13 October 2023

General Manager, Policy
Australian Prudential Regulation Authority
GPO Box 9836
Sydney NSW 2001

By email: PolicyDevelopment@apra.gov.au

Dear Mr Holland,

Draft Prudential Practice Guide CPG 230 Operational Risk Management

The Australian Financial Markets Association (**AFMA**) welcomes the opportunity to comment on the Australian Prudential Regulation Authority's (**APRA**) draft Prudential Practice Guide CPG 230 Operational Risk Management (**draft CPG 230**).

AFMA remains supportive of APRA's initiatives to modernise the prudential framework and APRA's aims, with regards to the Prudential Standards CPS 230 Operational Risk Management (**CPS 230**) and CPG 230, to:

- Strengthen operational risk management;
- Improve business continuity planning; and
- Enhance third-party management.

AFMA and its members welcome the pragmatic modifications to the draft CPS 230 which help reduce uncertainty regarding the standard's requirements and the burden on industry, and service providers to industry, while still achieving APRA's policy aims. Notwithstanding these changes, AFMA remains concerned that the reforms still create an unnecessary level of uncertainty and burden, that in some circumstances outweigh their benefits.

To reduce these negative impacts and to better align the policy reforms to their aims, AFMA strongly recommends that APRA:

1) Allow flexibility in implementation timelines. APRA's implementation timeline remains aggressive by international standards. Allowing entities flexibility in comprehensively implementing the new reforms, in appropriate circumstances, is a pragmatic approach particularly given the competing regulatory reforms currently underway;
2) Further refine the scope of the reforms. By, for example, following the approach taken internationally and in the Prudential Practice Guide PPG 231 Outsourcing (**PPG 321**) to explicitly identify services that are typically considered not to be critical business operations (**CBO**) or material service providers (**MSP**);
3) Enhance proportionality and substituted compliance. Such as clarifying where a Foreign ADI can rely on being compliant with its home regulator's requirements, where those requirements align with the Basel Committee on Banking Supervisions' (**BCBS**) principles; and

4) Take a systems approach to managing interdependencies. APRA and the Council of Financial Regulators (**CFR**) are in a unique position to identify, reduce and manage the risks from interdependencies within, across and from outside the finance industry.

Further detail on these, and other, suggestions are attached for APRA's consideration.

For more information or if you have questions in relation to this letter, please contact on 0411 281 562 or at brendonh@afma.com.au.

Yours sincerely

Brendon Harper

Head of Banks and Prudential

Appendix A

1. Allow flexibility in implementation timelines

While APRA has delayed the effective date of this Prudential Standard, the timeline is still very aggressive when compared to offshore regulators, for example, compared to the United Kingdom's Prudential Regulation Authority which is working towards a four year timeline.

APRA's expectation of full compliance within two years, and their stated expectations / potential on-site inspections, coupled with the fact that a significant amount of further clarity is still required prior to implementation, despite already extensive and detailed industry feedback, makes the implementation both challenging and resource intensive. This is exacerbated by the concurrent implementation of other frameworks across the industry including the foreign financial services providers and the financial accountability regime reforms. More specifically:

- While CPS 230 paragraph 7 extends the timeframe for application of the standard to 1 July 2026, this does not factor in i) potentially prolonged negotiations, and ii) entities that are both APRA regulated *and* also a critical service provider to other APRA regulated entities;
- For the latter, these entities (and their affiliates) effectively wear a "double hat" and may face the need to renegotiate existing contractual requirements as both a critical service provider and a critical service receiver;
- Under, CPS 230 paragraph 49, a register of MSPs must be maintained with the need to manage associated risks, while under CPS 230 paragraph 50, certain service providers are deemed material. The broadening of the definition of service providers beyond "outsourcing" under CPS 231 will potentially bring vendors into scope that do not have pre-existing contracts that meet CPS 230 requirements. Any prolonged negotiations risk those vendor arrangements not being able to meet the go-live timeframe of 1 July 2025;
- CPS 230 paragraph 48 contains requirements for service provider management policies to address the APRA-regulated entity's approach to managing risks associated with fourth parties (relied upon to deliver critical operations to the APRA-regulated entity). Any such risk assessment and treatment will potentially require significant time; and
- The proposed timeline allows insufficient time to comprehensively implement system modifications in a controlled manner to accommodate CPS 230 requirements, for example to record required datapoints for the register of MSPs.

