21/10/2022

Gideon Holland
General Manager, Policy
Australian Prudential Regulation Authority
Level 12, 1 Martin Place
Sydney NSW 2000

Via email to PolicyDevelopment@apra.gov.au

Dear Gideon

**AustralianSuper submission to APRA proposals in relation to Operational Risk Management**

AustralianSuper welcomes the opportunity to provide a submission to APRA's discussion paper 'Strengthening operational risk management' and draft prudential standard CPS230 Operational Risk Management (the draft Standard).

As Australia's leading superannuation fund for members, we are the custodian of the retirement savings of around 2.9 million Australians. Because of this, AustralianSuper supports the objectives of strengthening regulated entities' operational risk management, improving business continuity planning and enhancing third-party risk management. We also support the principles-based approach adopted in the draft Standard.

We recommend a number of areas where the draft Standard could be improved to meet its objectives:

1. Some key definitions are unduly prescriptive and as a result may have unintended consequences, including a broader application than intended (see responses to questions 5 and 6 below, regarding the definitions of 'critical operations' and 'material service providers').
2. Applying a one-size-fits-all approach to operational risk across the financial services sector risks creating sector specific anomalies (see response to question 1 below).
3. Consideration should be given to the start date and a transition period should be included. We have concerns about the feasibility and cost of reviewing and renegotiating contracts to meet the terms of the draft Standard in advance of the proposed 1 January 2024 commencement date.

Responses to the questions in the discussion paper and additional comments are provided in the Attachment.

We would be pleased to provide additional information or to discuss this submission in further detail. If that would be of assistance, please do not hesitate to contact Nick Coates, Senior Manager, External Affairs (**ncoates@australiansuper.com**).

Regards

**Sarah Adams**
Group Executive, Strategy, Reputation and Corporate Affairs

T 03 8648 3900
Level 30, 130 Lonsdale Street
Melbourne VIC 3000 Australia
australiansuper.com

# Attachment: Responses to Questions and Additional Comments

## Overall design

**1. Is a single cross-industry standard for operational risk management supported?**

AustralianSuper's preference is for either separate standards for each of the superannuation, banking and insurance industries or one standard but with segmented commentaries for each industry. We note that the discussion paper provides examples for different industries, but the draft Standard does not.

A disadvantage of a cross-industry standard is that some of the obligations are not well tailored to each industry. For example, the draft Standard is prescriptive in terms of the definition of material service providers stating that they include those that provide the following services: "*risk management, core technology services, internal audit, credit assessment, funding and liquidity management, mortgage brokerage, underwriting, claims management, insurance brokerage, reinsurance, fund administration, custodial services, investment management and arrangements with promoters and financial planners*" (paragraph 49). The relevance of many of these services and their link to a critical operation varies between sectors. Please also refer to our response to question 5, below.

**2. Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?**

Fourth parties

Paragraph 47(d) and footnote 13 of the draft Standard introduce the concept of 'fourth parties' defined as a '*party that a service provider relies on in delivering services to an APRA-regulated entity'*. Entities are required to include, in their service provider management policy, their approach to managing the risk associated with any fourth parties that material service providers rely on.

This definition is a new concept. We are concerned that the draft definition could capture a broad range of parties (including for example utility providers and telecommunication providers). We therefore recommend the definition should be tightened to only capture the entities that APRA is most concerned with.

Systemically Important

Paragraph 52(c) of the draft Standard requires an entity to *'take reasonable steps to assess whether the provider is systemically important in Australia'*. Guidance from APRA as to ascertaining whether a provider is 'systemically important' would be beneficial. The discussion paper envisions APRA using registers of material service providers to assess the nature and extent of service providers relied on by each industry with a view to identifying and responding to potential systemic issues (page 25). As this implies, with its visibility across entities and sectors, APRA may be better placed to identify potential concentration risks than individual entities.

