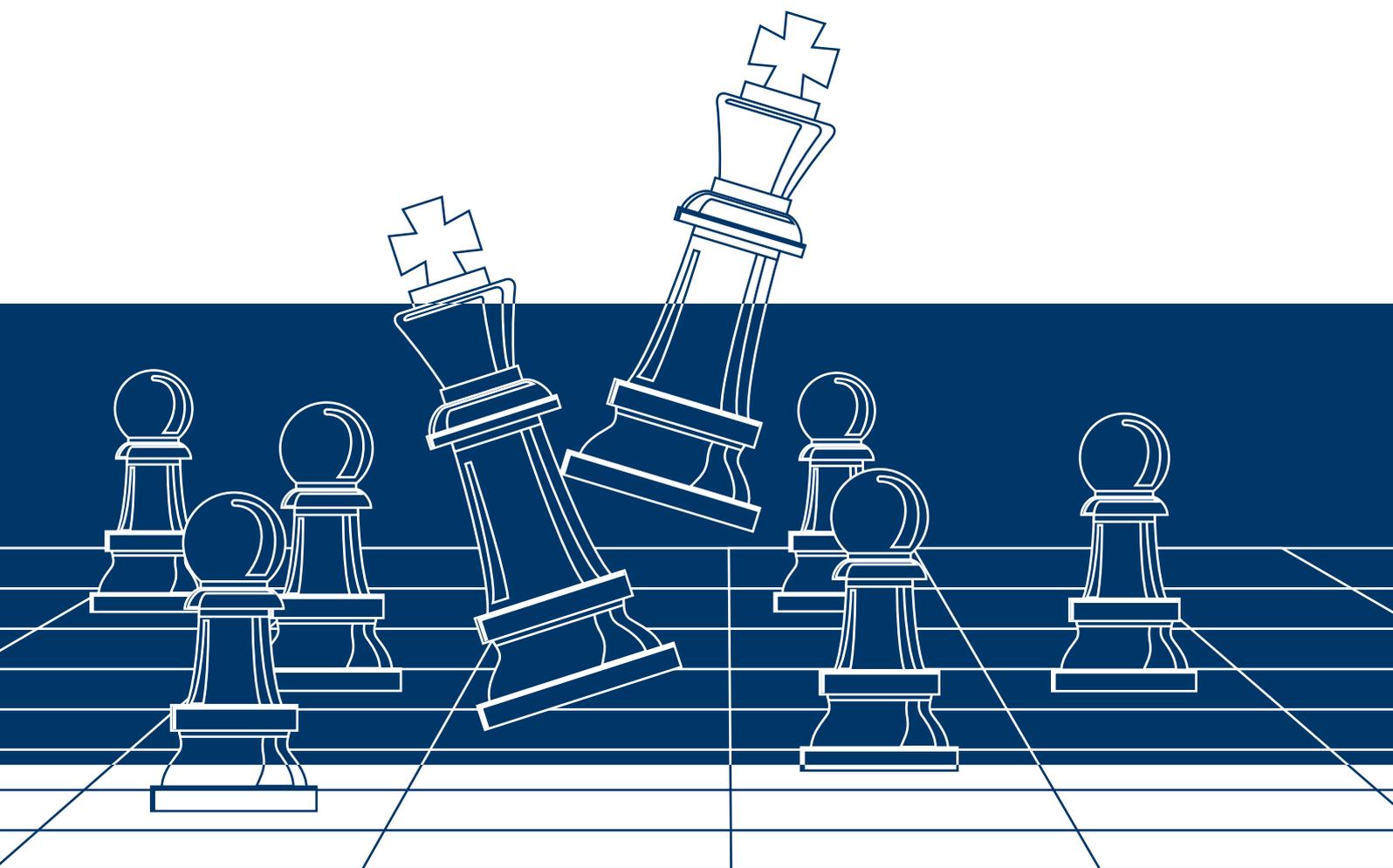


GOVERNANCE TOOLKIT

Risk Management

Version 1: 1 October 2016



THIS TOOLKIT PROUDLY SUPPORTED BY



Australian Institute of Superannuation Trustees

Purpose of the Governance Toolkits

AIST has developed the Governance Toolkits to assist **Trustees** with maintaining strong prudential frameworks. They are created specifically to assist **AIST** members and are a benefit of membership.

The Toolkits contain functional tools such as diagrams, decision trees, flowcharts and checklists, to assist **Trustees** with understanding and applying their legal obligations, regulatory guidance and **AIST** governance guidelines.

How to use this Toolkit

The Risk Management Toolkit is designed to assist **Trustees** with understanding and implementing the Australian Prudential Regulation Authority's (**APRA**) Prudential Standard SPS 220 *Risk Management* (**SPS 220**).

Tools

| | |
|---------------------------------|--|
| Obligations Map | showing the source of the risk management requirements and how they interconnect with the broader regulatory framework |
| Implementation Flowchart | to implement risk management obligations |
| Checklists | <ul style="list-style-type: none">– to develop a Risk Management Framework (RMF)– to develop a Risk Management Strategy (RMS)– to develop a Risk Appetite Statement (RAS)– to prepare the Risk Management Declaration (RMD) |
| Dictionary | Words in bold font are defined in a Dictionary at the back of the Toolkit. AIST recommends that members of the Board and other relevant staff familiarise themselves with the key concepts in the Dictionary. |
| Alerts | <p>Symbol  is used to identify a legal requirement, which have been outlined in the Obligations Map below. It is expected that the Board is able to satisfy all of these legal requirements. If the answer is “NO” to any of the questions in the checklists, the RSE licensee should reconsider the issue and address the requirements necessary so as to satisfy itself that it can provide a positive response to the issue.</p> <p>Symbol  is used to identify an issue that needs particular care. It may denote:</p> <ul style="list-style-type: none">– An issue or uncertainty arising from different, overlapping requirements; or– A matter that requires care in interpretation or application to a Trustee's particular circumstances. |
| Workshops | <p>AIST recommends that Trustees consider training workshops to assist them with understanding their duties and the duties of the Trustee directors in relation to risk management.</p> <p>For more information about available workshops, contact info@aist.asn.au</p> |

Warning & Disclaimer

The Toolkit is intended to assist **Trustees** but does not replace or exhaustively replicate primary sources of a **Trustee's** legal obligations, such as general law, legislation, regulations, prudential standards and regulatory guidance.

