management* and Prudential Standard GPS 220 *Risk management*. In addition, APRA has now been given power to make prudential standards for superannuation and released Draft Prudential Standard SPS 220 *Risk management* in April 2012.

12 RG 104 provides some guidance to AFS licensees generally about what we expect of them in meeting the obligation to have adequate risk management systems.

13 Specifically, RG 104.61–RG 104.66 provide the following guidance for AFS licensees:

> The requirement for risk management systems ensures that you explicitly identify the risks you face and have measures in place to keep those risks to an acceptable minimum.
>
> We expect your risk management systems will:
>
> (a) be based on a structured and systematic process that takes into account your obligations under the Corporations Act;
>
> (b) identify and evaluate risks faced by your business, focusing on risks that adversely affect consumers or market integrity (this includes risks of non-compliance with the 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.
>
> Note: In thinking through your risk management obligations, you might find it helpful to look at: Australian and New Zealand Standard AS/NZS 4360:2004 *Risk management* [this has now been superseded by ISO 31000:2009] and the related handbook, HB 436:2004 *Risk management guidelines—Companion to AS/NZS 4360:2004*, available for purchase from www.saiglobal.com/shop; and Joint Forum *High-level principles for business continuity* (August 2006), available from IOSCO (www.iosco.org), IAIS (www.iaisweb.org) and BIS (www.bis.org).

Nature, scale and complexity of your business

Your risk management systems will depend on the nature, scale and complexity of your business and your risk profile. They will be different for each licensee.

Your risk management systems will need to adapt as your business develops and your business risk profile changes over time.

If you use external providers to provide functions that relate to your AFS licence, we think your risk management measures will need to be different from those you would need if you performed those functions in-house.

Financial risks

Your risk management systems will normally need to address the risk that your financial resources will not be adequate. We have set out the financial requirements for licensees not regulated by APRA in Regulatory Guide 166 *Licensing: Financial requirements* (RG 166). [For further details, see paragraphs 61–62.]

14 We consider that ISO 31000:2009 is a helpful starting point for establishing and maintaining adequate risk management systems. ISO 31000:2009 is a standard that sets out principles and generic guidelines on risk management, although it is not specific to any particular industry sector. It covers establishing the context of the risk management process in an internal and external environment, risk assessment (identification, analysis and evaluation), risk treatment, and risk monitoring and review.

15 ISO 31000:2009 emphasises that risk management should be an integral part of all organisational processes and decision making. Risk management is not a stand-alone activity that is separate from the main activities of an organisation. It should help decision makers in an organisation make informed choices. When implemented appropriately and adequately, risk management will help an organisation increase the likelihood of achieving its objectives and reduce the likelihood of not doing so, or failing.

16 Nonetheless, we understand that responsible entities implement varied approaches that may go beyond ISO 31000:2009 to appropriately manage different types of risk.

Risk management in the managed funds sector

17 Responsible entities do not have prescriptive requirements for maintaining risk management systems under the Corporations Act. Our guidance applies across all AFS licensees, not responsible entities only.

18 What is ‘adequate’, therefore, is expected to vary between licensed responsible entities to take account of the nature, scale and complexity of their businesses.

19 Nonetheless, in addition to the requirements outlined in RG 104, there are certain core principles of risk management that we consider should be addressed to some degree by all responsible entities maintaining 'adequate' risk management systems. These include processes to:

(a) identify, analyse, evaluate, treat and monitor current and emerging risks;

(b) specifically manage the risk that the responsible entity may not have adequate financial resources to conduct its financial services business and meet its financial obligations; and

(c) specifically manage the risk that a responsible entity may not meet the investment objectives of its managed investment scheme(s) or may not maintain appropriate levels of liquidity within its fund(s).

20 The development of adequate risk management systems should also not be regarded as a 'set and forget', 'compliance-ticking', 'one-off' process by responsible entities. As highlighted by the global financial crisis and ongoing market volatility and uncertainty, as market conditions change, so too should risk management systems adapt and evolve. They should take account of the changing external environment, as well as internal changes within responsible entities and their managed investment schemes, all of which may have a significant impact on the risk profile of a business.

B Scope of review and methodology

Key points

In 2011–12, we completed a review of selected responsible entities to assess:

- the adequacy and strategic and operational effectiveness of their risk management systems; and
- how they specifically manage financial, investment and liquidity risks.

Using a consultative approach, we gathered information from each of the selected responsible entities and assessed the adequacy of each responsible entity's risk management system. Our conclusions and key findings are based on these individual assessments.

Scope of review

21 In 2011–12, we completed a review of 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. This was with a view to:

(a) determining the ability of these AFS licensees to comply with their general obligation to maintain adequate risk management systems;

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

(c) encouraging better preparedness for market volatility and uncertainty, and any severe market disruption in the future.

