CALI Council of Australian Life Insurers

Mr Gideon Holland
General Manager, Policy
Australian Prudential Regulatory Authority

By email: policydevelopment@apra.org.au

10 October 2023

Dear Mr Holland,

Re: Draft CPG 230 Operational Risk Management

The Council of Australian Life Insurers (CALI) was formed in late 2022 to support Australians to make informed choices about their future and help them live in a healthy, confident and secure way over their lifetime. We advocate for national policy settings that expand Australians' access to the life insurance protection that suits them when they need it most.

Our 19 members represent 99% of the life insurance market and all reinsurers in Australia. Their products and services give people peace of mind when making important decisions and provide a financial safety net during life's biggest challenges.

This submission highlights a number of sections of CPG 230 which would benefit from additional clarification by the Australian Prudential Regulatory Authority (APRA) to make the intent of the guidance clearer. These include clarification on a number of definitions, including material service providers, transition arrangements, potential issues with legally binding contracts, and requests for a range of practical implementation clarifications.

CALI would welcome the opportunity to discuss further with APRA. Please reach out to Ben Marshan at ben.marshan@cali.org.au or myself at christine.cupitt@cali.org.au.

Kind regards,

Christine Cupitt
Chief Executive Office
Council of Australian Life Insurers

CALI response to APRA draft CPG 230 operational risk management

CALI welcomes the opportunity to provide feedback through this submission on the draft CPG 230. This submission has been prepared following consultation with our members and represents broadly the views and points of clarification across the life insurance and reinsurance industry. While CALI and our members support the uplift in operational resilience afforded by the CPS 230 Standard, the life insurance and reinsurance industries operate in a variety of ways and positions within the broader financial services industry, and we therefore seek clarification in relation to some points within the draft CPG 230.

CALI notes the definition for criticality of operations will be determined by the entity based on proportionality, for example the scope of claims processing and customer enquiries as it relates to identification of critical operations. Likewise, the materiality of service providers and service arrangements will be subject to the entities assessment based on proportionality. As such, the submission below reflects this consideration.

CALI's submission therefore focuses on seeking clarification as our members look to implement CPS 230 and take into account this guidance.

Unless otherwise stated, paragraph references in this submission are in relation to draft CPG 230 operational risk management.

1. Expectations of 'Better Practice'

As noted above, CALI understands that CPGs do not create enforceable requirements, however the structure of the document consistently reinforces expectations APRA has through the use of 'better practice' statements. Based on this, CALI seeks clarification of whether:

- APRA will treat these statements as ones that an entity should meet (effectively quasi-requirements) in future compliance reviews?
- APRAs' intention for the 'better practice' statements should align to "*proportionality and business size, nature and complexity*" (i.e. SFI/non-SFI) of the entity in terms of expected compliance with these, and if so, how will this be set out?

If APRA expects 'better practice' to be achieved (now or in the future), CALI recommends clarification of expectations to be made clear from the outset so this can be incorporated into implementation plans and ongoing strategy accordingly.

2. Definitions

CPS 230 contains a number of terms for operations or functions, some of which are specific to particular regulated industries and some of which are used in broader contexts for all regulated entities. CALI and our members highlight the following definitions would benefit from additional clarification or specific definitions in CPG 230 to improve the guidance and assist in meeting APRA's expectations in relation to implementing CPS 230.

- Insurance Brokerage

Paragraph 50(b) of CPS 230 provides a definition of insurance brokerage which would benefit from a clearer definition. CALI notes that insurance brokerage as a term could relate to insurance brokerage function as a whole, rather than individual brokers, and therefore at what level an assessment of the function is required. Paragraph 50(b) suggests it may be the operation risk associated with the whole level, however paragraph 96 relates to the management of operational risk associated with cohorts of service providers where the aggregate impact of those service providers is material, but each

individual provider is not. Based on this, and given the importance of this function in the life insurance industry, CALI recommends a clearer definition on insurance brokerage be developed.

