Insurance Council of Australia

21 October 2022

[redacted]
General Manager, Policy
Policy and Advice Division
Australian Prudential Regulation Authority

By email: policydevelopment@apra.gov.au

Dear [redacted]

Prudential Standard CPS 230: Operational Risk Management

The Insurance Council of Australia **(Insurance Council)**[1] thanks APRA for the opportunity to provide comment on the *Discussion Paper: Strengthening operational risk management* (**Discussion Paper**) and the proposed *Prudential Standard CPS 230: Operational Risk Management* (**Draft CPS 230**).

The Insurance Council makes the following comments which we trust are of assistance. These comments are supplemented with observations on the consultation questions at page 28 of the Discussion Paper at **Appendix One**.

Overview comments

The Insurance Council recognises that the financial services industry is ever more integrated and that participants operate in a closely connected, but importantly not a closed, ecosystem. Therefore, success in achieving operational resilience as an industry will depend on the collective effort of participants, combined with a realistic assessment by APRA as to linkages between the industry and the broader economy.

The Insurance Council therefore considers that APRA's operational risk management requirements should apply to all regulated entities, but in a proportionate manner which allows entities to use their discretion in an appropriate manner consistent with the scale and complexity of their business. Such an approach will require substantial guidance from APRA explaining how different entities could function in a way which meets APRA's expectations.

It follows that the Insurance Council supports "a proportionate approach" to operational risk management. However, it considers that the approach currently outlined in the Discussion Paper and Draft CPS 230 requires further clarification and refinement to realise that objective. In particular, we note with concern the following changes:

- the excessive broadening of scope, most notably in relation to fourth-parties and note that assessing whether a provider is systemically important in Australia will be challenging, if not

[1] The Insurance Council is the representative body of the general insurance industry in Australia and represents approximately 89% of private sector general insurers. As a foundational component of the Australian economy the general insurance industry employs approximately 60,000 people, generates gross written premium of $59.2 billion per annum and on average pays out $148.7 million in claims each working day ($38.8 billion per year).

impossible, for institutions to determine given the limited visibility of the downstream supply chain and the overall system;

- the explicit and granular level of detail which APRA expects Boards to review and which expectation will further blur the critical governance distinction between Board and Management, thereby incrementally adding to the challenge of recruiting and retaining suitably qualified board members; and

- the planned implementation timeline, which is notably shorter than in other jurisdictions, for example in the UK, which allowed entities one year to implement but up to three years to demonstrate that they could stay within tolerance levels.

Further, the cumulative impact of the Discussion Paper and Draft CPS 230, as currently framed, is likely to significantly increase the regulatory costs imposed on insurers due to, amongst other things:

- its probable effect in driving up labour costs due to the operation of supply and demand - the proposed APRA approach increases demand (given it implies a high volume of work to be performed within a short time frame) at a time of constrained supply of expertise. The inevitable outcome will be to increase inhouse labour unit costs, or oblige insurers to incur expensive consultancy fees, as regulated entities seek additional expertise to perform the additional work;

- the lengthy contract negotiations (and/or renegotiations) which will need to be conducted with a significantly increased pool of material third-party suppliers;

- the amount of work required to retool regulated entities' processes, including comprehensive end-to-end mapping, software changes to systems which support operational risk, business continuity management and service provider networks, completion testing etc.

This probable increase in regulatory costs is of particular concern to the insurance industry given its focus on consumer and business insurance affordability, which is currently being challenged in a number of areas due to underlying systemic issues eg climate change, hardening global reinsurance markets etc. In this context, the Insurance Council is concerned about excess regulatory costs arising from poor policy design, which costs will ultimately be borne by consumers and needlessly add to affordability pressures.

