28 October 2022

Mr Gideon Holland
General Manager Policy Development
Policy & Advice Division
Australian Prudential Regulation Authority

Via email: PolicyDevelopment@apra.gov.au

Dear Mr Holland

CPS 230 Operational Risk Management

COBA welcomes the opportunity to respond to APRA's Discussion paper - Strengthening operational risk management and the draft CPS 230 Operational Risk Management.

COBA is the industry association for Australia's customer-owned banking institutions (mutual banks, credit unions and building societies). Our sector has over $150 billion in assets and 5 million customers. Customer-owned banks account for around two-thirds of the total number of domestic ADIs and deliver competition and market-leading levels of customer satisfaction in the retail banking market.

Incorporating proportionality for simpler and smaller ADIs

We welcome APRA seeking views on incorporating proportionality into its revised standard.

Proportionality is important as it ensures that regulation, how regulators apply regulation and how regulated entities respond to regulation is right-sized to the underlying risks. This ensures regulatory responses are targeted to minimise the burden of the chosen intervention. Targeting increases the likelihood that an incremental change will have a positive net benefit.

As smaller, simpler and less risky ADIs, we are a strong supporter of proportional regulation. We represent a diverse range of customer-owned banks with some members expected to be significant financial institutions (SFIs) and some that even may be considered small businesses under employee number definitions. While our members vary in size, they remain simple retail banking businesses, unlike their larger listed ADI peers.

The first way that APRA can include proportionality in CPS 230 is through a complexity lens. More complex entities may need greater focus while simpler entities less. APRA can support proportionality in this aspect by ensuring that any definitions relating to scope (e.g. critical functions, critical operations, material service providers) can scale up and down with complexity. Simpler businesses should have few in-scope requirements.

The second way is through an entity size element. Smaller entities are likely to have less bargaining power compared to larger entities. This difference means negotiations regarding contract terms may take more time, particularly if material service providers (MSPs) are unfamiliar with these terms. It is likely the smaller entities with need more time to meet APRA's requirements, particularly the contractual requirements. This extends beyond just the SFI/non-SFI distinction. We note we have some members that may become SFIs via merger in mid-2023, which could make meeting a short timeline difficult.

We would also welcome further engagement to examine APRA's potential scope for proportionality for specific requirements as outlined in APRA's discussion paper.

Focusing operational risk management on key suppliers to ensure proportionality

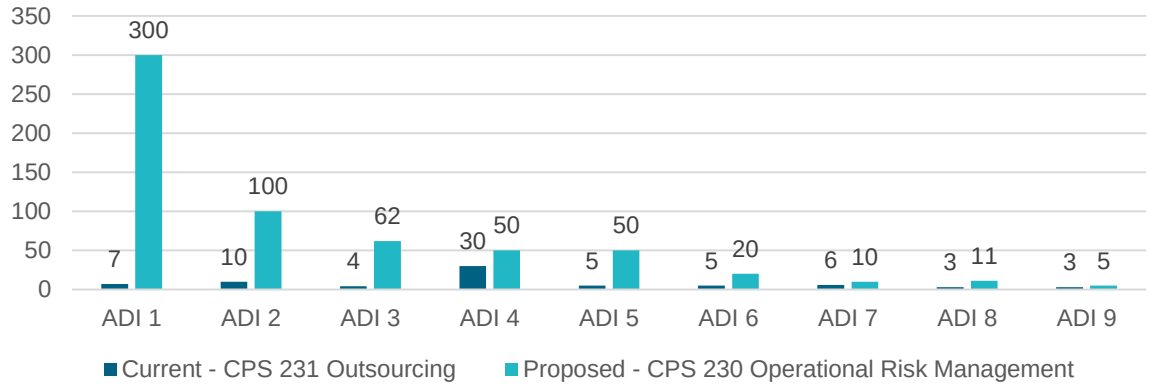
We are concerned about the potential for a significant increase in MSPs in the proposed CPS 230. While we expect an increase due to the scope change to all service providers, COBA believes that APRA should clarify and narrow the MSP scope. This change will help to ensure that the number of MSPs is at a level where costs better align with benefits.

The proposed MSP definitions can lead to a significant increase in the number of entities covered by the revised material service provider requirements. The elements of the definitions include CPS 234 Information Security coverage[1], designated service provider types[2] and the critical operation or materiality test.[3] These multiple elements can lead to an overprescription of MSPs. We provide an outline of this in **Attachment A**.

