

GS 002
(September 2010)

Guidance Statement GS 002
Special Considerations in the
Audit of Risk Management
Requirements for Registrable
Superannuation Entities and
Licensees

Issued by the **Auditing and Assurance Standards Board**



Australian Government

Auditing and Assurance Standards Board

Obtaining a Copy of this Guidance Statement

This Guidance Statement is available on the AUASB website:
www.auasb.gov.au

Contact Details

Auditing and Assurance Standards Board Phone: (03) 8080 7400
Level 7, 600 Bourke Street Fax: (03) 8080 7450
Melbourne Victoria 3000 E-mail: enquiries@auasb.gov.au
AUSTRALIA

Postal Address:
PO Box 204
Collins Street West
Melbourne Victoria 8007
AUSTRALIA

COPYRIGHT

© 2010 Auditing and Assurance Standards Board (AUASB). The text, graphics and layout of this Guidance Statement are protected by Australian copyright law and the comparable law of other countries. Reproduction within Australia in unaltered form (retaining this notice) is permitted for personal and non-commercial use subject to the inclusion of an acknowledgment of the source. Requests and enquiries concerning reproduction and rights for commercial purposes within Australia should be addressed to the Executive Director, Auditing and Assurance Standards Board, PO Box 204, Collins Street West, Melbourne Victoria 8007. Otherwise, no part of the Guidance Statement may be reproduced, stored or transmitted in any form or by any means without the prior written permission of the AUASB except as permitted by law.

ISSN 1833-7600

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

CONTENTS

AUTHORITY STATEMENT	<i>Paragraphs</i>
Application.....	1
Issuance Date	2
Introduction.....	3
Background	6-8
Regulatory Requirements for the RMS and the RMP	9-17
Audit and Review Procedures.....	18
Agreeing on the Terms of the Engagement with the RSE Licensee	19-21
Clarifying the Approved Auditor’s Role.....	22-30
Planning the Audit and Review	31-37
Matters to be Considered During the Audit and Review	38-43
The Auditor’s Audit Report and Auditor’s Review Report	44-50
Conformity with International Pronouncements	51
Appendix 1: Example Engagement Letter	
Appendix 2: Example RSE Licensee Representation Letter	

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

AUTHORITY STATEMENT

The Auditing and Assurance Standards Board (AUASB) formulates Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees* pursuant to section 227B of the *Australian Securities and Investments Commission Act 2001*, for the purposes of providing guidance on auditing and assurance matters.

This Guidance Statement provides guidance to assist the auditor to fulfil the objectives of the audit or assurance engagement. It includes explanatory material on specific matters for the purposes of understanding and complying with AUASB Standards. The auditor exercises professional judgement when using this Guidance Statement.

The Guidance Statement does not prescribe or create new requirements.

Dated: 20 September 2010

M H Kelsall
Chairman - AUASB

GUIDANCE STATEMENT GS 002

Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees

Application

- 1 This Guidance Statement has been formulated by the Auditing and Assurance Standards Board (AUASB) to provide guidance to auditors on matters relating to:
 - (a) the audit of compliance with Risk Management Strategies (RMS) for Trustees of the Registrable Superannuation Entity (RSE) Licensee;
 - (b) the audit of compliance with Risk Management Plans (RMP) of RSEs; and
 - (c) the review of risk management systems (being the relevant processes and procedures) to maintain future compliance with the RMS and RMP.

Issuance Date

- 2 This Guidance Statement is issued on 20 September 2010 by the AUASB and replaces GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees* issued in July 2007.

Introduction

- 3 The audit of compliance with the RMS or the RMP and the review of risk management systems may give rise to a number of special audit considerations. Accordingly, this Guidance Statement clarifies certain responsibilities of the auditor on such engagements, and to provide guidance to the auditor on additional factors which the auditor may consider when planning, conducting and reporting on the audit of compliance with the RMS and RMP and review of the risk management systems of the RSE and the RSE Licensee.

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- 4 This Guidance Statement provides guidance on the existing responsibilities of the auditor of the RSE Licensee and RSE imposed by Australian Auditing Standards (ASA)¹, Standards on Assurance Engagements (ASAE), Standards on Review Engagements (ASRE) and the requirements of the *Superannuation Industry (Supervision) Act 1993* (SIS Act) and the *Superannuation Industry (Supervision) Regulations 1994* (SIS Regulations) but does not add to the auditor's responsibilities contained therein.
- 5 This Guidance Statement is to be read in conjunction with ASAE 3000 *Assurance Engagements Other than Audits or Reviews of Historical Financial Information* and relevant Australian Prudential Regulation Authority (APRA) guidance in this area. This Guidance Statement only applies to APRA regulated superannuation entities and does not apply to self-managed superannuation funds (Australian Taxation Office (ATO) regulated funds).