Scope requires clarification and refinement

The Insurance Council agrees that it is appropriate to update the scope of the existing guidance under CPS 231 to extend to service providers beyond those involved in "out-sourcing" arrangements. However, we are of the view that in doing so APRA the scope of the current drafting is too expansive and that the scope of Draft CPS 230 needs to be further clarified and refined. This is due to factors, such as:

- the current expansion from the existing focus on "outsourcing" material business activities to a broader concept of "material service provider" will likely capture business providers which are ordinarily managed under existing procurement processes. It is unclear, and undesirable, for the Draft CPS 230 to capture the general functions required to operate a business (eg internet, building maintenance, data warehouses etc) as compared to those which relate to "a business activity" as defined under existing CPS 231;

- the apparent lack of appropriate parameters within the Draft CPS 230 definition of "material service provider", as compared to the CPS 231 definition of "material activity". This lack of an appropriate definition may lead to inconsistent interpretation across the insurance industry (as well as the banking and superannuation industries) and therefore inconsistent application of the standard. Further guidance will be required from APRA as to the parameters to enable the industry to identify more clearly "which" suppliers are material; and

- the evident challenges of APRA seeking to regulate businesses which are not "regulated entities" further up the supply chain. APRA's proposed approach to fourth parties is fraught with difficulty and additional cost. How will a regulated entity know if the supplier, or a fourth party to the supplier, is systematically important in Australia? What capacity does an insurer have to negotiate contractual changes with that supplier eg to require notification by the supplier in relation to its use of material suppliers to it? How will a regulated entity be able to put in place cost effective compliance arrangements to monitor a supplier's arrangements with a fourth party?

The Insurance Council is of the view that the scope of "material service provider" should be narrowed to explicitly exclude arrangements with providers of "fixed business services", including but not limited to utilities, banking services, insurance brokers and reinsurers.

The scope should be further narrowed by the introduction of a minimum materiality threshold. This narrowing will minimise the risk of absurd outcomes, such as, an investment manager being considered material, notwithstanding that it manages only an insignificant portion of an insurer's portfolio, as will currently occur under para 49.

Commencement date

The proposed 1 January 2024 commencement date does not allow insurers sufficient time between publication of the final CPS 230 to meet the requirements, given:

- changes to frameworks and implementation will realistically take longer than the timeline proposed by APRA;
- there are limited business continuity, third party risk and operational risk resources in the market to support these changes due to prevailing external market conditions and increasing demand in these areas post-pandemic; and noting
- peer regulators have allowed a longer transition with timelines prescribed for designing internal frameworks and implementation.

As a matter of commercial reality when a party to a contract opens-up one aspect of a contract for renegotiation (for example, in order to make the contract CPS 230 compliant) this almost inevitably leads to other contractual terms being brought into question. Thus, what starts as a limited update will typically end up as a full contractual renegotiation. Therefore, as a matter of efficient process, the Insurance Council considers that APRA's starting point should be that regulated entities are able to update third party service contracts to comply with CPS 230 either as they are entered, or as they are renewed or extended, subject to fixed start and sunset dates which accommodate legitimate exceptions.

The Insurance Council recommends in relation to regulated entities that final CPS 230 apply to:

- new material service provider contracts from 1 January 2024; and
- existing material service provider contracts from 1 January 2026, subject to certain specified exceptions (to be further developed before CPS 230 is finalised).

The Insurance Council notes that in relation to insurers it will be challenging to renegotiate certain large and complex contracts within the two-year timeframe, and similarly for some smaller insurers to complete the process within the same period. We would be pleased to work with APRA to frame with clarity those identified exceptions which should apply to the insurance industry.

Specific issues

Reputational risk is an outcome not an operational risk

The Insurance Council notes that common industry practice is to treat reputational risk as an outcome of other risks rather than a form of operational risk and was explicitly excluded from APRA Prudential Standard APS 115 Advanced Measurement Approaches to Operational Risk. We seek further guidance

from APRA on its expectations for reputational risk management and the extent and sophistication of such frameworks for institutions.

Cloud Computing

The Insurance Council seeks clarity from APRA in relation to its approach to cloud computing, given this involves a material service provision and should be included in CPS 230.

Draft CPS 230 is silent on cloud computing. It is therefore unclear how draft CPS 230 relates to APRA's Cloud Computing Information Paper. Has the Cloud Computing Paper been superseded, or is it still relevant?

Incident notification

The Insurance Council asks APRA to provide guidance on operational risk incident types and incident classification, as this will be relevant to determining whether the maximum 72-hour incident notification timeframe is realistic or not.

Draft CPS 230 currently requires a regulated entity to notify APRA as soon as possible, and no later than 72 hours after becoming aware of an operational risk incident likely to have a material financial impact (para 32). Whether the 72-hour timeframe is feasible depends upon how this threshold criteria is defined.

