PRUDENTIAL PRACTICE GUIDE

DRAFT CPG 230 OPERATIONAL RISK MANAGEMENT

SUBMISSION TO THE AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY

13 October 2023

KEY POINTS

1. ANZ acknowledges and thanks the Australian Prudential Regulation Authority **(APRA**) for considering ANZ and industry's feedback to the Prudential Standard CPS 230 Operational Risk Management **(CPS 230)** consultation and for the opportunity to comment on the draft Prudential Practice Guide CPG 230 Operational Risk Management **(CPG 230)**.

2. We refer to the Australian Banking Association's **(ABA)** Submission to the consultation of CPG 230 **(ABA Submission)** which we support. Our Submission is to be read in conjunction with the ABA Submission. Where relevant in this Submission, we expand on the matters raised in the ABA Submission including how the CPG 230 guidance specifically impacts ANZ.

3. We appreciate the clarification and guidance provided by CPG 230, however note that further clarifications / amendments on scope and key concepts outlined in CPG 230 will assist in meeting the intent of **CPS 230** within required timeframes. This is to minimise potential unintentional increase in scope of Critical Operations (COs), mapping of end-to-end business operations as well as the size of the Material Service Provider (MSP) portfolio that may result in difficult, or almost impossible, enforcement of fourth party commitments.

4. We have three key points for APRA's consideration on CPG 230 (further detailed below in **'Detailed Observations'**).

5. Firstly, amendments to CPG 230 to increase alignment to the scope of **CPS 230** such as:

    a. Reference to approaches that may involve end-to-end business process mapping across all business operations, including those performed by Service Providers.

    b. Consideration of additional indirect material adverse impacts for identifying COs.

    c. Fourth party risk management extending beyond those that support COs, to downstream Service Providers (i.e., nth parties) including management of the correlated risk that arises from reliance on the same fourth parties by Services Providers.

    d. Extending the application of aggregation of services to also consider aggregation of services provided by a 'cohort' of Service Providers rather than just a particular Service Provider.

6. Secondly, further specificity or guidance would be welcomed to assist with implementation and application of **CPS 230** requirements across areas such as:

    a. Expectations in relation to Business Continuity risk management for operations that are not classified as COs, providing flexibility for each regulated entity to appropriately manage disruption risk of non-COs as part of their operational risk management approach.

    b. Consideration of 'aggregate/ totality of services' provided by the service provider to include flexibility to the regulated entities to aggregate services where it is reasonable and logical to do so.

    c. Criteria, considerations, and / or key factors that APRA regulated entities would typically be expected to consider when assessing concentration and country / region risks.

7. Thirdly, consistent with the Banking Executive Accountability Regime **(BEAR)** and Financial Accountability Regime **(FAR)** we suggest amendments to CPG 230 to ensure it is in-line with the oversight responsibilities of the Board.

8. We have set out more detailed feedback in the **Detailed Observations** section of this document highlighting ANZ's recommendation to each area of feedback as stated below.

DETAILED OBSERVATIONS

Glossary

9. We recommend extending the glossary to include definition of key terms referenced throughout the guidance document, such as operations, business operations, function and process. This will assist in connecting various paragraphs within the guidance and assist in consistent interpretation where the terms are used in different contexts throughout CPG 230.

Key Principles

10. CPG 230 uses the terms 'senior management', 'senior management of APRA regulated entity' and 'senior managers within business.' We recommend CPG 230 is updated to reference 'senior management of the institution' to provide consistency throughout the document and in line with Prudential Standard **CPS 220** Risk Management (**CPS 220**).

Operational Risk Management

End-to-end Process Mapping

11. Paragraph 24 of CPG 230 references 'APRA expects that senior management would ensure that the operational risk management framework operates effectively...This may involve end-to-end business process mapping across all business operations, including those performed by service providers'. It may prove difficult or impractical to map all components of service providers' processes. We recommend this be amended to 'end-to-end business process mapping across relevant components of business operations, including consideration of those performed by service providers' to better align with the better practice outlined in paragraph 36.

12. Paragraph 35 of CPG 230 states that 'clearly defining the end-to-end processes, as set out in Figure 1 … enables an entity to identify risks, obligations, key data and controls'. With the reference to COs in Figure 1 and the intent of **CPS 230** to focus on COs, we recommend an amendment to add 'across critical operations.'