In respect of the above, AFMA recommends the draft CPG 230 provide guidance that in such circumstances where entities are facing time constraints, they should be able to notify APRA to outline these challenges and be granted an extension of time.

2. Refinement of scope to reduce uncertainty and burden

AFMA welcomes the pragmatic changes in the final CPG 230 that provide greater clarity on the scope and capture of the reforms. These changes should assist in reducing the significant cost of implementing the new requirements. For example, allowing the

justification of why some items on the prescribed lists of CBOs and MSPs should be considered not critical/material for a particular entity is a sensible modification that reflects the diversity of business models and activities across the regulated population.

Noting, however, that the prescribed lists are presented as being "at a minimum", there remains considerable uncertainty regarding the full scope of the reforms and how entities are expected to assess this scope. For example, it is unclear if APRA intends to align with international precedent by excluding global network infrastructures, such as Visa and MasterCard, and/or clearing and settlement arrangements, from the scope of the prudential requirements. AFMA also encourages APRA to consider additional exclusions, such as global IT infrastructure providers.

In addition to providing greater clarity on how APRA expects entities to assess if an operation/service provider is a CBO/MSP, AFMA encourages APRA to follow international precedent[1] and the approach taken in PPG 231 to provide examples of operations/services that would typically not be considered CBOs or MSPs – PPG 231, paragraph 4 states:

> *APRA does not envisage that a material business activity would ordinarily include contractor relationships — that is, relationships where there are numerous service providers in the marketplace, the agreement is short-term (i.e. less than 12 months) and the cost of switching between providers is low and switching is relatively easy. Examples of contractor relationships include utility services (e.g. mail and telephone services), legal services, advertising, recruitment and other personnel functions, printing services, travel and transportation services, repair and maintenance of fixed assets, purchase of goods, background investigation and information services, specialised training and software licensing arrangements.* (Emphasis added)

This approach reinforces the definition of outsourcing provided in the Prudential Standard CPS 231 Outsourcing (**CPS 231**):

> *'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.* (Emphasis added)

Greater clarity of APRA's expectations regarding the assessment of CBOs and MSPs would increase the consistency of implementation across the financial industry, reduce

---

[1] Such as:
- the Monetary Authority of Singapore's *Guidelines on Outsourcing* (page 27) which includes lists of "arrangements [that] would generally not be considered outsourcing arrangements";
- The European Banking Authority's (**EBA**) *Guidelines on outsourcing arrangements* (paragraph 28) which includes a list of functions and operations that "*As a general principle, institutions and payment institutions should not consider… as outsourcing*"; and
- The UK's Prudential Regulation Authority's (**PRA**) Supervisory Statement, *Outsourcing and third party risk management*, (pages 8-9) which references the EBA's Guidelines on outsourcing arrangements and provides additional examples.

implementation and ongoing costs, while increasing the intended benefits from the reforms.

Clarifying the scope of end-to-end business process mapping

To align with the changes to the draft CPS 230, AFMA recommends that APRA similarly adjust the draft CPG 230, paragraph 24, such that it reads:

> "This may involve end-to-end business process mapping conducted across all *critical* business operations, including those performed by *material* service providers".

3. Enhancing proportionality and substituted compliance

AFMA appreciates that APRA has provided some guidance in CPG 230 as to how different types of entities would be expected to demonstrate compliance with CPS 230. It would be useful to complement this material with more specific guidance on the application of these principles to Foreign ADIs that may not be significant financial institutions (**SFIs**) in Australia but are subject to global regulatory requirements, including where they face different regulatory timelines.