Background

- 6 On 1 July 2004, the *Superannuation Safety Amendment Act 2004* (the SSA Act) introduced requirements for all superannuation trustees to be licensed and for all superannuation entities to become registered by 30 June 2006. As part of obtaining and retaining a licence, the SIS Act requires a Trustee (the RSE Licensee) to maintain the RMS for its operations and a RMP for each superannuation entity (RSE) managed by the RSE Licensee. Where the RSE Licensee manages several similar funds, it may have very similar or identical RMPs for each RSE, if the risks are similar for each fund.
- 7 The SSA Act introduced sections 29E and 29L in the SIS Act, which require the RSE licensee to maintain the RMS and the RMP for each RSE. The SSA Act also introduced section 113(3)(c) of the SIS Act which requires an opinion by the auditor confirming compliance with the RMS and each RMP for the RSEs, and that the RSE Licensee's risk management systems (being the relevant processes and procedures) are adequate to maintain future compliance with the RMS and each RMP for the RSEs.
- 8 The prescribed format of the auditor's audit reports and review reports are specified in APRA's Approved Form titled

¹ The Australian Auditing Standards (ASAs) referred to in this guidance statement are those ASAs issued by the AUASB in October 2009, which apply to audits of financial reports with reporting periods commencing on or after 1 January 2010.

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

Superannuation Industry (Supervision) Act 1993 Act 1993 (SIS Act)
Section 35C – Approved issued June 2010 for reporting periods commencing on or after 1 July 2009, and subsequent versions.

Regulatory Requirements for the RMS and the RMP

Contents of the RMS

- 9 Before APRA will grant a Trustee the RSE Licence, the Trustee is required to have the RMS in place that satisfies the requirements of section 29H of the SIS Act. Once a licence has been granted, the RSE Licensee is required to maintain compliance with the RMS under the SIS Act.
- 10 In August 2010, APRA issued Prudential Practice Guide SPG 200 – Risk Management² which provides guidance on areas the RMS should include.

SPG 200 paragraph 32, states that a non-exhaustive list of the areas of inherent risk that should be considered in developing the *RSE Licensee's RMS* includes:

- Governance risks;
- Investment risks;
- Solvency Risk;
- Liquidity risk;
- Operational risks;
- Outsourcing risk;
- Agency risk;
- Fraud risk;
- External risks; and
- Any other risks - relevant to the operations of the trustee and its compliance with relevant legislation.

² SPG 200 – Risk Management supersedes Superannuation Guidance Note SGN 120.1 Risk Management July 2004

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

Maintaining and reviewing the RMS

- 11 Section 29HA(1) of the SIS Act requires the RSE Licensee to:
- (a) ensure that at all times the RMS is up to date;
 - (b) ensure that the RMS is reviewed at least once each year to ensure that it complies with section 29H of the SIS Act; and
 - (c) modify, or replace, the RMS in accordance with section 29HB of the SIS Act if at any time the RSE Licensee becomes aware that the RMS no longer complies with section 29H of the SIS Act.
- 12 Section 29HA(2) of the SIS Act requires the RSE Licensee to review its risk management strategy within 60 days after the RSE Licensee becomes the RSE Licensee of an additional fund or becomes an acting trustee appointed under Part 17 of the SIS Act. Section 29HC of the SIS Act requires the Trustee to provide a copy of any modified RMS to APRA within 14 days of making the modification.

Contents of the RMP

- 13 The RSE Licensee is required under the RSE licence to register all superannuation entities for which it is responsible. For each superannuation entity that is registered, the RSE Licensee is required to provide the RMP that meets the requirements of section 29P of the SIS Act. Once the RSE has been registered, the RSE Licensee is required to remain in compliance with the RMP under the SIS Act.
- 14 SPG 200 provides guidance on areas the RMP may contain. SPG 200 paragraph 53, states that a non-exhaustive list of inherent risks that could be included in the RMP are:
- Specific fund or trust governance risks;
 - Risks associated with benefit design;
 - Investment risks;
 - Operational risks;
 - Liquidity risk;

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- Valuation risk;
- Outsourcing risk;
- Agency risk;
- Fraud;
- Insurance risk; and
- Any other risk particular to the fund.

Maintaining and reviewing the RMP

- 15 Section 29PA(1) of the SIS Act requires the RSE Licensee of the RSE that has been registered to:
- (a) ensure that at all times the RMP for the RSE is up to date; and
 - (b) ensure that the RMP for the RSE is reviewed at least once each year to ensure that it complies with section 29P of the SIS Act; and
 - (c) modify or replace, the RMP for the RSE in accordance with section 29PB of the SIS Act if at any time the RSE Licensee becomes aware that the RMP no longer complies with section 29P of the SIS Act.
- 16 Section 29PA(2) of the SIS Act requires the RSE Licensee to review the RMP within 60 days after the RSE licensee becomes the (new) RSE Licensee or becomes the acting trustee appointed under Part 17 of the SIS Act. Section 29PC of the SIS Act further requires the Trustee to provide a copy of any modified RMP to APRA within 14 days of making the modification.