We support a principles-based approach focussed on CPS 230 para 48. Our view is that the interpretation of CPS 230 para 49 can lead to a large number of MSPs due to their service type rather than due to critical operations or material operational risk thresholds. This list may lead to MSP overidentification given the cross-industry nature of the standard. Some service types may not be considered material for all of APRA's regulated entity types. It may be more appropriate to provide MSP guidance (i.e. CPS 230 para 49) on an industry-type basis. Some functions may also be easily in-sourced or 'switched' (e.g. mortgage brokers to proprietary channels). We suggest that APRA move CPS 230 para 49 into guidance, with the caveat not all providers in these categories are MSPs, to ensure proportionality as this would allow entities more discretion to identify MSPs to ensure proportionality.

We also note that not all CPS 234 providers would be MSPs under a materiality test (e.g. para 48). However, CPS 230 para 50 means that are likely to be designated as MSPs. We also seek clarity on this para given that CPS 234 refers to a spectrum of "criticality and sensitivity" rather than a binary "critical and sensitive".

Graph 1: Expected number of CPS 230 Material Service Providers – selection of ADIs



Overprescribing the number of MSPs will be costly as ADIs will need to divert resources away from higher value risk and compliance activities to work with additional MSPs. Graph 1 shows the variance in the potential number of MSPs from CPS 230 for a subset of COBA members.

[1] Draft CPS 230 para 50

[2] Draft CPS 230 para 49

[3] Draft CPS 230 para 48

We have concerns about how smaller ADIs with limited bargaining power will be able to negotiate these clauses into service contracts in a timely fashion, particularly if there are expected to be a large number of MSPs.

Creating reasonable implementation timeframes

Our view is that APRA should provide more time for smaller entities (i.e. non-majors) to implement the revised CPS 230 requirements. We note that APRA currently proposes to introduce this standard on 1 January 2024 and "plans to finalise the standard in early 2023 and release draft guidance for consultation." This provides just over 14 months from today, less than one year from the release of the final standard and an even shorter time from the final guidance.

We suggest that APRA implement CPS 230 at least 24 months after the finalisation of its guidance. This will provide time for smaller ADIs to adjust to the new requirements in an orderly manner. We note that the impending implementation of FAR and CPS 190 is likely to be on the implementation radar for 2023, impacting the ability to get ready for CPS 230.

Based on the above timeline, we suggest that APRA take a next contract renewal or at least 12 months after the implementation date to update MSP contracts. Given the potential difficulties of introducing some APRA-specific clauses in MSP contracts, we suggest that more time is also given to smaller ADIs for the negotiation of these clauses. Additional time will also mean that larger APRA-regulated entities will help establish APRA's CPS 230 requirements as a 'ticket to play' amongst MSPs with APRA-regulated entities. COBA believes that APRA should communicate its expectations around CPS 230 directly to any potential MSPs. This will support smaller ADIs' ability to meet APRA's requirements in a timely and efficient manner. We note that in this model smaller ADIs will still be updating contracts as they come up for renewal.

As noted above, we would like to reiterate that specific entities currently in merger processes may find meeting the contractual requirements particularly burdensome. COBA and impacted members will engage with APRA on this.

Outlining common definitions

APRA should provide common definitions for certain terms to help minimise implementation costs for all entities, including non-APRA regulated entities. This clarity will support all entities to understand APRA's requirements and reduce ambiguity in definitions. It will also assist to provide discipline around the use of certain terms.

Clarifying APRA expectations on fourth parties

We note that extending expectations to fourth parties can be difficult so we request more clarity on APRA's expectations. The identification of fourth parties, their risks and management of these risks can be difficult for smaller APRA-regulated entities with limited bargaining power.

We suggest that APRA provide more clarity around what it expects ADIs to do concerning fourth parties, whether it is engaging with individual fourth parties or having a policy to address risks as a collective. We also note that the size of this task can exponentially increase with the MSP definition.

Clarifying the status of the cloud computing guide

We seek clarity on the status of APRA's cloud computing outsourcing guide given that the standards of which this guide 'hangs off' are being consolidated into CPS 230. We note that APRA outlines the proposed new framework in Table 2 of the Discussion Paper. However, this does not include the cloud computing guide.