Cloud consulting

APRA's Information Paper, 'Outsourcing Involving Cloud Computing Services', dated 24 September 2018, includes APRA's specific expectations about notification and consultation for cloud computing services. We note that the draft Standard does not reference this paper. Given the overlap in subject matter, clarification around APRA's expectations about the impact of a new outsourcing prudential standard on the arrangements for cloud computing services would be beneficial.

Operational risk profile

Paragraph 15(b) provides that an entity must develop and maintain an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits. This suggests a requirement for more specific risk appetites being set with indicators and limits in relation to the use of suppliers in general not just when deciding to insource or outsource. If that is not the policy intent then this should be tightened. If it is the policy intent then it should align with SPS220 to ensure entities' obligations are consistent.

**3. How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs?**

AustralianSuper notes the discussion of proportionality on page 14 of the discussion paper and the two approaches to incorporating proportionality into the prudential framework that are reflected there.

The first approach of allowing entities to use discretion to meet the requirements in a proportionate manner commensurate with the scale and complexity of their business is more desirable as it allows entities to meet their regulatory obligations aligned to their business needs and, in the case of superannuation funds, our purpose to help members achieve their best financial position in retirement.

The second approach of allowing APRA to exempt smaller less complex entities that are deemed to be non-significant financial institutions (non-SFIs) from specific requirements may lead to an uneven playing field between entities.

**4. What are the estimated compliance costs and impacts to meet the new and enhanced requirements?**

The main compliance costs and impacts will relate to:

- the revision of policies, processes, systems and templates to address the requirements of the standard including change management
- identification of material service providers that meet the proposed definition
- engaging with material service providers, including to identify fourth parties and related risks
- reviewing contracts with all material service providers and negotiating changes to those contracts, and
- ongoing costs associated with matters such as due diligence, third party management and reporting.

There will be both implementation costs and ongoing costs. The implementation costs (and timeframe) will vary considerable depending on the transitional arrangements (if any) that are included in the final standard.

A number of additional dedicated resources would be needed for the implementation phase, together with time from existing resources that will need to be diverted from other priorities.

## Specific requirements

**5. How could APRA improve the definitions of critical operations, tolerance levels and material service providers?**

Critical operations

AustralianSuper supports the principles-based approach adopted in the draft Standard. The current list specifying certain operations to be critical operations in paragraph 35 of the draft Standard should be removed. At the very least, only operations that would be critical to all entities covered should be listed. The current list undermines the principled approach to defining a critical operation in paragraph 34 of the draft Standard. The discussion

paper states that 'it is the responsibility of the entity to define, identify and maintain a register of its critical operations' (page 21). This statement is at odds with lists specifying certain operations in paragraph 35 of the draft Standard.

The list of critical operations in the draft Standard does not distinguish between the superannuation sector and other sectors. Paragraph 35 states that "*critical operations include, but are not limited to critical operations payments, deposit-taking and management, custody, settlements, clearing, claims processing, investment management, fund administration, customer enquiries and the systems and infrastructure needed to support these operations."* As currently drafted, the standard would deem each of these to be a critical operation for each entity covered by the standard. By contrast, we note that table 4 of the discussion paper proceeds on the assumption that these operations will only be critical to certain sectors, allocating the operations between the banking, insurance and superannuation sectors.

Tolerance levels

Greater clarity about what is intended by the definition of tolerance levels should be included. Is the standard referring to the Board approving the measures to be applied in determining the tolerance levels which management then apply to each critical process or is it expecting the Board to approve the tolerance level for each critical process? If the latter, we consider that it is more appropriately the remit of senior management, rather than the Board, to approve tolerance levels. As noted in paragraph 12 of SPG 510, *"[s]enior management has responsibility for day-to-day management of an RSE licensee's business operations. This includes the implementation and monitoring of systems, structures, policies, processes, information and oversight arrangements used in managing the RSE licensee."* Similarly, it is unclear why the draft Standard specifically ascribes to APRA broad powers to step in and set tolerance levels (paragraph 38). Greater clarity on the circumstances in which APRA envisions this power would be used would be beneficial.