Risk Management Systems

- 17 In order to develop the RMS and the RMP for each RSE, the RSE Licensee is required by SPG 200 to establish a risk management system. SPG 200 sets out the main elements of an effective risk management system. These include:

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- A continuous process of identification and assessment of all material risks that could adversely affect current and future operations.
- Risk tolerance objectives/thresholds to be determined regarding the overall risk posed to the trustee's business.
- A process to determine and rank residual risks and in the context of the Trustee's risk appetite, develop a risk management plan to accept, mitigate, transfer or avoid the identified risk.
- Control mechanisms in place to mitigate identified risks and to ensure compliance with the risk management framework.
- A process to be implemented and documented to regularly monitor risk profiles and material exposures to losses according to the nature, scale and complexity of the operations.
- Effective management information systems to be established, maintained and documented commensurate with the size and complexity of the operations.

Audit and Review Procedures

Those Who May Conduct the Audit and Review

- 18 Section 113(1) of the SIS Act, states that "For each year of income, each trustee of a superannuation entity must ensure that an approved auditor is appointed to give the trustee, or the trustees, a report, in the approved form, of the operations of the entity, and the RSE licensee (if any) of the entity, for that year." SIS Regulation 1.04(2) defines an "approved auditor" as follows:

"For the purposes of the definition of "approved auditor" in section 10 of the Act, the following class of persons is specified, namely, individuals each of whom:

- (b) *in the case of an auditor of a superannuation entity other than a self managed superannuation fund:*

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- (i) *is, under Division 2 of Part 9.2 of the Corporations Law, registered, or taken to be registered, as an auditor and is either:*
 - (A) *associated with a professional organisation specified in Schedule 1AAA in the manner specified, in respect of that organisation, in that Schedule; or*
 - (B) *approved by the Regulator under subregulation (2A); or*
- (ii) *is the Auditor-General of the Commonwealth, a State or Territory.”*

Schedule 1AAA includes the following professional organisations:

1. CPA Australia (Member);
2. The Institute of Chartered Accountants in Australia (Member);
3. National Institute of Accountants (Member);
4. Association of Taxation and Management Accountants (Member or Fellow); and
5. National Tax and Accountants Association Ltd (Fellow).

The approved auditor may conduct both the financial report audit and the audit and review required under section 113(3)(c) of the SIS Act.

Agreeing on the Terms of the Engagement with the RSE Licensee

- 19 The approved auditor and the RSE Licensee agree on the terms of the engagement. Such terms may be detailed in a terms of engagement letter³. The auditor has regard to Auditing Standard ASA 210 *Agreeing the Terms of Audit Engagements* when agreeing on the terms of the engagement.

³ Or other suitable form of audit contract.

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- 20 The terms of engagement may also detail arrangements for liaison with the RSE Licensee's audit and/or compliance committee (if applicable), other compliance advisors, and other auditors, including the internal auditor of the RSE Licensee and the auditor of the RSE Licensee's outsourced service provider(s) (if applicable).
- 21 The approved auditor may also use the terms of engagement to clarify the respective roles of the RSE Licensee's directors or individual trustee members, by contrasting the respective statutory responsibilities of the RSE Licensee and the approved auditor under Part 13 of the SIS Act. In particular, it is important to highlight in the terms of engagement the RSE Licensee's obligation to establish and maintain an adequate risk management system and have in place adequate measures and structures to ensure compliance with the RMS, RMP and the SIS Act. The auditor obtains acknowledgment of this obligation from the RSE Licensee's directors or individual trustee members when obtaining agreement on the terms of the engagement. An example engagement letter illustrating such agreement is provided in Appendix 1 to this Guidance Statement.

Clarifying the Approved Auditor's Role

Role of the RSE Licensee

- 22 The RSE Licensee is required under the SIS Act to develop the RMS for its own operations and the RMP for each RSE it manages, together with descriptions of the measures in place to monitor and control material risks identified in the RMS and RMP. These measures are to be in place and fully operational once the RSE licence is granted. Section 29HA of the SIS Act requires the RSE Licensee to ensure that at all times the RMS is up-to-date and to review the RMS at least once a year to ensure that it complies with section 29H of the SIS Act. The RMS is required, under the SIS Act, to be modified once the RSE Licensee becomes aware that the RMS no longer complies with section 29H of the SIS Act. Section 29PA of the SIS Act imposes similar requirements on the RSE Licensee to maintain the RMPs for the RSEs that it manages.
- 23 The RSE Licensee's directors or individual trustee members are responsible, under the SIS Act, for establishing and maintaining an appropriate risk management system. The RSE Licensee's directors or individual trustee members are responsible, under the SIS Act, for identifying risks, setting risk tolerances and designing and implementing processes to manage and monitor those risks. The RSE Licensee's directors or individual trustee members are

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

responsible, under the SIS Act, for determining the adequacy of the RSE Licensee's response to the identified risks.

