ASIC
Australian Securities & Investments Commission

REGULATORY GUIDE 000

Risk management systems of responsible entities

July 2016

About this guide

This guide is for Australian financial services (AFS) licensees that are responsible entities.

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.

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 guide was issued in July 2016 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 Australian financial services (AFS) licensees, responsible entities (including dual-regulated entities) are legally obliged to have adequate risk management systems. These systems are fundamental to mitigating exposure to relevant risks and informing business decision making.

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

- establishing and maintaining risk management systems that are suitable for the responsible entity's business and the schemes operated (see Section B);
- identifying and assessing risks (see Section C); and
- managing risks (see Section D).

Legislative obligation

RG 000.1 Under s912A(1)(h) of the *Corporations Act 2001* (Corporations Act), responsible entities have an ongoing obligation to maintain adequate risk management systems. This obligation also applies to responsible entities that are dual-regulated entities. A dual-regulated entity is a registerable superannuation entity (RSE) licensee that also operates schemes.

RG 000.2 In Regulatory Guide 104 *Licensing: Meeting the general obligations* (RG 104), we set out our general guidance for AFS licensees on what is required to comply with s912A(1)(h).

RG 000.3 Based on our experiences and changes in the managed investment sector, we considered that additional tailored guidance would assist responsible entities.

RG 000.4 In 2011–12, we reviewed the risk management systems of a selected group of responsible entities, ranging in size and complexity, to assess the systems' adequacy and strategic and operational effectiveness: see Report 298 *Adequacy of risk management systems of responsible entities* (REP 298).

RG 000.5 In 2015, we surveyed 118 responsible entities asking them about their risk management systems, including their processes for managing liquidity risk and conducting stress testing. The survey was a proactive response to increased volatility in global and domestic markets: see Media Release (15-020MR) *ASIC enquires into risk management by responsible entities* (13 February 2015).

RG 000.6 Based on these reviews, we identified that there were inconsistencies between the risk management systems of responsible entities and improvements could be made to some responsible entity's arrangements.

RG 000.7 Further, there have been a number of significant developments in relation to responsible entities that highlight the importance of having an adequate risk management system in place, including:

(a) an increase in the amount of assets managed in the managed funds sector;

(b) growth in the number of schemes operated;

(c) diversification in the size, complexity and nature of the types of schemes managed by responsible entities;

(d) changes in market conditions; and

(e) a number of high-profile collapses of responsible entities.

RG 000.8 This guide draws on the findings of our reviews and provides guidance on specific areas to improve the risk management systems of responsible entities.

What this guide covers

RG 000.9 This guide outlines our expectations of responsible entities when complying with the obligation within s912A(1)(h).

RG 000.10 While RG 104 gives guidance on risk management systems for AFS licensees generally, this guide focuses specifically on the business of responsible entities, the schemes they operate and the particular risks they face.

RG 000.11 The sections of this guide detail our expectations for responsible entities to have:

(a) overarching risk management systems in place (Section B);

(b) processes for identifying and assessing risks (Section C); and

(c) processes for managing risks that are appropriate for the nature, scale and complexity of the business and schemes operated (Section D).

RG 000.12 We have also included in this guide additional good practice guidance. This guidance is not mandatory; it is intended to help responsible entities improve their risk management systems to operate at a level above their statutory obligations.

RG 000.13 Table 1 provides a summary of our expectations of responsible entities and the good practice guidance.

Table 1: Summary of guidance

Section	Expectations for compliance with s912A(1)(h)	Good practice guidance (not mandatory)
Section B (Establishing a risk management system)	Responsible entities should: • maintain documented risk management systems that support: – a risk governance structure; – clearly defined roles and responsibilities; – policies and procedures for identifying, assessing and understanding each of the material risks of the responsible entity's business and the schemes operated; – policies and procedures for ensuring that there are adequate controls in place to manage the risks identified; – policies and procedures for ensuring there is adequate oversight of the risk management systems by both the party responsible for ownership of the risk and the compliance function, including appropriate reporting; and – a policy or statement on the responsible entity's risk appetite and the risk tolerance for each material risk identified; • foster a strong risk management culture; • take into account relevant industry, local and international standards; • include, as a component of the risk management systems, a liquidity risk management process; • ensure the board or its delegate reviews whether the risk management systems have been complied with, are operating effectively and remain current as frequently as appropriate, given the nature, scale and complexity of the responsible entity's business and the schemes it operates (at a minimum, annually); and • if relying on external service providers for risk management functions, maintain a strong understanding of risk management and have sufficient skills to independently monitor and assess the performance and ongoing suitability of the service provider.	Responsible entities may: • at least annually, conduct an independent review to determine whether the risk management systems have been complied with and are operating effectively; • at least every three years, conduct a comprehensive independent review of the appropriateness, effectiveness and adequacy of the risk management systems; • segregate functions to allow for independent checks and balances; • establish a designated risk management function and/or risk management committee; • appoint a chief risk officer; and • publicly disclose appropriate details of the responsible entity's risk management system.

Section	Expectations for compliance with s912A(1)(h)	Good practice guidance (not mandatory)
Section C (Identifying and assessing risks)	Responsible entities should: • maintain one or more risk registers as part of their risk identification and assessment process; • ensure that their risk management systems address all material risks—including (but not limited to) strategic risk, governance risk, operational risk, market and investment risk, and liquidity risk—at both the responsible entity and scheme level; • when choosing methodologies for identifying and assessing risks, take into account: – the nature, scale and complexity of the business; – processes based on forward-looking analysis; – ensuring an appropriate level of human input; – ensuring senior management involvement in the process; and – whether different processes should be used for different schemes; and • adopt appropriate methods to assess risks, which may include: – self-assessment; – stress testing and/or scenario analysis; – loss data analysis; – change management; and – electronic systems.	Responsible entities may use risk indicators and regularly report on these to the board and senior management.

Section	Expectations for compliance with s912A(1)(h)	Good practice guidance (not mandatory)
Section D (Managing risks)	Responsible entities should: • implement appropriate strategies for managing each of the risks identified, including: – a control monitoring and assurance process; – conducting stress testing and/or scenario analysis of liquidity risks of the business and the schemes they operate as part of their risk management systems as frequently as appropriate, given the nature, scale and complexity of the business (at a minimum, annually); – reviewing their framework for stress testing and/or scenario analysis—to ensure the tested scenarios are relevant and appropriate in light of the business and market conditions—as frequently as appropriate, given the nature, scale and complexity of the business (at a minimum, annually); and – if stress testing and/or scenario analysis is not conducted, document why this is the case, keep appropriate internal records of this rationale and review this decision regularly; • have adequately experienced staff regularly review and monitor the risks identified; • ensure there is regular reporting and escalation of issues to the board, risk committee and compliance committee, as appropriate; and • ensure compliance with other relevant obligations as an AFS licensee.	Responsible entities may: • conduct regular stress testing and/or scenario analysis of all material risks of the business and the schemes they operate; • have a written risk treatment plan; and • include in the compliance plan for their schemes, procedures for ensuring that the key risks identified for the responsible entity and relevant scheme are managed on an ongoing basis.

RG 000.14 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. These examples may help responsible entities establish and review their arrangements to identify, assess and manage risks, and may be considered by responsible entities as part of these processes.

RG 000.15 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 relevant to their business and the schemes they operate in an ongoing and dynamic way.

Who this guide applies to

RG 000.16 This guide is for responsible entities, including dual-regulated entities, but may also apply to:

(a) AFS licensees not currently operating a scheme;

(b) investor directed portfolio services (IDPS) and managed discretionary account (MDA) operators; and

(c) entities operating unregistered managed investment schemes.