Technology and Crypto assets

13. Paragraph 27 of CPG 230 states 'emerging technologies may result in novel operational risks for entities' and that 'better practice is for these risks to be considered on a regular basis.' We would welcome further clarity / guidance including examples of emerging technologies from the previous 5 to 10 years where it would fall within the category of novel operational risks and whether regular review should be based on the adoption of these technologies by the entity and/or the risk of non-adoption of such technologies.

APRA Reporting

14. Paragraphs 11, 51 to 53 of CPG 230 provide guidance on managing 'operational risk incidents.' We recommend CPG 230 is updated to reference the term 'risk events and incidents' as provided in paragraph 35(d) of **CPS 220**.

Risk Management

15. CPG 230 paragraph 45(b) sets out better practice to capture controls owned by related parties and Service Providers. We would welcome clarity / guidance that this is focused on MSPs.

16. Paragraph 46 of CPG 230 states that 'the frequency of testing would reflect the ratings of the risks the controls are mitigating, as well as the frequency of control usage'. We would welcome clarity in CPG 230 to confirm this is the inherent rating of the risks the controls are mitigating.

Critical Operations / Business Continuity

Scope and definition of Critical Operations (COs)

17. Paragraph 59 of CPG 230 describes 'outward-facing services' as the focus for identifying COs We note that Paragraph 58 (b) of CPG 230 states that an APRA regulated entity would also consider indirect material adverse impacts such as on the entity's profitability and financial soundness for identifying COs. This may unintentionally increase the number of COs and related effort without an equivalent benefit to the policy objectives of **CPS 230**. We recommend APRA limiting Paragraph 58 (b) and Paragraph 64 (b) to focus on outward-facing services in line with paragraph 59.

18. The guidance set out in Paragraph 58 (c) and 64 (c) of CPG 230 appear to broaden and elevate the scope of an entity's COs beyond 'its role in the financial system'. It will be difficult for APRA regulated entities to assess and address impact on the broader financial system or economy individually, including flow on effects or contagion. We suggest these requirements better align with the objectives of Prudential Standard **CPS 900** Resolution Planning (**CPS 900**), and recommend APRA considers removing Paragraph 58 (c).

19. Paragraph 36 (d) of **CPS 230** requires APRA regulated entities to classify 'systems and infrastructure needed to support Critical Operations' as COs in their own right. We would welcome additional clarity in CPG 230 regarding what APRA prescribes as a CO versus components of or a dependency of a Critical Operation to avoid any potential unintentional increase in the number of COs without benefiting the policy objectives of **CPS 230**.

20. Paragraph 61 of CPG 230 expects all APRA determined Critical Functions under **CPS 900** to be classified as COs. ANZ agrees that Critical Functions may also be COs, however due to differences in definition and focus, which may not always be the case. This may unintentionally increase the scope of COs and create further complexity and effort (e.g., when setting tolerance levels, developing BCPs and scenario testing). For example, 'Home Loans' have been classified in consultation with APRA as a Critical Function under **CPS 900**, however under **CPS 230** the 'Mortgage Settlement' component of the Home Loan life cycle would be considered a CO. We recommend amendments to CPG 230 to suggest consideration of Critical Functions under **CPS 900** as COs.

Setting Tolerance levels and Business Continuity Management (BCM)

21. We would welcome further clarity within CPG 230 on APRA's expectations in relation to BC for operations that are not classified as COs, including:

a. References to BC / plans and tolerance levels are in the context of, and relevant to, COs only (for example CPG 230 Paragraphs 17, 18 and 19 and **CPS 230** Paragraph 21).
b. APRA expects regulated entities to appropriately manage Disruption Risk of non-COs as part of the Operational Risk management approach.

22. Paragraph 17 of CPG 230 provides an example of a 'Board-approved entity-wide BCP, supported by ... divisional BCPs'. We would welcome further guidance and sample contents within CPG 230 of an entity-wide BCP and relationship with divisional BCPs, noting the better practice in Paragraph 56 of CPG 230 which states BCM is to be approached by ADI 'irrespective of organisational structures.'

23. Paragraph 18 of CPG 230 refers to 'overall tolerance levels.' ANZ would welcome APRA to expand the examples provided in Paragraph 19 of CPG 230 to illustrate and explain this concept.

24. In alignment with **BEAR/ FAR**, the role of (members of) the Board is to be responsible for oversight of the relevant APRA regulated entity. We would welcome further specificity and guidance in Paragraphs 17, 18 and 19 of CPG 230 to:
    a. Provide clear guidance on the distinct and specific accountabilities of the Board versus senior management.

    b. Limit the Board's responsibilities to those already in place under Corporate and the **BEAR/FAR** Laws.