Role of the Approved Auditor

- 24 Section 113(3)(c) of the SIS Act states that an approved form "must if it is approved for a registrable superannuation entity that is registered under Part 2B, include a statement by the auditor as to whether, in the opinion of the auditor, the RSE licensee of the entity:
- (i) *has complied with each risk management plan for the entity that applied during that year; and*
 - (ii) *has adequate systems to ensure future compliance with any risk management plan for the entity; and*
 - (iii) *has complied with each risk management strategy that applied to the RSE licensee during that year in relation to risks arising from any activities, and proposed activities, as RSE licensee of the entity, and all other activities, or proposed activities, relevant to those activities; and*
 - (iv) *has adequate systems to ensure future compliance with the risk management strategy for the RSE licensee in relation to future risks arising from any proposed future activities as RSE licensee of the entity, and all other proposed future activities relevant to those activities."*

APRA has specified that reports (i) and (iii) above will contain auditor's audit opinions providing reasonable assurance and reports (ii) and (iv) will contain auditor's review conclusions providing limited assurance. The prescribed format of the reports is set out in APRA's Approved Form titled *Superannuation Industry (Supervision) Act 1993 (SIS Act) Section 35C – Approved Form* issued June 2010 for reporting periods commencing on or after 1 July 2009, and subsequent versions.

- 25 The approved auditor's responsibility, under the SIS Act, is to assess whether the RSE Licensee has complied with the requirements contained within the RMS and RMP. This may include whether key controls identified in the RMS or RMP are in place and/or whether any residual risk treatment strategies have been implemented.
- 26 During the course of the audit and review the approved auditor may become aware of material deficiencies in the RMS and RMP and/or material control weaknesses in the RSE Licensee's risk management

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

systems. Section 129 of the SIS Act requires the approved auditor to report these instances to the Trustee and APRA, if the matter affects the interests of members or beneficiaries. SPG 200 paragraph 77 further notes that '*matters identified with respect to the RMS and RMP by the approved auditor would be reported to the Trustee and not excluded by a financial materiality threshold*'. The auditor may also find Auditing Standard ASA 260 *Communication with Those Charged With Governance* useful for this purpose.

Inherent Limitations of Auditing Compliance with the RMS and RMP

- 27 Due to the nature of audit testing and other inherent limitations of an audit, together with the inherent limitations of the RMS and the RMP and their related control measures, there is a possibility that a properly planned and executed audit will not detect all deficiencies in the RSE Licensee's compliance with its RMS and RMP. Accordingly, the auditor's audit reports under section 113(3)(c) are expressed in terms of reasonable assurance and cannot constitute a guarantee that the RSE Licensee's compliance with the RMS and RMP is completely free from any deficiency, or that all breaches have been detected.
- 28 There are also practical limitations in requiring an auditor to perform a continuous examination of compliance with the RMS and RMP and in forming an opinion that the entity has complied at all times with the RMS and RMP during the reporting period. The approved auditor performs tests periodically throughout the financial year to obtain evidence and have reasonable assurance that the Licensee has complied with the written descriptions within the RMS and RMP throughout the period under examination.

Inherent Limitations of Reviewing Systems to Ensure Future Compliance with the RMS and RMP

- 29 Due to the nature of review procedures and other inherent limitations of a review, together with the inherent limitations of the RMS and the RMP and their related control measures, there is a possibility that a properly planned and executed review will not detect all deficiencies in the RSE Licensee's risk management systems (being the relevant processes and procedures) to manage and monitor future compliance with the RMS and the RMP, ie., the twelve month period following the date of the auditor's review report. Accordingly, the auditor's review reports under section 113(3)(c) provide limited assurance and cannot constitute a guarantee that the risk management systems are completely free

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

from any deficiency, or that they will always ensure future compliance with the RMS and RMP.

- 30 There are also practical limitations in requiring an auditor to provide limited assurance that the RSE Licensee's risk management systems are adequate to ensure future compliance with the RMS and RMP. The approved auditor performs procedures appropriate to provide limited assurance on the risk management systems to confirm that they exist at the review date and whether those systems have operated as documented throughout the period and considered risks that may arise from the RSE Licensee's business operations and business planning. APRA's Approved Form titled *Superannuation Industry (Supervision) Act 1993 (SIS Act) Section 35C – Approved Form* defines the future to be the 12 month period following the date the review report is signed. Another inherent limitation is that after the auditor's review reports are signed, the RSE Licensee's risk management processes may change and/or its business operations and business plans may change such that deficiencies may emerge that result in non-compliance with the current RMS and RMP.

Planning the Audit and Review

Materiality

- 31 The auditor considers materiality when:
- (a) determining the nature, timing and extent of audit and review procedures;
 - (b) evaluating the effect of identified breaches of the RMS and/or RMP when forming an auditor's audit opinion on compliance with the RMS and RMP; and
 - (c) considering whether identified weaknesses in risk management systems (being the relevant processes and procedures) may affect the Licensee's future compliance with the RMS and RMP for the purposes of providing an auditor's review report on the adequacy of systems to ensure future compliance with the RMS and the RMP.
- 32 Materiality is addressed in the context of the RSE Licensee's risk management objectives, which are developed having regard to the protection of the interests of the RSE members as a whole. Materiality considerations are therefore viewed within the context of setting out adequate measures that the RSE Licensee is to apply in

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

managing its business operations to ensure compliance with the RMS and RMP.