While the  symbol identifies issues requiring particular care, content without a  symbol should not be regarded as any less significant. The **Trustee** will have to make its own judgments on how to apply the information in this Toolkit and should seek professional advice if uncertain.

Symbol  is used to identify a legal requirement; these have been outlined in the Obligations Map below. It is expected that the **Board** is able to satisfy all of these legal requirements. If the answer is “NO” to any of the questions in the checklists, the **RSE licensee** should reconsider the issue and address the requirements necessary so as to satisfy itself that it can provide a positive response to the issue.

This Toolkit does not constitute legal advice and should not be relied upon to demonstrate compliance with any legal obligation or standard of conduct expected of **Trustees** or their **directors**. While this Toolkit is a valuable tool for a **Trustee** considering its obligations, it will not guarantee compliance or sound prudential outcomes.

Content in this Toolkit is adapted from the **APRA** Prudential Standard SPS 220 – *Risk Management (SPS 220)*, and Prudential Practice Guide SPG 220 – *Risk Management (SPG 220)*.

The information is current as at 1 October 2016. The Prudential Standards and Practice Guides can change and any changes made on or after 1 October 2016 will need to be taken into account.

Further assistance

If you would like further assistance, contact your professional advisers or alternatively contact **AIST** at info@aist.asn.au or PwC at nicole.oborne@pwc.com.

Index

| | |
|----------------------------------|----|
| RSE licensee’s obligations..... | 4 |
| Obligations map..... | 5 |
| Implementation flowchart..... | 6 |
| Risk Management Framework..... | 7 |
| Risk Management Strategy..... | 11 |
| Risk Appetite Statement | 14 |
| Risk Management Declaration..... | 16 |
| Dictionary..... | 18 |

1. RSE licensee’s obligations

1.1 Sources of risk management obligations

SPS 220 establishes requirements for an **RSE licensee** to have systems for identifying, assessing, managing, mitigating and monitoring **material risks** that may affect the **RSE licensee’s business operations** or its ability to meet its obligations to **beneficiaries**. The totality of these systems, including structures, policies, processes and people within an **RSE licensee’s business operations** supporting them, comprise an **RSE licensee’s RMF**.

SPG 220 provides additional guidance for the implementation of **SPS 220**, sets out **APRA’s** expectations with regard to an **RSE licensee’s RMF** and outlines sound practices in relation to the management of risks throughout an **RSE licensee’s business operations**.

The **Board** of an **RSE licensee** is ultimately responsible for having a RMF that is appropriate to the size, business mix and complexity of the **RSE licensee’s business operations** and that enables the **RSE licensee** to implement risk management approaches that appropriately manage different types of risk. The RMF must be aligned with the **RSE licensee’s** business plan.

At the time of finalising this Toolkit we acknowledge that **ASIC** Consultation Paper 263 *Risk Management Systems of Responsible Entities: Further Proposals* was in progress. This paper sets out **ASIC’s** proposed guidance to **RSE licensees** who also hold an Australian Financial Services (AFS) License, on **ASIC’s** expectations for compliance with the AFS licensee’s obligation to maintain adequate risk management systems under section 912A of the **Corporations Act**.

1.2 Key requirements

The following are key requirements of the **RSE licensee** under **SPS 220**:

- (a) Maintain a written business plan that sets out the high-level strategic direction of the **RSE licensee’s** approach to managing its **business operations**; 
- (b) Maintain a **Board**-approved Risk Appetite Statement (RAS) that covers the **RSE licensee’s business operations** and each category of **material risk**; 
- (c) Maintain a **Board**-approved Risk Management Strategy (RMS) that describes the key elements of the RMF that give effect to the **RSE licensee’s** strategy for managing risk; 
- (d) Maintain **technical, human** and **financial resources** at a level that is adequate for the **RSE licensee’s business operations**;  and
- (e) Undertake each year, a review of the appropriateness, effectiveness and adequacy of the RMF where the triennial comprehensive review of the RMF is not scheduled. 