22 Consequently, the review focused on the following key areas:

(a) the extent to which a responsible entity's risk management system is embedded in its business—that is, the extent to which a responsible entity considers its risk appetite and strategic and business planning in developing and reviewing its risk management system;

(b) how a responsible entity identifies and manages key current and emerging risks, including investment and liquidity risks, and whether it adopts stress testing to assess and review these risks;

(c) whether a responsible entity has adequate resources, how it assesses the adequacy of those resources and how it specifically manages its financial risk;

(d) whether a responsible entity has made changes to its risk management system as a result of the global financial crisis or other internal or external factors; and

(e) the documentation underpinning a responsible entity's risk management system.

23 Although insurance is typically used as a means of managing risk, this review did not focus on the adequacy of professional indemnity insurance cover held by responsible entities as such a risk mitigant.

> Note: For further details on professional indemnity insurance cover requirements for responsible entities, see Regulatory Guide 126 *Compensation and insurance arrangements for AFS licensees* (RG 126).

24 We chose the selected responsible entities on the basis of the number of schemes they operate and/or their funds under management using the following parameters:

(a) large—responsible entities operating more than 75 managed investment schemes or with significant funds under management;

(b) medium—responsible entities operating between approximately 20 and 75 managed investment schemes; and

(c) small—responsible entities operating less than 20 managed investment schemes.

25 Some of the selected responsible entities also operate hedge funds and private equity funds.

26 Of the selected responsible entities, our focus generally did not include unlisted property trusts, exchange-traded funds or money market funds. Such funds have been, or are, the subject of separate ASIC review.

> Note: For further details, see Media Release 12-168MR *ASIC review of unlisted property MIS sector* and Regulatory Guide 46 *Unlisted property schemes: Improving disclosure for retail investors* (RG 46) and Media Release 12-57MR *ASIC released exchange traded funds report* and Report 282 *Regulation of exchange traded funds* (REP 282).

27 In addition, our focus did not extend to agribusiness funds, mortgage schemes or infrastructure funds. These funds are subject to recently revised disclosure guidance.

> Note: For further details, see Regulatory Guide 45 *Mortgage schemes: Improving disclosure for retail investors* (RG 45), Regulatory Guide 231 *Infrastructure entities: Improving disclosure for retail investors* (RG 231) and Regulatory Guide 232 *Agribusiness managed investment schemes: Improving disclosure for retail investors* (RG 232).

Review methodology

28 We engaged and met with each of the selected responsible entities that participated in this project on a voluntary basis. During the engagement, our focus was on each entity's risk management system, including how financial, investment and liquidity risks are managed.

29 Using a consultative approach, we gathered information from each of the selected responsible entities and assessed the adequacy of each responsible entity's risk management system. In doing so, we had regard to our guidance in RG 104 (see paragraphs 12–13), as well as ISO 31000:2009 (see paragraphs 14–15).

> Note: For further details of some of the practical key elements of risk management systems, as set out in ISO 31000:2009, including risk identification, assessment and management, see Section C.

30 Our conclusions and key findings are based on these individual assessments.

C Risk management systems

Key points

There appears to be compliance with the ongoing general obligation to maintain adequate risk management systems, although improvements to risk management systems could be made—in particular, for those selected responsible entities that are not part of an APRA-regulated group.

Selected responsible entities that are part of an APRA-regulated group have more sophisticated risk management systems than those that are not part of an APRA-regulated group.

Our review identified significant variance among selected responsible entities in the following areas, which may require further attention by some of them:

- embedding risk management in strategic and business planning, as well as day-to-day operations;
- risk appetite;
- risk identification, assessment and management;
- treatment of residual risk; and
- the impact of the global financial crisis on risk management systems.

Most selected responsible entities did not change their risk management system itself as a result of the global financial crisis, although changes to internal processes and procedures and business operations appear to have been made.

31 Having regard to the nature, scale and complexity of a responsible entity's business, RG 104 clearly outlines our expectations that the responsible entity's risk management system will be:

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

(b) identifies and evaluates the risks faced by the responsible entity's business, focusing on risks that adversely affect consumers or market integrity;

(c) establishes and maintains controls designed to manage or mitigate those risks; and

(d) fully implements and monitors those controls to ensure they are effective.

32 Table 2 lists our key findings on general compliance with the ongoing general obligation to maintain adequate risk management systems.