- 33 The explanatory guidance on the meaning and application of the concept of materiality contained in Auditing Standard ASA 320 *Materiality in Planning and Performing an Audit* is adapted by the approved auditor, as appropriate, to the task of judging adherence to the RMS and RMP and considering other qualitative factors such as conformity with the relevant provisions of the SIS Act. However, it is not possible to give a definitive view on what may constitute a significant or material breach of the RMS or the RMP. The auditor exercises appropriate professional judgement having regard to the RSE Licensee's obligations, together with the size, complexity and nature of the RSE Licensee's activities when determining whether a breach is to be considered significant or material. Section 29JA(1)(b) of the SIS Act requires the RSE Licensee to report all significant breaches of the RMS or the RMP to APRA. Section 129 of the SIS Act requires the auditor to report all detected instances of non-compliance with the SIS Act to APRA if the breach is of such a nature that it may materially affect the interests of members or beneficiaries of the entity. Breaches can be reported to APRA via the breach reporting portal, D2A and/or the auditor's report.
- 34 As identified in ASA 320, when assessing materiality, the auditor considers qualitative factors. The following are examples of qualitative factors that may be relevant:
- The specific requirements of the terms of the engagement.
 - The significance of identified RMS/RMP breaches or weaknesses in existing risk management measures.
 - The nature of any incidents which indicate a weakness in the governance structures.
 - The length of time for which an identified breach or weakness was in existence, both before it was identified and before it was rectified.
 - Indications of systemic and pervasive weaknesses in the existing risk management systems.

Other Planning Considerations

- 35 The approved auditor considers:

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- (a) the date the RMS and RMP were last reviewed by the RSE Licensee and updated, and whether the modified version was provided to APRA in the required timeframe;
 - (b) key responsibilities and risks identified in the RMS and RMP;
 - (c) processes established by the RSE Licensee to identify and manage risks;
 - (d) processes established by the RSE Licensee to identify risks emerging from current or proposed business activities;
 - (e) processes established by the RSE Licensee to monitor adherence to the RMS and RMP; and
 - (f) processes established to ensure that the RMS and RMP comply with the relevant requirements of the SIS Act.
- 36 When evaluating the RSE Licensee's adherence to the RMS and RMP, the approved auditor obtains from the RSE Licensee a copy of each RMS and RMP that applied during the period covered by the audit, together with a written description of the procedures and structures which the RSE Licensee has established to ensure compliance with the relevant RMS and RMP. As the RMS and RMP are high level summaries of the risk management systems the RSE Licensee has in place, the approved auditor obtains sufficient information to enable an understanding of the risk management systems and supporting processes and procedures.
- 37 To further assist in the audit and review, the approved auditor considers various matters when planning the work, including:
- The structure of the RSE Licensee and the nature of its operations.
 - The most recent business plan of the RSE Licensee.
 - The nature and extent of any changes to the RMS and RMP in the reporting period.
 - The nature and extent of any changes to the RSE Licensee's operations.

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- Correspondence with APRA and other regulators including, the results of any recent field visits.
- Reports and other documents submitted to the compliance committee and/or the board of the RSE Licensee regarding the operation of the Trustee and the RSEs and its risk management functions.
- Previous auditor's reports, including the auditor's report on financial statements of the RSE Licensee, the RSE and related management letters.

Matters to be Considered During the Audit and Review

Reasonable Assurance on Compliance with the RMS and RMP

38 As part of the audit of compliance with the RMS and RMP and review of the risk management systems for compliance with the RMS and RMP, the approved auditor considers the measures in place which relate to the RSE Licensee's monitoring of, and reporting on, specific matters incorporated into the RMS and RMP. Such a consideration may include the following matters:

- Whether breaches of the RMS and RMP have been detected and reported by the monitoring systems implemented by the RSE Licensee. Where breaches of the RMS and or RMP have been detected, the approved auditor considers whether such breaches are material either in themselves, or where they are of a recurring nature and have not been rectified, whether their cumulative effect renders them to be a material non-compliance.
- Identifying systems which the RSE Licensee uses to ensure that business units and staff comply with the measures in the RMS and RMP on a day to day basis.
- Whether the RSE Licensee has a process in place to identify and review the risks arising from its business processes and operations on a periodic basis so as to ensure that its RMS and RMP remain up-to-date at all times.
- Testing of selected controls identified in the RMS and RMP.

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- 39 As part of the audit of compliance with the RMS and RMP the approved auditor may seek the following types of information and documentation to the extent relevant:
- Documentation that identifies the policies and procedures that are in place to manage identified risks and representations that policies and procedures have been complied with.
 - Details of changes to the RMS and RMP and related policies and procedures and the reasons for the revisions.
 - Minutes of the meetings of Board and sub-committees that are responsible for monitoring compliance with aspects of the RMS and RMP and the RSE Licensee's risk management framework.
 - Reasons for changes to outsourced service providers and documentation of the tender process to the extent that this impacts upon the material risks identified in the RMS and/or RMP.
 - Results of monitoring of outsource service providers.
 - Reports from outsourced service providers confirming compliance with the service level agreements.
 - Breach registers and complaints registers and follow up actions taken to the extent that recorded items may indicate a failure to comply with the RMS or RMP.
 - Training registers and new responsible officer induction processes.
 - Internal audit reports.
 - Results of disaster recovery and business continuity planning and testing.
 - Conflicts register.
 - Business plan of the licensee.