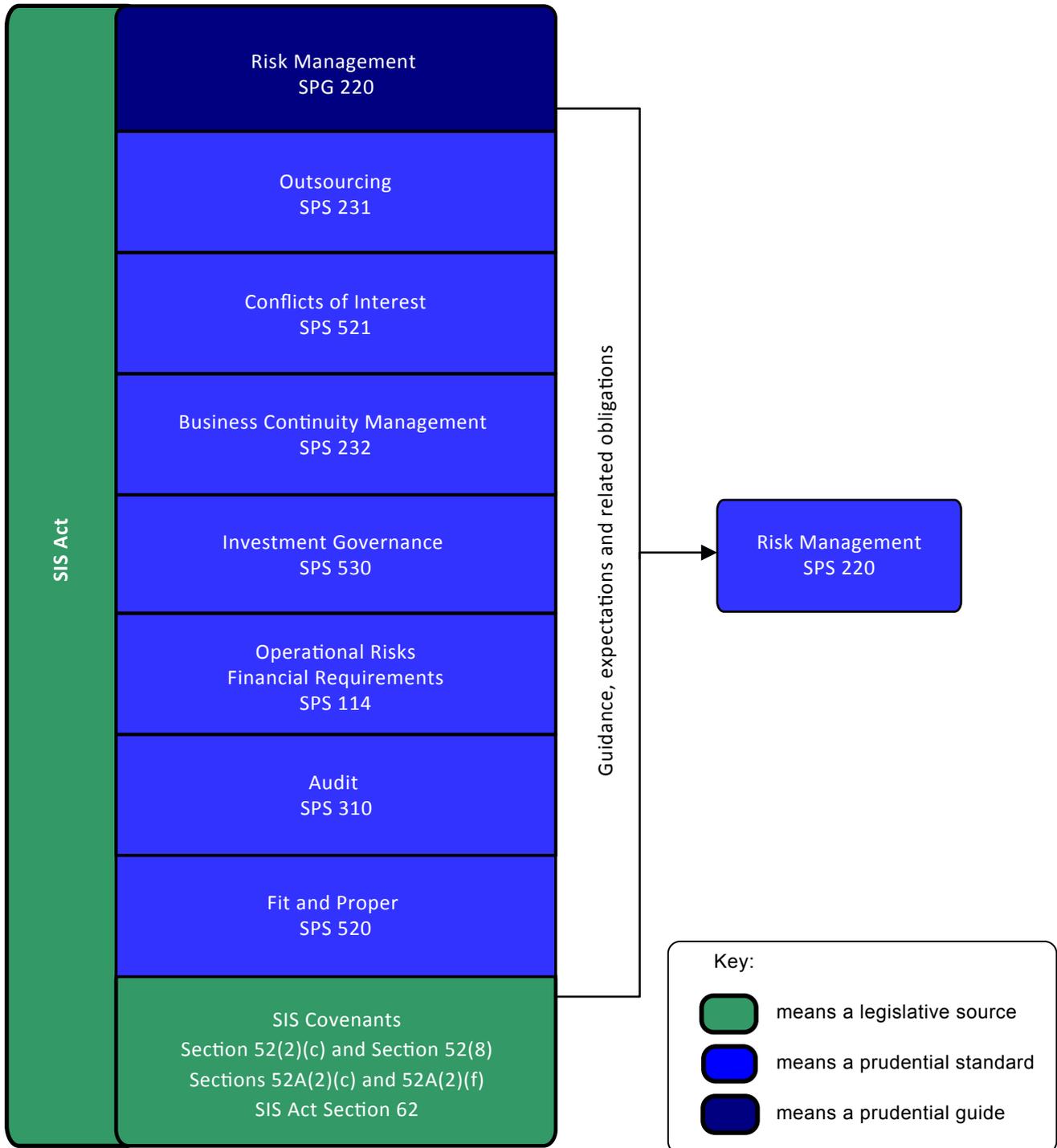
1.3 Obligation to notify APRA

The **RSE licensee** has an obligation to notify **APRA**:

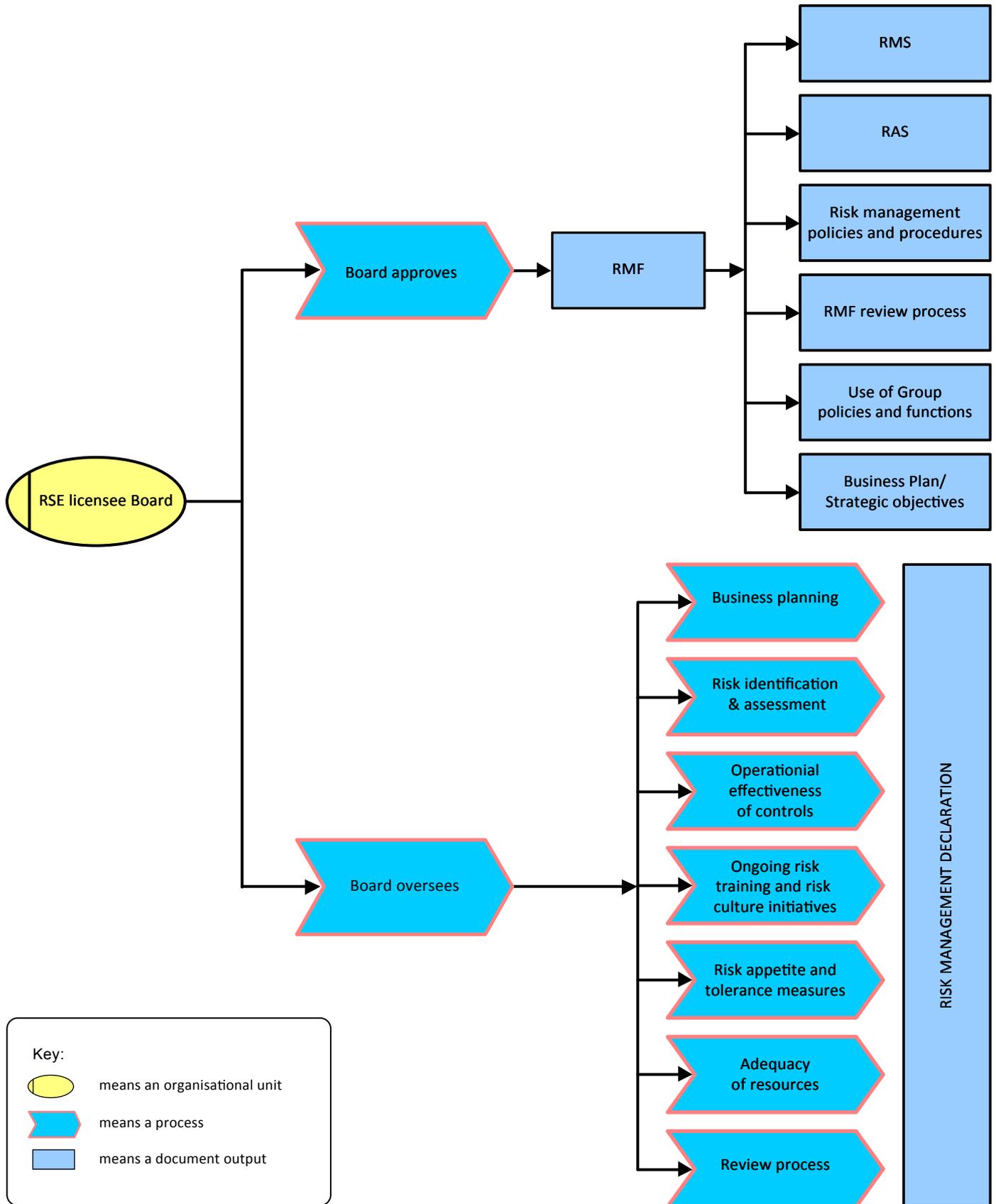
- (a) Within 10 business days of when it:
 - i. Becomes aware of a significant breach of, or material deviation from, the RMF; 
 - ii. Discovers that the RMF did not adequately address a **material risk**. 
- (b) As soon as practicable when it becomes aware of any material change to the size, business mix and complexity of its **business operations**. 

