Australian Banking Association

CPG 230 – Operational Risk Management Guidance

13 October 2023

Australian Banking Association

Table of Contents

Australian Banking Association

Key Recommendations

Critical operations

- The ABA recommends that the scope of critical operations are further clarified in CPG 230. The Guide could not only clarify what are the minimal classifications of critical operations, but also set out examples of what may not be critical operations.
- Paragraph 58 (b) of the Guide states that an APRA regulated entity would consider additional 'indirect material adverse' impacts for identifying critical operations. This is misaligned with Paragraph 59, which describes 'outward-facing services' as the focus for identifying critical operations. Moreover, adopting the approach outlined in Paragraph 58 (b) would result in a 15-20 per cent increase in the number of critical operations and related effort, which we understand is not PARA's intent. ABA recommends APRA remove the expectations as stated in Paragraph 58 (b) and Paragraph 64 (b) to limit critical operation's focus.
- CPG 230 Paragraph 61 sets out that APRA would expect all CPS 900 Critical Functions to also be classified as CPS 230 Critical Operations. Requiring every critical function to meet the obligations that apply to critical operations will result in potentially significantly higher implementation costs (Further details in Appendix B). The ABA recommends that Paragraph 61 should be removed and, instead, CPS 900 should be added as a consideration under Paragraph 58 (in other words each entity will consider critical functions but need not automatically adopt these as critical operations). Further time should also be provided after implementation of CPS 230 so that entities can integrate CPS 900 functions without reworking current processes for implementing CPS 230 critical operations.
- CPS 230 and CPG 230 are unclear on the treatment of operations that are not classified as critical operations in relation to Business Continuity Management. ABA seeks confirmation within CPG 230 that:
    - all references to Business Continuity Management / Plans and tolerance levels are in the context of, and relevant to, critical operations only; and
    - each ADI will manage disruption risk of other non-critical business operations.

End-to-End process mapping

- The inclusion of an end-to-end process lens for operational risk management could require a fundamental shift in Industry Operating Models. ABA recommends the Guide is amended to allow for flexibility and discretion for entities to be able to determine the extent of End-to-End Process Mapping (e2e) required for critical operations. For example:
    - an entire value chain;
    - e2e operational process as a component of a value chain; or
    - discrete start and end points within a critical operation with most impact to customers.

Material service providers

- Industry remains concerned about the widening requirements for monitoring material service providers. For example, Paragraph 91 explicitly notes that monitoring extends to other downstream parties beyond fourth parties, which does not align with the intent of the Standard or communication from APRA. The ABA suggest this is clarified.
- Some service providers have indicated that they are unable to support aspects of CPS230, such as providing business continuity plans, because such information is commercially sensitive. ABA recommends the inclusion of an 'exemptions process' in the Guidance, along the lines of paragraphs 23 and 24 of CPG 234. This would allow executives to accept (and document acceptance of) non-compliance with CPS 230 where a service provider:

    - does not accept contractual obligations requested by an ADI to comply with CPS 230; but
    - an entity has no practical commercial ability to transition to an alternative provider or cease obtaining the services.
- The ABA note that there are potential anti-competitive impacts that flow from the requirements of managing material service provider arrangements, as this standard burdens smaller service providers disproportionately to larger service providers.

Proportionate regulation

- APRA should exercise proportionality with respect to the obligation associated with managing third- and fourth-party service providers, the extent of e2e mapping expected for banks and the number of operations deemed critical. Further details are in Appendix A.

Policy Lead: Craig Evans, Policy Director, craig.evans@ausbanking.org.au

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

ABA submission to APRA

The ABA would like to thank APRA for their willingness to engage with industry, including through workshops, and accommodating industry views throughout the process. We acknowledge the importance of CPS 230 and ensuring that APRA-regulated entities maintain sound operational risk management practices.

Industry see the Guidance as an important tool to ensure accuracy in how the Standard is implemented. APRA has in the past referred to guidance as setting expectations of industry and it has led to member banks changing or adopting different approaches in line with guidance.

The ABA welcomes the clarifications provided in the Guidance, but note it has raised some issues that could be further improved or clarified – particularly in relation to the scope of critical operations, material service providers and the expectations on ADIs in relation to the oversight and monitoring of third and fourth parties.

The ABA would welcome further engagement on these matters, including the potential for additional implementation workshops to ensure entities can raise further detailed questions and understand their obligations.