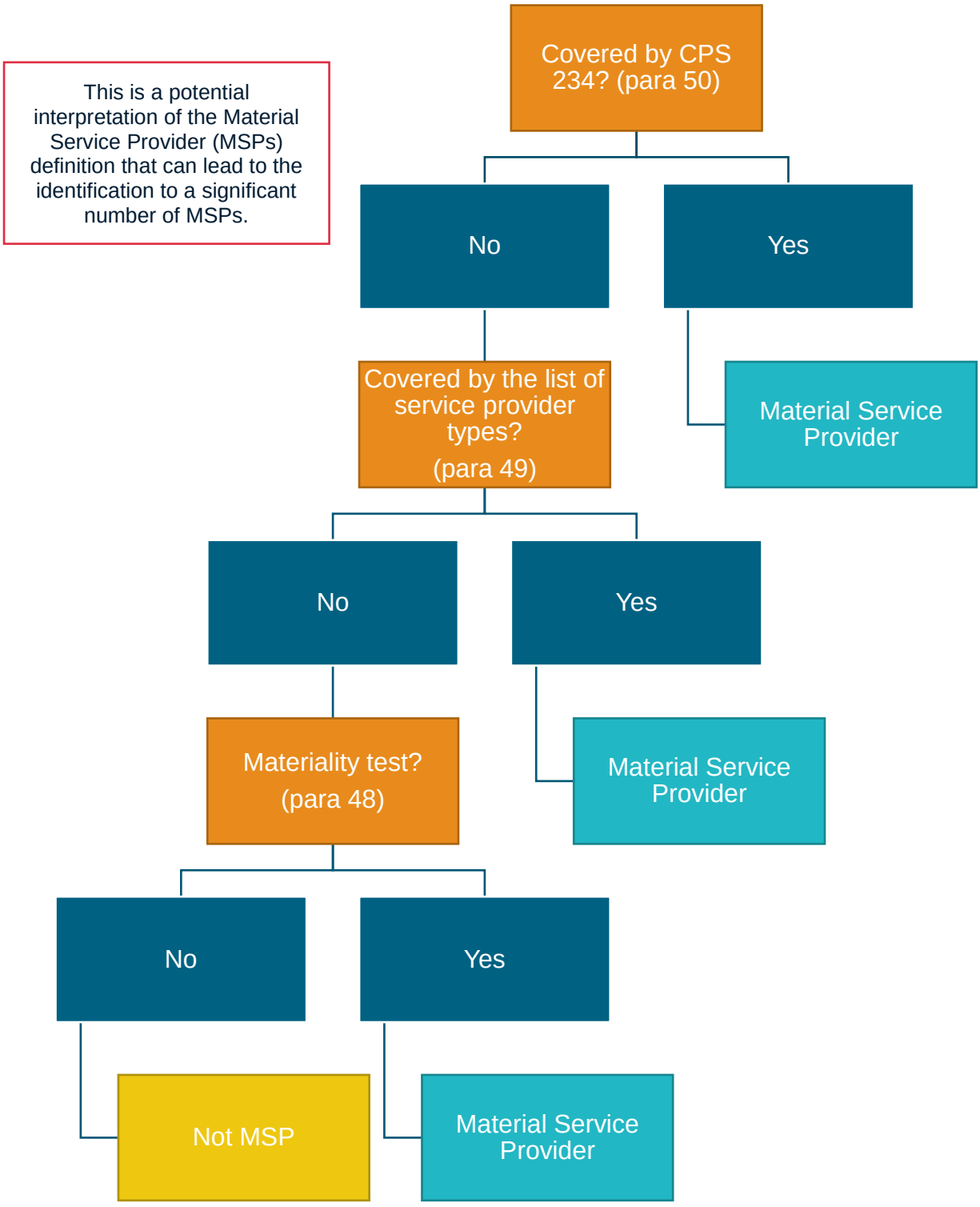
We provide some specific comments on CPS 230 in **Attachment B**. If you wish to discuss any aspect of this submission, please contact Mark Nguyen (mnguyen@coba.asn.au).

Yours sincerely

MICHAEL LAWRENCE
Chief Executive Officer

Attachment A: Material Service Providers

This is a potential interpretation of the Material Service Provider (MSPs) definition that can lead to the identification to a significant number of MSPs.



Attachment B: Specific CPS 230 Comments

Section	Item	Comment
Para 14	**Reliance on service providers and meeting prudential obligations**	We seek more information on the intent and interpretation of para 14. “An APRA-regulated entity must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks” We believe this should be qualified with to take reasonable steps given it is not possible to “ensure” given the wide range of service providers. We query if there are the transitional arrangements with this paragraph and also if this covers all service providers or just material service providers.
Para 15f	**Risk Management Framework**	On requirements to “develop and maintain processes for the management of service provider arrangements”. Is this for all service providers or just for material service providers?
Para 19	**Role of the Board**	We seek clarity that this would allow delegation to Board subcommittees[4] or delegation to senior executive where appropriate. A COBA member notes that “Boards should be focused on framework and policy level, as the lower level detail is not aligned to their skillsets and broader due diligence role. Senior management should be assigned responsibility at a detailed level as they are SMEs and involved in a daily basis in operations.”