Table 2: Key findings—Risk management systems

1	The selected responsible entities generally appear to demonstrate compliance with their obligation as AFS licensees to maintain adequate risk management systems, although improvements to risk management systems could be made—in particular, for those selected responsible entities that are not part of an APRA-regulated group.
2	Each of the selected responsible entities has a unique risk management system, which reflects the nature, scale and complexity of their financial services business. Of the selected responsible entities, those that are part of an APRA-regulated group have more sophisticated risk management systems than those that are not part of an APRA-regulated group. This usually means embedding risk management in strategic and business planning (as well as day-to-day operations), a well-considered risk appetite, and a strong risk management culture. While there are a number of variations, some of the most sophisticated risk management systems observed adopt a 'three lines of defence' risk management model focused on checks and balances for management, compliance and risk management, and independent audit (internal and/or external). A number of the selected responsible entities have implemented electronic compliance and risk management monitoring systems, which track their business's compliance obligations by requiring completion of business managers' attestations.
3	Most of the selected responsible entities indicated that their risk management system itself did not change as a result of the global financial crisis.
4	A number of the selected responsible entities made changes to internal processes and procedures and business operations as a result of the global financial crisis and other internal and external developments.

33 Specific areas that warrant further discussion on which varied practices were identified as a result of our review include:

(a) the extent to which risk management systems are embedded in strategic and business planning, as well as day-to-day operations;

(b) risk appetite;

(c) risk identification, assessment and management;

(d) treatment of residual risk; and

(e) the impact of the global financial crisis on risk management systems.

Embedding risk management in strategic and business planning

34 ISO 31000:2009 specifies that risk management in an organisation should be set in context. The context for an organisation includes the strategic and operational context in which the organisation operates, as well as external and internal factors.

35 The sophistication of the risk management systems of the selected responsible entities varies significantly.

36 Generally, the larger the responsible entity's business, the more sophisticated their risk management system appears to be. Most of the larger selected responsible entities have an enterprise-wide, integrated approach to risk management, some on a global scale. This may be related to the level of available resourcing in larger organisations.

37 However, typically, the most distinguishing factor that determines sophistication is whether the selected responsible entity is part of an APRA-regulated group. This is probably because bodies regulated by APRA, such as banks, superannuation fund trustees and insurance companies, are prudentially supervised and must meet principles-based prudential requirements for comprehensive risk management systems. APRA expects its regulated entities to implement robust risk management systems to identify, assess, mitigate and monitor all material risks that may affect their ability to meet the reasonable expectations of beneficiaries and maintain a sound financial position.

> Note: For further details about APRA's requirements for bodies it regulates, see paragraph 11.

38 Of the larger selected responsible entities, most tend to follow group risk management systems required to satisfy these prudential standards (where it is appropriate to do so). For example, the aggregate risk of a group can be expressed by setting a global risk limit tested to cope with prolonged and severe market downturns, as evidenced in the global financial crisis. For material risks in this context, responsible entities have the ability to use both quantitative and qualitative tools to examine worst case outcomes and determine whether these are acceptable (including stress testing at the group level).

39 The more sophisticated systems we observed usually have one or more of the following features:

(a) risk management is embedded in strategic and day-to-day operational decision making;

(b) the risk management system is centralised where risk management resources and staff are shared among the business;

(c) there appears to be greater clarity of roles and responsibilities within documented policies and procedures, which are generally owned by the business, although supported by risk management staff who ensure compliance with these policies and procedures, and focus on continuous improvement; and

(d) there is a strong risk management culture where management and staff see the value that risk management adds to the business, leading to

greater focus and compliance with the organisation's risk management system—for example, a strong risk management culture is demonstrated in selected responsible entities where staff in a risk management function are consulted by the business in making decisions and those staff also often sit on committees that have direct oversight of the business.

40 These features were less evident or not evident at all in selected responsible entities that are not part of an APRA-regulated group.

Risk appetite

41 Determining an organisation's risk appetite—that is, 'the amount and type of risk that an organisation is willing to pursue or retain' (ISO Guide 73:2009 *Risk management—Vocabulary*)—is a key step in setting the context in which risk management in an organisation is set. It allows the organisation to appropriately set its objectives and business strategy. It is the measure of risk that an entity is willing to take to achieve its objectives, and a risk management system that is set in the right context assists the business to achieve those objectives. If an organisation has not understood or articulated its risk appetite, its business strategy is less likely to reflect the acceptable risk levels, nor will its risk management system be as effective.

42 With the exception of those selected responsible entities that are part of an APRA-regulated group, most of the selected responsible entities observed in this review do not appear to have a well-articulated risk appetite (if any). This could indicate the non-methodical approach taken by some of these responsible entities in establishing their risk management systems, although it is more likely explained by their risk management system not being embedded within the rest of their business: see paragraph 39.