In addition to the above recommendations, Appendix A below considers some thematic matters with the Guidance that members have raised, while Appendix B refers to specific matters in the Guidance and Standard.

Appendix A: Thematic observations

Proportionate regulation

The Government's Statement of Expectations for APRA included the requirement to 'minimise the costs and burdens of regulatory requirements for regulated entities, including by applying proportionate requirements, considering different businesses models, and taking a principles-based approach to regulation, ultimately to benefit consumers'.[1]

While the Guidance makes reference to APRA's expectation that 'an entity's approach to operational risk to be proportionate to its size, business mix and complexity', we are keen to understand how this can work in practice, especially for mid-tier sized banks.

In our view, using a tiered approach better addresses the need for proportionality. The ABA would be happy to facilitate a discussion between APRA and member banks as to how proportionality could be applied in this instance. Such issues would be addressed through APRA adopting a consistent approach to proportional regulation, which, as noted above, in the ABA's view should be based on a supervisory risk tiering approach. The ABA looks forward to working with APRA with respect to implementing a consistent approach to proportional regulation.

In this instance, industry expects that proportionality could be exercised towards these banks regarding:

- Third- and Fourth-party reviews – given small banks and mid-tier banks have less purchasing power to request monitoring. In this case, where the third-party provider is also a provider of similar services to a larger ADI, proportionality could be applied in terms of the requirement for ongoing reviews and fourth-party oversight (e.g., Equifax, Telstra and Mastercard are examples of third parties that provide services to the ADI sector). This list could be maintained centrally by APRA where APRA has been satisfied with the compliance of those providers in those cases.

[1] APRA's Statement of Expectations, https://www.apra.gov.au/statement-of-expectations, Paragraph 4.3.

  - If that is not pursued, then instead the timetable for complying with the guidance should be extended for smaller and mid-tier entities. This would allow the smaller providers more time to potentially renegotiate agreements with their material providers, potentially leveraging off the renegotiations that would have taken place between larger providers and larger banks.

- The extent of e2e mapping expected for banks, especially for third parties.
- Assessment of fewer categories of critical operations. For example, APRA could be satisfied if smaller ADIs met the minimum requirements outlined in Paragraph 36 (a) in the Standard.
- In the case of a related entity under a NOHC structure, where the related entity is not regulated by APRA, there should be an exemption for the application of CPS 230. The risks related to this related entity should be managed under the provision of APS 222.

Implementation Readiness: Further Guidance needed on pre-1 July 2025 Phased Transition Approach Milestones

Industry is happy to outline its expectations on how it interprets the widely communicated dates (per APRA's 'Discussion Paper' & APRA Member GRC August 2023 speech) for identification of critical operations and material service providers, tolerance levels set & pre-existing commercial compliance.

- By 30 June 2024, identification of critical operations and material service providers: Industry interprets this as meaning the list of critical operations and material service providers (subset of the Service Providers Consolidated List) will be identified & Board (or delegate) reviewed by 30 June 2024, with mapping of dependencies progressed but not necessarily completed.
- By 31 December 2024, Tolerance Levels Set: Industry interprets this as meaning from 30 June 2024, the ADI Board(s) (or delegates) will iteratively approve critical operations tolerance levels (based on sequencing of critical operations implementation work).

We seek early engagement from APRA on whether this expectation aligns with its own. Further, industry notes that whilst the Guidance is not finalised, there are risks to these deadlines as shifting requirements will impact project plans and implementation.

Treatment of cloud computing

Industry notes that CPS 230 does not include reference to APRA's Cloud Paper or explain the relationship between that paper and the CPS. With CPS 231 being superseded (with the implementation of CPS 230) and the Cloud Paper being considered a reference paper to CPS 231, industry seeks confirmation on the application of the existing Cloud Paper until this alignment is undertaken.

We acknowledge APRA's response to consultations that CPS 231 continues to apply and that it will be updated in due course to reflect the requirements under CPS 230. We note, however, that as member banks are currently implementing CPS 230, we would welcome the update to the Cloud Information Paper to occur earlier rather than later to ensure any changes arising from the updated Cloud Paper aligns with the CPS 230 implementation.

Industry would also welcome guidance on the regulatory mechanism and application of the Cloud Addendum Paper (2018), given it has been suggested in ABA/APRA sessions that this paper will still apply under CPS 230. Even under CPS231, the status of that paper at law was unclear.