[4] COBA notes the paper defines board as “Board of directors of an institution”

Section	Item	Comment
Para 21c	**Performance reporting on material service provider arrangements.**	Is this a board or management responsibility - our preliminary overview of material service providers is 62 – for the board to review the risk and performance of each material service provider seems onerous. Management should enforce the Board approved policy and report by exception to the Board – also note para 23 where the onus is on Senior Management
Para 22	**Comprehensive information**	We seek more information on what is considered to be comprehensive. We do not believe it is APRA's intent to overload Boards with information. We consider this could be comprehensive in the context of fulfilling the Board's oversight duties or comprehensive in terms of the universe of information.
Para 24	**Information technology (IT) infrastructure definition**	We seek clarity on the definition of IT infrastructure. Is it more than just physical? How broad is this definition? Does it include databases and applications? What is considered to be health? We note in consideration that age and health are only two factors. Another key factor that is the level of support.
Para 25	**Operational risk profile and operational resilience definition**	We seek definitions of the following to ensure consistency.
Para 26b	**Critical operations**	We need more clarity on what APRA considers critical operations and does this link back to Material Service Providers. We note this defined for BCP in para 34/35 so clarification if it applies the same for application to strategic decisions.
Para 27	**Comprehensive risk assessments and before providing a material service to another party**	We note that a broad interpretation of "another party" could include a retail customer of an ADI if the provided service is material. We do not believe this is APRA's intent given its example in the Discussion Paper on page 18. APRA should clarify this.

Section	Item	Comment
		We seek clarity as to who assesses materiality and from whose point of view is this materiality (to the ADI or other party)
Para 29	**Focusing on key internal controls**	We suggest that any requirements relating to controls clarify whether they refer to all controls or material/key controls. We suggest that APRA focus requirements on key controls to ensure maximum relative value.
Para 32	**Material notifications**	We seek further guidance on the definition of materiality when it comes to incident notification. It is also of interest what support APRA may provide in these situations. We suggest any definition include duration and criticality in order to focus the reporting on critical incidents.
Para 33	**Clarity on business continuity planning frameworks and plans**	We note that there is some confusion around the use of BCP. In some cases, it appears as though it is referring to a BCP framework, while in other specific plan. We seek further clarification on this.
Para 34 & 35	**Definition of critical operations**	We note that some of these critical operations can be brought back online quite quickly. For example, customer inquiries can be handled by a number of staff. A wider definition here also feeds into an expanded Material Service Provider definition.
Para 37	**Data loss definition**	We seek more information on the definition of data loss.
Para 42	**Clarity on testing requirements**	We seek more information on whether this the testing requirement applies to the framework or to all the plans. Does it all need to be tested annually? Or does it just require a testing process to be in place?

Section	Item	Comment
Para 43	. **APRA-determined scenario**	We seek more information on how this works in practice – how much notice would institutions get? Would APRA provide a playbook of expected scenario testing exercises?
Para 46	**Comprehensive service provider management policy**	We seek clarity that this policy would only relate to material service providers rather than all service providers given that para 47 clearly refers to MSPs.
Para 47	**Fourth party risks**	We seek more clarity on APRA's expectations. The identification of specific fourth parties, their risks and management of these risk can be difficult for smaller APRA-regulated entities with limited bargaining power.
Para 48-50	**Material service providers definition**	Comments provided in main body.
Para 51	**Submission of MSP register**	We suggest that this replace the 20 day notification process. We query how quickly APRA intends to act on this information and what APRA needs this information. We also seek guidance around APRA's use of its APRA-required classification powers. We have concerns that there may be 'benchmarking' in terms of MSP classification where one ADI may consider a provider a supplier an MSP and another may not. We note there may be valid reasons that this is not the case.
Para 52a	**Due diligence - appropriate tender**	We note that to incorporate renewals this may better be worded to include a "where appropriate" for a tender and selection process, given this may not be appropriate for renewals or even new contracts.
Para 52c	**Assessing systemically important providers**	We believe APRA is better placed to do this than small APRA-regulated entities. The major banks may be able to do this given their own systemic importance but this is a far task for others. We also query what APRA would expect entities to do with this information once obtained.

Section	Item	Comment
Para 53c	**Ensuring ability to meet legal obligations**	We assume this refers to the APRA-regulated entity. As in our comment for para 14, this could be difficult to "ensure" and may be hard for entities to include given the disparate bargaining power between entities and MSPs.
Para 58	**Notification requirements of new MSPs**	We seek more guidance on the notification process. We note that for para 58a this appears to be a simple notification after the fact in line with the existing CPS 231 Outsourcing. However, para 58b removes the consult requirement of CPS 231 but still requires before the act notification.
Para 59	**"material service provider for a critical operation"**	We note that this introduces 'material service provider for a critical operation' when other paragraphs just refer to material service providers. Is this the same?