From an operational perspective, a further complication in relation to insurance brokerage relates to life insurers not necessarily having formal contracts in place with intermediaries such as insurance brokerage firms or independent financial advisers, either at an individual or licensed entity level. Given the nature of most life insurance brokerage is provided by small businesses (either as an AFSL or a CAR) without a formal distribution agreement in place, it will be difficult to practically implement the data requests required to obtain the required information to undertake assessments either at the whole, individual or cohort level.

CALI also seeks clarification from APRA on whether insurance brokerage is intended to also refer to independent financial advisers?

- Fourth Parties

Paragraph 48(c) of CPS 230 refers to fourth parties, however it is unclear whether the definition of a fourth party refers to a situation where the entity uses a third party to undertake a function/activity and that third party:

- then uses another vendor (fourth party) to complete that function/activity wholly or partly; or
- has significant dependencies on the provision of services from a fourth party that relate to its ability to perform the function/activity?

CALI recommends APRA clarify the definition of fourth party in CPG 230.

- Core Technology

Paragraph 50(d) of CPS 230 refers to the classification of core technology providers as material service providers, however it is unclear as to what level of importance a piece of core technology is required to have to be considered core.

CALI recommends APRA provide clarification (either directly or through reference to other prudential standards or guidance) on what level of importance core technology relates to.

- Material Arrangements

Paragraph 49 of CPS 230 states '*Material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk. Material arrangements are those on which the entity relies to undertake a critical operation or that expose it to material operational risk.*'

In addition, paragraph 50 prescribes '*The following services*' that must be classified as a material service provider and includes '*Underwriting, insurance brokerage and reinsurance*' for insurer, and '*Risk management, core technology services and internal audit*' for all APRA-regulated entities.

However, the definition of a material arrangement is not clearly differentiated from a material service – both being those on '*which the entity relies to undertake a critical operation or that expose it to material operational risk*'.

CALI recommends APRA provide a clearer definition in CPG 230 on the difference between Material service providers and Material arrangements.

- **Systems and Infrastructure**

Paragraph 36 of CPS 230 states '*An APRA regulated entity must, at a minimum, classify the following business operations as critical operations, unless it can justify otherwise*' and includes in 36(d) '*the systems and infrastructure needed to support critical operations*'. However, there is no further guidance in the CPG as to the definition of systems/infrastructure.

CALI recommends APRA clarifies in CPG 230 if:

- organisations are required to capture systems and infrastructure as they relate to Critical Operations in the process maps as key dependencies; and
- where a system or infrastructure may not meet the criteria for criticality themselves, will it be important to capture them as part of the overall operational risk as it relates to the Critical Operation?

3. Transitional arrangements

CALI notes that CPS 230 forms part of a broader set of operational risk management prudential standards and builds on or replaces existing standards. Additionally, regulated entities have a complex series of service agreements and contracts in place which may have a variety of expiration time frames or existing information sharing agreements in place. Given this, CALI recommends APRA address the following in CPG 230 or through other measures:

- If formal agreements are entered into for a material arrangement that is also an outsourcing agreement (CPS 231 and CPS 232 currently apply and CPS 230 applies post 1 July 2025), can an entity choose to comply early with CPS 230 rather than CPS 231 and CPS 232 as new agreements are entered into?
    - If this is acceptable practice, CALI recommends APRA publish a 'no action' position in relation to non-compliance with CPS 231 and CPS232, where an organisation complies early with CPS 230.
- Alternately CALI recommends either APRA:
    - clearly defines its expectations in relation to compliance with CPS 231 and CPS 232 before 1 July 2025 and the requirement to amend agreements between 1 July 2025 and 1 July 2026 through a letter, statement or guidance; or
    - if there is no transition period planned, given the potential number of third-party assessments required, CALI recommends APRA allow initial assessments be staggered on an exceptions basis.

4. Comprehensive Risk Assessments

CALI understands that the requirement for risk assessments is similar to that of CPS 231 but applied to a broader set of material service providers as defined by applying CPS 230 and that entities must conduct risk assessments for each material service based on their organisational risk tolerance. To ensure consistent understanding and clarity, CALI recommends APRA amends CPG 230 to:

- confirm the application of similar risk assessments to CPS 231 to the broader set of material service providers;
- clarify whether a lighter touch level of risk assessment can be conducted on external providers who are also APRA regulated entities; and
- while materiality is subjective for each business and on a case by case basis, APRA to outline the level of materiality for a service provider to be required to provide an assessment through some further examples.

