



SHORT TOPIC PAPER TWO

Risk Management

Introduction

As described in the *'Post-implementation review of APRA's superannuation prudential framework'* discussion paper released on 23 May 2018, this is the second paper in a series of short topic papers covering six specific areas of the prudential framework.

This paper, as with the other papers, provides:

- the objectives and key requirements of the prudential and reporting standards (including guidance material) that fall within the relevant topic area;
- links to the final prudential and reporting standards; and
- a series of questions aimed at determining whether the prudential standards (including guidance material) and/or reporting standards have achieved their objectives and continue to remain fit for purpose.

The short topic papers seek to facilitate discussion and consideration of key elements of the prudential framework, and the provision of feedback from stakeholders that will:

- enable appropriate consideration of differing views on the effectiveness of the current prudential framework;
- provide a greater insight into the practical impact of the prudential framework;
- identify areas where improvements may be warranted;
- identify areas that could be streamlined to reduce compliance costs or improve outcomes; and

- ensure that full and appropriate consideration of the relevant areas and topics covered by the prudential and reporting standards is achieved.

APRA is undertaking this comprehensive post-implementation review to determine whether the prudential and reporting standards (and related guidance material) have achieved their objectives and remain fit for purpose. The review is not intended to revisit the original policy intent or objectives of the reforms, and is not seeking to either weaken or strengthen the prudential framework. Rather, APRA wishes to assess whether the prudential framework is operating effectively and efficiently, and to identify and seek to address any unintended consequences or areas for improvement in the framework.

Consultation on this and the other short topic papers will form part of APRA's industry engagement over the course of the review process, which will also comprise roundtables, small group discussions and bilateral meetings.

While formal written submissions close on 26 September 2018, written submissions (formal or informal) on any aspect of the review can be submitted at any time throughout the review process.

Risk Management

Objective of the risk management elements of the prudential framework

The risk management elements of the prudential framework seek to ensure registrable superannuation entity (RSE) licensees have effective frameworks and systems in place to identify and mitigate any material risks that may affect their ability to meet their obligations to beneficiaries.

Scope

In the context of this review, the risk management elements of the prudential framework cover prudential standards – *Prudential Standard SPS 220 Risk Management* ([SPS 220](#)) and *Prudential Standard SPS 310 Audit and Related Matters* ([SPS 310](#)) and their related guidance material which can be found on APRA's website.

Prudential Standards

SPS 220 and its associated guidance material

Objectives and key requirements

The objective of SPS 220 is to seek to ensure that RSE licensees have in place effective risk management frameworks that include systems for identifying, assessing, managing, mitigating and monitoring material risks, and accompanying structures, policies, processes and people to support their effective implementation.

The key requirements of SPS 220¹ are that an RSE licensee must:

- have a written business plan that sets out the high-level strategic direction of the RSE licensee's approach to managing its business operations;
- maintain a Board-approved risk appetite statement;
- maintain a Board-approved risk management strategy that describes the key elements of the risk management framework that give effect to the RSE licensee's strategy for managing risk;
- notify APRA when the RSE licensee becomes aware of a significant breach of, or material deviation from, the risk management framework, or discovers that the risk management framework does not adequately address a material risk; and
- maintain adequate technical, human and financial resources at a level that is adequate for the RSE licensee's business operations.

APRA has issued three prudential practice guides to assist RSE licensees in complying with the requirements in SPS 220, *Prudential Practice Guide SPG 220 Risk Management* (SPG220),

¹ APRA is currently consulting on changes to SPS 220 to better position RSE licensees to deliver outcomes for beneficiaries. These proposed changes do not fall within the scope of this review.

Prudential Practice Guide SPG 221 Adequacy of Resources (SPS 221) and Prudential Practice Guide SPG 223 Fraud Risk Management (SPS 223).

SPG 220 includes commentary on risk culture and its importance in establishing and maintaining an effective risk management framework, including its reflection of an RSE licensee's corporate values as well as attitudes and behaviours of individuals within its business operations.

SPG 220 also outlines APRA's expectations with respect to key elements of SPS 220 including (but not limited to): the determination of material risks (including risks arising from non-superannuation activities); the risk management framework; the risk appetite statement and risk management strategy; control and mitigation mechanisms of an effective risk management framework; review of the risk management framework; and APRA notification.

When considering the requirement in SPS 220 to maintain adequate resources, SPG 221 provides further detail on matters that should be taken into account when: establishing adequate levels of financial resources; demonstrating adequate levels of human resources; and looking at the types of evidence required to demonstrate that an adequate level of technical resources have been maintained.

SPG 223 provides guidance on APRA's expectations for the treatment of fraud risk in an RSE licensee's risk management framework particular 223 discusses key considerations in the development and implementation of a fraud risk management framework. SPG 223 also outlines sound practices in relation to the management of fraud risk throughout an RSE licensee's business operations.

SPS 310 and its associated guidance material

Objectives and key requirements

The objective of SPS 310 is to seek to ensure that the Board and senior management of an RSE licensee obtain independent advice in relation to the operations, financial position and risk controls of the business operations of an RSE licensee. This is intended to assist them in carrying out their responsibilities for the sound and prudent management of the business operations of the RSE licensee.

The key requirements of SPS 310 are:

- an RSE licensee must make arrangements to enable an RSE auditor to undertake his or her role and responsibilities;
- the RSE auditor must audit the financial statements and annual information required under reporting standards made by APRA in relation to each RSE, and review other aspects of that RSE, and provide a report to the RSE licensee of that RSE. The audit and review must cover the RSE licensee's business operations in respect of the RSE;
- an RSE auditor may also be required to undertake special purpose engagements; and
- an RSE licensee must submit to APRA all reports required to be prepared by an RSE auditor under this Prudential Standard.

The supporting prudential practice guide for SPS 310, *Prudential Practice Guide SPG 310 Audit and Related Matters* (SPG 310) outlines sound practices for an effective external audit

framework to assist the Board and senior management to carry out their responsibilities. In particular, SPG 310 covers the obligations of RSE licensees in relation to the appointment and assessment of auditors and the auditor's report, and responsibilities of the RSE auditor in respect of their reporting practices.

Prudential Standard and Prudential Practice Guide Questions

Questions

- 1) What outcomes have been achieved through the implementation of the prudential standards and are these outcomes consistent with the objectives of the standards?
- 2) Have the prudential standards, when read in conjunction with their relevant prudential practice guides:
 - a) provided increased clarity and certainty for trustees in relation to their obligations as trustees of superannuation entities? If not, how could they be improved/amended?
 - b) provided sufficient flexibility for RSE licensees to achieve the objectives in a manner best suited to their business?
 - c) been embedded in the decision-making processes and practices of trustees, and used in practice to support sound decision-making? If not, why not and how could they be improved/amended to achieve this?
- 3) Do the prudential standards and their relevant prudential practice guides continue to remain fit for purpose? If not why not?
- 4) Are any of the principles or requirements contained in the prudential standards or prudential practice guides no longer applicable? If so please elaborate?
- 5) Are there any material gaps in the areas covered by the prudential standards or their relevant prudential practice guides that need to be remedied to achieve the original intent and objectives of the prudential framework?
- 6) Are there any aspects of the prudential standards or prudential practice guides that could be improved to:
 - a) achieve better governance outcomes?
 - b) reduce compliance costs?
 - c) facilitate better supervision of the superannuation industry?
- 7) Are there any ongoing compliance costs associated with the prudential standards and their associated prudential practice guides? If so can you please provide additional information on those costs?