AIST

19 October 2022

General Manager, Policy
Policy and Advice Division
Australian Prudential Regulation Authority

Email: [redacted]

Dear Sir/Madam

Strengthening operational risk management – CPS 230

Brief

AIST is supportive of the consolidation of business continuity and outsourcing into a single operational risk standard, subject to segmentation of industry-specific clauses and guidance.

AIST has specific concerns about the materiality of service providers and the expanded role of the Board proposed by the draft standard, the lack of clarifying guidance and the short timeframe for commencement with no transition period. Considerable work will be required to review and upgrade existing outsourcing frameworks which will be difficult to achieve by the 1 January 2024 commencement date.

About AIST

Australian Institute of Superannuation Trustees is a national not-for-profit organisation whose membership consists of the trustee directors and staff of industry, corporate and public sector superannuation funds. As the principal advocate and peak representative body for the $1.7 trillion profit-to-members superannuation sector, AIST plays a key role in policy development and is a leading provider of research. AIST advocates for financial wellbeing in retirement for all Australians regardless of gender, culture, education, or socio-economic background. Through leadership and excellence, AIST supports profit-to-member funds to achieve member-first outcomes and fairness across the retirement system.

Submission

AIST thanks APRA for the opportunity to provide input to this consultation.

The draft standard contains some increased requirements for data capture and scenario testing, but these are not unwelcome changes as they will provide an uplift in capability and accentuate funds'

business impact analysis processes. Inclusion of downstream service provider considerations will provide a clearer picture of entities' risk exposures and have the potential to trigger review and renegotiation of existing service provider contracts.

Answers to consultation questions

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

We are supportive of the intent behind the consolidation of standards to reduce repetition of similar or identical requirements. Applying a single consolidated prudential standard on operational risk is logical and practical. However, consolidated standards need some level of industry-based segmentation to be explicit about the differences in application between industries. In the absence of segmented commentary, separate standards should be retained to ensure clarity of requirements.

- **In the absence of different industry-specific standards, clauses within the standard that require industry-specific interpretation should be segmented for clarity.**

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

Provision of standards without accompanying guidance makes it difficult to ascertain APRA's intentions when making particular statements and clauses. While we can understand the intent to consult on areas requiring clarification prior to releasing guidance, many of the questions that arise in these consultations could have been pre-managed. It is difficult to form a view on the operation and intent of many of the clauses presented in a standard without a framework in which they are intended to operate, particularly for cross-industry standards that may be interpreted or operate differently depending on the industry application.

Several of the clauses in the draft standard would benefit from being moved into guidance rather than the standard. For instance, the lists of potential critical operations (paragraph 35) and material service providers (paragraphs 49 and 50) would be better addressed in industry-specific guidance. The discussion paper differentiates these by industry-type but the standard does not. Inclusion of these within the standard makes them prescriptive rather than flexible to each industry and risks capturing processes and providers that are not actually critical or material to the business.

One such example is the inclusion of promoters and financial planners as material service providers. In a banking, insurance or commercial trustee context, these providers act as product distribution channels. In the profit-to-member super fund context, the interpretation is more likely to be drawn to intrafund financial advisers and suppliers of marketing and advertising services that are neither material nor critical.

The inclusion of these paragraphs within the standard also appears to be at odds with the more principled approaches taken in paragraphs 34 and 48 of the standard and the comment in the discussion paper at page 21 that "it is the responsibility of the entity to define, identify and maintain a register of its critical operations".

- **Clear industry-sector guidance is needed.**
- **Industry would benefit from receiving the draft guidance at the same time as draft standards in future consultations.**

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

AIST does not see FUM as a defining metric for the complexity of a business and its operational risk management so does not support differentiating between SFIs and non-SFIs.

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

Funds will be required to engage with all providers to put in place new agreements that comply with the standard. This may require renegotiation of existing agreements and may be particularly onerous for service providers with multiple financial services clients seeking contract amendments at the same time.

Funds will be required to assess and manage risks associated with downstream service providers that material service providers rely on (paragraph 47(d)). This is in place of the requirement in SPS 231 to simply include an indemnity in outsourcing agreements for any sub-contracting done by the service provider. Suppliers will be required to do additional work to collate their sub-contracting arrangements. This will particularly impact providers of IT services, but the identification of relevant fourth party providers as those that material service providers "rely on" in "delivering services to an APRA regulated entity" could be interpreted to extend to utility and telecommunications providers.