Dual-regulated entities

RG 000.17 Dual-regulated entities also need to meet the risk management requirements set out in various legislation and the prudential standards regulated by the Australian Prudential Regulation Authority (APRA).

Note 1: The *Superannuation Legislation Amendment (Service Providers and Other Governance Measures) Act 2013* amended 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. This guide applies to these entities in addition to requirements under the *Superannuation Industry (Supervision) Act 1993*; however, the obligation to have an adequate risk management system excludes risks that relate solely to the operation of a regulated superannuation fund by the RSE licensee.

Note 2: APRA has issued Prudential Standard SPS 220 *Risk management* (PDF 55.5 KB) to help RSE licensees develop their risk management systems (www.apra.gov.au).

RG 000.18 Responsible entities that are part of a corporate group subject to regulation by APRA may take into account APRA's prudential standards and prudential practice guidance on risk management when developing and implementing risk management systems as required in this guide.

RG 000.19 This guidance is intended to act in unison with APRA's requirements for risk management. It is not expected that there will be any conflict between the requirements of either regulator; however, if for any reason a responsible entity believes they cannot comply with this guidance because of a conflicting APRA requirement, they should inform ASIC as soon as practical.

Other entities that may benefit from this guidance

RG 000.20 We expect all AFS licensees authorised to operate a scheme to consider this guide, even if they are not currently operating any schemes. This will help ensure they have in place a compliant risk management system that can be applied to the schemes on commencement of their operation.

RG 000.21 We expect IDPS and MDA operators to consider this guidance when establishing and reviewing their risk management systems, as these services would need to be registered as managed investment schemes if they could not rely on our relief for IDPSs and MDAs.

RG 000.22 All aspects of this guide may not be relevant to entities operating unregistered managed investment schemes. However, we recommend that operators of such schemes consider this guidance when establishing and reviewing their risk management systems.

ASIC's interim approach to compliance

RG 000.23 The requirements outlined in this guide are not new but are ASIC's view of the current requirements regarding risk management for responsible entities. As such there is no transitional period for compliance with these requirements. However, we intend to take a constructive and conciliatory approach to any breaches of this guidance for a period of 12 months from the date of release, if the relevant responsible entity can show that it is taking steps to bring its risk management system into compliance with this guidance.

B Establishing a risk management system

Key points

A responsible entity should ensure its risk management system comprises documented processes to identify, assess and treat risks and that this system is suitable for its business and the schemes it operates.

This section sets out our guidance for responsible entities on:

- developing a risk management system;
- implementing and reviewing risk management systems;
- setting risk management in context;
- risk appetite;
- the role of culture and structure in risk management systems;
- liquidity management; and
- relevant industry, local and international standards.

This section also sets out our good practice guidance for establishing a risk management system.

Risk management systems

RG 000.24 The international standard for risk management defines risk as the 'effect of uncertainty on objectives' and risk management as 'coordinated activities to direct and control an organization with regard to risk': see International Standard ISO 31000:2009 *Risk management: Principles and guidelines.*

RG 000.25 An effective risk management system:

(a) creates and protects value;

(b) is an integral part of all organisational processes;

(c) is part of decision making;

(d) explicitly addresses uncertainty;

(e) is systematic, structured and timely;

(f) is based on the best available information;

(g) is tailored;

(h) takes human and cultural factors into account;

(i) is transparent and inclusive;

(j) is dynamic, iterative and responsive to change; and

(k) facilitates continual improvement of the organisation.

Developing risk management systems

RG 000.26 A risk management system includes all structures, systems and subsystems, policies, procedures, and staff that a responsible entity uses to identify, assess and treat risks or to monitor and review the relevant controls or measures. It may be regarded as a framework (similar to that referred to in APRA's requirements and guidance on risk management) comprising all elements that allow the responsible entity to perform its risk management functions as required by the Corporations Act.

RG 000.27 An adequate risk management system enables material risks faced by the responsible entity and the schemes it operates to be identified, analysed and treated in a comprehensive and systematic way.

RG 000.28 The adequacy of a responsible entity's risk management system will depend on the nature, scale and complexity of its business and the schemes it operates.

RG 000.29 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 the risk management system operates, including a policy or statement on the responsible entity's risk appetite (see RG 000.38–RG 000.39);

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

(c) managing risks, including reviewing and monitoring the risk management system (see Section D and RG 000.35–RG 000.37).

RG 000.30 A responsible entity should ensure that:

(a) its risk management system comprises documented processes to identify, assess and manage material risks; and

(b) these processes are suitable for its business and the schemes it operates.

RG 000.31 We expect responsible entities to maintain a strong understanding of risk management in the context of the business, even if the establishment and the monitoring of the risk management systems are done by a small group of employees or external third-party service providers (e.g. compliance and risk management consultants). We expect those who carry out the risk management function to have appropriate knowledge and skills.

RG 000.32 Where external third-party service providers are used, we expect responsible entities to have sufficient skills to independently identify key risks and to monitor and assess the service provider's performance and ongoing suitability. We note that under s601FB, responsible entities retain ultimate responsibility for the operation of the scheme.

RG 000.33 We understand that if a responsible entity is part of a corporate group, the risk management system of the responsible entity, or the policies and procedures for its risk management system, may be subject to the overarching approach of the corporate group or form part of its risk management framework. Some responsible entities may rely on the risk management system of a related entity to assist with complying with their risk management obligations.

RG 000.34 This may be appropriate for businesses that are part of a larger corporate group; however, if this approach is adopted, each responsible entity should take into consideration their specific individual risks and requirements. The responsible entity should carefully assess the risk management system of the corporate group or related entity to ensure that it is appropriate and tailored as necessary.

Implementation and review of risk management systems

RG 000.35 Risk management systems are most effective if applied and adhered to in day-to-day decision making at all levels. Therefore, it is essential that a responsible entity ensures that all processes, policies and procedures that form part of its risk management system are implemented and applied to the day-to-day operation of its business and the schemes it operates.

RG 000.36 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 the schemes it operates, as well as changes in the external environment.

RG 000.37 We consider that the responsible entity's senior management has a specific role in ensuring that the risk management system is current, relevant, effective and appropriate to the business on an ongoing basis. To ensure that risk management systems are always current, they should be monitored and reviewed by the board or its delegate as frequently as appropriate, given the nature, scale and complexity of the business and the schemes operated. This should be at least annually. The nature, scale and complexity of the business and the schemes operated will also determine the level of detail of the review.

Setting risk management in context

RG 000.38 A responsible entity should 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.

RG 000.39 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 goals and objectives. Table 2 lists some examples of these factors.

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 schemes (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 and the schemes. • New product offerings in the market that compel a responsible entity to compete more effectively.

Policy or statement on risk appetite

RG 000.40 A responsible entity should set out in writing its risk appetite. This statement should outline the responsible entity's attitude towards risk taking while carrying out its business plans, including the amount of risk (which may refer to the level of losses) it is willing to take to pursue its business strategies and achieve its objectives. This statement should address the risks relevant to the responsible entity's overall strategy to achieve its objectives and set out the limits to these risks.

RG 000.41 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). The policy or statement should be approved by the board or its delegate.

RG 000.42 During this process the risk tolerance for each material risk should be identified. This can be expressed in qualitative or quantitative terms, where appropriate. The risk tolerance will reflect the risk appetite.