Other areas where guidance is sought include:

- Application of notification requirements as per paragraph 59 of CPS 230 vs. consultation requirements under APRA's Cloud Information paper for Material Outsourcing Arrangement's with Heightened/Extreme Inherent Risk'. Industry's preferred view is that the CPS 230 standard will take precedence for those material service providers involving cloud computing and supporting critical operations (i.e., Notification only).
- Industry also seeks guidance in relation to existing arrangements involving cloud computing that are currently classified as 'Outsourcing & Not Material or Not Outsourcing' pursuant to CPS 231 but could be classified as material under CPS 230. We are seeking confirmation whether banks need to engage with APRA as they are existing arrangements, and if so, whether we can undertake the APRA consultation / notification per CPS 230 after the Standard's implementation in July 2025?

Treatment of overseas branches or subsidiaries

Is it expected under CPS 230 that International Branches/Offices of an APRA-regulated entity also comply with the requirements of CPS 230 if they operate in an overseas country which already requires detailed operational risk management procedures, including Business Continuity Plans and management of material service providers, and has been vetted by the national supervisors. In these circumstances it may be appropriate for CPS 230 not to apply. The Guidance is currently silent on this point and industry would benefit from further clarification.

Additionally, the Guidance is unclear with respect to what would count as offshoring by overseas branches or subsidiaries in the context of the CPS 230 requirements to manage material service providers and business continuity planning. For example, if an Australian incorporated bank has a branch or subsidiary entity in an overseas country which is engaged in a service arrangement with a provider also located in the same overseas country (or outside the same country, but not in Australia), does this qualify for the offshoring requirements for APRA notification?

Australian Banking Association

Appendix B: Specific observations on CPG 230

	CPS / CPG reference	Issue/question	Industry position
Notifications to APRA			
	CPG Paragraph 11 – Table 1	Industry seeks clarification as to whether 'operational risk incidents' in the table is the same definition as 'operational events'. Note that CPS 230 paragraph 16 (d) implies a distinction between operational events and incidents. Industry would appreciate further clarification in the Guidance on the difference between what would constitute a 'material impact on the ability to maintain a critical operation' (paragraph 33 in CPS 230) and the reference in paragraph 42 of the Standard to a disruption to a critical operation outside tolerance. Understanding the triggers is important given the difference in timing for notifications (24 hrs vs 72 hrs).	ndustry interprets the guidance outlined in Table 1 regarding notification of operational risk ncidents to APRA within 72 hours such that the only information required at that time is a notification that an incident has occurred.
End-to-end (e2e) Mapping			
	CPG Paragraph 35 and 36	The Guidance identifies the concept of a critical operation as 'the end-to-end process' across a product lifecycle (in Figure 1) and asserts that this represents a 'better practice' approach (in paragraph 36). The reference to what would constitute 'better practice' is also reflected throughout the Guidance – in some situations, reflecting a 'different' approach rather than an approach with direct traceability to the Standard. Industry questions whether the reference to 'better practice' is putting industry participants at risk (including the risk of legal action from Stakeholders) when a 'different' approach is taken to the Guidance, while still meeting the requirements of the Standard.	ndustry recommends that guidance in paragraph 36 should be amended/expanded to reflect that not all elements of the 'end-to-end operation' would be considered as having a material adverse impact to customers, the economy or the company if disrupted.

Operational risk controls			
	CPG Paragraph 44	Many members do not have supplier-owned controls documented in their current operational risk frameworks, making the 'better practice' aim of having designated owners a significant burden and significant widening in scope from current practice. APRA should consider whether the benefits from such an expansion would outweigh the additional costs, especially for smaller and mid-tier organisations.	ndustry recommends "all relevant related risks and controls" to apply to those owned by material service providers, not all service providers.
	CPG Paragraph 45	CPG 230 paragraph 45 (b) sets out the expectation to capture controls owned by related parties and service providers.	We recommend CPG 230 clarify the scope of this and whether the expectation is that an entity should be aware of every control owned by related parties and service providers, or limit to controls linked to material operational risks (Industry's expectation is the latter). ndustry interpretation is also that para 45 (b) should be only include material service providers, noting that the 'better practice' outlined here is onerous and a significant burden on industry.
Business continuity			
	CPG Paragraph 56	Seeking confirmation on whether the reference to Business Continuity Management in this paragraph is tied to critical operations or to the wider operations.	ndustry's interpretation is that for the purposes of this Standard, it refers to critical operations, with individual entities to judge how to apply BCM on non-critical operations
	CPG Paragraph 58 (b), Paragraph 59	The description of "Indirect Impact" in CPG 230 indicates significant cross over with CPS 900. Industry anticipates at least a 15-20 per cent increase in critical operations. Industry also seek clarification on how this should be balanced against the paragraph 59 focus on 'on outward-facing services'. Expanding the concept of Indirect Impact beyond 'outward facing services' has the	We recommend APRA remove the expectations as stated in Paragraph 58 (b) and Paragraph 64 (b) to limit critical operation's focus on outward-facing services