Related body corporates

It is common for regulated entities to use a service model where a related body corporate supplies critical services. CPS 231.26 and CPS 237.27 used different criteria for assessing third party outsource arrangement from those required when assessing related bodies corporate. In contrast Draft CPS 230 contains no such concession and requires "an appropriate tender and selection process" (CPS 230.52(a)). We recommend that APRA introduce alternate criteria for related bodies corporate.

Outsourcing to Head Office

Category C insurers which are branches typically rely on their overseas head office for the provision of critical operations. As a branch they cannot, as a matter of law, contract with their head office given legally they are one and the same entity. Where under CPS 231 this would otherwise have been considered an outsource arrangement, it provided for their exemption under CPS 231.32. Draft CPS 230 currently does not contain a similar exemption. The Insurance Council recommends that APRA introduce an equivalent exemption to CPS 230.

Material services to the regulated entity only

The concept of material services should be limited to those services which are provided to a regulated entity. This is because it is only those service providers over whom the regulated entity will be able exercise the required degree of control (via contractual provision) to be able to comply with their obligations under Draft CPS 230.

Draft CPS 230 presently includes "insurance brokerage" within the list of services that would be material, Table 6, Discussion Paper. As a matter of law insurance brokers act as agents for their clients to whom they provide services. Insurance brokers do not act as agents on behalf of insurers and insurers do not exercise contractual control over brokers (in the performance of brokerage services to their clients) in the way that they do with other service providers (to the insurer).

Given the absence of this control, which will be needed by an insurer in order to comply with its Draft CPS 230 obligations, it is inappropriate for "brokerage services" to be listed as a material service. The Insurance Council recommends that the reference to brokers and reinsurers be deleted.

The proposed population of Material Service Providers outlined in Table 6 in the discussion paper could be further focused and refined to reflect the particular characteristics of the general insurance industry and prevailing prudential standards.

Specifically, reinsurance is already governed by the APRA Prudential Standard GPS 230 Reinsurance Management which requires that "Regulated institutions must at all times have a reinsurance management framework to manage the risks arising from its reinsurance arrangements". Therefore, we consider the inclusion of reinsurance in CPS 230 an overlap which will likely increase complexity, cost and confusion. We consider that it would be preferable to include any additional dimensions contemplated by CPS 230 in GPS 230 rather than adding reinsurance as a material service.

Business Continuity Planning reviews

Some of the current requirements in Draft CPS 230 are likely to be particularly onerous for smaller entities where everything is done by a small group of people. Larger entities may be able to support specialised personnel to perform this work, but that option is cost prohibitive for smaller entities.

The Insurance Council is concerned that the cumulative effect of this increasing regulatory cost will be to price smaller insurers out of the market. To forestall this unintended outcome, we recommend that APRA take a more granular view of proportionality, beyond merely distinguishing between SFI and non-SFI, when determining regulatory burden.

In this context, the Insurance Council seeks guidance from APRA as to its expectations in relation to the annual exercises contemplated in paras 42 and 43 of Draft CPS 230. For example, it is not clear whether APRA contemplates that "a range of severe but plausible scenarios" will be tested each year.

We suggest that an appropriate level of testing is:

- likely scenario testing each year; with
- a full range of scenarios tested across multiple years.

We trust that our initial observations are of assistance. If you have any questions or comments in relation to our submission please contact [redacted] General Manager, Policy – Regulatory Affairs, on telephone: [redacted] or email: [redacted].

Yours sincerely

[redacted]

[redacted]
Executive Director and CEO

Appendix One

APRA Consultation Questions

Overall Design

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

The guidance risks being a more prescriptive and/or a 'one-size fits all' approach to operational risk management, which does not take account of the varying size, nature and complexity of APRA-regulated entities.

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

Can APRA please clarify expectations around 'timely manner' per paragraph [230.31].

Can APRA please provide further guidance as to how entities are to determine whether a supplier is 'systemically important' and how entities might then meet these requirements at paragraph [230.52]:

"(b) 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; and

(c) take reasonable steps to assess whether the provider is systemically important in Australia."

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

The Insurance Council agrees that there is merit in less burdensome requirements for non-SFIs. We would also like to see more granularity recognised in the ability to apply proportionality since there are a large range of entities in the non-SFI category.