1.4 Obligations Map

The following Obligations Map sets out the breadth of sources from which obligations in relation to risk management arise:



1.5 Implementation Flowchart



2. Risk Management Framework

The RMF must enable the **RSE licensee** to develop and implement strategies, policies, procedures and controls to appropriately manage different types of **material risks**. **APRA** expects that the primary focus of the RMF would ordinarily be the management of risks in a way that is consistent both with the best interests of **beneficiaries** and the maintenance of the sound financial position of the **RSE licensee's business operations**.

The following checklist will assist the **Board** in assessing whether its RMF complies with the minimum requirements in **SPS 220** and with **SPG 220**.

| BOARD SIGN OFF | YES/NO |
|--|--------|
| (a) At a minimum, does the RMF include: | |
| i. The RAS?  | |
| ii. The RMS?  | |
| iii. A designated risk management function?  | |
| iv. Risk management policies, procedures and controls to: | |
| a. Identify and assess material risks ?  | |
| b. Monitor and report on material risks ?  | |
| c. Mitigate and manage material risks ?  | |
| v. Clearly defined and documented roles, responsibilities and formal reporting structures for managing material risks throughout the RSE licensee's business operations ?  | |
| vi. A review process to ensure that the RMF remains effective?  | |
| (b) Can the Board demonstrate that the RMF: | |
| i. Enables the RSE licensee to develop and implement strategies, policies, procedures and controls to appropriately manage material risks ?  | |
| ii. Is appropriate to the size, business mix and complexity of the RSE licensee's business operations ?  | |
| iii. Provides reasonable assurance that each material risk is being prudently and soundly managed?  | |
| (c) As the Board is ultimately responsible for the RMF, are the components of the RMF approved and overseen by the Board ?  | |
| GROUP STRUCTURE | YES/NO |
| (d) Where the RSE licensee is part of a Group and utilises Group policies and functions, has the RSE licensee's Board : | |
| i. Approved the use of Group policies and functions?  | |
| ii. Assessed the Group policies and functions and are they satisfied they give appropriate regard to the RSE licensee's business operations and its specific requirements?  | |
| (e) Where the RSE licensee is part of a Group and any element of the RSE licensee's RMF is influenced, controlled, or subject to approval by another entity in the Group , does the RSE licensee's RMF: | |
| i. Take into account risks arising from Group policy objectives and strategies?  | |
| ii. Clearly identify whether the RSE licensee's RMF is derived wholly or partially from Group risk management policies or functions?  | |

GROUP STRUCTURE YES/NO

iii. Clearly identify the linkages and significant differences between the **RSE licensee's** RMF and **Group** risk management policies or functions? 

iv. Clearly identify the process for monitoring by, or reporting to, the **Group** on risk management including key procedures, frequency of reporting and the approach to reviews? 

RISK GOVERNANCE YES/NO

(f) Does the **RSE licensee** have a formalised risk governance structure to support risk based decision-making and oversight across all its operations?

The risk governance structure is based on the size, business mix and complexity of the entity and would typically be represented by the three lines of defence model.

(g) Has the **RSE licensee** considered adopting a 'three lines of defence' approach to assist in the management and control of risk:

i. First line of defence:

a. Does the **RSE licensee** assign the ownership of risks to business management?

b. Does the **RSE licensee** ensure the identification and management of risks is consistent and integrated with the RMF?

ii. Second line of defence:

a. Does the **RSE licensee** have a risk management function that:

1. Develops risk management policies, systems and processes to facilitate a consistent approach to the identification, assessment and management of risks? 

2. Provides risk support and training to the **Board, Board** Committees (if appropriate) and the first line of defence on risk-related matters?

3. Reviews and challenges the components of the RMF?

4. Assesses the integrity of data and information captured as part of the RMF?

5. Has the necessary authority and reporting structure to the **Board, Board** Committees and senior management to conduct its risk management activities in an effective and independent manner? 

6. Reports to the **Board** and its Committees (if appropriate), on the risk profile of the organisation having regard to its **risk appetite**?