		potential to materially widen the scope by increasing the number of critical operations.	
	CPG Paragraph 61	CPG 230 sets out that all CPS 900 critical functions are also CPS 230 critical operations – this is a significant expansion of scope. The obligations that apply to each CPS 230 critical operation require significant effort. If critical functions are also in scope for CPS 230 this may cause conflict, overlap and duplicated outcomes for the impacted business operations mapping, risk frameworks, policies and standards. This will result in potentially significantly higher implementation costs and ongoing effort, specifically in relation to the requirements for mapping critical operations. An example of where the distinction applies might be in the case of home loans. Under CPS 900, the provision of home loans could be classed as a critical function for an ADI. However, ADIs may not choose to class the entire home loan value chain (for example, Origination – Assessment – Settlement/Drawdown – Release/Variation) as a critical operation, instead choosing to focus only on the critical parts of the value chain (for example, Settlement/Drawdown) as a critical operation under CPS 230.	ndustry's position is that not all critical functions as defined by CPS 900 are critical operations under CPS 230. Instead, CPS 900 should be a consideration but not automatic adoption as critical operations.
	CPS Paragraph 36 (c)	Industry seeks confirmation that this part of the standard applies to funds management operation and not to the raising of funds.	ndustry position is that it applies only to funds management operations.
	CPS Paragraph 36 (d)		As it was not clarified in the Guidance, industry nterprets the reference to 'systems and nfrastructure needed to support critical operations' to apply to the extent that the critical operations are dependent on the infrastructure and that the infrastructure is not a critical system in itself.

Management of service provider arrangements			
	CPG Paragraphs 88 and 92		ndustry interprets the reference to service providers as material service providers.
	CPG Paragraph 89		ndustry's preference is for 'consistent process mapping' to include flexibility for ADIs to use existing control measures/procedures. Also, the guidance should be amended to reflect that service provider process mapping is imited to critical services or material services the ADI relies on, and not indirect services such as marketing
	CPG Paragraphs 90 and 91	Industry note the clarification with respect to language regarding fourth parties in the Standard but the draft guidance still makes reference to 'other downstream providers' which does not appear in line with intent, nor reflect the verbal discussion at the ABA and APRA industry session (on 9 August 2023) wherein APRA confirmed the intent is to focus on material subcontractors for material service providers. To ensure that this is a manageable and realistic process for banks to undertake, especially smaller institutions, industry requests this language be clarified in the guidance.	ndustry recommend APRA amend paragraphs 90-91 further to clearly limit the scope of fourth party risk management to be in line with paragraph 48(c) of CPS 230 (i.e. those fourth parties that support critical operations only).
	CPS Paragraph 50 (d)	The Standard requires APRA-regulated entities to classify a provider of the 'core technology services' as a material service provider. The Guidance does not provide guidance on identification of core technology services.	Noting that, industry proposes that core technology services are underlying services on which critical operations are dependent. Core technology services might or might not form a direct part of the critical operations value chain and / or has potential to expose entity to material operational risk. For example, payment as critical operations has subset / part of its processing hosted on Microsoft Azure (cloud)