RG 000.43 A responsible entity should ensure its risk appetite is reviewed at appropriate intervals and that it takes 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 000.44 Responsible entities may adopt the following approach in setting and applying a policy or statement on risk appetite:

(a) Senior management sets the policy or statement on risk appetite for the business.

(b) The board or its delegate approves the policy or statement on risk appetite.

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

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

Risk management culture

RG 000.45 We expect responsible entities to foster a strong risk management culture throughout their organisations. The effectiveness of an adequate risk management system depends on the whole organisation understanding the value of managing risks effectively, and acting accordingly.

RG 000.46 We expect responsible entities to ensure that all relevant staff understand the purposes of risk management, including ensuring legal and regulatory compliance, as well as its value to the organisation. This can be done through induction, training and education programs.

RG 000.47 The board and senior management have specific responsibilities to ensure that a responsible entity as an AFS licensee complies with its obligation to have an adequate risk management system. We acknowledge that the board may not be directly involved in the day-to-day operation of the policies, procedures and processes for the risk management system and may delegate the supervision of these roles. However, 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 and make sure that relevant measures are implemented effectively.

RG 000.48 An effective risk management culture may include:

(a) communicating with staff about the importance of managing risks to achieve strategic business objectives;

(b) providing sufficient resources for all risk management functions;

(c) relevant staff receiving ongoing training about risk management (e.g. general risk management training and/or training that is relevant to a staff member's role and responsibilities) to help them identify risks and understand how they can be managed;

(d) discouraging breaches of any risk management procedures by staff through adequate consequence management; and

(e) assigning a designated director the responsibility of making sure the risk management system for the responsible entity and schemes it

operates are adequate (or a designated director having responsibility over particular parts of the risk management system).

RG 000.49 We expect responsible entities to maintain and implement remuneration policies that are aligned with, and supportive of, the risk management systems of their business, including the schemes they operate.

Structure and risk ownership

RG 000.50 A responsible entity's risk management system should include details of the functions, roles and responsibilities for implementing and carrying out specific risk management activities.

RG 000.51 We consider that an adequate risk structure requires:

(a) staff who perform risk management functions to have the appropriate knowledge and skills;

(b) decision making that is cognisant of the risk management system;

(c) key staff to take responsibility for owning risks and developing processes to mitigate them;

(d) regular reviews; and

(e) that risk owners regularly monitor and report on those risks.

RG 000.52 We expect responsible entities' risk management systems to require relevant staff to report internally to identified escalation points (e.g. the risk management committee, the designated risk management function or the board) about compliance with risk management processes, policies and procedures on a regular basis, and whenever any issues are identified (e.g. exceeding the risk tolerance for particular risk, or a failure to follow the relevant processes). Such reporting increases the risk-related information available in the organisation, to assist decision making and improve risk management systems where systemic issues about their operation are identified.

RG 000.53 We also consider that responsible entities should ensure that there are processes for regular reporting and escalation of issues to the board and/or any risk or compliance committee established.

Liquidity risk management

RG 000.54 Effective liquidity risk management is important for a responsible entity to ensure the financial obligations and needs of the business and schemes operated are met, including:

(a) investor redemptions;

(b) payment of distributions;

(c) changes in operational needs; and

(d) unexpected expenses.

RG 000.55 We expect risk management systems of responsible entities to include a liquidity risk management process, designed to ensure there are adequate financial resources to meet the financial obligations and needs of the responsible entity and the schemes operated.

Relevant industry, local and international standards

RG 000.56 In developing, implementing and reviewing its risk management system, we consider that a responsible entity should take into account relevant industry, local and international standards.

RG 000.57 We appreciate that in many cases compliance with the guidance may not be mandatory and a wide range of material may exist. We consider at a minimum responsible entities should take into account the guidance that exists for the key risk areas identified for the business and schemes operated.

RG 000.58 As outlined above, we consider liquidity is a key risk area for schemes and that a responsible entity should consider the liquidity risk management principles outlined in the International Organization of Securities Commissions' (IOSCO's) Principles of Liquidity Risk Management for Collective Investment Schemes.

Note: See IOSCO, *Principles of liquidity risk management for collective investment schemes: Final report* (PDF 231 KB), March 2013.

Good practice guidance

RG 000.59 Additional strategies that may be implemented by responsible entities in establishing and maintaining risk management systems include:

(a) supplementary reviews of the risk management system;

(b) segregating functions to allow for independent checks and balances;

(c) designating a risk management function and committee;

(d) appointing a chief risk officer; and

(e) publicly disclosing appropriate details about their risk management system.

Review of risk management systems

RG 000.60 Responsible entities may undertake the following additional independent reviews of their risk management systems:

(a) a review to determine whether the risk management systems have been complied with and are operating effectively (at least annually); and

(b) a comprehensive review of the appropriateness, effectiveness and adequacy of the risk management systems (at least every three years).

RG 000.61 The above reviews should be carried out by an independent, appropriately trained and competent person. This does not require an external party and can be done internally, as long as the responsible entity is satisfied that any other roles carried out by the person reviewing the risk management systems do not have an impact on their ability to perform an objective review and will not limit the robustness of the review.

RG 000.62 These additional reviews are similar to those referred to in APRA's requirements and guidance on risk management.

Segregation of functions to allow for independent checks and balances

RG 000.63 Depending on the nature, scale and complexity of the business, we encourage responsible entities to segregate functions to allow for independent checks and balances. This may include, for example, segregating the internal function in charge of valuing assets from the investment management function. We consider this will help manage conflicts of interests that may arise, and builds in an additional level of oversight to identify any issues.

Designated risk management function and committee

RG 000.64 Depending on the nature, scale and complexity of the business, we consider it is good practice for responsible entities to establish a designated risk management function and/or risk management committee. We understand that this may not be feasible for some responsible entities.

RG 000.65 The designated risk management function may have a hands-on role in ensuring the day-to-day operation of a responsible entity (including the schemes it operates) is conducted in alignment with its risk management system. To achieve this, the designated risk management function may be independent from the operating units of the responsible entity's business. It may also have the specific responsibility of monitoring compliance with risk management processes, policies and procedures, as well as reporting to the board and any risk management committee all significant breaches of the processes, policies and procedures.

RG 000.66 The responsibilities of a risk management committee may include:

(a) helping senior management develop the risk management system;

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

(c) reporting to the board and/or senior management on breaches of risk tolerance or risk management processes, policies and procedures, according to the responsible entity's escalation policy; and

(d) reporting to the board and/or senior management on the risk management system and its performance.

Appointing a chief risk officer

RG 000.67 Depending on the nature, scale and complexity of the business, we consider it is good practice for responsible entities to appoint a dedicated chief risk officer. Generally, the chief risk officer will be a key member of senior management to ensure they have sufficient stature and authority to influence risk-based decision making. It is important for any chief risk officer to communicate freely and have direct and unfettered access to the board, senior management and any risk or compliance committee established.

Disclosure of risk management policies

RG 000.68 In addition to its obligation to disclose information about significant risks and risk management arrangements in the Product Disclosure Statement (PDS) under Pt 7.9 of the Corporations Act, a responsible entity may provide additional transparency to investors about its arrangements by publicly disclosing appropriate details of its risk management systems—for example, on its website or in its annual report.

C Identifying and assessing risks

Key points

This section sets out our guidance for responsible entities on identifying and assessing risks, including:

- maintaining documented processes for identifying and assessing risks. The processes should be suitable for the business's objectives and operations, including for the schemes it operates;
- ensuring its risk management system addresses all material risks. These may include strategic risk, governance risk, operational risk, market and investment risk, and liquidity risk;
- addressing risks for its business (i.e. at the responsible entity level) and for the schemes it operates (i.e. at the scheme level);
- maintaining one or more risk registers as part of their risk identification process; and
- taking into account certain factors when choosing processes for identifying and assessing risks.