43 Of the more sophisticated approaches to risk appetite we observed:

(a) the Board sets the risk appetite, providing direction for strategic planning and acting as a driver for how business units accept operational risks as part of their daily operation, while enabling the Board to see how decisions in one entity in a group or operating area may affect the entire organisation;

(b) the risk appetite, once established, sets the tone and culture for risk management across an organisation; and/or

(c) the 'three lines of defence' model (see paragraph 46) is adopted—for example, some of the selected responsible entities designate management as the first line of defence within their risk management system, responsible for the application of the risk appetite and controls at the operational level. A key aspect of this procedure is generally to

deconstruct the risk appetite into clearly defined 'risk metrics', which allow for tolerances to be incorporated into the decision-making process at the day-to-day operational level. This is supported by separate risk appetite statements for individual business units, which set out the risks responsible entities are prepared to take, together with the circumstances in which those risks can and will be taken.

Risk identification, assessment and management

44 The practical key elements of risk management, as set out in ISO 31000:2009, include risk identification, assessment and management. Risk identification is about identifying the source of the risk, areas of impact, events and their causes, and potential consequences. Assessment and management of risks require the organisation to determine the significance of the risk, including its positive and negative impact on the business and the likelihood of the consequences occurring. Once the risk is well understood, its management can be more easily determined, which normally involves implementing controls that reduce the probability and/or outcome of the risk to an acceptable level (i.e. to a level within the organisation's risk appetite).

45 There are various methods used for identifying, assessing and managing current and emerging risks by the selected responsible entities.

46 While smaller responsible entities appear to rely heavily on external compliance and risk management consultants to establish and monitor their risk management systems, some of the more sophisticated risk management systems assessed were based on the 'three lines of defence' model. We observed a number of minor variations. However, broadly, the model is made up of:

(a) management—the first line of defence comprises controls designed to ensure ongoing compliance is embedded in all relevant decisions and operations;

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

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

47 Where this model was observed, the Board is typically responsible for setting the risk appetite (see paragraph 43), fostering a risk management culture and overseeing the risk management system, including through

regular reporting to the Board. It is not designed to eliminate risks. Rather, if a particular risk is identified and assessed to be outside the risk appetite of a business, the risk can be treated appropriately so that it can be accepted by the business which, by definition, means that it is converted to a residual risk that can be managed within a responsible entity's acceptable risk appetite levels (see paragraphs 51–53).

Use of electronic compliance and risk management systems

48 One approach to identifying, assessing and/or managing risks that was observed in a number of the selected responsible entities involves the implementation of electronic compliance and risk management systems. These electronic systems generally track compliance obligations by requiring completion of business managers' attestations.

49 The electronic systems observed appear to monitor the risk and compliance of their businesses using system-generated questionnaires for relevant staff relating to pre-identified risks. They vary in sophistication with some offering risk assessments, monitoring of positive assurance, and central repositories for registers on breaches, complaints, fraud, exceptions and control integrity tests.

50 However, some of the electronic systems observed appear to require 'box-ticking' or participation in a 'rubber stamping' exercise that, on its own, appears insufficient to demonstrate adequate risk management systems. Particular concerns are more likely to arise where review controls are not in place, especially where the electronic systems are proprietary systems—for example, where the electronic systems are designed by external compliance and risk management consultants and the effectiveness of the controls is also tested by the consultants without more appropriate 'checks and balances' in place, such as consideration by the Board or independent risk and compliance committees.

Treatment of residual risk

51 Residual risk is the remaining risk after the exercise of risk controls. The understanding of the concept of residual risk is an important consideration during the risk identification and assessment process. We observed that the understanding of the concept of residual risk generally appeared limited among the smaller of the selected responsible entities that are not part of an APRA-regulated group.

52 The larger responsible entities demonstrated a stronger understanding of the concept, with clear treatment plans for dealing with residual risks, thereby

allowing high inherent risks to be converted to lower risks acceptable to businesses. For example, one of the selected responsible entities considers residual risks during their risk identification and assessment process. Residual risk is identified as part of the evaluation of the effectiveness, ranking and prioritising of controls. It is then determined within risk ratings and the risk appetites and tolerances for each risk.

53 This approach drives the need for the development of detailed risk treatment action plans for those risks that management believe may be in danger of operating outside a responsible entity's risk appetite level. Regular monitoring of the implementation of these action plans generally occurs at risk and compliance committee meetings to ensure these risks are managed within acceptable risk appetite levels.

Impact of global financial crisis on risk management systems

54 Most of the selected responsible entities indicated that they had not changed their risk management system as a whole as a result of the global financial crisis. The risk management systems themselves were generally considered by the responsible entities as adequate and appropriate without need for adaptation.

55 Of the selected responsible entities, we observed that many risk management systems appear to have withstood the global financial crisis reasonably well (subject to survival bias), although we encourage responsible entities to undertake regular reviews of these systems and, in any event, when market shocks occur.

56 A number of the selected responsible entities have made other changes as a result of the global financial crisis and other significant internal and external change, which include:

(a) changes to business operations and costs;

(b) rationalisation of the number of managed investment schemes offered to potential investors;

(c) a reduction of management costs to help make investing through managed investment schemes a more appealing proposition; and

(d) changes in product features.