AFMA recommends that CPG 230:

- Distinguish between SFIs / non-SFIs in the application of proportionality guidance; and
- Apply a substituted compliance approach to home jurisdiction requirements and allow for the level of review and testing to be adjusted by Foreign ADIs accordingly.

Without clarification, any regulatory overlap potentially increases complexities and inefficiencies, which does not align with APRA's broad principles of simplifying and modernising policy frameworks. For example:

- CPS 230 paragraph 32 – "near misses" – Can APRA's confirm that a risk-based / proportionate approach to near-misses is acceptable, that is, a threshold may be applied before the requirement to record? This would optimally allow reliance on existing organisational frameworks that may be globally consistent for international banks; and
- CPS 230 paragraph 27(c) / draft CPG 230 paragraphs 37-40 - 'Operational risk profile and assessment'– Scenario analysis – Can APRA confirm that scenario analysis undertaken at a global product aligned level is sufficient for this purpose?

Consistent understanding across the finance ecosystem

For the benefits of proportional regulation to be realised, it is vital that there is a consistent understanding among all industry participants, regarding APRA's expectations on how proportionality is to be considered across entities with differing "size, business

mix and complexity"[2]. APRA has a key role to play in ensuring this common understanding across not only regulated entities and their suppliers but also assurance and advisory firms. Without a common understanding, implementation and assurance requirements are likely to be 'scaled up'. AFMA notes a number of public submissions to the draft CPS 230 highlight this concerning evolution, such as where assurance and auditing providers seek demonstrated compliance on a 'line by line' manner.

To combat this, AFMA recommends that APRA engage widely, including with affected non-regulated firms in addition to assurance and advisory firms, regarding the proposed reforms. AFMA is available to assist with this engagement.

4. Systems approach to managing interdependencies

AFMA notes the removal of paragraph 53(c) from the draft CPS 230 which would have required entities to "take reasonable steps to assess whether the provider is systemically important in Australia". This is a welcome change as APRA and the CFR are better placed to make these systemic assessments. However, paragraph 91 in the draft CPG 230 creates a materially similar, and arguably unachievable, burden by requiring risk management of fourth and other downstream service providers.

To reduce the burden of this requirement and to better enable regulated entities to assess the impact and risks of service providers, AFMA encourages APRA to share its assessments of interdependencies in the finance industry. In making its assessments, AFMA encourages APRA to take a systems approach to identify, reduce and manage the risks from interdependencies. This could include:

- supervisory stress tests of central service providers;
- partnering with ASIC to ensure there is adequate due diligence over the ability of key industry service providers that pose systemic / contagion risk to comply with the requirements of CPS 230 prior to licences being granted;
- providing greater clarity on APRA's expectations where the industry places reliance on a concentrated number of key service providers;
- updating CPG 230 paragraph 91 to distinguish between the requirement to manage third, fourth, nth parties vs systemic third, fourth, nth parties over which there is either limited visibility and/or ability to influence; and
- recognising the limitations of due diligence for key industry providers and taking a less stringent approach on the regulated entity under CPG 230 paragraph 89 for process mapping and verification.

Such an approach would increase the overall resilience of Australia's financial system.

[2] Prudential Standards CPS 230 Operational Risk Management page 1 and Prudential Practice Guide draft CPG 230 Operational Risk Management, integrated version, page 7.

Appendix B: Specific Observation

CPS 230 paragraph 12 (Draft CPG 230 page 7)
Further guidance on the difference between 'manage operational risk' vs. 'control operational risk' would assist industry. It is unclear if APRA views these as separate activities and if so, how APRA views the differences between the two.

Draft CPG 230 paragraph 4
Clarification on 'high-level' for critical operations - does this relate to a subset of processes within the service, or all processes but 'bucketed' dependencies without the detail of a process flow?

Draft CPG 230 paragraph 6
Further guidance regarding how APRA expects ADIs to assess how a group policy is "appropriate to its size, business mix and complexity" would be welcomed.

Draft CPG 230 paragraph 12
Is it correct to interpret the usage of the term non-financial risk to be synonymous with operational risk?