Material service providers

Paragraph 48 defines material service providers as those '*on which the entity relies to undertake a critical operation or that expose it to material operational risk*'. The drafting of the paragraph should more clearly allow that not all service providers involved in providing critical operations are 'material service providers'. For example, an entity may have many service providers providing a critical operation. In these circumstances, the failure of an individual service provider would not present a risk to business continuity.

As with the definition of 'critical operation', the principled definition of 'material service providers' is inconsistent with the deeming of providers of a list of specified services to be 'material service providers' in paragraph 49.

As an example of the shortcomings of the current approach to defining 'material services providers' in paragraph 48, 'investment management service' providers are deemed to be material service providers in the draft Standard. While investment management services may be a critical operation for AustralianSuper, it does not automatically follow that each provider of investment management services should be considered a material service provider. Over 50% of AustralianSuper's investment management services are insourced. AustralianSuper outsources the balance of its investment management to a number of external managers. The percentage each of these external managers manages varies greatly, with some less than 0.5% of the total assets under management. Furthermore, unless we are invested in a pooled fund with that manager, our managers do not hold the investments themselves, but our custodian does. In these circumstances, the failure of an external investment manager would not have a material operational impact on AustralianSuper.

**6. What additions or amendments should be made to the lists of specified critical operations and material service providers?**

AustralianSuper considers that the lists should be removed. As discussed above in the response to question 5, deeming specific operations and types of providers to fall within these definitions undermines the principles approach to defining 'critical operations' and 'material service providers'. This overly prescriptive approach in paragraphs 35, 49 and 50 fails to account for differences between the entities to which the draft Standard would apply. Specifying certain operations that must be included appears to be at odds with the comment in the discussion paper at page 23 that *'it is the responsibility of the entity to define, identify and maintain a register of its critical operations*'.

By contrast, a principles-based approach to identifying operations and service providers that are captured by these concepts would allow the standard to be applied to each entity commensurate with the nature of each entity's business, operations and outsourcing arrangements. In place of the current lists, it may be more beneficial to provide potential adverse outcomes that an APRA-regulated entity should consider when determining whether an operation is critical or a service provider is material. For example, 'benefit payments cannot be made or are delayed' or 'funds cannot be invested'.

The approach in tables 4 and 5 of the discussion paper, which allocates operations and providers between the banking, insurance and superannuation sectors is preferable to the approach in the draft Standard which allocates all operations and providers to all entities regardless of sector. However, as discussed above in our response to question 5, even this approach may not account for variations in business operations and outsourcing arrangements between entities in the same sector.

**7. Are the notification requirements and the time periods reasonable?**

AustralianSuper supports the proposed notification periods. AustralianSuper notes that the notification period (24 hours) for activating the business continuity plan in paragraph 41 aligns with the current obligation in SPS 232. Similarly, if there is an operational risk event that has a material financial impact or material impact to maintaining critical operations, the period under paragraph 41 is 72 hours, which aligns with the existing CPS 234 obligation.

**8. What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers (if required)?**

Implementing the draft Standard would require a review of existing risk frameworks, service provider arrangements, the identification and review of related entities to which the new standard applies and the renegotiation and execution of contracts.

We note that, at present, the draft Standard includes no transitional provisions for existing contractual arrangements. We recommend that consideration be given to having the requirements of the new standard relating to service provider agreements apply only in relation to arrangements entered into or renewed after the commencement of the new standard. This would significantly reduce the implementation costs and timeframe as entities could uplift their agreements with material service providers as those contracts become due for renewal or as new agreements are negotiated.