It also sets out our good practice guidance for identifying and assessing risks.

Identifying risks

RG 000.69 Risk identification is the process used by responsible entities to identify risks that will affect their ability to pursue business strategies and achieve the objectives of their business.

RG 000.70 We do not consider that any one particular method for identifying risks is the most appropriate and applicable for all responsible entities.

RG 000.71 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 000.72 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 000.73 A responsible entity should document the processes, policies and procedures it uses to identify risks.

RG 000.74 We expect responsible entities to maintain one or more risk registers for recording material risks to the business and schemes as part of their risk identification process. A responsible entity should select the format of the risk register(s) that is most suitable for the business and schemes operated.

Risks relevant to the business and the schemes

RG 000.75 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. Our regulatory experience suggests that certain types of schemes (e.g. unlisted property schemes, mortgage schemes, agribusiness schemes, quoted schemes, hedge funds and novel schemes) are subject to more complex risks.

RG 000.76 A responsible entity should ensure that its risk management system addresses all the material risks faced by its business at both the responsible entity and scheme level. These may include, but are not limited, to the following risks:

(a) *Strategic risk*—Any risk that arises out of a responsible entity's business strategies and business plan.

(b) *Governance risk*—Any risk that threatens the ability of a responsible entity to make reasonable and impartial business decisions in the best interests of members. This risk may arise if a responsible entity does not have the appropriate 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 schemes are in the best interest of members.

(c) *Operational risk*—The risk of loss, for the business or schemes, resulting from inadequate or failed internal processes, people and systems or from external events.

(d) *Market and investment risk*—The risk that a scheme operated by a responsible entity will not meet its objectives. Specific investment risks include those relating to investment governance and structure, market conditions, counterparty failure, product suitability, and valuation and pricing.

(e) *Liquidity risk*—The risk that the responsible entity will not have adequate financial resources to meet its financial obligations and needs, either at the responsible entity level or at the scheme level (including meeting the scheme's objectives and members' expectations for redemptions). As previously outlined, we consider that liquidity risk is a key risk area for schemes.

Note: 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.

Strategies for assessing risks

RG 000.77 Risk assessment is the process of describing identified risks, including by reference to the inherent risk, determining the likelihood of a risk eventuating and the significance of its potential impact. This process can help a responsible entity determine whether the identified risks are acceptable in light of its risk appetite and develop appropriate treatments for those risks.

RG 000.78 Examples of different methods that responsible entities may adopt for assessing risks include the following:

(a) *Self-assessment*—The responsible entity, its senior management and those in the designated risk management function (if applicable) assess risks through the business and the schemes it operates. This may include risk mapping, where risks are prioritised according to the significance of the risk and likelihood of a risk eventuating and mapped into four quadrants.

(b) *Stress testing and/or scenario analysis*—The responsible entity uses techniques such as stress testing and/or scenario testing to assess how it will be impacted by different scenarios. See also RG 000.96–RG 000.103.

(c) *Loss data analysis*—The responsible entity implements processes to analyse observed incidents to evaluate the actual losses caused by risks.

(d) *Change management*—The responsible entity implements processes to assess how the business and schemes operated are affected by change, to ensure objectives are still met.

(e) *Electronic systems*—The responsible entity uses purpose-built computer software to assess risks.

RG 000.79 Responsible entities may also seek expert advice and appoint an external consultant to help in the process of assessing the likelihood of a risk eventuating and the significance of its potential impact.

RG 000.80 We do not consider that any one particular approach for assessing risks will be the most appropriate and applicable to the operation of all responsible entities.

RG 000.81 A responsible entity should document its risk assessment processes. Documenting the reasons why particular assessments are made, including the thinking that led to the decisions about identified risks, provides a useful context for future risk assessment.

Selecting risk identification and assessment methodologies

RG 000.82 When considering which approach or combination of approaches to adopt in identifying and assessing risks, responsible entities may consider:

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

(b) incidents and complaints, trends or developments in the industry, and changes to the business environment;

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

(d) the need to ensure there is an appropriate level of human input in the process—sole or disproportionate reliance on electronic systems may not be adequate;

(e) senior management involvement in the process (e.g. any determination about whether an identified risk is at an acceptable level in light of the policy or statement on risk appetite); and

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

Good practice guidance

RG 000.83 Responsible entities may use risk indicators to provide an early signal of increasing risk exposures in various areas of the business. Regular reporting on the risk indicators can give the board and senior management an insight into the changes in the external and internal environment that may indicate risk concerns. It can also help ensure that risk levels are managed within defined tolerances.

D Managing risks

Key points

This section sets out our guidance for responsible entities on managing risks, including:

- determining appropriate risk treatments;
- controls or measures to manage or mitigate risk;
- use of technology;
- compliance with other relevant obligations as an AFS licensee
- dealing with residual risks;
- monitoring and review; and
- stress testing and scenario analysis.

It also sets out our good practice guidance for managing risks.

Determining appropriate risk treatments

RG 000.84 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 that give rise to the risk;

(c) prevent the eventuation of the risk through specific actions, such as developing rules and documented policies and procedures;

(d) reduce or mitigate 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, through insurance, outsourcing or indemnification.

RG 000.85 Risks faced by the business should be considered as a whole, given that some risks may be interrelated (e.g. liquidity and valuation risks).

Controls or measures to manage or mitigate risks

RG 000.86 We expect responsible entities to have adequate controls to manage or mitigate risks (e.g. performance standards for external service providers). It is also important for the responsible entity to implement a control monitoring and assurance process that considers the:

(a) adequacy of coverage of controls and whether appropriate remediation and response strategies are in place for material risks;

(b) effectiveness of internal controls designed to ensure risks have been mitigated; and

(c) appropriateness of monitoring strategies and ongoing testing (e.g. self-assessment, real-time transaction monitoring and reporting, and control assurance reviews by independent teams).

RG 000.87 The appendix to this guide includes examples of controls and measures for treating the risks that we consider are most relevant to the business of a responsible entity. The examples of risk treatments in the appendix are not mandatory.

RG 000.88 Nor are the risk management strategies exhaustive. We expect responsible entities to implement strategies for managing risks that are appropriate to the nature, scale and complexity of the business and scheme operated.

Use of technology

RG 000.89 There are a variety of technological resources that can be used to help responsible entities manage risks. These technologies come in a variety of forms. These technologies can help by analysing and storing data, automating compliance processes, monitoring trading and streamlining regulatory reporting. External service providers may be used to facilitate this process and also to store data. The use of these technologies may result in enhanced and more cost-effective management of risks. However, it is important to ensure that there is appropriate human oversight and review of any technological resources used.

Compliance with other relevant obligations as an AFS licensee

RG 000.90 Apart from the obligations contained within s912A(1)(h), we expect responsible entities to comply with their other existing obligations as an AFS licensee. As outlined in Table 3, many of these obligations are also relevant to assisting the management of risks.