Draft CPG 230 paragraph 13
Does APRA expect local accountabilities to be set where group responsibilities are out of jurisdiction?

Draft CPG 230 paragraph 16e
It would not be feasible for the Board to consider 'expert opinion or other means' for all circumstances. Can APRA provide more guidance as to the situations where there is an expectation for the Board to consider 'expert opinion or other means' beyond Internal Audit?

CPS 230 paragraph 25 (Draft CPG 230 page 14)
Paragraph 25 states "In managing technology risks, an APRA-regulated entity must monitor the age and health of its information assets and meet requirements for information security in CPS 234…". AFMA notes that this is an additional control to monitor the age and health of information assets beyond CPS 234 which already outlines requirements with respect to managing information assets and security. AFMA recommends for the Prudential Guidance to align with CPS 234 paragraph 21.

Draft CPG 230 paragraph 24
In addition to the suggested drafting changes for paragraph 23 discussed in main body of this letter, AFMA notes that end-to-end process mapping across all business operations may not be feasible for large complex organisations. AFMA encourages APRA to allow a risk-based approach to this requirement, such as for end-to-end process mapping to focus on a sub-set of operations based on a set of pre-defined risk-based criteria, such as business operations aligned to critical services, or business operations that are high in complexity, or have a history of operational risk issues.

Draft CPG 230 paragraph 29
The definition of 'frequently' is unclear to industry. For example, this may vary between institutions given the differences in size, complexity, risk profile, etc. AFMA recommends APRA consider replacing 'frequently' with 'on a regular basis' commensurate with the institution's risk profile.

Draft CPG 230 paragraph 31
Real-time reporting will not practically always be possible. AFMA recommends redrafting paragraph 21 to refer to 'timely' reporting as an acceptable approach.

Draft CPG 230 paragraph 33
It is unclear to industry if this self-assessment is to be applied with the Operational Resilience lens. Further guidance on the steps within Table 2 would assist industry. For example, per the table, it would appear that assessment of residual risk occurs before identification of controls. However, residual risk takes into consideration controls and their effectiveness. As such, it cannot actually take place until after controls have been identified and their effectiveness determined.

Draft CPG 230 paragraph 35
This speaks to an entity's overarching Operational Risk, whereas Figure 1 explicitly relates to a subsection of these requirements through critical Operations.
Figure 1: It is unclear if this represents a critical operation split into its critical processes. If this is the intent, settlement would be a process within a critical operation.
Further guidance from APRA would be helpful.

Draft CPG 230 paragraph 36e
Paragraph 36e appears to extend the requirements beyond critical operations. AFMA recommends this drafting be removed.
If it is retained and/or redrafted, further clarity would assist industry understand if the mapping of non-critical operations is to be linked to the harm to clients, markets or the financial system, as opposed to the risks internal to the entity.
AFMA notes that identification of associated risks to processes driven by criticality of services / operations would diverge from other global regulation.

Draft CPG 230 paragraph 37
Where an ADI is not required to perform capital calculations, would this requirement still be applicable?

Draft CPG 230 paragraph 39
Can APRA provide guidance where operations are unable to remain within tolerance for disruptions (such a cyber scenarios in which a state-sponsored attack / denial of service)?

Draft CPG 230 paragraph 45b
Third Parties may be reluctant to provide controls information. As such, this requirement may be challenging for industry to accommodate. Can APRA provide guidance on how industry can achieve this requirement in obtaining control design and effectiveness testing results as they relate to a particular supplier / service provider including consistent application across external suppliers of DE/OE practices.

Draft CPG 230 paragraph 45c
Can a definition or an example be provided for 'responsive control'?

Draft CPG 230 paragraph 45f
If controls are deemed effective, this is typically because control testing results met the pre-defined success criteria. AFMA suggests clarifying this paragraph to require control effectiveness assessment to be supported by appropriate evidence.

Draft CPG 230 paragraph 45g
The impact on control effectiveness is difficult to determine unless controls are re-assessed. AFMA suggests clarifying to the effect that changes in the business

environment or business strategies should be considered to determine if controls need to be re-assessed for effectiveness.