Transitional arrangements will be required for evergreen contracts so that they can be renegotiated on commercial terms that are in members' best financial interests. The nature of these contracts are that they are open-ended and the new regime will result in the need to enter into commercial negotiations and therefore may

require additional transitional arrangements. Assuming transitional provisions along these lines are included in the final Standard, we consider it would be reasonable to have a start date that allows at least 12 months for implementation following the release of the final Standard.

At a minimum, the standard should incorporate transitional provisions similar to those used in SPS 231. For example, requiring entities to take reasonable steps to amend existing contracts but allowing non-compliance with the standard where the entity considers it is not in the best interests of members to do so.

The above approaches will also help address the potential scenario where some material service providers (both existing and proposed) do not agree to the contract clauses outlined in the draft Standard. It is unclear what entities will be required to do in such circumstances. If an entity were to be required to source alternative providers, this would involve significant transition costs and higher ongoing costs (including service fees).

## Additional comments on the draft standard (CPS 230)

### Key principles (paragraphs 11 to 14)

Paragraph 14 provides that an APRA-regulated entity must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks. The word "ensure" will make this obligation difficult to comply with as an APRA-regulated entity cannot guarantee the effectiveness of the systems, processes and controls implemented by a third party. As an alternative it may be more appropriate to require APRA-regulated entities to develop and maintain appropriate systems, processes, and controls in place to "help ensure" compliance.

### Role of the Board (paragraphs 19 to 22)

Consideration should be given to the allocation of responsibilities between the Board and senior management in the draft Standard. Specifically, we note the principle on page 18 of the discussion paper that *"senior managers within the business are responsible for the ownership and management of operational risk across an entity's end-to-end processes"*.

In the light of this statement, some functions assigned to the Board in the draft Standard are more appropriate for senior management. This is particularly the case in relation to the approval of the business continuity plan and tolerance levels for disruptions to each critical operation (assigned to the board in paragraphs 21(b) and 37).

In paragraph 21(c), the obligation to review risk and performance reporting may be overly onerous from a practical perspective. We query whether this is already covered in other paragraphs.

Paragraph 21(c) also suggests that decisions related to material service provider arrangements (for example, appointing, changing, ending an arrangement) require Board sign off. We suggest this is also more appropriately the role of Senior Management, with reporting and oversight provided by the Board and/or their sub-committees as appropriate.

The drafting of the standard, including the definition in footnote 7, should allow for delegation of functions assigned to the Board to sub-committees. Similarly, it would be beneficial for guidance to be provided on APRA's expectations regarding 'regular' updates and 'key internal controls' (paragraph 21).

**Operational Risk Management (paragraph 12 and paragraphs 23 to 32)**

There is inconsistency between the 'operational risk' definitions applied in the proposed standard and SPS 114 Operational Risk Financial Requirement, in particular reputational risk:

- the draft Standard defines operational risks as *"risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external drivers and events. Operational risk is inherent in all products, activities, processes and systems"* (paragraph 12). The draft Standard goes on to define operational risks to include *"legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, reputational risk and change management risk*" (paragraph 23).
- by contrast, in SPS 114 (paragraph 6) operational risk is defined as *"the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk but excludes strategic and reputational risk"*.

Paragraph 33(b) requires an entity to take '*reasonable steps to minimise the likelihood and impact of disruptions to its critical operations'*. It is unclear what this would mean in practice.

Paragraph 33(c) provides that an entity '*must maintain a credible BCP that sets out how it would maintain its critical operations within tolerance levels through disruptions, including disaster recovery planning for critical information assets'*. It would be desirable for the guidance to be provided on the level of specificity that should be provided in the BCP. Additionally, the intended effect of including the word 'credible' in relation to the BCP in paragraph 33(c) is unclear.

**Service provider agreements – requirements prior to entry or modification (paragraph 52)**

Paragraph 52(a) suggests that there is a need to run a tender process when entering into a new material arrangement, renewing the arrangement or materially modifying the arrangement. This would not be a practicable outcome. In any circumstances regarding entering into, renewing or materially modifying a contract, an entity needs to take into consideration market conditions, timing requirements and the purpose of the modifications.