Table 3: Other relevant AFS licence obligations

Obligation	Explanation	Further guidance
Compensation for retail clients: s912B	If financial services are provided to retail clients, an AFS licensee must have arrangements for compensating those persons for loss or damage suffered due to breaches by the licensee or its representatives. We consider adequate PI insurance is another important measure to manage operational risk.	Regulatory Guide 126 *Compensation and insurance arrangements for AFS licensees* (RG 126)

Obligation	Explanation	Further guidance
Adequate financial resources: s912A(1)(d)	An AFS licensee must have adequate financial resources. All responsible entities must comply with minimum financial requirements. We consider these requirements are another important measure to assist and manage liquidity risk affecting the responsible entity itself. We expect responsible entities to ensure that their financial resources will be adequate to be able to carry on their business in compliance with their licensee obligations, or to wind up their business in an orderly manner.	Regulatory Guide 166 *Licensing: Financial requirements* (RG 166) and Class Order [CO 13/760] *Financial requirements for responsible entities and operators of investor directed portfolio services*.
Adequate records of scheme operation: s601HA(1)(e)	The compliance plan of a registered scheme must set out the arrangements for ensuring adequate records of the scheme's operations are kept. In complying with this obligation, we expect that a responsible entity will ensure that it keeps adequate records of the establishment, implementation and review of its risk management system for the schemes operated.	Regulatory Guide 134 *Managed investments: Constitutions* (RG 134)
Adequate technological resources: s912A(1)(d)	An AFS licensee must have adequate technological resources. We expect that in complying with this obligation a responsible entity will maintain secure and stable information systems. This will assist in managing relevant risks, including system failure and malicious cyber activity.	Report 429 *Cyber resilience: Health check* (REP 429)
Breach reporting: s912D	An AFS licensee must tell ASIC in writing within 10 business days about any significant breach (or likely breach) of their obligations. We expect that a responsible entity will ensure that it reports any breach of s912A(1)(h). We consider processes to identify, escalate, report and analyse breaches (including trends) can help manage risks.	Regulatory Guide 78 *Breach reporting by AFS licensees* (RG 78)

Residual risks

RG 000.91 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. It can also help inform future risk assessments. Monitoring residual risks can help ensure they do not increase to a level above the responsible entity's risk appetite, and determine whether further treatment should be applied to manage those risks.

Monitoring and review

RG 000.92 A responsible entity should ensure that staff members follow the processes, policies and procedures put in place to manage risks.

RG 000.93 We expect responsible entities to have adequately experienced staff who regularly review and monitor the risks identified.

RG 000.94 As previously outlined, we consider that a responsible entity should review and monitor its risk management system as frequently as appropriate—given the nature, scale and complexity of the business and schemes operated—to ensure it is operating effectively. We expect this to be done at least on an annual basis.

RG 000.95 Such reviews may:

(a) comprehensively cover all aspects of the responsible entity's risk management system, including the policy and statement on risk appetite and all processes, policies and procedures related to this system;

(b) take into account changes affecting the responsible entity's business and the schemes it operates, including changes to:

(i) the operation of the responsible entity or its schemes;

(ii) the context in which the responsible entity operates the business or schemes;

(iii) the responsible entity's risk appetite or strategic business objectives;

(iv) changes to laws that affect the business or schemes; and

(v) changes to business plan objectives, including starting any new business;

(c) monitor compliance with the risk management system, including the processes, policies and procedures put in place to identify, assess and manage risks;

(d) ensure information systems are effective and up to date;

(e) ensure escalation policies and procedures are operating and effective; and

(f) ensure reporting of breaches is occurring, document the review process and any issues identified, and report to the board or senior management.

Stress testing and scenario analysis

RG 000.96 We expect a responsible entity to conduct stress testing and/or scenario analysis of the liquidity risks identified for the responsible entity's business and the schemes it operates as frequently as appropriate, given the nature,

scale and complexity of the business. At a minimum, we expect this to be undertaken annually. We consider liquidity risk a key risk area for all responsible entities to undertake stress testing and/or scenario analysis.

RG 000.97 We also expect responsible entities to review their framework for stress testing and scenario analysis as frequently as appropriate—given the nature, scale and complexity of the business—to ensure the nature, currency and severity of the tested scenarios are relevant and appropriate, in light of the business and market conditions. At a minimum, we expect this to be undertaken annually.

> Note: This is consistent with IOSCO Principles of Liquidity Risk Management for Collective Investment Schemes.

RG 000.98 If a responsible entity does not conduct stress testing or scenario analysis we expect it to document why this is the case, and to review this decision regularly.

RG 000.99 While terminology varies, stress testing and scenario analysis are 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 schemes it operates). This is essentially a 'what if' exercise that examines what may happen to, for example, the cash flow, profit or capital of a responsible entity when subjected to particular circumstances that affect the business.

RG 000.100 There is no common methodology for stress testing or scenario analysis; however, stress testing needs to be tailored to the responsible entity and the schemes it operates.

RG 000.101 The testing and analysis can include short-term and prolonged adverse environmental impacts, and take into account entity-specific and market-wide 'shocks'. For example:

(a) the impact of significant market movements;

(b) liquid assets becoming illiquid;

(c) significant regulatory change;

(d) a requirement to repay finance if a debt rollover or an extension cannot be arranged;

(e) significant reductions in net cash inflows through reduced applications or increased redemption requests; or

(f) significant asset revaluations.

RG 000.102 The results of any stress testing or scenario analysis will inform future risk identification, assessment, evaluation and management. A range of approaches may be useful, such as:

(a) sensitivity testing;

(b) stress testing based on experience;

(c) reverse stress testing designed to identify a stress scenario that would cause failure;

(d) longer term scenarios (e.g. prolonged low interest rate environment) and short-term scenarios (e.g. natural disasters); or

(e) a combination of scenarios (e.g. a series of less significant events occurring within a short timeframe).

RG 000.103 Stress testing can be used for different objectives, including:

(a) stress testing as an internal risk management tool;

(b) supervisory stress testing as an assessment tool;

(c) surveillance stress testing to identify sources of systemic risk or crisis management; and

(d) stress testing for business restructuring plans.

Note: For further details, see International Monetary Fund, *Macrofinancial stress testing—Principles and practices* (PDF 1.18 MB), August 2012 and the IOSCO Principles of Liquidity Risk Management for Collective Investment Schemes.

Good practice guidance

RG 000.104 Additional strategies that may be implemented by responsible entities to manage risks include:

(a) stress testing and/or scenario analysis of all material risks identified for the responsible entity's business and the schemes it operates;

(b) risk treatment plans; and

(c) compliance plan procedures.

Stress testing and/or scenario analysis of all material risks

RG 000.105 We consider that stress testing and/or scenario analysis of all material risks to a responsible entity's business and the schemes it operates is good practice. A key risk area for testing and analysis is market and investment risk.

Risk treatment plan

RG 000.106 We consider it good practice for responsible entities to have documented risk treatment plans setting out how each material risk will be treated, including:

(a) details of the risk treatment;

(b) the intention or objective of the treatment;

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

(d) 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

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

Compliance plan procedures

RG 000.107 We also consider it good practice for the compliance plan of the scheme to detail procedures for ensuring that the key risks identified for the responsible entity are relevant and are managed. This may be in addition to the existing content obligations under s601HA.

Appendix: Examples of risks and risk treatments

RG 000.108 This appendix lists the risks that we consider most relevant to responsible entities and the schemes they manage. It gives examples of these risks, including specific risks under each category and examples of measures that responsible entities may consider in treating these risks. The examples are not intended to be exhaustive; they reflect common risks and measures we have observed through our regulatory experience. The examples of risks treatments are not mandatory.

Strategic risk

RG 000.109 Strategic risk is any risk that arises from a responsible entity's strategic and business plans.

RG 000.110 Market conditions (e.g. instability or volatility) and market sentiment (e.g. uncertainty) can lead to cost pressures and reductions in cash flow for many responsible entities. This raises risks to the operating model of some responsible entities and may endanger the continuity of particular entities and schemes.

