AustralianSuper

12/10/2023

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 consultation - CPG 230 - Operational Risk Management

AustralianSuper welcomes the opportunity to provide a written submission in relation to APRA's draft CPG 230 Operational Risk Management.

AustralianSuper is Australia's largest superannuation fund and is run only to benefit members. AustralianSuper has over 3.2 million members and manages over $300 billion of members' assets.

AustralianSuper's vision is to be Australia's leading superannuation fund, in the world's best system for members. AustralianSuper takes a best-practice approach to operational risk management, with a significant focus on identifying and controlling operational risks across the business and identifying any systemic issues. We are prioritising the evaluation and assessment of the resiliency of operational processes, including in relation to external providers. We support CPG 230's objectives of strengthening operational risk management, improving business continuity planning and enhancing third party risk management.

Detailed comments on the draft prudential practice guide, CPG 230, 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 me or Nick Coates, Head of Government Relations and Public Policy (ncoates@australiansuper.com).

Regards

Paula M. Benson

Paula Benson AM
Chief Officer, Strategy & Corporate Affairs

Attachment: Detailed Comments

Key principles [CPS 12-15; CPG 1 – 4]

Paragraph 4

We note APRA's comment in the Response Paper – Operational Risk Management that "*CPS 230 will apply commensurate with the size, business mix and complexity of an entity's operations*". Paragraph 4 refers to the level of granularity expected in assessing operational risk profile including identifying and documenting processes, resources and scenario analysis. However, it only does so in the context of smaller entities. In our view, the guidance should include more about the granularity expected of larger entities.

Risk management framework [CPS 16-19; CPG 5-11]

Paragraph 10

Paragraph 10 of CPG 230 states that "*where an entity has identified material weaknesses in its operational risk management, APRA expects that the entity would keep it informed of the progress of its remediation*." The wording in paragraph 10 is not consistent with paragraph 19 of CPS 230. Paragraph 19 of CPS 230 refers to circumstances where *APRA considers* that an APRA-regulated entity's operational risk management has material weaknesses, rather than the entity. Accordingly, paragraph 10 should be amended to refer to APRA identifying material weaknesses, rather than the entity.

Roles and responsibilities [CPS 20-22; CPG 12-21]

AustralianSuper notes and agrees with APRA's comment in the Response Paper that the Board is ultimately accountable for the oversight of operational risk management and is expected to ensure that senior management effectively implement and maintain a regulated entity's operational risk framework. We also agree with APRA's comment in paragraph 21 of draft CPG 230 about the importance of boards being provided with important and relevant information on operational risk when making strategic decisions.

Paragraph 16

Paragraph 16 of CPG 230 includes a list of expectations for a Board to provide effective oversight of the operational risk profile of an entity.

Paragraph 16(b) describes APRA's expectation that the Board would typically '*regularly review and challenge the effectiveness of the key internal control environment that impacts the operational risk profile'*. We seek guidance on how this would be achieved: for example, could this be achieved via an internal audit plan that reports to the Board or relevant Board committee? We presume that the Board is not being asked to undertake control testing.

Paragraph 18

We wanted to provide a comment on the example in paragraph 18 of CPG 230. This paragraph notes that, while the Board approves the entity's overall tolerance levels, senior management can set more granular tolerance levels and indicators that would be consistent with and not undermine the Board-approved levels.

We understand the current drafting of the guidance to mean that, while the Board should approve the Business continuity plan (BCP) (paragraph 22(b), CPS 230), tolerance levels for disruptions to critical operations (paragraph 22(b), CPS 230) and the service provider management policy (paragraph 22(c), CPS 230; paragraph 20, CPG 230), a Board committee could consider and recommend such documents for approval to the Board. We would welcome clarification in the guidance from APRA along these lines.

Paragraph 18 states that *'while the Board approves the entity's overall tolerance levels, senior management are able to set more granular tolerance levels and indicators that would be consistent with, and not* ***undermine****, the Board-approved levels* (emphasis added)*.'* It is unclear what the word 'undermine' adds in addition to the words 'consistent with'.

Paragraph 19

Paragraph 19 of CPG 230 gives the example that, for superannuation, more granular tolerances may be set for parts of the investment and fund administration processes, such as for the timely investment of contributions and any payments that may have a direct impact on members (such as retirement benefits or early release payments for severe financial hardship and processing of rollovers).

While we agree that these are examples of tolerances that should be the preserve of senior management, it is unclear what higher-level Board-approved tolerances would apply in the context of these particular examples, especially given that these examples appear to correspond to relatively fundamental and high-level (as opposed to granular) processes. We believe further explanation from APRA around the distinction between the levels that can be set by the Board as opposed to senior management is required to operationalise this effectively.

Operational risk management [CPS 24-33; CPG 22-53]

Paragraph 24

Paragraph 24 of CPG 230 provides that *'APRA expects that senior management would ensure that the operational risk management framework operates effectively and is regularly updated. This may involve end-to-end business process mapping conducted across all business operations, including those performed by service providers'.* We would appreciate guidance about the level of process mapping expected.