Paragraph 52(b) requires the entity to assess the financial and non-financial risks from reliance on a particular service provider, including risks associated with geographic location or concentration of the service provider(s) or parties the service provider relies upon in providing the service. It would be useful to have some more guidelines as to whether these assessments are required in all circumstances, as depending on the ultimate scope of the standard there could be many more service providers that would require these assessments.

Paragraph 52(c) requires an entity to *'take reasonable steps to assess whether the provider is systemically important in Australia'*. We query whether it is appropriate for entities to be responsible for this item. With its visibility across entities and sectors, APRA may be better placed to identify potential concentration risks than individual entities. As discussed above, the discussion paper envisions APRA using the register of material service providers to assess the nature and extent of service providers relied on by each industry with a view to identifying and responding to potential systemic issues (page 25). At the very least, guidance from APRA as to how to ascertain whether a provider is 'systemically important' would be beneficial.

**Service provider agreements – required clauses (paragraphs 53 to 56)**

Paragraph 53 of the draft Standard includes a list of requirements for material service provider arrangements. As an overarching comment, consideration should be given to allowing for scenarios where an entity is satisfied that the absence of such a clause does not materially impact its ability to manage the risks associated with the arrangement. This would reflect the commercial reality that some material service providers may refuse to agree to the inclusion of one or more of the clauses in circumstances where the entity considers that it can adequately address the underlying risks through other controls.

Paragraph 53(b) requires that agreements set out the rights, responsibilities and expectations of each party to the agreement, including in relation to the ownership of assets, ownership and control of data, dispute resolution, audit access, liability and indemnity. We suggest that the word 'expectations' be removed; the words 'rights and obligations' are less ambiguous and are sufficient on their own.

Paragraph 53(c) requires provisions to be included to ensure the ability of the entity to meet its legal and compliance obligations. The scope and intent of this provision is unclear.

Paragraph 53(f) requires that agreements include a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event. We consider that this may not be in the interests of APRA-regulated entities, and, in the case of RSEs, it may not be in members' best financial interests. By way of example, AustralianSuper notes that in contractual negotiations it is often the service provider who wishes to provide for a force majeure clause as generally it is the service provider who has substantive delivery obligations that may be impacted by force majeure events and wants to be excused from performance obligations. Generally, a customer's interests can be better protected through other contractual mechanisms such as obligations on the service provider in relation to performance, business continuity planning, notification of material events and indemnities for breach.

Paragraph 53(g) requires that agreements "*include the ability for the RSE licensee to terminate the arrangement where to continue the arrangement would be inconsistent with the RSE licensee's duty to act in the best financial interests of beneficiaries*". Based on AustralianSuper's experience with negotiating termination for convenience clauses, we consider that many service providers will resist a termination right connected to the best financial interests duty or require long notice periods, rights of first refusal, higher contract pricing or break fees, particularly given such a clause might permit, for example, an APRA-regulated entity to terminate a contract part way through because it receives a better offer from another supplier. Such a termination right could also act as a disincentive to service providers investing in long-term relationships including infrastructure and personnel. AustralianSuper considers that a members' best financial interest assessment should only need to be made at the time of entering into or renewing a contract. While we understand that the intent of this paragraph in the draft Standard is to safeguard members' best financial interests, when applied to contractual negotiations in a commercial market this paragraph may have the opposite effect.

Paragraph 56 states that *"APRA may require an APRA-regulated entity to review and make changes to a service provider arrangement where it identifies heightened prudential concerns"*. Many service providers will likely refuse to agree to a clause that requires them to agree to unknown contract variations that may be required by APRA at some future time or will otherwise increase the contract pricing, require the APRA -regulated entity to pay for any costs associated with the change or require other onerous terms. At a minimum, the paragraph should require APRA to act reasonably and also anticipate a scenario where a material service provider declines to agree to the requested change.