The widened scope of impacted providers introduces onerous requirements for funds to implement and maintain. It will require significant uptick in systems and process and require procurement staff to become front line risk specialists necessitating investment in training and recruitment.

Costs of the regime will ultimately be borne by members through their administration fees.

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

SPS 231 Outsourcing applies standards to the outsourcing of "material business activities" while the CPS 230 draft broadens the focus to any service provider "on which the entity relies to undertake a critical operation or that expose it to material operational risk". This means that the list of material service providers will be greatly expanded - indeed the draft contemplates extensive examples of critical business operations and service providers that far exceed those in existing prudential standards.

Materiality is not, however, contemplated with any nuance. Both the SPS 231 and CPS 231 standards provide a list of factors that entities should have regard to in considering whether a business activity is material. In the absence of similar subjective assessments in CPS 230, materiality is extended to all

outsourced providers that perform an operation deemed critical. This will have a significant impact on procurement and contract management processes and resourcing as an expanded list of providers will now be subject to the structured oversight activity required by the standard.

Materiality is also not contemplated in circumstances where a critical business function is partially insourced or spread across a range of providers such that the level of reliance on a single provider may be of less criticality in the event of an operational risk incident. Examples in superannuation include internal audit and investment management functions. Within the investment management function alone, risk is not apportioned equally to all providers as the size of their mandate and underlying asset makeup will vary.

Paragraph 50 extends materiality to all providers covered under CPS 234. This means that agencies that would be subject to the narrow set of cyber security controls under that standard are captured with no regard as to whether they would be viewed as material to the fund's business operations. For example, a research house dealing with a small amount of sensitive member data for a survey or research report would be captured within the regime.

- **Materiality of service providers needs to be better defined.**
- **The concept of "reliance" on fourth party providers needs to be better defined.**
- **Consideration should be given to introducing tiers of materiality for those service providers that are identified as material and addressing higher impact providers in the first instance before rolling out to other service providers.**

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

See comments at question 2.

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

Funds already have a range of existing notification obligations in addition to those contained in the draft:

- **SPS 220 Risk Management** – An RSE licensee must notify APRA within 10 business days when it: (a) becomes aware of a significant breach of, or material deviation from, the risk management framework; or (b) discovers that the risk management framework did not adequately address a material risk.
- **CPS 234 Information Security** – An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that: (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or (b) has been notified to other regulators, either in Australia or other jurisdictions

- **Breach reporting per sect 29JA of the SIS Act** – the RSE licensee must give APRA a written report about the breach as soon as practicable, and in any case within 30 days, after becoming aware of the breach.
- **Critical Infrastructure Part 2B—Notification of cyber security incidents** Critical incidents must be notified to the Australian Signals Directorate's Australian Cyber and Security Centre as soon as is practical and, in any event, within 12 hours of becoming aware of the event. The report may be made orally or in writing and must be followed up with a written report in the approved form within 84 hours of the initial report. Non-critical incidents must be notified within 72 hours and followed up with the approved format report within 48 hours of the initial report.

Paragraph 32 provides that *"An APRA-regulated entity must notify APRA as soon as possible, and not later than 72 hours, after becoming aware of an operational risk incident that it determines to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations."* This is in alignment with the CPS 234 notification requirement but would benefit from additional clarity about whether the timing relates to identification or assessment.

Paragraph 41 provides that *"An APRA-regulated entity must notify APRA as soon as possible, and no later than 24 hours, if it has activated its BCP. The notification must cover the nature of the disruption, the action being taken, the likely impact on the entity's business operations and the timeframe for returning to normal operations.*" This is broadly a reiteration of the requirement in SPS 232 Business Continuity Management but removes the wording around "potential for material impact" after experiencing a major disruption, and the obligation to notify APRA when normal operations resume.

- **Industry would benefit from over-arching guidance from APRA about their expectations across all incident and breach reporting obligations.**

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

The commencement date of 1 January 2024 is too soon to allow for entities to implement the new standard, which is yet to be settled. Implementing the standard would require a review of existing risk frameworks, service provider arrangements, a review of captured related entities and the renegotiation and execution of contracts.

Increased Board responsibilities (discussed below) will require clarification and contribute to implementation time.