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- Certifications made by the licensee and relevant supporting documentation to substantiate compliance with the RMS and RMP during the reporting period.
- Internal and external incident and breach reports.
- Other supporting evidence to confirm that the controls identified in the RMS and RMP have been in place during the reporting period.
- Unit pricing systems, procedures and controls.

The above is not meant to represent a complete list and there may be other evidence that is relevant to the specific circumstances of each RSE Licensee and the RSEs it manages.

- 40 Some RSE Licensees may have a number of RSEs with very similar RMPs, or a master RMP covering more than one RSE under the control of a single RSE Licensee. In such situations, the approved auditor may choose to design and apply common audit tests and review procedures across more than one RSE, as considered necessary in the circumstances. However, the approved auditor ensures that the tests and procedures which are applied are representative across all RSEs under the master RMP, and that they provide sufficient and appropriate evidence to enable the expression of the auditor's audit opinion on each RMP as required by section 113(3)(c) of the SIS Act.
- 41 In addition, the RSE Licensee may choose to outsource various functions (e.g. administration and custody services) and engage external service providers. The RSE Licensee includes measures in the RMS and RMP to supervise these service providers, given that the RSE Licensee is considered to be accountable under the SIS Act both for the compliance of those activities which are performed within the RSE Licensee itself, as well as those functions which may be outsourced to external service providers, which where material will be subject to a 'complying' service agreement.
- 42 In such circumstances, the approved auditor reviews compliance with the measures in the RMP and RMS relating to the supervision by the RSE Licensee of its service provider(s). However, the approved auditor is not expected to conduct an audit of the service provider(s), as it is the obligation of the RSE Licensee and not the approved auditor, to ensure that the service provider(s) adhere to the RSE Licensee's RMS and RMP for each RSE under its control. The

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

auditor may also be mindful of the ‘access to premises’ clause contained in any material service agreement. In this context, the auditor has particular regard to matters raised in Auditing Standard ASA 402 *Audit Considerations Relating to an Entity Using a Service Organisation*.

Limited Assurance on Adequacy of Systems to Ensure Future Compliance with the RMS and RMP

43 As part of the review of the risk management systems (being the relevant processes and procedures) to assess the ability of the RSE Licensee to maintain compliance with the RMS and RMP the approved auditor may seek the following types of information and documentation to the extent relevant:

- The most recent business plan of the RSE Licensee and confirmation of the activities it proposes to undertake in the 12 months following the review.
- Details of proposed changes to the RMS and RMP which reflect initiatives identified in the business plan.
- Minutes of meetings of the Board and sub-committees that are responsible for monitoring compliance with aspects of the RMS and RMP (since the end of the reporting period).
- Confirmation of the use of experts by the RSE Licensee where appropriate.
- Progress reports on major business or operational initiatives.
- Proposed future activities, changes to its business plan or any other significant changes to its current activities or operations identified from enquiries of the RSE Licensee and/or management.
- Whether the RSE Licensee has a process in place to identify emerging risks arising from its current or proposed activities.

The above is not meant to represent a complete list and there may be other evidence that is relevant to the specific circumstances of each RSE Licensee and the RSEs it manages.

The Auditor's Audit Report and Auditor's Review Report

- 44 Prior to issuing the auditor's audit reports on compliance with the RMS and RMP and the auditor's review reports on the risk management systems, the auditor may seek a written representation from the RSE Licensee's directors or individual trustee members which contain their assertions that the RSE Licensee has complied with the RMS and RMP during the financial year, and that the RSE Licensee has adequate systems to ensure future compliance with the RMS and RMP. This representation will include a statement to the effect that the RMS and RMP have been updated to reflect identified risks arising from proposed future business activities after the assessment of possible risks emerging from those activities by the RSE Licensee and the assistance of outside experts if required. An example representation letter is provided in Appendix 2 to this Guidance Statement.
- 45 Reports required to be issued under section 113(3) of the SIS Act are required to be issued no later than 4 months after the financial year end of the RSE. The auditor's audit reports and review reports are required to be addressed to the RSE Licensee. The auditor's audit reports and review reports on the RMP are available to RSE members on request via the RSE Licensee.
- 46 The auditor's audit reports on the RMS and RMP will be for the year of income of the fund. The auditor's review reports will be expressed as being for "the twelve month period following the date of this review report". Where the licence is granted during the financial year, the auditor's audit report will be for the period commencing on the date the licence was granted to the end of the financial year.
- 47 Where the financial year of the RSE Licensee and the RSE differ, it may be appropriate to align the RMS and the RMP audit reporting periods.
- 48 When reporting on the matters required by section 35C, the auditor adheres to APRA's Approved Form titled *Superannuation Industry (Supervision) Act 1993 (SIS Act) Section 35C – Approved Form* issued June 2010 for reporting periods commencing on or after 1 July 2009, and subsequent versions. If the auditor is required to modify the audit report because of a material breach of the RMS or RMP or because of some ongoing material weakness in the adequacy of systems to manage and monitor future compliance, the auditor refers to Auditing Standard ASA 705 *Modifications to the*

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

Opinion in the Independent Auditor's Report, which may be helpful when drafting the modified audit reports or review reports.

