



11 October 2023

Mr Gideon Holland  
General Manager, Policy  
Australian Prudential Regulation Authority

By email: [PolicyDevelopment@apra.gov.au](mailto:PolicyDevelopment@apra.gov.au)

Dear Mr Holland,

### **Prudential Practice Guide CPG 230 Operational Risk Management (CPG230)**

The Insurance Council of Australia (Insurance Council) welcomes the opportunity to provide a submission in response to draft CPG230 and thanks APRA for the meeting on 25 September 2023 to discuss challenges pertaining to *Prudential Standard CPS230 Operational Risk Management* (CPS230). We reiterate the criticality of proportionate regulation and the need for sufficiently clear guidance pertaining to the identification and management of critical operations and material service providers in the general insurance context.

#### *Identification and management of material service providers*

We reiterate the challenges relating to paragraph 96 of CPG230, which suggests that regulated entities manage operational risks associated with cohorts of service providers, where the aggregate impact of those service providers is material, but each individual provider is not. Should the expectation from APRA involve requiring individual providers within a cohort to be treated as material, this will introduce unintended consequences such as administrative burden, delays to claims resolution and disproportionate regulation of small businesses.

For example, requiring material service agreements to be in place with each individual builder before any work can begin to restore the homes and livelihoods of consumers following the impact of a significant weather event will likely cause delays to the claims process and result in poorer consumer outcomes. For instance, following consistent feedback from consumer advocates following natural disasters, insurers have sought to create flexible procurement processes to engage local providers during a catastrophe to speed up necessary work and ensure local businesses can get back on their feet as quickly as possible. A potentially unintended impact of the guidance as currently drafted is that insurers would be precluded from engaging local suppliers without a more extensive legal engagement to ensure CPS230 requirements were met for this potentially short-term engagement.

We agree with APRA that it may be appropriate to consider operational risk, and to manage those risks, for particular cohorts of service providers where their risk profile may differ when considered collectively. However, it is our view that, where a cohort of providers present risks as a collective, those specific risks can be managed without imposing the material service provider obligations on each individual provider in the cohort. Otherwise, it would impose a disproportionate regulatory response to the risk being managed. We recommend that APRA clarifies paragraph 96 of CPG230 to ensure that individual service providers can be engaged with flexibility.

Further, paragraph 94 a) of CPG 230 requires materiality determinations to consider if the service provider supports a critical business operation. There may be instances where the service provider supporting a critical operation may be providing a service that enhances customer experience rather than being the sole provider of a critical service and an operational failure or incident relating to that service is unlikely to disrupt a critical operation beyond tolerance levels. For example, within the claims operation for an insurer, a service provider's smart application may provide claims management services that add convenience to a regulated entity's value proposition and enhance the customer experience. However, it may not impact the core service offering in the event of a disruption as the customer could still be able to lodge the claim via email, which could be processed within agreed timeframes. Providing greater clarity in the guidance regarding whether a material service provider is one that 'supports' a critical operation or is relied upon to carry out a critical operation will assist regulated entities in determining materiality thresholds and identifying material service providers.

#### *Proportionate and scalable requirements*

Many small businesses, be it individually or as a cohort, play an important role in critical operations identified by APRA. We also consider that should an event, such as a global pandemic, impact a whole cohort of suppliers where the aggregate impact of those service providers is material, but each individual provider is not, this event would not be mitigated by the material service provider requirements pursuant to paragraphs 47 to 60 of CPS230 and the relevant sections of CPG230. It would be more appropriately addressed as part of an insurer's business continuity plan. There is added complexity where providers are not contracted but are relied upon to undertake claims management services, such as medical practitioners selected by customers in the context of personal injury claims management.

The CPS230 guidance, as currently drafted, will likely:

- Unfairly disadvantage small businesses that do not have the resources to uplift risk practices to meet APRA's standards and provide the required level of assurance, which may have the effect of reducing market competition. For example, the guidance may encourage regulated entities to only select material service providers with the risk and compliance resources to emulate risk practices aligned to financial services. This could also result in increasing supplier concentration risks as larger cohorts of regulated entities gravitate towards a smaller cohort of service providers, increasing the risk within the third-party ecosystem;
- Have the unintended effect of increasing the governance costs to manage a larger cohort of material service providers. Smaller institutions that lack the size and scale to absorb these costs may have to ultimately pass the costs to the end consumer; and
- Have the unintended effect of causing both large and small businesses to withdraw from the market to avoid disproportionate regulation, noting that it will be challenging for regulated entities to negotiate with service providers to incorporate requirements pursuant to paragraph 55 of CPS230, as an example, which may leave the regulated entities underserved.