25. Paragraph 66 of CPG 230 provides guidance on the three types of tolerance levels as outlined in the table. We would welcome further clarification in CPG 230 whether the 'Maximum period of time' reflects the maximum period following a disruption event until the 'Minimum service levels' can be provided. We recommend amending paragraph 66 to specifically include:
    - Following a severe disruption, resuming business-as-usual may require a protracted period. To avoid unacceptable impact, entities would restore operations to 'Minimum service levels' within the 'Maximum period of time.'
    - Additionally, APRA regulated entities may not be able (to expedite restoration) or choose not to provide minimum level of services during restoration. We recommend including flexibility in application of these requirements for such cases.

Management of Material Service Providers (MSPs)

MSPs supporting crypto-assets

26. Paragraph 28 of CPG 230 states that it would be better practice to treat any service providers that are relied upon for services associated with crypto assets as material. We recommend that APRA amends this wording so that materiality assessment of service providers associated with crypto assets may be applied in a manner that is commensurate to the regulated entity's risk exposure having regard to its business objectives and risk appetite, rather than a blanket application. In its current form, it may result in excessive regulatory burden on the regulated entity and may also impede innovation and delivery of new / improved services and products to our customers.

Fourth party risk management extended to downstream service providers

27. Paragraphs 90 - 91 of CPG 230 seek to extend the requirements of fourth party risk management beyond those that support COs, but to also downstream Service Providers (i.e., nth parties) including management of the correlated risk that arises from reliance on the same fourth parties by Services Providers. This appears broader than what is required under paragraph 48(c) of **CPS 230**. It would be extremely challenging and impractical to meet this guidance. As such we recommend amendment to CPG 230 to:

    a. Limit the scope of fourth party risk management to be in line with paragraph 48(c) of **CPS 230** (i.e., those that support COs only).

    b. Provide flexibility for the regulated entity to determine and undertake appropriate minimum due diligence of material fourth parties as deemed appropriate.

    c. Specify that the assessment of 'material' fourth parties should be from the regulated entity's perspective (i.e., their assessment), and not of the MSP.

Aggregation for MSP Identification

28. Paragraph 94 (b) of CPG 230 requires consideration of 'aggregate/totality of services' provided by the Service Provider for assessing Materiality but does not clearly articulate APRA's expectation on how and what should be aggregated. We recommend amendment to paragraph 94(b) of CPG 230 to be clear when assessing Materiality, consideration of 'totality of services provided by the service provider' should be limited to where it is reasonable and logical to do so. This is because requiring regulated entities to aggregate arrangements where the business activities provisioned by the same service provider have no relationship/interdependencies, or where there is no potential for the aggregate to become material will result in unnecessary regulatory burden and compliance costs.

29. In addition, paragraph 96 of CPG 230 seeks to further extend the application of aggregation of services beyond what APRA requires under **CPS 230**. Specifically, it suggests that APRA regulated entities will need to consider aggregation of services provided by a 'cohort' of Service Providers rather than just a particular service provider. We recommend APRA to remove this expectation in CPG 230 to ensure alignment with obligations required under **CPS 230**. Further in our view, unrelated service providers will not generally give rise to operational risk in aggregate.

Monitoring / Reporting of MSPs

30. Paragraph 89 of CPG 230 expects that a prudent entity would have visibility of risk management practices of the Service Provider, including consistent process mapping for all services, whether maintained by the entity or a Service Provider. We recommend amendments to CPG 230 to permit compliance to these requirements through ongoing governance practices, onsite visits, or control monitoring & assurance rather than documentation/maintenance of Service Provider processes as that will be an onerous task for the entity and unnecessary if other assurance mechanisms are in use. Additionally, negotiating these requirements into contractual arrangements with the Service Providers may be difficult or impractical given the scale and complexity of this activity and limited by the commercial bargaining power of the respective parties and other legal obligations.

31. Further to above, we request APRA to assist in communicating obligations, including **CPS 230** timelines, to impacted MSPs to support our compliance with these obligations and drive consistency in application and interpretation of **CPS 230** across the material service

provider community. This includes MSPs who are systematically important and are relied upon across APRA regulated entities, such as financial market intermediaries, messaging and payment processing networks and market data providers.

32. Paragraph 97 of CPG 230 expects that any justification to not classify a service provider prescribed by APRA as material would be reviewed by the entity on at least an annual basis. In our view, this will cause unnecessary burden on entities, particularly where it is very unlikely that on an annual basis there may be any change to the arrangement themselves or if there were to be, that could result in a change in classification of Materiality. Hence, we recommend CPG 230 be amended by APRA so that such review be triggered when there is a material change to the scope of arrangement.