- **The 1 January 2024 timeframe for implementation is too short.**
- **A transition period is needed, with particular regard given to existing contract periods to allow a phased approach to renegotiation and renewal of agreements.**

Other comments

Role of the Board

The existing SPS 231 Outsourcing provides for a role of the Board, a Board Committee or senior manager with delegated authority from the Board in the assessment and approval of outsourcing options, while SPS 232 Business Continuity Management expressly permits that the Board may delegate day-to-day operational responsibility for BCM to a responsible committee and/or senior management.

The current draft CPS 230 contains no such delegation provisions, appearing to allocate enhanced responsibilities solely to the full Board. The drafting recognises that senior managers will be set roles and responsibilities by the Board, but only tasks them with providing the Board with information (paragraphs 20 and 22.). The specific roles of oversight, approval and review (paragraph 21) are reserved for the Board. This approach seems at odds with the principles on page 18 of the discussion paper about the respective roles of the Board and senior managers, including the statement that "senior managers within the business are responsible for the ownership and management of operational risk across an entity's end-to-end processes"

Noting that the Board already has ultimate responsibility for risk management, including setting risk tolerances and approving the Risk Management Framework, the extension of oversight responsibilities to cover BCP and supplier agreements in detail will distract from the Board's core role of strategy and direction. Any expansion of the Board's role should also consider the considerable impact of the increased scope of material service providers and enhanced contract management responsibilities proposed by the draft standard.

Operational issues such as approval of the BCP, setting the detail of operational risk tolerances for each critical operation, reviewing risk and performance reporting on material service provider arrangements and signing off on decisions relating to supplier agreements should remain under the purview of senior executive management, with reporting and oversight to the Board and/or their sub-committees as appropriate.

- **The Board's role should be limited to oversight and approval with clearer delegations of certain responsibilities to senior management.**
- **Clarity is required in whether reference to the Board includes sub-committees of the Board.**

Service Provider Agreements

As drafted, paragraph 52 and 52(a) require a full assessment and tender process for a contract renewal or modification. This is excessive, particularly in light of the significant expansion of the service provider list. The lack of nuance in materiality of providers previously discussed will have knock-on effects to the work required for otherwise straight-forward renewals.

While the use of the terms "materially" in relation to a contract modification and "appropriate" in relation to due diligence and selection processes appear to somewhat temper the requirements for

lesser service provider arrangements, this is left open to interpretation. The wording of this clause would benefit from clarification.

It is unclear what clause 52(c) is intended to achieve and whether it has any linkage to other regimes such as the Critical Infrastructure legislation.

- **Clarity is required around due diligence requirements for contract modifications and renewals.**
- **Clarification is required about the purpose of 52c.**

Register of providers

Paragraph 47(a) places the material service provider register within the service provider management policy. The Policy is not the right place for the register when vendor lists change regularly and policy updates require more rigorous compliance oversight and high-level approval processes.

- **The register should be referenced by inclusion in the policy but not be specifically housed within it.**

Overlap & interaction with other obligations

Conduct and accountability frameworks

References to conduct and compliance and role-setting in paragraphs 11, 19 and 20 overlap with CPS511/CPG511 Remuneration that specifically address the Board setting "… clear accountabilities and expectations for risk management, effective consequence management and a strong tone from the top on risk culture."

Other prudential standards specifying a role for the Board use the term "responsible for" rather than "accountable for". It is unclear whether this is a deliberate change and whether it is intended to reflect or interact with other regulatory frameworks, e.g. the Financial Accountability Regime applicable to executives and senior managers.

Risk Management

There is considerable overlap with CPS/SPS 220 Risk Management which already contemplates operational risk and applies materiality measures to those risks. Much of the text in the sections headed "Risk management framework" and "Operational risk management" can be amended to reference that standard rather than reiterate existing requirements. As drafted, the standard blurs the distinction between framework expectations and operational standards.

"Operational risk" and "operational risk event" are defined in SPS 114 Operational Risk Financial Requirement but there is inconsistency with the definitions in the proposed standard. Reputational risk is captured in CPS 230 but explicitly excluded in the SPS 114 definition.

- **Clarity is required on the use of certain terminology in the draft CPS 230.**

- **Overlaps and interactions with other prudential standards, governance frameworks and regulatory regimes need to be addressed.**

For further information regarding our submission, please contact [redacted].

Yours sincerely,

Eva Scheerlinck

Chief Executive Officer