D Adequacy of financial, technological and human resources

Key points

Unless they are bodies regulated by APRA, AFS licensees must have available adequate financial, technological and human resources. Any failure to do so may create an unacceptable risk that the licensee may not comply with its general obligations.

The selected responsible entities appear to have adequate financial, technological and human resources, and manage financial risk appropriately.

Smaller responsible entities face the following specific resource adequacy risks:

- key person risk; and
- the risk of overreliance on external compliance and risk management consultants.

57 Section 912A(1)(d) of the Corporations Act requires an AFS licensee that is not a body regulated by APRA to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence and to carry out supervisory arrangements. Bodies regulated by APRA need to meet prudential resourcing requirements.

58 RG 104 states that the AFS licensee must have measures in place to ensure there are adequate resources and measures to regularly review these resources to ensure they are adequate on an ongoing basis: see RG 104.84.

59 Any failure to do so may create an unacceptable risk that the AFS licensee may not comply with its general obligations.

60 Table 3 lists our key findings on general compliance with the ongoing general obligation to maintain adequate financial, technological and human resources.

Table 3: Key findings—Adequacy of financial, technological and human resources

5	Subject to finding 6 below, the selected responsible entities generally appear to have adequate financial, technological and human resources. Adequacy of financial resources is more easily demonstrated than the adequacy of other resources. Each of the selected responsible entities was able to demonstrate compliance with its financial resource requirements as an AFS licensee, and financial risk of the selected responsible entities appears adequately managed and monitored, including through regular reporting to Boards.
6	Of the selected responsible entities, those categorised as 'small' carry the following specific resource adequacy risks: • the risk that the skills and experience required by the responsible entity to successfully run a financial services business are concentrated in one or two people crucial to its operation, or who have dominance in its culture (key person risk); and/or • the risk of overreliance on external compliance and risk management consultants to establish and monitor risk management systems. These risks may be an indicator of inadequacy of the risk management systems in place and/or a lack of adequate skills and/or resources to independently assess the quality of external consultants' contributions and their ability to value-add to a business.

Adequacy of financial resources

61 RG 166 specifies the financial resource requirements for all AFS licensees, including responsible entities, unless they are bodies regulated by APRA. Bodies regulated by APRA need to meet prudential resourcing requirements.

62 Current financial resource requirements for licensed responsible entities include that they must:

(a) be solvent and have more assets than liabilities;

(b) elect one of five options to demonstrate that they meet the cash needs requirement of Pro Forma 209 *Australian financial services licence conditions* (PF 209), including preparing a cash flow for the next three months; and

(c) have minimum net tangible assets (NTA) of at least 0.5% of the value of scheme property with a minimum requirement of $50,000 and a maximum requirement of $5 million.

Note: Changes to the financial resource requirements for responsible entities have been made by Class Order [CO 11/1140] *Financial requirements for responsible entities* and will commence on 1 November 2012. The new financial resource requirements for responsible entities include the preparation of 12-month cash projections; having an NTA of the greater of $150,000, 0.5% of the average value of scheme property (capped at $5 million) or 10% of the average responsible entity revenue (uncapped); and a liquidity requirement of at least 50% of its NTA requirements in cash or cash equivalents and an amount equal to the NTA requirement in liquid assets.

63 Our review assessed whether the selected responsible entities meet the current financial resource requirements, and we found they generally

demonstrate compliance with these requirements. Our review did not consider whether the selected responsible entities will be in a position to meet the new financial resource requirements, and we will undertake a separate review of compliance with these requirements in 2012–13.

64 In contrast to human and technological resources, the demonstration of adequacy of financial resources appears easier because it is usually achieved by reference to financial statements and cash flow projections in compliance with AFS licence conditions and our guidance in RG 166.

Managing financial risk

65 RG 104.66 specifically sets out our expectation that risk management systems will address the risk that financial resources will not be adequate.

66 A key focus of our review was to assess how the selected responsible entities managed certain types of risk that they faced during the global financial crisis and how these risks could be better managed. This includes financial risk at the responsible entity level—that is, the risk of a responsible entity not being able to meet its financial obligations as and when they fall due.

67 Financial risk appeared to be generally adequately managed and monitored by the selected responsible entities, with regular reporting on meeting financial resource requirements, including solvency, to their Boards.

68 While the review did not generally observe stress testing of financial risk on an entity-by-entity basis, of those selected responsible entities that are part of an APRA-regulated group, financial risk is sometimes stress-tested at a group level. For example, we observed stress testing at the group level through aggregate risk measures like global risk limits or capital adequacy management ratios formulated by reference to the impact of a range of adverse scenarios, including prolonged and severe downturn, and prudently calibrated to minimise risks.