7. Notifies the **Board** of any material deviation from, or material breach of, the RMF? 

8. Is operationally independent from each of the **RSE licensee's** business units? 

9. Has adequately experienced staff with relevant technical knowledge to develop and review the RMF? 

10. Has access to all aspects of the **RSE licensee's business operations** that have the potential to generate **material risk**, including information technology systems and systems development resources? 

b. Where the **RSE licensee** is part of a **Group** and uses the risk management function of another entity in the **Group** the does the function satisfy the 10 requirements listed above? 

c. Where the **RSE licensee** engages an external **service provider** to perform the risk management function does the function satisfy the 10 requirements listed above? 

RISK GOVERNANCE YES/NO

iii. Third line of defence:

a. Does the **Board** and its Committees (if appropriate), obtain independent assurance that the RMF has been complied with and is operating effectively?

APRA notes that the independent assurance function could, for example, include an internal audit and/or a third-party assurance provider. It would be prudent for an **RSE licensee** to have regard to any potential assurance provider’s independence, technical knowledge and experience.

b. Do the relevant **Board** Committees such as Audit or Risk, assist the **Board** in overseeing management’s operation of the RMF?

APRA expects the **Board** to obtain recommendations and advice from **Board** committees, external advisers and management as it considers prudent.

STRATEGIC AND BUSINESS PLANNING YES/NO

(h) Does the **RSE licensee** have a written business plan that:

i. Considers the following:

a. The impact of the **RSE licensee’s business operations** on its risk profile?

b. Potential changes to **material risks**?

ii. Is a rolling plan of at least three but no more than five years duration?

iii. Is reviewed at least annually?

iv. Is approved by the **Board**?

v. Covers the entirety of the **RSE licensee’s business operations**?

(i) Does the RMF provide relevant information on areas of increased risk and changes in the environment to assist senior management and the **Board** in the strategy and business planning process?

ADEQUACY OF RESOURCES YES/NO

(j) Based on an assessment of the business plan, the RMF and the size, business mix and complexity of **business operations** does the **RSE licensee** ensure it maintains adequate levels of:

i. **Financial resources**?

ii. **Human resources**?

iii. **Technical resources**?

The **RSE licensee** may hold the resources itself or have the resources available under an enforceable agreement.

REVIEW OF THE RISK MANAGEMENT FRAMEWORK YES/NO

(k) Does the review process provide for a comprehensive review of the RMF, at least every three years, by an operationally independent, appropriately trained and competent person?

(l) At a minimum, does the scope of the comprehensive review include a review of:

i. The size, business mix and complexity of the **RSE licensee’s business operations** and any subsequent changes to these factors?

ii. The extent of any changes to the external environment in which the **RSE licensee** operates?

| REVIEW OF THE RISK MANAGEMENT FRAMEWORK | YES/NO |
|--|--------|
| iii. Whether the RMF remains appropriate for the RSE licensee's business operations ?  | |
| iv. Whether risk resources are appropriately utilised?  | |
| v. The RAS?  | |
| vi. The RMS?  | |
| vii. All risk management policies and procedures?  | |
| viii. All risk management and internal control systems?  | |
| (m) Does the review process provide for an annual review of the RMF, each year the comprehensive review is not conducted?  | |
|  The annual review may explore particular elements of the RMF in depth on a rotational basis. | |
| (n) Are elements of the RMF reviewed in the context of the RSE licensee's strategic and business planning processes? | |
|  APRA expects that the development and review of the RMS and RAS will generally be performed as part of the strategic and business planning process. | |
| (o) Where developments that materially affect the size, business mix and complexity of business operations are identified outside the review process, does the RSE licensee assess whether the RMF needs to be reviewed or amended to take account of these developments?  | |

3. Risk Management Strategy

The **SIS Act** requires the **RSE licensee** to formulate, review regularly and give effect to a RMS.

APRA acknowledges that the strategy to manage each **material risk** category is likely to differ according to the size, business mix and complexity of the **RSE licensee**. **APRA** expects an RMS to contain sufficient information to communicate, in general terms, the **RSE licensee's** approach to risk management. Further, it is envisaged that the RMS would assist the effective review of the RMF.

The following checklist will assist the **RSE licensee** in assessing whether its RMS complies with the minimum requirements in **SPS 220** and with **SPG 220**.

| BOARD SIGN OFF | YES/NO |
|--|--------|
| (a) Is the RMS approved by the Board ?  | |
| (b) Has the Board approved other risk management policies and procedures described in the RMF?  | |
| <p>APRA Where risk management policies and procedures require Board approval under other Prudential Standards, APRA expects the Board to approve the individual documents.</p> | |
| RMS COMPONENTS | YES/NO |
| (c) At a minimum, does the RMS address the following material risks : | |
| i. Governance risk?  | |
| ii. Investment Governance risk?  | |
| iii. Liquidity risk?  | |
| iv. Operational risk?  | |
| v. Insurance risk?  | |
| vi. Strategic risk?  | |
| (d) Where the RSE licensee conducts business that has a purpose other than superannuation, is the Board satisfied that the RMS covers all material contagion risks that any non-superannuation business might have on the superannuation business?  | |
| <p>Section 62 of the SIS Act provides details of the sole purpose test to identify business that has a purpose other than superannuation. </p> <p>APRA may require an RSE licensee to amend its RMS or develop and maintain a separate RMS with respect to one or more RSEs within its business operations where APRA considers that the RSE licensee's RMS does not adequately cover the risks to that RSE. </p> | |
| (e) Is the Board satisfied that the RMS adequately describes: | |
| i. The process for ensuring continued alignment between the RMF and the business plan?  | |
| ii. The risk management function and relationships between the Board , its Committees (if appropriate) and senior management with respect to risk management?  | |
| iii. The timings for reviewing the RMF and the intended coverage of these reviews?  | |

RISK IDENTIFICATION AND ASSESSMENT

YES/NO

(f) Does the RMS describe the process for:

- i. Identifying **material risks**? 
- ii. Assessing **material risks**? 
- iii. Managing **material risks**? 