RG 000.111 Developments of new products and systems or changes of strategic direction are examples of strategic risk.

RG 000.112 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 schemes it operates.

RG 000.113 Similarly, consolidation through merger and acquisition activity can raise the risk of unsatisfactory business integration for the merging entities. If the consolidation is not managed appropriately, it could undermine each of the relevant businesses' risk management systems and lead to practical implementation issues, especially if full integration and consolidation may take long periods of time to complete.

Examples of risk treatments

Responsible entities can treat this risk by:

- engaging in regular 'horizon scanning';
- engaging with regulatory bodies; and
- stress testing key assumptions or factors that underpin the business model.

For mergers and acquisitions, responsible entities can implement policies and procedures that ensure consideration is given to:

- the alignment of systems, processes, policies and procedures, and cultures before business integration; and
- appropriate resources and attention for effective implementation under direct supervision of the board during and after business integration.

Governance risk

RG 000.114 Governance risk is any risk that threatens the ability of a responsible entity to make reasonable and impartial business decisions in the best interests of members.

RG 000.115 This risk arises if a responsible entity does not have appropriate processes in place to support sound and transparent decision making that is in the best interests of members and is not adversely influenced by conflicts of interests.

RG 000.116 When considering whether to enter into a transaction with a related party, the interests of the related party may influence the entity's decision making to the detriment of scheme members' interests or the scheme as a whole.

Note: See also Regulatory Guide 76 *Related party transactions* (RG 76).

Examples of risk treatments

Responsible entities can treat this risk by:

- having policies and procedures that guide decision making, including specifying who has the authority to make material decisions;
- certifying compliance regularly;
- implementing policies and procedures that ensure compliance with laws concerning related party transactions;
- getting independent advice on related-party transactions;
- obtaining member approval for related-party transactions;
- appointing independent directors;
- maintaining a diverse board; and
- publicly disclosing appropriate details of the risk management system.

Operational risk

RG 000.117 Operational risk is the risk of loss, for the business or schemes, resulting from inadequate or failed internal processes, people and systems, or from external events.

RG 000.118 Specific operational risks include those relating to:

(a) legal and compliance requirements;

(b) technological resources;

(c) human resources (including key persons);

(d) outsourcing;

(e) transitioning of the business;

(f) any conduct of employees not aligned with the interests or the obligations of the responsible entity; and

(g) fraud.

RG 000.119 Operational risk is relevant to both the responsible entity's business and the schemes it operates.

Overview of operational risk

RG 000.120 Operational risk includes the risk of a responsible entity having insufficient capacity and/or competence 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: 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).

RG 000.121 The factors influencing this risk are often dynamic and evolving, and need to be monitored closely.

Examples of risk treatments

Responsible entities can treat this risk by:

- ensuring material aspects of operational procedures are documented and training is provided;
- periodically testing compliance procedures;
- auditing compliance with policies and processes; and
- in areas where potential conflicts could arise (e.g. valuation, risk management, compliance), segregating these activities from the investment management function with separate reporting lines.

Legal and compliance requirements

RG 000.122 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 its registered schemes 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.

Examples of risk treatments

Responsible entities can treat this risk by:

- documenting compliance plans and arrangements for the responsible entity and the schemes it operates;
- having breach registers and breach notification protocols;
- arranging for ready access to legal advice, whether internal or external; and
- ensuring timely breach reporting to regulators.

Technological resources

RG 000.123 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. This risk may be higher for smaller responsible entities (due to resource constraints) or where the business is heavily reliant on technological resources. There may also be difficulties in assessing the adequacy of technological resources where the responsible entity is part of a corporate group that shares resources.

RG 000.124 Some responsible entities may use resources such as software integration tools, real-time and system-embedded compliance evaluation tools, and cloud-based technologies as part of their compliance and data storage arrangements.

Examples of risk treatments

Responsible entities can treat this risk by:

- implementing disaster recovery and business continuity plans; and
- systematically assessing the adequacy of technological resources, including where the entity forms part of a corporate group and shares resources.

Human resources (including key persons)

RG 000.125 There is a risk that the responsible entity will not have adequate human resources or competence to conduct its financial services business. This risk may arise as a result of resource constraints, a lack of training or an excessive reliance on a small number of key staff.

RG 000.126 Key person risk is often inherent in smaller responsible entities where there is a reliance on the skills and experience of one or two people who are crucial to its operation. The dominance of such key persons can unduly influence a business's culture and may lead to operational decisions being

made that would not be considered appropriate within the responsible entity's risk management system.

Examples of risk treatments

Responsible entities can treat this risk by:

- implementing succession planning to address key person risk;
- training staff to promote competence in the provision of financial services;
- auditing staff skills;
- taking out key person insurance;
- having effective recruitment policies;
- regularly reviewing resource requirements, particularly during periods of growth or change;
- appointing independent directors; and
- maintaining a diverse board.

Outsourcing

RG 000.127 Some responsible entities outsource functions instead of having the required technological or human resources in-house.

RG 000.128 The risk involved with outsourcing can be exacerbated when there is inadequate supervision of these functions, particularly where these functions are outsourced internationally. Failing to adequately supervise outsourced functions can have significant detrimental effects on the reputation of a business. The more critical the outsourced function, the greater the risks involved.

Examples of risk treatments

Responsible entities can treat this risk by:

- implementing effective and comprehensive due diligence processes for choosing suitable service providers;
- having service level agreements;
- monitoring processes to address the ongoing performance of service providers;
- maintaining adequate staff and skill sets in-house to effectively monitor external service providers;
- having mechanisms for dealing appropriately and swiftly with any actions by service providers that breach service level agreements; and
- having policies and procedures to ensure agreements are always formalised and documented.

Transitioning of the business

RG 000.129 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:

(a) appointment of a receiver over assets of the scheme (if a responsible entity becomes subject to external administration); or

(b) a change of responsible entity for the scheme.

Examples of risk treatments

Responsible entities can treat this risk by implementing:

- business continuity plans;
- transition plans to facilitate an orderly transfer of the responsible entity's business in stressed conditions;
- succession planning; and
- policies to ensure clear records identifying scheme assets.

Malicious cyber activity and ensuring cyber resilience

RG 000.130 There is a high risk that a responsible entity may be subject to malicious cyber activity, which is an attempted or actual incident that either:

(a) uses computer technology or networks to commit or facilitate the commission of traditional crimes, such as fraud and forgery—for example, identity or data theft (computer assisted); or

(b) is directed at computers and computer systems or other information communication technologies.

RG 000.131 Cyber resilience is the ability to prepare for, respond to and recover from malicious cyber activity. Resilience is more than just preventing or responding to an attack—it also takes into account the ability to adapt and recover from such an event.

Examples of risk treatments

Responsible entities can treat this risk by:

- conducting regular cyber resilience health checks. For additional guidance, see REP 429;
- updating policies and procedures to reflect current industry and international standards;
- regularly testing information technology (IT) systems; and
- implementing disaster recovery and business continuity plans.

Employee misconduct

RG 000.132 This is the risk of the conduct of employees (deliberately or inadvertently) not being aligned with the interests or obligations of the responsible entity. For example, employees mis-selling financial products or mis-advising investors, causing loss to investors and the responsible entity or schemes (including reputational damage), or both.