In addition to concerns related to proportionality (see Question 1 above), we also note the following concerns:

(a) The proposal for 'material service providers' to include service providers that manage information assets classified as critical or sensitive under CPS 234 (see paragraph [230.50]) will lead to an expansion of the number of service providers deemed material. We recommend this be limited only to 'providers that support an entity's critical business operations'. For example, a supplier managing personal information or company confidential information may not automatically be deemed a material provider from a business continuity perspective (e.g. printing of annual reports). We note suppliers managing an entity's information assets are already under stricter diligence and oversight practices by entities under CPS 234.

(b) potential for duplication with other regulatory requirements for regulated entities. For example, the requirement in paragraph [230.27] for an "*APRA-regulated entity [to] conduct a comprehensive risk assessment before providing a material service to another party to ensure that it is able to continue to meet its prudential obligations*". Where an insurer provides services to another regulated entity, for example an LMI, this will be an onerous obligation which goes beyond the existing CPS and will require them to assess materiality for our customers. Arguably what is material may depend on the size, nature and complexity of each regulated entity's business/ operations.

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

The broad application of Draft CPS 230 (beyond the current 'material outsourced provider' in CPS 231) to 'material service providers', will lead to increased costs for regulated entities to ensure ongoing compliance, including cost of additional internal resourcing and system changes. The expansion to 'material service providers' will increase the number of service provider arrangements which are subject to reporting to the Board and APRA (at para 230.58-59). Initial estimates provided to the Insurance Council are that this will increase by a factor of between 5 and 10.

The broad application of Draft CPS 230 and its effect as a prerequisite to doing business with insurers may also serve as "a barrier to entry". If so, it will have the unintended effect of reducing the number of third parties who are willing to provide services to insurers. The detrimental impact of this diminished competition will be felt most by smaller insurers.

In addition, in relation to certain obligations, compliance costs will increase for our material service providers to ensure ongoing compliance (although these are not APRA regulated) – for example

(a) to monitor "*the age and health of its IT infrastructure*" (para [230.24]); and

(b) the "*assessment of the execution risks, required resources, preparatory measures, including key internal and external dependencies needed to support the effective implementation of the BCP action*" (see para [230.39])

will have a flow through impact on a regulated entity's material service providers.

Specific Requirements

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

As noted in our comments to Questions 1 and 3 above, we recommend that 'critical operations' be determined by each entity on a principles-based approach. As per response to question 3 above, we recommend the definition of 'material service provider' be limited only to 'providers that support an entity's critical business operations'.

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

Paragraph [230.47] (a) requires the entity's policy to include a register of the entity's material service providers. A policy is a statement of intent approved by the Board, and not a register of information that changes when suppliers are onboarded and offboarded.

We suggest that APRA consider amendments to [230.55], paragraphs (a) to (c), as follows:

(a) Paragraph [230.55] (a) seems to suggest the entity will manage the Service Providers risks in parallel to the Service Provider. Risks of a Service Provider should be the Service Provider's responsibility. In practice the entity would seek evidence of an effective Risk Management framework, in much the same way the entity seeks evidence of an effective Business Continuity Management framework.

(b) Paragraph [230.55] (b) suggests transparency to the entity by the Service Provider for active risk records. Some procedural guidance may be necessary so only relevant risk data is reported by the Service Provider to the entity.

(c) Paragraph [230.55] (c), This clause is about the entity's BCP. Some readers might make a mistake and interpret this as the Service Providers BCP.

We note that the list of critical operations at Paragraph [230.35] seems to be an ADI-centric view, which is not appropriate for other APRA-regulated entities, including insurers.

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

The Standard could benefit from the alignment of reporting requirements between business continuity activations (24 hours) and Operational Risk (72 hours).

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

Based on application of this Standard to 'material service providers' (as currently defined), initial assessments shared with the Insurance Council indicates that the number of service providers that will be deemed 'material' will increase by a factor of between 5 and 10. The increase in work implicit in multiplying the numbers of suppliers to captured by Draft CPS 230, is in addition to the increased in work involved in embedding the additional reporting and monitoring requirements to comply with Draft CPS 230.

We therefore recommend that Draft CPS 230 only apply to new arrangements entered into from 1 January 2024 with renewals of existing contracts to be compliant by 1 January 2026.