33. Paragraph 106 of CPG 230 expects regular review of key information in relation to an engagement with a Service Provider. We recommend CPG 230 to permit flexibility on determining the appropriate frequency and level of review (including provision of reporting to the senior management on MSPs) to be commensurate with the level of risk, nature and complexity associated with MSP arrangements. Additionally, we recommend APRA provide flexibility in the ongoing management of MSPs at volume and based on risk categorisation i.e., we segment / group MSPs based on the level of risk exposed to the entity, instead of managing all MSPs one-way-same-way.

34. The final clause of **CPS 230**, Paragraph 60 states 'internal audit function must review any proposed material arrangement involving the outsourcing of a critical operation'. We seek confirmation within CPG 230 that the following is the intent and correct interpretation.
    a. As the term 'outsourcing' is no longer defined by APRA within **CPS 230**, we understand the clause is referring to proposed arrangements with MSPs on which the entity relies to undertake a CO.
    b. We understand that there is no expectation for Internal Audit to review arrangements with MSPs that can expose the entity to Material Operational risks or that supports services listed as Material by APRA as **CPS 230** requires the review to be limited to only those that support COs.

Service Provider Arrangements

35. Paragraph 99 of CPG 230 requires an APRA regulated entity to consider country or region risk and concentration risk against our risk appetite. We would welcome further specificity on what types of criteria, considerations or key factors that APRA regulated entities would typically be expected to consider when assessing these types of risks. This will help to ensure consistency in application of these requirements across APRA regulated entities.

36. Paragraph 54 (f) of **CPS 230** seeks to require APRA regulated entities to 'include a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event'. As we anticipate challenges in negotiating these clauses as Service Providers may not be able to specifically identify the services that they can continue to operate in a force majeure event, that flexibility be provided, and outlined in CPG 230, in its application to limit to circumstances where it is reasonably practicable for the Service Provider to identify those parts of the contract that would continue in such an event and has been agreed to by the regulated entity.

37. In relation to paragraph 56(b) of **CPS 230**, we recommend CPG 230 to provide further guidance on APRA's expectations to identify and manage step-in risk or contagion risk that could result from the service provider arrangement given its coverage within Prudential Standard **APS 222** Association with Related Entities (**APS 222**).

38. Paragraph 57 of **CPS 230** states that 'APRA may require an APRA-regulated entity to review and make changes to a service provider arrangement where it identifies heightened prudential concerns.' We would welcome APRA's guidance or examples of scenarios where APRA could request changes to an arrangement to ensure we understand the implications of such changes to cater for this requirement if deemed necessary to support our contractual negotiations with service providers.

39. Footnote 16 of **CPS 230** states the definition of offshoring, however, does not include clarity in relation to international business aspects of a group relying on a Service Provider in its local jurisdiction. This scenario does not constitute to offshoring as per the current requirement pursuant to **CPS 231** Outsourcing standard. As we understand this continues to be the intent, we request APRA to amend CPG 230 to include this guidance to ensure clarity in offshoring requirements.

Alignment of Requirements

40. We note that APRA has confirmed in its 'Response Paper – Operational Risk Management' that **APRA's Cloud Information Paper** remains current including that APRA regulated entities should continue to engage with APRA on the use of cloud. We would welcome further clarity/guidance to ensure consistency in application across **CPS 230**, CPG 230, and the Cloud Information Paper. Specifically:
    a. Clarity in identification of MSP for cloud arrangements given that the Outsourcing test has been removed in **CPS 230** but is still referenced in APRA's Cloud Information Paper.
    b. Paragraph 59 of **CPS 230** Notification requirements versus consultation requirements under APRA's Cloud Information paper for Material Outsourcing Arrangements with Heightened/Extreme Inherent Risk. Which will take precedence? Is APRA's intention to move away from the practice of Consultation to Notification for MSPs supporting COs or involving offshoring, regardless of whether the arrangement involves Cloud noting this will lessen the regulatory burden associated with the preparation of APRA consultation Submissions.

APRA Engagement Requirements for Back Book Arrangements

41. We would welcome APRA's guidance within CPG 230 in relation to existing arrangements which may be classified as Material under **CPS 230**. Specifically, whether we need to Notify APRA post or prior (if it involves Offshoring) or consult with APRA for cloud arrangements (if requirement still holds subject to comments outlined above) by 1 July 2025, or whether they could be exempted from these requirements?

ENDS