Paragraph 35 and 36(b)

Paragraph 35 of CPG 230 states that '*effective operational risk management relies on a thorough understanding of an entity's business processes*'. Paragraph 36(b) of CPG 230 states that better practice in identifying and documenting end-to-end processes and resources would include, '*use of these maps to identify risks, obligations, key data and controls, as well as interdependencies'*. In our view to map all end-to-end processes by the 1 July 2025 commencement date is a significant task that would divert resourcing unreasonably.

Paragraph 39

Paragraph 27 of CPS 230 requires the entity to maintain a comprehensive assessment of its operational risk profile. Paragraph 27(c) states that, as part of this, the entity must *'undertake scenario analysis to identify and assess the potential impact of severe operational risk events, test its operational resilience and identify the need for new or amended* controls *and other mitigation strategies*'. Paragraph 39 of CPG 230 provides that APRA expects that prudent entities would ensure the scenarios used are *'sufficiently stressed'* to test the suitability of

the risk and control environment. We seek guidance on what *'sufficiently stressed'* means in this context: e.g. does it mean stressed to failure?

Paragraph 53

Paragraph 53 of CPG 230 refers to incidents as a trigger for re-assessing operational risk and controls, with the example of an entity suffering a high-rated fraud incident which is deemed material. In these circumstances, the draft CPG recommends that the entity could re-assess fraud risk in the entity's risk profile, re-assess the controls linked to fraud risk and conduct a root cause analysis. Paragraph 53(d) states that the entity could consider business process mapping to support the above. It is unclear to us what business processing mapping would mean in these circumstances. For example, is APRA referring to business mapping the risk event or the incident process?

Business continuity [CPS 34-46; CPG 54-82]

Paragraph 58

Paragraph 36 of CPS 230 sets out the minimum requirements for which operations should be described as critical operations. The critical operations provided for in paragraph 36 are described at a high level. For RSEs, these are, investment management, fund administration, customer enquiries and the systems and infrastructure needed to support critical operations.

Paragraphs 58 and 59 of draft CPG 230 outline considerations in identifying critical operations additional to the list in paragraph 36. Is it APRA's expectation that these additional critical operations would be similarly identified at a high level, or is a more granular approach expected?

The high-level approach to the parameters of critical operations, reflected in paragraph 36 of CPS 230 represents an approach that allows necessary operations to be captured while supporting the practical implementation of CPG 230.

Management of service provider arrangements [CPS 47-60; CPG 83-108]

AustralianSuper maintains strong arrangements and takes a risk-based approach for oversighting third party service providers. We welcome strengthened requirements regarding management of operational risk in service providers. These will also assist entities in ensuring that service providers provide the information and material required to support appropriate oversight and management of operational risk.

As a general matter in this section, in some of the clauses it is unclear whether the reference is to material service providers or service providers more broadly. It seems from the relevant clauses of the prudential standard that the reference is to material service providers, however, it would be useful to make this explicit.

Paragraph 83

We recognise the value in gaining more detail about the risk management practices of fourth parties that third parties rely on in terms of operational risk. However, fourth parties may be based in a range of jurisdictions and the applicable regulatory frameworks are not uniform. The ease of obtaining the required information from parties may vary depending on the respective bargaining positions of the APRA-regulated entity, the service provider and the fourth parties.

Paragraph 92

Similarly, paragraph 92 of CPG 230 refers to entities ensuring that service providers undertake appropriate monitoring of risks managed by fourth parties. We are concerned that this paragraph does not adequately address the operational complexity of the work of some third parties, such as fund managers. In certain circumstances, the more granular detail may be considered commercial in confidence.

Paragraph 99

Paragraph 99 of CPG 230 states that when selecting and assessing a service provider for material arrangements an entity would consider several factors against its risk appetite. It would be useful to have further detail here about the meaning of concentration risk in paragraph 99(d). In particular, is this determined at the RSE level or the supplier level?

If the answer is the latter, we note concerns raised in relation to the draft standard that APRA, with its visibility across entities and sectors, may be better placed to identify potential concentration risks than individual entities. We note that, following consultation on draft CPS 230, APRA removed the proposed requirement in the corresponding clause of CPS 230, which stated that, '*before entering into an agreement with a material service provider, an entity should take reasonable steps to assess whether the provider is systemically important in Australia'*.

Paragraph 106

Paragraph 106(f) of CPG 230 recommends that entities monitor the ongoing viability (financial and non-financial) of the service provider and the services delivered. It would be useful to have further information about what APRA means by non-financial risks in this context.

Conclusion

AustralianSuper supports CPG 230's objectives of strengthening operational risk management, improving business continuity planning and enhancing third party risk management. We appreciate APRA's consideration of the above points and would be pleased to provide further background and information as APRA proceeds to consider feedback and finalise CPG 230.