5. Material Service Providers

CPS 230 requires both life insurers and reinsurers to consider whether the service providers they use to operate are material to their organisations operations and services. However given materiality is a broad concept and can be interpreted in a variety of ways, both at the organisations and the regulator, CPG 230 would benefit from addressing the following areas further.

- **Materiality considerations**

CALI recommends APRA provide further guidance in CPG 230 on whether the materiality considerations that must be applied to a service provider under CPS 230 are the same factors for consideration as per paragraph 13 and 14 in CPS 231 either by referencing these or restating in CPG 230.

- **Intra-group arrangements**

Paragraph 41 states there is a requirement to conduct a comprehensive risk assessment prior to entering into a new arrangement to provide a material service to another party which would apply to intra-group arrangements and services to non-APRA-regulated parties. CALI recommends APRA confirm that a comprehensive risk assessment is not required to be undertaken for inter-group or APRA regulated entities. As noted above, in instances where an entity is both intra-group and APRA regulated, CALI recommends APRA provide clarity on which would take precedence for completeness.

- **Multiple regulated arrangements**

Further to more clarification being required in relation to paragraph 41, where an organisation is providing two regulated services (for example both insurance and reinsurance), is information required to be collected at both levels?

- **Fourth Party Monitoring**

CALI understands that per paragraph 92 of CPG 230, '*Better practice would be for an entity to ensure that service providers undertake appropriate monitoring of risks managed by fourth parties*'. It is therefore assumed that entities may rely on fourth party risk assessments completed by the third party for assurance. CALI recommends APRA provide clarification on what level of information is required on fourth parties, such as subcontractors.

CALI notes that it is possible that the third party entity and a related fourth party are unlikely to have a contractual relationship and therefore there may be no requirement in place for them to supply the entity with information above and beyond what they are required to supply to the third party which may create challenges for the regulated entity.

- **Reinsurance**

While CALI notes that reinsurance is defined as a "*material service provider*" at paragraph 50 (b) of CPS 230, it is not a service which is directly provided to life insurers, but rather a financial arrangement used for capital efficiency to minimise operational risk and regulated by APRA under LPS 230.

Given this, CALI recommends APRA clarify in CPG 230 that transactional reinsurance contracts and treaties are outside the scope of the requirements set out in paragraph 28 of CPS 230 and paragraph 41 of CPG 230 as a material service provider, unless there are specific circumstances under which the arrangement would extend beyond a financial arrangement and become a critical operation.

6. Standardisation

CALI notes that the life insurance industry is made up of organisations with intertwined relationships (e.g. reinsurers to multiple life insurers, life insurers providing products to multiple Group Funds). There is therefore an associated risk of a significant administrative burden being created across the industry in providing information to multiple entities, including different data and at different intervals.

The key concerns relate to the diversity of information and data requested, wider ranging assurances to be provided and the potential for these requests to be received all at different time periods, which would result in significant capacity constraints for providers in responding to these varied and sporadic requests. Particularly, this relates to:

- Information sharing and data sharing;
- Provision of information for risk assessments;
- Due diligence requirements; and
- Contract negotiations.

Lessons learned from previous regulatory programs have evidenced the efficiencies to be gained through working collectively as an industry to align on requirements where there are broad similarities and potential for crossover between interlinked parties. Therefore, there is a potential to explore development of industry principles for information requirements, risk assessments and due diligence requirements to achieve a level of standardisation and consistency. CALI seeks clarity from APRA that if this was explored, would APRA be broadly supportive of this approach?

Aligned to this concept of consistency in approach and understanding, it would be helpful for APRA to clarify the language used relating to the requirements for risk assessments, particularly as it relates to proportionality and to offer any further support that may assist with the development of guiding principles across regulated entities including the life insurance industry.