(g) Does the RMS describe **material risk** controls? 

(h) Can the **RSE licensee** demonstrate how it determines the materiality of risks? 

A determination of materiality needs to have regard to the **business operations** of the **RSE licensee**, each **RSE**, and the impact the risk may have on **beneficiaries**.

 **APRA** expects the **RSE licensee** to be able to demonstrate how it determines and communicates the 'materiality' of risks, to ensure that a consistent risk management approach is applied across its operations.

(i) Does the risk identification and assessment process consider emerging risks within the **RSE licensee's business operations**?

(j) Does the **RSE licensee** conduct risk and control self-assessments on a periodic basis to:

- i. Identify and assess risk?
- ii. Monitor the control environment?

CONTROL AND MITIGATION

YES/NO

(k) Does the RMS describe the processes for establishing, implementing and testing mitigation strategies and control mechanisms for **material risks**? 

(l) Does the **RSE licensee** consider its appetite for risks when assessing the adequacy and efficacy of controls in managing and mitigating risks?

(m) Where the **RSE licensee** considers engaging a **service provider** to provide a service related to a **material business activity**, does the **RSE licensee** assess what risk mitigation controls that **service provider** has in place?

(n) Does the **RSE licensee** have a system for:

- i. Assessing the design and effectiveness of risk controls?
- ii. Monitoring compliance with risk controls?

(o) Has the **RSE licensee** established escalation procedures for accelerated reporting to the **Board**, **Board Committees** (if appropriate) and senior management of:

- i. Material control failures and exceptions?
- ii. Compliance failures and exceptions?

(p) Has the **RSE licensee** implemented internal audit procedures and external audit arrangements to attest that the risk management and internal control systems in place are:

- i. Operating effectively? 
- ii. Adequate? 

(q) Does the **RSE licensee** have a system to capture risk incidents to assess the incident and identify areas where the controls and mitigation might be enhanced to prevent similar events from occurring?

 **APRA** notes that this information would assist an **RSE licensee** in reviewing the appropriateness of the RMF and, in particular, the application of the RAS.

MONITORING AND REPORTING

YES/NO

- (r) Does the RMS describe the processes for monitoring, communicating and reporting risk issues, including escalation procedures for the reporting of material events and incidents? 
- (s) Does the **RSE licensee** have a system in place for monitoring and ensuring ongoing compliance with all prudential requirements and is this process described within the RMS? 
- (t) Do the **Board** and senior management receive regular and meaningful information on risks relative to the **RSE licensee's** RAS, and the operation and effectiveness of controls?
- (u) Does the **Board** receive regular reporting on:
- i. The exceptions in relation to:
 - a. **Risk appetite?**
 - b. **Risk tolerances?**
 - c. Risk limits?
 - d. Key indicators of risk?
 - e. Risk incidents?
 - ii. Trend analysis of **material risks**, operation of controls and risk assessments?
 **APRA** Through time this information is valuable to understand changes in the business environment that may alter the risk profile of an **RSE licensee**.

RISK TRAINING AND ONGOING AWARENESS

YES/NO

- (v) Has the **RSE licensee** established risk education and awareness training programs for new and current staff?
 **APRA** expects that behaviour is monitored and managed within **risk appetite**, and robust and prudent policies are in place for responding to potentially damaging incidents.
- (w) Does the risk management function facilitate the building of risk management capabilities by providing specialist education, training and advice to **directors**, senior management and staff?

RISK CULTURE

YES/NO

- (x) Does the RMS describe the **RSE licensee's** approach for instilling an appropriate risk culture across the **RSE licensee's business operations**? 
- (y) Does the **RSE licensee** have a risk culture which:
- i. Supports transparency and openness of risk events and issues?
 - ii. Encourages awareness of risks and responsibility for managing those risks?
 - iii. Ensures that appropriate actions are taken in a timely manner where risks are outside of **risk tolerance** limits?
 - iv. Rewards staff for appropriate risk management behaviours?
 **APRA** states that incorporating risk management as a core responsibility within individual roles and responsibilities can assist in building and maintaining a risk culture.
- (z) Are the **RSE licensee's** remuneration policies designed to encourage and incentivise employees to act responsibly, with integrity and in line with the RMF?
 **APRA** believes this initiative will positively influence the desired risk culture.

4. Risk Appetite Statement

The RAS is a fundamental element of the RMF as it articulates the **Trustee's** accepted risk exposure having regard to the **RSE licensee's business operations** and strategic direction.

 **APRA** expects that an **RSE licensee's** RAS would identify the strategic and business risks of its **business operations** and clearly communicate its boundaries and expectations of how much risk it is willing to accept.