CPS 230 paragraphs 32 and 33 (Draft CPG 230 page 20)
Can APRA clarify if material impact is to be based on the institution's internal materiality threshold, or does APRA have a prescribed threshold for materiality?

Can APRA provide further guidance regarding the relationship between the notification requirement of 72 hours, in CPS 230 paragraph 33, and the requirement to notify under 'Business continuity plan' (CPS 230 paragraph 42) – "*As soon as possible and not later than 24 hours after a disruption to a critical operation outside of tolerance*".
This could be provided, for example, by including a footnote to Table 1 page 10 of the draft CPG 230, along the lines of "where an operational risk incident is also a business continuity event, a notification should be made at the earliest of the two definitions in Table 1. Where an operational risk incident becomes a notifiable business continuity event, APRA would expect an additional notification to inform them of the development in line with paragraph 42 of CPS 230".
Furthermore, a worked example in the Prudential Guidance would provide greater clarity.

Draft CPG 230 paragraph 51
Incidents and near-misses can only be linked to controls if the event was caused by a control breakdown. Where the cause was an absence of control, it would not be possible to link the event to a control. AFMA recommends clarifying language to account for these two types of situations.

Draft CPG 230 paragraph 52
AFMA recommends that, from an order of steps perspective, it may be more prudent for containment to come before escalation, since focusing on escalation before containment could allow the impact to continue growing.

Draft CPG 230 paragraph 59
Does APRA expect the capture of businesses including internal services that directly underpin outward facing services, such as availability of Hedging, internal Funding & Liquidity?

CPS 230 paragraph 38 (Draft CPG 230 page 24)
Can APRA provide some examples for tolerance levels and indicators?

CPS 230.38(a) - The PRA in the UK notes that an Impact Tolerance is different to Risk Appetite (See PRA Statement of Policy, Operational Resilience, March 2021, Section 3 "The relationship between operational resilience and operational risk policy"). AFMA recommends further consideration be given to aligning the guidance with other definitions of Impact Tolerance or Tolerance for Disruption, as seen in, for example, the BCBS, UK, HK and Switzerland.

Draft CPG 230 paragraph 62
Global regulation states tolerances for disruption under 'severe but plausible' disruptions to sit outside of risk appetite. AFMA suggest this should be clarified within paragraph 62.

Draft CPG 230 paragraph 63
To industry, this appears to differ from the criteria set for dependency mapping for non-critical operations in 36e. Further guidance from APRA would be appreciated.

Draft CPG 230 paragraph 64f
This paragraph states "an entity could consider… recovery objects that have previously been defined by the entity under the superseded CPS 232" (emphasis added).' This contrasts to paragraph 58e, which states "a prudent entity would consider… business operations that have previously been defined by the entity as critical through business impact analysis required under the superseded CPS 232" (emphasis added). AFMA recommends paragraph 58e be modified to include the term 'could'.

Draft CPG 230 paragraph 66
Does APRA expect testing for both minimum service levels and maximum data loss on an annual basis?

CPS 230 paragraphs 40-42 (Draft CPG 230 page 26)
CPS230 paragraph 40(b) – Can APRA provide further clarity around "triggers" it would expect to identify a disruption?

CPS230 paragraph 42 – AFMA recommends updating CPG 230 to include guidance to the point from which the 24-hour period is triggered. Practically, this should be from the point of becoming aware of the disruption which is consistent with the terminology in CPS 234 paragraph 35.

CPS 230 paragraphs 43-44 (Draft CPG 230 page 27)
CPS 230 paragraph 43 requires an annual business continuity exercise while CPG 230 paragraph 71 provides for a multi-year timeframe. Can APRA clarify this discrepancy?

CPS 230 paragraph 44 – AFMA recommends the guidance be updated to incorporate an example of an APRA-determined scenario.

Draft CPG 230 paragraph 72
Does APRA foresee including requirements for joint testing? Will this be more productive once the industry has become more standardised with the tolerances for disruption?