- 49 Evidence gathered to support the auditor's audit opinions and review conclusions is documented in accordance with Auditing Standard ASA 230 *Audit Documentation*. APRA may seek to review the approved auditor's working papers to obtain an understanding on how the approved auditor's views were formed and APRA has stated that it expects the documentation to be consistent with the requirements of the Australian Auditing Standards.
- 50 Where the RSE licensee has trusteeship of Small APRA Funds (SAFs) and has used the same RMP for each SAF (where specific requirements have been met), it is acceptable to APRA, as noted in the instructions to APRA's Approved Form titled *Superannuation Industry (Supervision) Act 1993 (SIS Act) Section 35C – Approved Form* issued June 2010 for reporting periods commencing on or after 1 July 2009, and subsequent versions, to issue one auditor's audit report on the RMP provided that all SAFs to which the RMP applies are identified by the auditor.

Conformity with International Pronouncements

- 51 There is no equivalent International Auditing Practice Statement (IAPS) or Auditing Standard to this Guidance Statement.

Appendix 1

EXAMPLE ENGAGEMENT LETTER

The following example audit and review engagement letter is for use as a guide only, in conjunction with the considerations described in this Guidance Statement, and will need to be varied according to individual requirements and circumstances.

To [the governing body of the Trustee (e.g. the directors or individual trustee members)]:

Engagement Letter for Risk Management Strategy and Risk Management Plans

Australian Auditing Standards require that there is a common understanding in writing, between the auditor and the client as to the terms of the audit engagement. Accordingly, following our recent discussions with you, we set out below brief details of our responsibilities as auditors and our understanding of the services you require us to perform. This letter relates to the audit of compliance with the Risk Management Strategy for [name of Trustee] (“Trustee”) and to the following superannuation entities’ Risk Management Plans:

- [Name of Superannuation Fund]
- [Name of Superannuation Fund]

We will also conduct a review of the Trustee’s systems which are designed to manage and maintain future compliance with the RMS and RMP.

Audit and Review

Our function as auditor under section 113(3)(c) of the *Superannuation Industry (Supervision) Act 1993* is to examine and report on the Trustee’s Risk Management Strategy (“RMS”) and each superannuation entity’s Risk Management Plan (“RMP”) which has been supplied to us by the Trustee. We are required to report whether:

- The Trustee has complied with the RMS in all material respects for the year ended [date].

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- The Trustee has complied with the RMP for each superannuation entity in all material respects for the year ended [date].
- Based on our review, which is not an audit, nothing has come to our attention that causes us to believe that the Trustee does not have adequate systems, to manage and monitor future compliance with the risk management plan of each superannuation entity.
- Based on our review, which is not an audit, nothing has come to our attention that causes us to believe that the Trustee does not have adequate systems, to identify future risks arising from proposed future activities and to manage and monitor future compliance with the risk management strategy.

As auditors we are not responsible for the identification of risks, design, documentation, operation and monitoring of the RMS and RMP, nor for the adequacy of controls, risk assessments contained in the RMS and RMP, including the relevant internal control systems, policies and procedures and compliance, including future compliance therewith. These duties are imposed on the Trustee by the *Superannuation Industry (Supervision) Act 1993*.

The work undertaken by us to form an opinion is permeated by judgement, in particular, regarding the nature, timing and extent of the audit and review procedures for gathering of audit and review evidence and the drawing of conclusions based on the audit and review evidence gathered. In addition, there are inherent limitations in any audit and review, and these include the use of testing, the inherent limitations of any internal control and compliance structure, the possibility of collusion to commit fraud, and the fact that most audit evidence is persuasive rather than conclusive. As a result, our audit can only provide reasonable, not absolute assurance, that in all material respects the Trustee, as the registered entity, has complied with the RMS and RMP presented to us by the Trustee and our review can only provide limited assurance that the Trustee has adequate systems to manage and maintain future compliance with the RMS and RMP.

In accordance with normal practice, our audit and review will be planned primarily to enable us to express our professional opinion and reach conclusions. It should not be relied on to disclose fraud or error, but their disclosure, if they exist, may possibly result from the audit and review tests we undertake.

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

Procedures

The work we do to enable us to form our opinion on the auditor's audit reports and conclusion on the review reports will include the following:

- Auditing compliance with the relevant RMS and RMP to ensure that they are up-to-date and approved by the Trustee.
- Reviewing the processes (including monitoring and reporting procedures) the Trustee has in place to ensure ongoing compliance with the RMS and RMP and the law and other licence conditions.
- Reviewing the evidence supporting the Trustee's attestation in the APRA annual return in relation to compliance with the RMS and RMP.
- Testing the controls in place used by the Trustee to manage the risks identified in the RMS and RMP.

The auditor's review report on future compliance defines "future" as the twelve month period following the date of the review report.