Examples of risk treatments

Responsible entities can treat this risk by:

- carrying out comprehensive employment screening;
- implementing a conflicts of interest policy;
- adequately training employees regarding the conflicts of interest policy;
- having appropriate remuneration systems that support risk management and do not create incentives for employee misconduct;
- monitoring employee conduct through, for example, exceptional reporting of unusual events and random review or audit of transaction records;
- maintaining an internal audit function;
- conducting peer reviews;
- having whistleblower policies and procedures;
- electronically monitoring high-risk functions; and
- implementing other controls to prevent misappropriation of client funds, such as co-signing policies.

Fraud risk

RG 000.133 Fraud is dishonest activity causing actual or potential financial loss, including theft of money or other property by employees or persons external to the entity.

RG 000.134 Fraud risk also includes the deliberate creation, concealment, destruction or use of falsified documentation or the improper use of information or position for personal financial benefit. It includes:

(a) bribery and corruption—for example, the acceptance of bribes in exchange for assisting with a fraudulent transaction, such as false investment instructions to a custodian;

(b) collusion—for example, an employee colluding with a custodian to process false investment instructions, causing investors' money to be misappropriated to fake investment accounts;

(c) false documents—as many processes are often document driven, the risk of false documents being used to perpetuate the misappropriation of investor money is a significant threat;

(d) manipulation of IT systems—for example, false payments to suppliers or 'ghost' employees; and

(e) securities fraud—this type of fraud may expose investors to significant losses and includes:

(i) front running;

(ii) penny-stock schemes;

(iii) boiler rooms; and

(iv) microcap stock frauds.

RG 000.135 The following are red flags that may indicate an increased risk of fraud:

(a) penny stocks or unusual over-the-counter (OTC) investments;

(b) investments located in tax havens;

(c) investments lacking in transparency. This might be due to the use of nominee accounts hiding the identity of beneficial owners;

(d) complex company structures surrounding funds resulting in a 'captured fund' scenario;

(e) lack of audited accounts;

(f) lack of independent directors;

(g) any unusual or unexplained adjustments to accounts; and

(h) unusual valuations and asset statements.

Examples of risk treatments

Identification of effective fraud risk treatments relies on the implementation of:

- an enterprise-wide fraud risk management framework that effectively identifies, analyses, evaluates and treats fraud risks affecting its operations; and
- a fraud and corruption control plan that binds all employees' conduct and clearly sets out expectations of employee behaviour, measures used to monitor behaviour, processes for managing conflicts of interest and methods of internal reporting.

Responsible entities can treat this risk by:

- segregating duties, particularly for staff involved in high-risk functions;
- maintaining an internal audit function;
- conducting peer reviews;
- reporting unusual events;
- implementing whistleblower policies, including externally managed hotlines;
- rotating staff involved in high-risk functions;
- requiring dual approvals for significant transactions;

- obtaining regular valuations of underlying assets;
- ensuring transparency of investments;
- being alert to any back-channel or undisclosed commission payments, particularly between investment managers and product providers;
- ensuring regular reporting from external service providers;
- taking care when dealing with products that are not researched and have no proven track record; and
- implementing effective and comprehensive due diligence processes.

Market and investment risk

RG 000.136 Market and investment risk is the risk that a scheme operated by a responsible entity will not meet its objectives.

RG 000.137 Specific investment risks include those relating to:

(a) investment governance and structure;

(b) market conditions;

(c) counterparty failure;

(d) product suitability; and

(e) valuation and pricing.

Investment governance and structure

RG 000.138 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 schemes.

RG 000.139 A risk also arises if a responsible entity's scheme is exposed to a financial product through a multi-layered structure where the scheme invests in an investment vehicle, which in turn invests in another investment vehicle. Such a structure may create difficulties in identifying the scheme's extent of exposure to a particular financial product, or type of product, arising from investment in multiple investment vehicles. This risk may be exacerbated when one or more of the investment vehicles are not subject to the regulation of Australian laws.

Examples of risk treatments

Responsible entities can treat this risk by establishing and implementing an adequate investment governance framework that takes into account:

- whether the scheme will be a liquid scheme and how withdrawals will be made available;

- whether the scheme is exposed to counterparty risk and, if so, monitoring the extent of that risk exposure regularly;
- comprehensive and effective due diligence processes for investment selection when implementing investment strategies; and
- objective measures to monitor the performance of investments at appropriate intervals, provide feedback information to review investments and, if appropriate, update the investment governance framework.

Responsible entities can also implement control processes to track the scheme's adherence to its stated objectives, investment policy and strategy, and other restrictions, and take appropriate action if a breach occurs.

Market conditions and volatility

RG 000.140 There is a risk that the performance of the underlying assets of a scheme will be adversely impacted as a result of changes in market conditions.

RG 000.141 Our regulatory experience indicates that some responsible entities consider disclosure of this risk to investors alone as sufficient. We do not consider 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 uses complete physical replication of the index, we would expect that responsible entities would have processes in place to effectively manage market risk in other circumstances in addition to disclosure.

Examples of risk treatments

Responsible entities can treat this risk by:

- implementing policies and procedures for assessing forecast performance of the assets of the schemes the responsible entity operates on an ongoing basis, to identify whether the performance is consistent with expectations and can withstand a range of stress-tested events; and
- continuously monitoring the market for assets the scheme holds to identify any emerging issues or trends.

Counterparty failure

RG 000.142 There is risk a counterparty will fail to meet its obligations and that the responsible entity cannot put in place a replacement transaction economically and efficiently to meet any ongoing obligations.

RG 000.143 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.

Examples of risk treatments

Responsible entities can treat this risk by:

- having a process for setting up counterparty relationships, including the assessment of creditworthiness and setting of risk limits;
- carrying out due diligence inquiries into counterparties;
- regularly assessing the creditworthiness of the counterparty and the impact of counterparty default on the financial position of the business or relevant schemes;
- adjusting risk limits where required; and
- avoiding excessive reliance on a limited number of counterparties.

Product suitability

RG 000.144 There is a risk that a product design may become unsuited to the needs of current and potential scheme members or the needs of the business.

Examples of risk treatments

Responsible entities can treat this risk by:

- carrying out consumer research on product suitability;
- having consumer warnings and knowledge tests for complex products; and
- regularly assessing ongoing product suitability.

Valuation and pricing

RG 000.145 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.

> Note: Where issue and redemption of scheme interests is permitted, valuation policies may be required to be consistent with ordinary commercial practice and result in a value that is reasonably current: see RG 134. In accordance with s601HA(1)(c), the compliance plan must set out adequate procedures for ensuring that the scheme property is valued at regular intervals appropriate to the nature of the scheme property.

RG 000.146 This risk is generally 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 the market price of scheme assets is more difficult to determine.

RG 000.147 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.

Examples of risk treatments

Responsible entities can treat this risk by:

- implementing 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 issue and redemption of interests);
- carrying out regular independent valuations;
- rotating valuers used to value scheme assets; and
- segregating the internal functions in charge of calculation of net asset value (NAV) and maintenance of accounting records from the investment management function.

Liquidity risk

RG 000.148 Liquidity risk is the risk that the responsible entity will not have adequate financial resources to meet its financial obligations and needs, either:

(a) at the responsible entity level; or

(b) at the scheme level (including meeting the scheme's objectives and members' expectations for redemptions).

At the responsible entity level

RG 000.149 RG 166 sets out the financial requirements for AFS licensees that are responsible entities. In summary, responsible entities must meet:

(a) the standard solvency and positive net assets requirement;

(b) a tailored cash needs requirement;

(c) a tailored audit requirement;

(d) a net tangible assets (NTA) requirement, including requirements for holding at least 50% of the NTA requirement in liquid assets; and

(e) depending on the financial products and services offered, any other requirements set out in RG 166 that apply.