7. Formally legally binding agreements

CALI notes that a number of sections in CPG 230 relate to legally binding agreements which will require changes to both new and existing contracts with service providers. Given the challenges of potentially renegotiating contracts, negotiating contracts with foreign or non-APRA-regulated entities and the time frames for complying with CPS 230, CALI recommends additional consideration be given by APRA to the following areas:

- **Flexibility**

CALI notes that paragraph 101 states formal legally binding agreements should 'typically be sufficiently flexible to accommodate changes'. Further, paragraph 57 of CPS 230 states APRA may require a '*regulated entity to review and make changes to a service provider arrangement where it identifies heightened prudential concerns*'. There is a concern that this is likely to be difficult in practice and it is unlikely the other party will agree to unilaterally vary the agreement or agree to these terms, particularly if the variation is made at the request of APRA, particularly where the other party is a non-APRA-regulated entity.

CALI recommends more consultation be undertaken by APRA in relation to the operation of these sections.

- **Access**

CALI notes the provision per paragraph 55 of CPS 230 regarding APRA's access and notes this is consistent with CPS 231. However, we seek clarification on the expansion of the provision to '*agree not to impede APRA*' which under CPS 231 was more specific to '*related body corporates*' (per paragraph 35 CPS 231) verse all service providers (paragraph 55(c) in CPS 230).

CALI recommends APRA provide guidance on this expanded application.

Additionally, as a specific example, where a material service provider imposes reasonable protections to prevent APRA from accessing its privileged information, would this constitute '*impeding APRA in fulfilling its duties as prudential regulator*' under paragraph 55(c) in CPS 230?

- **Contract Negotiations**

CALI notes the difficulties that are likely to be encountered through the timing of widespread ongoing negotiations/contract variations where many of the industry share the same providers but will have different timeframes and dates for renewal. Additionally, there are likely to be challenges posed with implementing these for non-APRA-regulated entities or organisations in other jurisdictions. As a matter of commercial reality, organisations will be required to contract with very large-scale service providers that have few or no viable competitors for the services provided (e.g. software or cloud service providers). If these providers chose not to renew/renegotiate contract terms with entities, this could cause disruption across the industry.

CALI recommends APRA recognise this challenge in the guidance.

- **Applicability**

Paragraph 54 of CPS 230 relating to service provider agreements and the degree of applicability of *'formal legally binding agreements'* in respect to intra-group (offshore/within same company) arrangements that are deemed material. Paragraph 31 of CPS 231 details an agreement does not apply to related body corporates and CPG Paragraph 19 states a service level agreement is sufficient.

CALI recommends APRA provide clarification in relation to the same applying for CPS 230.

- **Short term/one off agreements**

CALI notes a short period contract or one-off scenario creates a level of unnecessary administrative burden under CPS 230 as there is no provision for these types of circumstances. In contrast, CPS 231 through CPG 231 paragraph 4 has consideration for these (i.e. contracts up to 12 months).

Additionally, CPS 230 does not provide special provision for secondments. For larger organisations it is commonplace to operate with several different entities and to utilise staff accordingly (e.g. Risk, Audit, etc) across the different entities under secondments. We again note such a provision in CPG 231 paragraph 5.

CALI recommends including similar statements to CPG 231 paragraphs 4 and 5 in CPG 230.

- **Frequency**

CPS 230 does not reference the level of frequency as a determining factor for materiality. CALI notes that CPS 231 provides a pragmatic approach to assisting in defining materiality as stated in paragraph 10 which states '*Outsourcing' involves an APRA-regulated institution, or an institution within a group that is not an APRA-regulated institution, entering into an arrangement with another party (including a related body corporate) to perform,* ***on a continuing basis****, a business activity that currently is, or could be, undertaken by the institution itself.*'

CALI recommends including a similar provision in CPG 230. For example, where there is an existing amount of rigour related to these assessments such as a one off service assessed under CPS 234.

8. Process Mapping/Value Chain

Paragraph 35 and 36 appears to merge the concepts of value chain process mapping and Critical Operations. End to end processes (as set out in Figure 1) can be a high-level value chain view which is very different to mapping of critical operations. Further to the above, the CPG 230 guidance does not define the expectation of granularity for process mapping.