The following checklist will assist the **RSE licensee** in assessing whether its RAS complies with the minimum requirements in **SPS 220** and with **SPG 220**.

| BOARD SIGN-OFF | YES/NO |
|---|--------|
| (a) At a minimum, does the RAS articulate the: | |
| i. Trustee's risk appetite?  | |
| ii. Trustee's risk tolerance for each material risk category?  | |
| iii. Process to ensure that risk tolerances are set at an appropriate level?  | |
| iv. Process for monitoring compliance with each risk tolerance and taking appropriate action where the risk tolerance has been breached?  | |
| v. Timing and process for review of the: | |
| a. Risk appetite?  | |
| b. Risk tolerances?  | |
| (b) Is the RAS developed with the involvement of the Board and management as part of the strategic and business planning process? | |
| (c) Can the Board's ownership of the RAS be demonstrated through its active engagement with management in developing and reviewing the statement? | |
|  APRA expects the Board to own the RAS. | |
| (d) Is the RAS approved by the Board ?  | |
| RISK APPETITE AND TOLERANCE MEASURES | YES/NO |
| (e) Does the Trustee's articulated risk appetite represent the risks which the RSE licensee is willing to assume to achieve its strategic objectives and business plan giving consideration to the interests of beneficiaries ? | |
|  Generally risk appetite is expressed as a high level qualitative statement about the attitude and level of acceptance of different risks and where appropriate would include quantitative measures. | |
| (f) Has the Trustee established measurable risk tolerance limits for each material risk category taking into consideration its risk appetite ? | |
|  To facilitate implementation and monitoring of the risk appetite in day-to-day business activities, risk tolerances may be set for more granular risks within each material risk category. Further, where a qualitative risk tolerance is appropriate, it should be well articulated to determine when the risk tolerance has been exceeded. | |
| (g) Does the Board or the Board Committee with the main responsibility for risk: | |
| i. Understand how senior management interprets and applies risk tolerances ? | |
| ii. Consider senior management interpretation and application of the risk appetite to be appropriate? | |

KEY RISK INDICATORS

YES/NO

(h) Has the **Trustee** established defined **key risk indicators** with thresholds around the **risk tolerance**?

⚠️ Traffic light reporting could be used to identify risks that are outside of **risk tolerance** limits.

(i) Does the **Trustee** monitor **key risk indicators** that are outside of **risk tolerance** limits for extended periods of time?

⚠️ When **risk tolerance** limits are exceeded for extended periods of time **APRA** believe that this could indicate complacency or lack of funding in the overall management of risk.

MONITORING AND REPORTING

YES/NO

(j) Does the **RSE licensee** communicate a summary of its RAS throughout its operations including to its **outsourced service providers**?

⚠️ **APRA** expects that the summary should only include relevant information for the intended audience and exclude any confidential or commercial sensitive information.

(k) Is the **Trustee's risk appetite** considered when developing policies in relation to key decision-making processes?

⚠️ **APRA** expects that the RMF is used to identify and assess risks associated with key business activities and the **risk appetite** is considered in the decision making process and implementation of those activities.

(l) Where risk exposure exceeds established **risk tolerance** limits, does the **Trustee's** plan of action to reduce risk exposure to an acceptable level consider:

i. The appropriateness of the set **risk tolerance** limit?

ii. The adequacy and effectiveness of relevant controls?

iii. Timeframe to complete execution of the action plan and follow up procedures?

5. Risk Management Declaration

The **Board** must, on an annual basis, provide **APRA** with a RMD signed by two directors.

The following checklist will assist the **RSE licensee** in assessing whether the RMD process complies with the minimum requirements in **SPS 220** and with **SPG 220**.

| PREPARATION PROCESS | YES/NO |
|---|--------|
| (a) Does the annual RMD to APRA cover the following matters, confirming that in all material respects:  | |
| i. The RSE licensee has systems in place for ensuring compliance with all prudential requirements? | |
| ii. The systems and resources that are in place for managing and monitoring risks, and the RMF, are appropriate for the RSE licensee , having regard to the size, business mix and complexity of the RSE licensee's business operations ? | |
| iii. The RSE licensee has assessed the risks of outsourcing any business activity, and is satisfied that the risks and relevant controls relating to these risks are appropriate to the RSE licensee , having regard to the size, business mix and complexity of the RSE's licensee's business operations and the operational capabilities of the RSE licensee itself? | |
| iv. The risk management and internal control systems in place are operating effectively and are adequate having regard to the risks they are designed to control? | |
| v. The RSE licensee has: | |
| a. An RMS that complies with SPS 220 ? | |
| b. Complied with each measure and control described in the RMS? | |
| vi. The RSE licensee is satisfied with the efficacy of the processes and systems surrounding the production of financial information for each RSE within its business operations ? | |
| vii. The RSE licensee has adequate reporting systems and internal controls supporting the preparation and reporting of accurate financial and statistical information to APRA ? | |
| viii. Information provided to APRA accurately represents the transactions for the financial year and financial position at year end in accordance with the provisions of the SIS Act and the <i>Financial Sector (Collection of Data) Act 2001</i> ? (FSCOD Act) | |
| TIMEFRAME FOR SUBMISSION OF THE RMD | YES/NO |
| (b) Does the RSE licensee have a process in place to ensure the RMD is submitted to APRA within the required timeframe? | |
| (c) Does the RSE licensee ensure that it can submit the RMD to APRA on, or before, the day that the RSE licensee is required to submit annual information under reporting standards made by APRA under FSCOD Act ?  | |
| BOARD SIGN OFF | YES/NO |
| (d) Is the annual RMD signed by two directors of the Board ?  | |
| (e) Prior to signing the RMD, does the Board obtain reasonable assurance from management or seek independent advice on the matters covered by the declaration? | |
|  APRA expects the Board to judge the extent of enquiry required prior to making the declaration. | |

BOARD SIGN OFF

YES/NO

(f) Where management assurance is qualified does the **Board** assess the materiality of the qualifications on the matters covered by the declaration prior to signing?

 It is recommended that **RSE licensees** define the criteria they apply when assessing materiality of issues which may impact on the RMD matters. A criteria assessment will enable stakeholders to understand the entity's appetite for issues impacting the declaration and enable a consistent approach to be applied during the declaration process each year.