Adequacy of technological and human resources

69 Not all selected responsible entities appeared to deal with the question of the adequacy of their technological and human resources directly (or did not provide the documentation that indicated that they did so). They generally demonstrate adequacy of these resources retrospectively through their ability to do what they are required to do.

70 Most of the selected responsible entities do not generally seem to have a forward looking analysis of the resources required. They do not appear to systematically assess the adequacy of their technological and human resource needs as part of forward planning to provide the financial services

covered by their AFS licence and to carry out supervisory arrangements. Where such analysis is undertaken, it is typically undertaken at the business unit or group level, rather than at the responsible entity level.

71 It seems especially difficult to undertake this analysis in larger responsible entities where the responsible entity is part of a group and the group's resources are made available to all parties of the group, including the responsible entity. Under such arrangements, the selected responsible entities typically have written agreements between themselves and their parent entities relating to the use of commonly available resources. Where additional resources are required, the larger selected responsible entities tend to rely on their parent entity or obtain external resources.

Specific resource adequacy issues in smaller responsible entities

Key person risk

72 Key person risk appears to be inherent in the smaller of the selected responsible entities and risk mitigation strategies addressing business continuity in these circumstances are limited. Some of the selected responsible entities categorised as 'small' also have 'key person' AFS licence conditions.

> Note: For further details on 'key person' AFS licence conditions, see Regulatory Guide 105 *Licensing: Organisational competence* (RG 105).

73 The management of key person risk is difficult in smaller responsible entities because key persons are not easily replaced. In a resource-constrained environment, the dominance of an organisation's agenda can override what could otherwise be adequate risk management systems. Such dominance may be problematic if it leads to decisions being made that would not be considered appropriate within a responsible entity's risk management system. We expect responsible entities to have in place appropriate strategies, such as business continuity or succession plans, to mitigate key person risk.

74 Of the selected responsible entities, the key person risk is sometimes also exacerbated by an apparent dominance of personality and/or power in one or two people within the business. This generally appears to be derived from the fact that these people are either business founders or holders of expert skills necessary for the effective and efficient running of their business. Observed in both larger and smaller selected responsible entities, this type of dominance can be indicated by membership of a number of decision-making risk management bodies within an organisation, including the Board and risk and compliance committees. We expect responsible entities to give

consideration to Board and committee composition to manage this potential risk.

Use of external compliance and risk management consultants

75 RG 104 recognises that many AFS licensees outsource functions that relate to their licence, including administrative functions, although licensees remain responsible for complying with their general obligations: see RG 104.33–RG 104.34.

76 Where functions are outsourced, RG 104.36 sets out our expectations—namely, that AFS licensees:

(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 the licensee's general obligations.

77 This means that Boards of responsible entities need effective and robust risk oversight processes for identifying, prioritising, sourcing, managing and monitoring critical risks, and need systems in place to ensure that these processes are improved continuously as the business environment changes.

78 A number of the selected responsible entities categorised as 'small' are heavily reliant on external compliance and risk management consultants. These responsible entities typically rely on such consultants to develop, implement and monitor their risk management systems.

79 The outsourcing of establishing and monitoring risk management systems, while not prohibited, raises a number of questions about the adequacy of a risk management system of a responsible entity and its ability to comply with its ongoing general obligations (including adequacy of compliance and risk management resources).

80 For example, adequacy of a risk management system can be demonstrated by clear linkage to a responsible entity's strategic business objectives and operations. It is arguably more difficult for an external consultant that is not closely linked to the organisation to develop a risk management system in a tailored manner that establishes this linkage. In addition, while external consultants are typically available more often, it appears most of the external consultants observed in selected responsible entities work part time in the business and have other clients to whom they offer similar services. Accordingly, it is difficult to envisage how a risk management system can be effectively monitored in such circumstances.

81 It also appears that, without the external consultants, the 'small' selected responsible entities that rely on them in the manner described above may lack the skills required to meet their risk management obligations. This is because they do not appear to have a strong understanding of risk management, which means that they may also not have sufficient skills to appropriately monitor and assess independently the performance of these external consultants.

82 In selected responsible entities that outsourced their risk and compliance functions, we observed some of the following specific risks:

(a) the engagement of external compliance and risk management consultants who report to the responsible entity on a periodic or on an as needed basis may not allow for the timely and effective identification of current and emerging risks;

(b) there appears to be inadequate Board involvement in the monitoring process relevant to the outsourced compliance and risk management functions;

(c) there appears to be a lack of independent review of the processes and testing of the results generated by the external compliance and risk management consultants; and

(d) the agreements between the responsible entities and the external compliance and risk management consultants show the absence of defined responsibilities and service level standards within which consultants' performance may be appraised. As such, there does not appear to be any regular (e.g. annual) process for performance review, nor any responsible entity oversight about how the consultants keep up-to-date with regulatory changes affecting the AFS licensee and whether they are required—under their contract—to maintain the same level of competency and training expected of the licensee.