CALI recommends APRA confirm the granularity of process mapping that is expected (if at all) in CPG 230.

9. Controls testing/responsibilities

Paragraph 47 states '*Better practice is for an entity to have controls testing that is monitored to ensure completion, with exceptions identified, escalated and remediated. Testing would typically include the objectives, scope, approach, success criteria, frequency and roles and responsibilities for testing controls. It would be conducted by staff and teams that are independent of those with operational responsibility for the controls being validated.*'

Further, paragraph 48 states '*Control owners are typically responsible for ensuring that controls are regularly tested and monitored. Control gaps, weaknesses and failures would be identified as issues and managed accordingly and be reflected in the entity's operational risk profile.*' This appears to contract the requirement for independence in Paragraph 47.

It is therefore unclear whether APRA is referring to independence of performance, or full independence, e.g. Line 1 and Line 2 both have operational responsibility but the oversight of Line 2 would normally suffice in terms of validating controls.

CALI recommends APRA provide clarity on what is meant by the independence in operational responsibility.

10. Critical Operations and Critical Functions

Paragraph 61 states that '*APRA expects that 'critical functions' defined for resolution planning would be classified as critical operations. Critical functions are functions an entity provides that are important to the financial system or a particular industry or community and are determined by APRA under Prudential Standard CPS 900 Resolution Planning (CPS 900).*' As noted in Table 5, the difference between Critical operations versus Critical functions, are that Critical functions are regulated per CPS 900 Resolution Planning and are determined by APRA on a case-by-case basis.

For entities not selected by APRA for the CPS 900 pilot, CALI seeks to understand when APRA will more broadly inform non selected entities of the Critical functions so they can be considered, noting many entities are well underway in identifying Critical operations in line with the APRA timeframe of July 2024.

11. Oversight and process mapping of providers

Paragraph 89 states that '*APRA expects that a prudent entity would have visibility of risk management practices of the service provider and take reasonable steps to ensure consistent standards are maintained that would not fall below those it would use if the service was maintained internally. This includes consistent process mapping for all services, whether maintained by the entity or a service provider, verified through practices such as onsite visits and control monitoring.*' It is unlikely to be feasible for entities to conduct process mapping of service provider functions, particularly for those that are non-APRA regulated and/or where the process mapping would require detail of commercially sensitive information. While this may be better practice in terms of operational risk oversight, it is unlikely to be practical to do so.

Should this paragraph be enforced (linked to Section 1 above), CALI recommends APRA provide additional guidance on the detail of mapping for oversight.

12. Materiality in changing service agreements

Materiality can vary by the risk appetite of the organisation. CALI recommends APRA define materiality as it relates to notifying APRA where the entity has 'materially changed an agreement for the provision of a service on which the entity relies to undertake a critical operation' per paragraph 59(a) of CPS 230 and Table 1. Notification to APRA in the Guidance.

Further, pending clarity on the definition of materiality in this context, CALI recommends APRA clarify whether this relates to material changes to the service provision or changes to the overall operational risk profile.

Likewise, CALI recommends APRA clarify or provide examples of what would constitute notification to APRA regarding material operational risk incidents as set out in Table 1.

13. Clarity on material weakness identification requirements

Paragraph 10 in CPG 230 states that '*Where* **'an entity'** *(emphasis added) identifies material weaknesses in its operational risk management, APRA expects that the entity would keep it informed on the progress of its remediation*'; however paragraph 19 of CPS 230 refers to 'APRA' considering/identifying material weaknesses in the entity's operational risk management.

CALI seeks clarification as to whether this relates to self-identification (per CPG 230), APRA identification (per CPS 230 Standard) or both - in which case this is not clear in the Standard.

14. Reporting

Paragraph 51 of CPS 230 states '*An APRA-regulated entity must submit its register of material service providers to APRA on an annual basis.*' CALI recommends APRA more clearly state in CPG 230 on the scope of APRA reporting in respect to material service providers. Is it to include material intra-group arrangements (e.g. offshoring within the same organisation) or intended to be external service providers only, given footnote 15 indicates this includes intra-group (e.g. related party or connected entity).