(g) If the **Board** qualifies the RMD, does the qualified declaration include a description of any material deviation from the **RSE licensee's** RMF and the steps taken, or proposed to be taken, to remedy those deviations? 

6. Dictionary

AIST means the Australian Institute of Superannuation Trustees.

APRA means the Australian Prudential Regulation Authority.

ASIC means the Australian Securities and Investments Commission.

Beneficiaries is defined under section 10 of the **SIS Act** to mean, in relation to a fund, scheme or trust, persons (whether described in the governing rules as a member, a depositor or otherwise) who have a beneficial interest in the fund, scheme or trust and includes, in relation to a superannuation fund, members of the fund.

Board means the Board of **directors** or group of individual Trustees of an **RSE licensee** and group of individual Trustees has the meaning given in section 10 of the **SIS Act**.

Business operations as defined in **SPS 220** includes all activities as an **RSE licensee** (including the activities of each **RSE** of which it is the licensee), and all other activities of the **RSE licensee** to the extent that they are relevant to, or may impact on, its activities as an **RSE licensee**.

Corporations Act means the *Corporations Act 2001*.

Director of a company or other body is defined under section 9 of the **Corporations Act** to mean a person:

- (a) who is appointed to the position of director or alternate director and is acting in that capacity regardless of the name that is given to their position; or
- (b) unless the contrary intention appears, persons who are not validly appointed as a director if they act in the position of a director or the directors of the company or body are accustomed to act in accordance with the persons instructions or wishes.

Financial resources is described in **SPS 220** and includes those resources which ensure the ongoing solvency and adequate liquidity to support the **RSE licensee's business operations**. These resources are in addition to the operational risk financial requirement required in SPS 114 of the **RSE licensee**.

FSCOD Act means the *Financial Sector (Collection of Data) Act 2001*.

Group means a group comprising of the **RSE licensee** and all connected entities (as defined in section 10 of the **SIS Act**) and all related bodies corporate (as defined in section 50 the **Corporations Act**) of the **RSE licensee**.

Human resources is defined in **SPS 220** and includes, but is not limited to, adequate levels of personnel with the necessary knowledge, skills and expertise to enable the **RSE licensee** to effectively carry out its operations and support its RMF, including its business continuity and disaster recovery plans.

Key risk indicator is a metric for measuring the likelihood that the combined probability of an event and its consequence will exceed the **RSE licensee's** risk appetite.

Material Risk(s) are those risks that may have a significant impact on the **RSE licensee's** ability to achieve its strategic objectives.

Material business activity is defined as an activity that has the potential, if disrupted, to have a significant impact on an **RSE licensee's business operations**, its ability to manage risks effectively, the interests, or reasonable expectations, of **beneficiaries** or the financial position of the **RSE licensee**, any of its **RSEs** or its connected entities.

Outsourcing means an arrangement with any other party to perform, on a continuing basis, a business activity that is a function or responsibility of an **RSE licensee** pursuant to its duties under the governing rules and where the business activity has been delegated to that other party. In this Toolkit, 'Outsourcing' refers to the outsourcing of a **material business activity**.

Service provider means an entity providing the outsourced activities to the **RSE licensee**.

Registrable superannuation entity (RSE) means:

- (a) A regulated superannuation fund; or
 - (b) An approved deposit fund; or
 - (c) A pooled superannuation trust;
- but not a self-managed superannuation fund.

Risk appetite is defined in paragraph 21 of **SPS 220** as the degree of risk that the **RSE licensee** is prepared to accept in pursuit of its strategic objectives, giving consideration to interest of **beneficiaries**.

Risk tolerance is defined in paragraph 21 of **SPS 220** as the maximum level of risk that the **RSE licensee** is willing to operate within expressed as a risk limit that, where possible, is based on a measurable limit of the risk remaining, after taking into account the mitigants for the risk where appropriate.

RSE licensee means an entity that holds an RSE licence granted under section 29D of the **SIS Act**. It is used interchangeably in this Toolkit with Trustee.

SIS Act means the *Superannuation Industry (Supervision) Act 1993*.

SPG 220 means **APRA** Prudential Practice Guide SPG 220 – Risk Management.

SPS 220 means **APRA** Prudential Standard SPS 220 – Risk Management.

Technical resources is defined in paragraph 38 of **SPS 220** and includes, but is not limited to:

- (a) Technical systems, including adequate hardware, data quality and software;
- (b) Systems and resources to ensure protection, security and privacy of confidential, personal and sensitive material;
- (c) Resources to handle transaction processing and other operations;
- (d) Technical resources to handle any significant changes or increases in size, business size or complexity that are planned, forecast or likely to occur;
- (e) A business continuity plan; and
- (f) Records maintenance systems.

Trustee, in relation to a fund, scheme or trust, means:

- (a) If there is a trustee (within the ordinary meaning of that expression) of the fund, scheme or trust – the trustee; or
- (b) In any other case – the person who manages the fund, scheme or trust.

Prepared by:

Australian Institute of Superannuation Trustees

Ground Floor, 215 Spring Street, Melbourne VIC 3000

+61 3 8677 3800

info@aist.asn.au

www.aist.asn.au

PwC

Melbourne

Level 19, 2 Southbank Boulevard, Southbank VIC 3006

Sydney

Darling Park Tower 2, 201 Sussex Street, Sydney NSW 2000

Brisbane

480 Queen Street, Brisbane QLD 4000

Perth

Brookfield Place, Level 15, 125 St Georges Terrace, Perth WA 6000

www.pwc.com.au