E Investment and liquidity risks within responsible entities

Key points

Responsible entities have a key role in managing investment and liquidity risks arising in the managed investment schemes they operate.

There are different approaches to managing investment and liquidity risks, depending on the nature, scale and complexity of a responsible entity, and the investment objectives of, and nature of underlying investments in, its managed investment scheme(s).

There is little or no stress testing conducted by most of the selected responsible entities that are not part of an APRA-regulated group. Where stress testing practices are adopted, there appears to be a diversity of approach, which may be explained by the nature, scale and complexity of each responsible entity's business.

83 As a result of the global financial crisis and to encourage better preparedness for market volatility and uncertainty in the future, a key focus of our review was to assess how the selected responsible entities manage:

(a) investment risk at the fund level—that is, the risk of a managed investment scheme not meeting its investment objective(s); and

(b) liquidity risk at the fund level—that is, the risk of a managed investment scheme not being able to meet its obligations as and when they fall due.

84 Table 4 lists our key findings on how these risks are managed by the selected responsible entities.

Table 4: Key findings: Investment and liquidity risk within responsible entities

7	Investment and liquidity risks at the fund level are generally considered by the selected responsible entities to be owned by the investors in the managed investment schemes. There appears to be significant reliance by the selected responsible entities on disclosure of these risks.
8	Of the selected responsible entities generally, there were different approaches to managing investment and liquidity risks at the fund level. There is little or no stress testing conducted by most of the selected responsible entities that are not part of an APRA-regulated group. Where stress testing practices are adopted, there appears to be a diversity of approach, which may be explained by the nature, scale and complexity of a responsible entity's business.

Managing investment and liquidity risks

85 RG 104.62 sets out our clear expectations that responsible entities will identify and evaluate risks faced by a business, focusing on those that adversely affect consumers or market integrity. The global financial crisis highlighted the need for responsible entities to better manage the investment and liquidity risks posed by their managed investment schemes.

86 Generally, of the selected responsible entities, there are different approaches to managing investment and liquidity risks. This can likely be explained by the varied nature, scale and complexity of each of the responsible entities, as well as the different underlying investments and investment objectives of their managed investment schemes.

Stress testing

87 Stress testing or scenario analysis is one recognised means of managing investment and liquidity risks, which is becoming more widespread in the managed funds sector following the global financial crisis. In April 2012, the Technical Committee of the International Organization of Securities Commissions (IOSCO) released CR 06/12 *Consultation report: Principles of liquidity risk management for collective investment schemes* (CR 06/12) and proposed that responsible entities adopt the following principles (among others):

(a) the integration of liquidity management in investment decisions; and

(b) the conduct of assessments of liquidity in different scenarios, including stressed situations.

88 In most of the selected responsible entities, there is little or no sophisticated management of investment and liquidity risks through stress testing. Some of the explanations given for this approach include:

(a) stress testing of investment or liquidity risks is not necessary because these risks are fully disclosed to retail investors—here, the view relied on is that, provided the responsible entity executes the investment strategy as disclosed, there is no need to test the risks;

(b) stress testing of investment or liquidity risks is not necessary given the nature of the investment products offered to retail investors (e.g. structured products, or liquid assets like cash or ASX 200 securities);

(c) a belief within the smaller selected responsible entities that formal stress testing would not provide management with additional information that would improve risk management within a business; and

(d) research shows that stress testing methodologies do not work.

89 Nonetheless, our review of selected responsible entities identified some noteworthy examples of sophisticated ongoing management of investment and liquidity risks, including through the use of stress testing—for example:

(a) some responsible entities use quantitative measures for managing and stress testing and scenario testing investment and liquidity risks, including:

(i) in equity portfolios, stress testing active specific risks and tracking errors, considering value, growth, momentum and size factors;

(ii) stress testing portfolio holding options to ensure the portfolios remain compliant after material market movements; and

(iii) undertaking scenario test analysis for fixed income using risk metrics like duration, currency and sector allocations, including through portfolio analytical tools;

(b) one responsible entity adopts a specific, methodical, bottom-up approach by modelling interactions between different risk types on the level of individual stocks and risk factors, which are then taken into consideration in portfolio construction and monitored by reference to prescribed risk tolerances established by financial modelling and valuations; and

(c) other responsible entities engage external consultants with stress testing expertise—for example, to conduct stress testing on strategic asset allocation across all managed investment schemes operated.

F Business integration risks in the managed funds sector

Key points

With increasing cost pressures and reductions in inflows, the managed funds industry is consolidating, and is expected to continue doing so in the foreseeable future.

Responsible entities need to manage business integration risks as their risk profile increases and the adequacy and adaptability of their risk management systems is tested.