We recommend that APRA:

- Refine the applications of CPS230 requirements to individual and/or small providers that may currently be identified as 'material' under CPG230 paragraph 96, or otherwise referred to in CPS230 paragraph 49, such that the obligations are scalable depending on the size and nature of the provider. In particular, the requirements and better practice referred to in paragraphs 44, 45, 76, 88, 89 of CPG230 will be challenging for small businesses and providers;

- Elaborate on its expectations of insurers in situations where contractual agreements do not exist with service providers that are chosen by the customer, without removing the customer's right to elect its preferred provider;
- Review the use of the words 'rely' and 'support' in identifying material service providers, which are used interchangeably in CPS230 paragraphs 15, 36(d) and 48(c) and CPG230 paragraphs 76, 90 and 94(a) as one could imply a lower materiality threshold than the other. We are of the view that services employed to 'support' critical operations, would not necessarily meet the definition of a material service provider; and
- Provide further guiding principles to facilitate consistent interpretation of paragraph 59 of CPG230 regarding customer segmentation analysis, acknowledging that the level of granularity would be dependent on the nature of the service and commensurate with the size and complexity of the regulated entity. We support a risk-based/outcomes-focussed approach to identifying customer segments to avoid unnecessarily complicating the identification of appropriate tolerance levels.

#### *Reinsurance as a material service*

Reinsurance is often a financing arrangement, utilised for capital efficiency, which exposes the business to minimal operational risk and is subject to requirements pursuant to *Prudential Standard GPS230 Reinsurance Management*. The application of CPS230 to this scenario will not deliver the intended benefits of futureproofing and uplifting the operational risk management of material service agreements relating to reinsurance.

We recommend that APRA:

- Consider the relevance to and potential unintended administrative burden on insurers and reinsurers, should paragraph 28, 53 and 54 of CPS230 apply to transactional reinsurance treaties or programs and if GPS230 already requires regulated entities to provide similar comprehensive reporting; and
- Clarify the instances in which CPS230 would apply to reinsurance i.e. when reinsurers are performing 'critical' operational tasks on behalf of the primary insurer.

Other topics that would benefit from further elaboration include:

- The scope and information request relating to the identification of material service providers by mid-2024 and APRA's assessment of preparedness;
- The intent of and the suggested approach to risk assessments prior to providing a material service, as well as the risks that APRA anticipates are particularly relevant in an insurance context in paragraph 41 of CPG230;
- Paragraph 27 b) of CPS 230 which is further elaborated in paragraph 31 of CPG 230, contemplates a more wholistic systems approach to mapping and managing interconnections and interdependencies related to business continuity, operational risks, and service provider management. Currently there may not be many GRC options available to smaller entities that fully address these requirements at a reasonable cost. Does APRA have a view on the capability of current GRC systems and their ability to meet the new standard and if significant uplifts are required in their capability and functionality;

- The level of granularity required in relation to assessing and documenting execution risks in the Business Continuity Plan (BCP) if regulated entities are expected to maintain a 'concise, and easy to action' BCP, as referred to in paragraph 67 of CPG230; and
- The definition of 'sufficiently stressed to test the suitability of the risk and control environment' in paragraph 39 of CPG230, with a suggestion to provide a likelihood and impact rating in the guidance, and discuss whether regulated entities can leverage the operational risk scenarios required under GPS118 for the purposes of the scenario analysis contemplated in paragraph 37 to 40 of CPS230.

The Insurance Council recommends consideration of the nuances in the general insurance industry and the disproportionate impact that CPS230 can have on general insurers and small businesses should APRA not provide sufficiently clear guidance on how CPS230 applies in real-life scenarios.

We look forward to ongoing engagement with APRA as consultation and implementation progresses. Please contact Alexandra Hordern, General Manager, Regulatory & Consumer Policy, at [ahordern@insurancecouncil.com.au](mailto:ahordern@insurancecouncil.com.au) or on 0411 281 790 if you have any queries regarding this submission.

Kind regards,



**Andrew Hall**  
Executive Director and CEO