			thus making Microsoft Azure a material service, noting dependency of payments on the platform. In this case, Microsoft is not performing any payment related services but managing / maintaining the underlying nfrastructure.
	CPG Paragraph 95	While noted as better practice, this line goes beyond the requirements of the standard which requires only a register of material service providers, rather than a list of all service providers. The standard also does not specify when APRA requires the major service provider register to be submitted each year.	ndustry suggest this reference to all service providers be removed in the Guidance. n its place, the Guidance could provide a timeline for the register of material service providers. ndustry recommends: The Register will be submitted on an annual cycle, commencing within the 12 months after final compliance in June 2026.
	CPG Paragraph 96	Industry note the challenge of identifying what constitutes an appropriate cohort of service providers in the absence of guidance, as well as the difficulty and burden of managing and getting information from non-material providers. Industry requests further clarification of the expectation for service providers that are not individually identified as material but are part of a cohort which is considered material. Specifically, industry are unclear what requirements should be attached to such a cohort, where the individual arrangements are not deemed material, and therefore request clarification as to the intent or application for a prudent entity. For example: • Would the contractual provisions outlined in paragraph 54 (c) of the Standard be required to be applied?	This statement is not reflected in the Standard and requires further clarity. We understand that aggregate services impact would not change individual service provider materiality status. Rather the aggregate exposure to the cohort should be considered as an Operational Risk category. As such we recommend APRA to clarify the requirements for an assessment and governance under the paragraph and to include a definition. Examples: Individually, Partnerships or Credit Bureaus would not considered material, however considered in aggregate it could be

		• Would the register of material service providers need to include non-material suppliers where an aggregate risk has been identified at cohort level? • Would performance monitoring and reporting to senior management be required at cohort level, even if the underlying individual arrangements are not material? • Is it expected that the cohorts be defined by performing the same or equal scope within the same value chain/critical operation, i.e., panel arrangements, dual providers etc?	assessed as material despite the service being provided by different services providers. Alternatively, given the concept is not in the Standard, we recommend this reference be removed in the Guidance.
	CPG Paragraph 97	Industry request guidance regarding APRA's process and timing to review an entity's justification and approval not to classify a service provider prescribed by APRA as material. In particular, the guidance should provide greater clarity on APRA's expectations of any entity to remediate where APRA disagrees with the entity's assessment. For example, if APRA determines that the justification process is not appropriate and uses its powers under paragraph 52 or 57 of the Standard to require an entity to treat an arrangement as a material service provider, this will likely result in significant remediation including, but not limited to, legal contractual negotiation.	
	CPS Paragraphs 49 and 51	Paragraph 49 from CPS 230 requires 'an APRA-regulated entity ..[to].. maintain a register of its material service providers'. Paragraph 51 from CPS 230 requires 'an APRA-regulated entity must submit its register of material service providers to APRA on an annual basis'.	ndustry would like to understand the data fields expected to be included in the register and the mechanism for submitting the register to APRA. ndustry notes that this detail is required well in advance of the 1 July 2025 implementation date, in order for appropriate procedures and data capture to be developed.

	CPS Paragraph 50	As some service provider arrangements will be material across APRA-regulated entities, the industry seeks clarification if APRA will engage these systemically important service providers and support APRA-regulated entities to uplift arrangements to CPS 230 requirements. For example, market infrastructure service providers such as SWIFT, VISA, Mastercard as well as regulated venues such as stock exchanges, central banks or market data providers (Bloomberg for terminals). The industry also seeks clarification of the CPS 900 Resolution contractual requirements. To assist with the renegotiation process and avoid duplication of effort, resolution requirements should be considered when existing arrangements with material service providers are reviewed.	We suggest that APRA detail its expectations for the renegotiation of contracts for resolution purposes in clear, publicly available guidance. n addition to the above, the timeframes set out n such guidance should take into account the timelines and requirements of CPS 230. Many ADIs have arrangements with numerous material service providers, some of whom are smaller vendors, and the ability to renegotiate all of these contracts in line with the outlined timetable could be challenging.
	CPS Paragraph 52	Guidance would be appreciated on some of the situations where APRA would require an APRA-regulated entity to classify a service provider, type of service provider or service provider arrangement as material (beyond those outlined in the Standard).	
	CPS Paragraph 54 (c)	Industry seek clarification on whether the ability of the service provider to meet its legal and compliance obligations is with respect to the specific arrangement with the ADI, or a broader requirement to meet their legal obligations as part of their broader business in Australia. Furthermore, industry would like clarification on what the treatment of market infrastructure / financial markets intermediaries, such as stock exchanges, central banks or market data providers (Bloomberg for terminals), where access to their services are not typically covered in detailed service agreements, negotiating leverage is very limited and audit and access rights rarely conferred.	The industry's expectations regarding compliance with paragraph 54(c) will take the form of a working combination of controls, ncluding a range of possible provisions to be ncluded in the agreement based on the substance, context and overall risk assessment of the material arrangement.
	CPS Paragraph 60	As outsourcing is not defined in the Standard, industry request confirmation in the CPG 230 if the outsourcing definition in CPS 231 Outsourcing will be maintained for CPS 230 purposes.	