90 The managed funds industry is undergoing significant transformation amid uncertain market sentiment exacerbating cost pressures and reductions in inflows. As a result, the managed funds industry is consolidating, and is expected to continue doing so for the foreseeable future. These periods of change can pose new and emerging risks, while also typically increasing the risk profile of responsible entities and testing the adequacy and adaptability of their risk management systems.

91 In mergers and acquisitions, there is a significant risk of unsatisfactory integration for the merging businesses. Where the integration and consolidation of responsible entities is not managed appropriately, it could undermine each of the relevant business's risk management systems and lead to practical implementation issues, especially where full integration and consolidation may take long periods of time to complete—for example, during the process, multiple responsible entities may need to comply with varying standards driven by different organisational cultures.

92 The key finding outlined in Table 5 therefore reflects a key emerging issue that arose from our review—the need for business integration risks to be addressed in the managed funds sector.

Table 5: Key finding: Business integration risks in the managed funds sector

9	The managed funds industry is undergoing significant transformation as a result of the global financial crisis and continuing market instability, volatility and uncertain market sentiment. This environment is exacerbating risk aversion and creating higher expectations from retail investors, as well as increasing cost pressures and reducing inflows; these factors are driving responsible entities to integrate and consolidate. Business integration poses new and emerging risks that need to be managed by a number of the selected responsible entities.

93 A number of the selected responsible entities in our review had undergone significant business integration, or were currently in the process of integrating businesses, as a result of merger or acquisition activity. This clearly involves change for each organisation involved, including their operations, systems, policies and procedures, culture, products and ability to comply with new regulatory requirements in a timely manner.

94 How business integration risk is managed in a particular situation varies depending on the nature of the merger or acquisition activity and the organisations involved. That said, some of the selected responsible entities presented what appear to be appropriate steps to help manage business integration risks. These include:

(a) before the merger or acquisition, business integration risk is considered as part of the due diligence completed to decide whether a merger or acquisition should proceed—consideration is given to the likely ease of business integration, including alignment of systems, processes, procedures and cultures; and

(b) after the merger or acquisition, the business integration is managed as a discrete, organisation-wide project owned and overseen by the Board—this approach helps ensure that it is given, and continues to be given, the appropriate resources and attention required for effective implementation.

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 on a financial services business to provide financial services Note: This is a definition contained in s761A.
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
body regulated by APRA	Has the meaning given in s3(2) of the *Australian Prudential Regulation Authority Act 1998*
Ch 5C (for example)	A chapter of the Corporations Act (in this example numbered Ch 5C), unless otherwise specified
Corporations Act	*Corporations Act 2001*, including regulations made for the purposes of that Act
general obligations	The obligations of an AFS licensee under s912A(1) of the Corporations Act
managed investment scheme	A managed investment scheme registered under Ch 5C of the Corporations Act
NTA	Net tangible assets
responsible entity	Has the meaning given to it in s9 of the Corporations Act
RG 104 (for example)	An ASIC regulatory guide (in this example numbered 104)
s912A (for example)	A section of the Corporations Act (in this example numbered 912A), unless otherwise specified

Related information

Headnotes

adequacy of resources, AFS licence, AFS licensee, business integration risk, electronic compliance and risk management systems, external compliance and risk management consultants, financial risk, global financial crisis, investment risk, liquidity risk, residual risk, responsible entities, risk, risk appetite, risk management, risk management systems, stress testing

Class orders and pro formas

[CO 11/1140] *Financial requirements for responsible entities*

PF 209 *Australian financial services licence conditions*

Regulatory guides

RG 45 *Mortgage schemes: Improving disclosure for retail investors*

RG 46 *Unlisted property schemes: Improving disclosure for retail investors*

RG 104 *Licensing: Meeting the general obligations*

RG 105 *Licensing: Organisational competence*

RG 126 *Compensation and insurance arrangements for AFS licensees*

RG 166 *Licensing: Financial requirements*

RG 231 *Infrastructure entities: Improving disclosure for retail investors*

RG 232 *Agribusiness managed investment schemes: Improving disclosure for retail investors*

Legislation

Corporations Act, s912A(1)(d) and 912A(1)(h)

Reports

IOSCO CR 06/12 *Consultation report: Principles of liquidity risk management for collective investment schemes*

REP 282 *Regulation of exchange traded funds*

Media and other releases

11-242MR *ASIC releases new financial requirements for responsible entities*

12-57MR *ASIC releases exchange traded funds report*

12-168MR *ASIC review of unlisted property MIS sector*

Standards

APS 310 *Audit and related matters*

AS/NZS 4360:2004 *Risk management systems*

GPS 220 *Risk management*

ISO 31000:2009 *Risk management: Principles and guidelines*

ISO Guide 73:2009 *Risk management—Vocabulary*

LPS 220 *Risk management*

SPS 220 *Risk management* (draft)