Note: Our general expectation is that the risk management system needs to address the risk that an entity's financial resources will not be adequate. For more information on the financial requirements for responsible entities, see Appendix 2 of RG 166.

RG 000.150 In our regulatory experience, we have seen a number of responsible entities become insolvent and unable to maintain their AFS licences or operate their schemes. 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).

RG 000.151 Such mismatches in the internal and external contexts in which the risk management system is developed give rise to risks that a responsible entity will not have sufficient financial resources to operate its business, including the relevant schemes, in accordance with its strategic and business objectives and those of the schemes.

RG 000.152 If the responsible entity also operates wholesale schemes or superannuation trusts or conducts any other business, the operation of these other schemes, trusts or businesses may affect its cash flow or liquidity and should be taken into account in assessing any liquidity risk.

Examples of risk treatments

Responsible entities can treat this risk by:

- carrying out regular independent valuations;
- rotating valuers used to value scheme assets; and
- internally auditing high-risk areas of the business, including management of liquid assets, pricing of assets and investment.

At the scheme level

RG 000.153 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.

RG 000.154 The importance of good liquidity risk management was 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 subsequent periods.

RG 000.155 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 the misalignment of members' expectations on liquidity and the capacity of the scheme's assets to be realised to meet those expectations.

RG 000.156 Other types of schemes may be subject to specific risks relating to market liquidity that need to be considered by the responsible entity. An example is market liquidity based risks for schemes that have interests quoted on a licensed financial market but which undertake regular issue and redemption, such as exchange traded funds. A risk is that a market is not adequately maintained for the schemes that allows trading at a price at or near the NAV

in line with investor expectations. Responsible entities of these schemes need to identify and address this risk.

Examples of risk treatments

Responsible entities can treat liquidity risk by establishing and implementing an effective liquidity risk management process that incorporates:

- compliance with any specific disclosure requirements that are relevant to the particular scheme. For example, Benchmark 1 and Disclosure Principle 1 in Regulatory Guide 45 *Mortgage schemes: Improving disclosure for retail investors* (RG 45), which applies to unlisted mortgage schemes, and Disclosure Principle 5 for hedge funds in Regulatory Guide 240 *Hedge funds: Improving disclosure* (RG 240);
- appropriate internal thresholds for liquidity, which are proportionate to the redemption obligations and ongoing commitments of the schemes;
- tools to identify an emerging liquidity shortage before it occurs. For example, comparisons of the performance of schemes to their peer groups, including trends in issue and redemption of interests;
- ongoing assessments of the liquidity profile of the assets and liabilities (including the scheme's investor profile and investors' historical and expected redemption patterns) held by the schemes to ensure they will be able to meet investor expectations about redemptions and other ongoing commitments;
- regular assessments of liquidity in different scenarios, including stress testing or scenario analysis;
- the use of tools to manage liquidity (when appropriate) and the regular assessment of those tools. Examples of liquidity risk management tools include redemption fees, suspension of withdrawal requests, redemption gates (a limit on the amount of redemptions), *in specie* transfers (transferring assets of an equivalent amount instead of providing cash proceeds), swing pricing (applying higher transaction costs adjustments on redemptions, reflecting the lack of offsetting issue of scheme interests), minimum or maximum limits on withdrawals, or satisfying withdrawals on a partial or staggered basis;
- access to relevant information about liquidity management for investments, such as information about the investor profile and liquidity management approach adopted by the underlying funds the schemes invest in;
- appropriate oversight of the ongoing liquidity assessments by senior management;
- liquidity practices consistent with industry and international guidance (for additional guidance, see the IOSCO Principles of Liquidity Risk Management for Collective Investment Schemes);
- regular periodic reviews of the effectiveness of the liquidity risk management process and updating the process as appropriate;
- consideration of how any advertising, marketing and distribution of the scheme may impact on liquidity and regular reviews of advertising and

marketing materials to ensure they accurately reflect the scheme's liquidity profile and any redemption rights offered;

- appropriate disclosure in PDSs for the scheme of investor redemption rights, liquidity risks, the liquidity management process and if the responsible entity has the power to use any liquidity risk management tools;
- disclosure to existing investors any material changes to the liquidity risk and the use of liquidity risk management tools;
- consideration of the potential impact of the investment on the scheme's overall liquidity before investments decisions are made; and
- that the frequency of dealing in units in the scheme and investor redemption rights are compatible with the scheme's liquidity profile, investment strategy and portfolio composition.

Market liquidity based risk for quoted schemes

Responsible entities of quoted schemes can manage market liquidity based risk by:

- having appropriate arrangements with a market maker, unless the responsible entity is making a market for the scheme and/or a sufficient number of authorised participants are reasonably likely trade the scheme in order to provide liquidity at or close to NAV on any ongoing basis;
- closely monitoring the scheme's market price on a continuous basis and, if it deviates materially from the NAV, considering suspending trading of the scheme;
- maintaining an up-to-date and reliable indicative NAV; and
- encouraging investors to check the market price against the indicative NAV before they trade and disclosing to investors the risk that there may be times where they cannot sell their interests or sell at a price near the NAV.

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 13/760] (for example)	An ASIC class order (in this example numbered 13/760)
Corporations Act	*Corporations Act 2001*, including regulations made for the purposes of that Act
dual-regulated entities	APRA-regulated RSE licensees that operate schemes
governance risk	Has the meaning given in RG 000.76(b)
IDPS	Investor directed portfolio service, as defined in [CO 13/763]
IOSCO	International Organization of Securities Commissions
liquidity risk	Has the meaning given in RG 000.76(e)
market and investment risk	Has the meaning given in RG 000.76(d)
MDA	Managed discretionary account
NAV	Net asset value
NTA	Net tangible assets, as defined in RG 166
operational risk	Has the meaning given in RG 000.76(c)
PDS	Product Disclosure Statement
PI insurance	Professional indemnity insurance

Term	Meaning in this document
Product Disclosure Statement	A document that must be given to a retail client for the offer or issue of a financial product in accordance with Div 2 of Pt 7.9 of the Corporations Act Note: See s761A of the Corporations Act 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 licensee	A 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
strategic risk	Has the meaning given in RG 000.76(a)

Related information

Headnotes

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

Regulatory guides

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

RG 76 *Related party transactions*

RG 78 *Breach reporting by AFS licensees*

RG 104 *Licensing: Meeting the general obligations*

RG 126 *Compensation and insurance arrangements for AFS licensees*

RG 134 *Managed investments: Constitutions*

RG 166 *Licensing: Financial requirements*

RG 240 *Hedge funds: Improving disclosure*

Legislation

Corporations Act, Pt 7.9, s601FB, 601HA, 912A(1)(d), 912A(1)(h), 912B, 912D

Superannuation Industry (Supervision) Act 1993

Superannuation Legislation Amendment (Service Providers and Other Governance Measures) Act 2013

Class orders

[CO 13/760] *Financial requirements for responsible entities and operators of investor directed portfolio services*

Media releases

15-020MR *ASIC enquires into risk management by responsible entities*

Consultation papers and reports

CP 204 *Risk management systems of responsible entities*

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

REP 429 *Cyber resilience: Health check*

Other documents

SPS 220 *Risk management* (PDF 5.5 KB)

International Monetary Fund, *Macrofinancial stress testing—Principles and practices* (PDF 1.18 MB)

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

IOSCO, *Principles of liquidity risk management for collective investment schemes: Final report* (PDF 231 KB)