Draft CPG 230 paragraph 80
While the most appropriate cadence for (additional) assurance 'through expert opinion and other means' will vary by organisation AFMA notes that other global regulators set this at every 2 to 3 years. While AFMA supports individual organisations defining their respective cadences taking into account their own organisational requirements, industry does not see a fixed period less than 2 to 3 years as necessary.

Draft CPG 230 paragraph 89
Given the commonality of various service providers, this requirement will likely be very duplicative and burdensome, for service providers and service recipients. Engagement with third party service provider by APRA will be an important component of ensuring consistent application across the finance industry, including the maintenance of APRA's intent regarding proportional application.

Draft CPG 230 paragraphs 91 and 92
Practically, short of cancelling a relationship with a third party provider, it is unclear how an entity could enforce these requirements (on third parties).

Where a power imbalance exists and entities cannot practically avoid using certain third party providers, it may be appropriate, that APRA engage these third party providers. Due to competition law restrictions, it may not be appropriate for industry, or industry associations, to lead this engagement.

Additionally, it is unclear to industry if the MSP notification/ offshoring consultation obligations extends to material 4th party arrangements in the context of a Foreign ADI where it has outsourced to head office or under intragroup arrangements. Similarly, it is unclear if the head office and the branch be seen as one entity and the service provider arrangements by head office is considered third party.

Specifically, regarding cloud computing, could APRA provide further guidelines on its expectations regarding these services arrangements, especially in light of a significant and ongoing increase in cloud arrangements (SaaS, PaaS, IaaS etc.) across the industry due to increased investment in technology and continuous advancement in product offerings?

CPS 230 paragraphs 49 and 50 (Draft CPG 230 page 32)
Paragraphs 94 and 96 set out matters relevant to the general materiality determination. Paragraph 97 sets out the requirements should a service prescribed by APRA as material not be classified as material. Can APRA clarify to what extent component parts of the overall risk management function provided through an intragroup agreement by a corporate parent or related parties would be subject to the prescribed classification as a material service? It is unclear if all and any component parts of the risk management function to be classified as material or if the reference is rather to the outsourcing of the overall risk management function.

It would help industry consistency if APRA clarified its expectations regarding what constitutes "core technology services". Can APRA provide some examples, for example, technology support; data hosting; data centres; cloud based service providers?

CPS 230 paragraph 51 (Draft CPG 230 page 33)
AFMA requests APRA specify minimum requirements for inclusion on the register and also consider to what extent this should be aligned with other regulators, for example in APAC. This clarification is extremely important as it may require system modifications to include the required datapoints. Any system modifications can potentially take significant time.
It would also be appreciated if APRA can specify the first date for submission of the register of material service providers. Also, whether submission is necessary if no material changes from the previous submission.

Draft CPG 230 paragraphs 94 and 97
There may be third parties identified through dependency mapping of critical operations that are not material in nature. Will APRA allow for the rationalisation of third parties deemed material following the designation of a critical operation?

Draft CPG 230 paragraph 96
In its revised format, CPS 230 clarifies APRA's intention to narrow the definition of MSPs and this is supported by the guidance under paragraphs 94, 95 and 97 which ensure "all service providers" are considered in the risk assessment and their impact to operational risk. Paragraph 96, however, is a tautology of such guidance and does not appear consistent with APRA's overall intention of clarifying the concept of a MSP. Given the ambiguity that this paragraph creates, AFMA strongly recommends it be removed.

Retaining Paragraph 96 may lead to wide ranging interpretation and would require further clarification when considered in conjunction with paragraphs 94, 95 and 97.

CPS 230 paragraphs 59 (Draft CPG 230 page 36)

AFMA notes that no guidance is provided by APRA in relation to this notification requirement. AFMA recommends the draft CPG 230 be updated to clarify that where there is a critical operation that is provided by an offshore service provider, and notification has been made under paragraph 59(b) before entering into the material offshoring arrangement, that further notification is not required within 20 days after entering into the agreement under 59(a).

Furthermore, a worked example in the draft CPG 230 would provide greater clarity.