In considering the systems which the Trustee has to identify future risks arising from its proposed future activities, we will assess the reasonableness of the processes and procedures used by the Trustee to identify risks which arise from current business operations. In this regard we will review the current business plan and confirm the activities which the Trustee proposes to undertake in the 12 months following the date of the review.

After the completion of our auditor's audit report and review report, it is our normal practice to report any matters of significance together with suggestions for their rectification and any other recommendations we may have on the systems and processes in general.

However, we should point out that the examination will be limited to the audit and review implications of the systems and processes and will not constitute a comprehensive study of the identified risks. You cannot assume that any matters reported to you indicate that there are no additional matters, or matters that you should be aware of in meeting your responsibilities.

Our Reporting Responsibilities Under s.129 of the SIS Act

Section 129 of the SIS Act requires us to report to you in writing if we believe a contravention of the legislation has occurred, is occurring or may occur. We need to also advise APRA at the same time as advising the

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

Trustee if we believe the contravention may affect the interest of members or beneficiaries.

Presentation of RMP on the Internet

It is our understanding that the [entity/Trustee] intends to publish a hard copy of the RMP and related auditor's audit and review reports for members, and to present electronically the RMP and related auditor's audit and review reports on its internet web site. When information is presented electronically on a web site, the security and controls over information on the web site should be addressed by the Trustee to maintain the integrity of the data presented. The examination of the controls over the electronic presentation of the RMP on the entity's web site is beyond the scope of the audit of compliance with the RMP. Responsibility for the electronic presentation of the RMP on the entity's web site is that of the governing body of the entity/directors of the Trustee.

Fees

We look forward to full cooperation from your staff and we trust that they will make available to us whatever records, documentation and other information we request in connection with our audits and reviews.

[Insert additional information here regarding fee arrangements and billings, as appropriate.]

Other

This letter will be effective for future years unless we advise you of its amendment or replacement, or the engagement is terminated.

Please sign and return the attached copy of this letter to indicate that it is in accordance with your understanding of the arrangements for our audit and review of the RMS and RMP(s).

Yours faithfully,

(signed)

.....

Name and Title

Date

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

Acknowledged on behalf of [entity] by (signed)

.....

Name and Title

Date

Appendix 2

EXAMPLE RSE LICENSEE REPRESENTATION LETTER

[Trustee Letterhead]

[Addressee – Auditor]

[Date]

This representation letter is provided in connection with your audit of compliance with the Risk Management Strategy (RMS) for [name of Trustee] (“Trustee”) and to the following superannuation entities’ Risk Management Plans (RMP):

- [Name of Superannuation Fund];
- [Name of Superannuation Fund];

and including your review of the Trustee’s systems to manage and maintain future compliance.

We acknowledge our responsibility for the identification of risks, design, documentation, operation and monitoring of the RMS and RMP, the adequacy of controls, risk assessments contained in the RMS and RMP, including the relevant internal control systems, policies and procedures and compliance, including future compliance therewith. These duties are imposed on the Trustee by the *Superannuation Industry (Supervision) Act 1993*.

We confirm that to the best of our knowledge and belief, the following representations made to you during your audit and review.

[Include representations relevant to the entity. Such representations may include the following examples.]

- 1 We have provided you with:
 - (a) copies of the RMS and RMP in force during the year ended [date], relevant business plans, policy and procedure documents, breach registers, other information,

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

- explanations and assistance necessary for the conduct of the audit and review; and
- (b) minutes of all meetings of the [audit and compliance committee and/or other relevant committees].
- 2 There:
- (a) has been no fraud, error, or non-compliance with laws and regulations involving management or employees who have a significant role in the internal control structure;
- (b) has been no fraud, error, or non-compliance with laws and regulations that could result in non-compliance with the RMS and/or RMP; and
- (c) have been no communications from regulatory agencies concerning non-compliance with, or deficiencies in, risk management systems that could have a material effect on future compliance with the RMS and RMP.
- 3 We have established and maintained an adequate internal control structure to facilitate compliance with the RMS and RMP, and adequate records have been maintained evidencing on-going compliance. There are no known breaches of compliance with the RMS and RMP that have not been properly recorded in the breach registers provided to you.
- 4 The business plan(s) provided to you adequately reflect the Trustee's proposed activities over the next 12 months. We have no plans or intentions that may materially impact future compliance with the RMS and RMP. [or] Material risks that arise from activities proposed in the business plan(s) have been factored into proposed changes to the RMS and/or RMP.
- 5 There are no violations or possible violations of laws or regulations the effects of which should be considered for disclosure to any regulator or which would impact compliance with the RMS and RMP.
- 6 No events have occurred subsequent to [reporting period date] that would impact the Trustee's ability to manage and maintain future compliance with the RMS and RMP.

Guidance Statement GS 002 *Special Considerations in the Audit of Risk Management Requirements for Registrable Superannuation Entities and Licensees*

We understand that your examination was made in accordance with Australian Auditing Standards, as applicable, and was, therefore, designed primarily for the purpose of expressing an opinion on compliance with the RMS and RMP and our ability to manage and maintain future compliance, and that your tests of our records and controls and other auditing procedures were limited to those which you considered necessary for that purpose.

Yours faithfully

[Name of signing officer and title]