Australian Banking Association

21 September 2022

Gideon Holland
General Manager, Policy
Australian Prudential Regulation Authority

By email: [redacted]

Dear [redacted]

Strengthening operational risk management

The Australian Banking Association (**ABA**) welcomes the Australian Prudential Regulation Authority's (**APRA**) consultation on the new prudential standard, CPS 230 Operational Risk Management (**CPS 230**). The ABA also welcome's APRA's early engagement with industry and willingness to conduct an industry workshop as part of its consultation.

The ABA is supportive of the proposal to replace CPS 231 Outsourcing (**CPS 231)** and CPS 232 Business Continuity Management (**CPS 232**) with a new CPS 230. Bringing together these related concepts into a single standard should support a more holistic approach to operational risk management.

Increase in disruption, intrusiveness and regulatory burden

However, the ABA is concerned that, as currently drafted, the proposed changes will not result in materially better operational risk outcomes despite adding significant additional regulatory burden through increased costs, resourcing, tooling, oversight and compliance in the 'design, implement and run' phases, including impacts to participants on banks' supply chains. While the ABA agrees that it is appropriate to update the scope of the existing guidance, under CPS 231, from "outsourcing arrangements" to the broader concept of material service providers (**MSP**) and under CPS 232, from 'critical business operations' to 'critical operations', the current drafting is problematic for several reasons.

Firstly, the scope of CPS 230, as currently drafted, is very wide and would, for example, capture service providers that are not material. The impact of this broad scope is exacerbated by the lack of or unclear definition of key terms, such as 'material' and 'relies', and unclear links to related standards, such as the link in the definition of MSP to CPS 234 Information Security (**CPS 234**).

CPS 231 and CPS 232 already impose wide ranging and intrusive obligations on APRA-regulated institutions and, by extension, their service providers. Initial estimates are that CPS 230 could increase the range of service providers captured by a magnitude of 10 to 20 times, with a commensurate increase in overall regulatory burden.

Secondly, there are requirements in CPS 230 which are more appropriately considered by APRA, the Council of Financial Regulators (**CFR**) and/or under other regimes, such as the Security of Critical Infrastructure (**SOCI**) Act. For example, paragraph 52 (c) requires banks to assess whether a provider is systemically important in Australia; this assessment is more appropriately conducted by APRA or the CFR, rather than individual banks.

Thirdly, the policy as drafted may have an anticompetitive outcome for smaller third and fourth party service providers due to the (proportionally high) cost of needing to comply with obligation (on banks and, by extension, on service providers). It may be that ABA members will not be able to contract with these providers where they are unable to adequately align with APRA's requirements.

The ABA understands it is not APRA's intent to materially increase the number of providers captures by CPS 230 (vis-à-vis CPS 231) or the overall burden on regulated and unregulated institutions (vis-à-vis CPS 231 and CPS 232). To achieve this intent, the ABA recommends that APRA narrow the scope of the CPS 230, provide greater clarity to definitions in the draft standard and ensure appropriate links to related standards. It is our view that the proposed CPS 230 could be simplified to reduce its complexity and burden, while maintaining its intent. Appendix A provides further detail in respect to the MSP obligations and coverage.

Unachievable implementation deadlines

While the related guidance will provide further insight into the requirements, it is highly likely that implementation by the currently proposed date will not be possible. For example, there appears insufficient time to complete:

- Comprehensive End-to-End (**E2E**) mapping of critical operations (including mapping critical operations (and potential vulnerabilities) such as services provided by third party providers and, whether they sit with the third party or beyond), which will be the foundation necessary to achieve the outcomes required across all areas;
- Management's expansion of scope for the newly defined 'material' service providers and associated fourth parties;
- Renegotiation of contracts with MSPs to include the requirements of the Standard (including tolerance levels) – which in some cases will need to be preceded by revision of internal bank policies and supplier facing policies;
- Software/tooling changes required across systems that support operational risk, business continuity management (**BCM**) and Service Provider frameworks including for fourth parties;
- Development of business continuity plans (**BCPs**) for critical operations, setting effective tolerance levels and completing annual business continuity exercise in line with the systemic testing plan; and
- BCM Program changes with plans to move from being Business Unit-aligned to a Service-based approach, with alignment to the prescribed critical operations including transfer of plan ownership and associated controls.

In recognition of these unavoidable hurdles, the ABA recommends APRA adopt a phased implementation approached, as detailed in Attachment B.

Appendix B also provides industry's observations and recommendations on other themes of the reforms, including the associated guides, APRA's Cloud Computing Information Paper (**Cloud Paper**), Head of Group considerations and business continuity. Appendix C provides specific observations on CPS 230.

The ABA and its members look forward to ongoing discussion with APRA regarding these important reforms and is available to further explore the issues and solutions raised in this submission. If you require further information or would like to discuss any of the content of this letter further, please do not hesitate to contact me on [redacted] or [redacted].

Australian Banking Association

Regards,

Brendon Harper

Policy Director
Australian Banking Association

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

Appendix A: Key issue: MSP

Definition and application of what is 'Material' under CPS 230

The concept of 'material' is central to the new CPS 230. To drive consistency and alignment on application of defined terms under CPS 230 across industry, the ABA seeks further guidance on what factors or indicia should be considered in assessing what is a critical operation, MSP, material weakness and incident, material financial impact, material operational risk, material impact on a bank's ability to maintain critical operations and material adverse impact.

The ABA is available to assist APRA, for example, by workshopping these critical definitions. The ABA notes that some discretion should remain for individual regulated entities to define and apply these concepts.

Material service providers

Material increase in MSPs captured

The extension of the MSP definition leads to a higher requirement across a significantly larger number of arrangements. Some of the clauses proposed in CPS 230 have been difficult to implement under CPS 231 (for example, APRA onsite visit clauses) and are typically agreed after extensive negotiation. Extending these provisions to fourth parties will be challenging and the scale could be cost prohibitive. The effect of fourth party risk management is to uplift the management of critical operations for banks' MSP to a standard similar to that found in banks themselves. This means parts of CPS 230 would unfairly impact non-APRA regulated entities.

It is not clear to industry if the benefits of this extension outweighs the increased cost and operational impact. It is also not clear if banks with relatively less bargaining power will be able to negotiate some of these clauses with service provider organisations.

Using the current Business Impact Analysis, one bank has estimated approximately 115 MSPs will be captured by the newly defined 'MSPs' versus the current 14 material outsourced arrangements. Other banks have estimated an increase of 10-20 times in captured 'MSPs' under the new definition.

As a further example of the combined impact of the proposals, one major bank has assessed the impact of the proposed CPS 230 in its delivery of Business Lending solutions to its customers with consideration of the E2E process (Product Design, Customer onboarding, Loan approval, Fulfillment, Portfolio Management and Information Technology (both Infrastructure and Software). The below table summaries potential changes in scope for Business Lending due to CPS 230 requirements:

	Current State (CPS 231)		Future State (CPS 230)	
	Suppliers	Contracts	Suppliers	Contracts
Material Outsource under current (CPS 231) vs future (CPS 230) for Business Lending.	15	30	47	98

The ABA understands that APRA is not intending a material increase in MSPs covered. The ABA and its members remain available to working with APRA to ensure the intent of CPS 230 is achieved while limiting any unnecessary increase in coverage and regulatory burden.

Definitional challenges

In order to ensure a minimum standard for managing fourth parties across financial institutions, industry suggests that APRA, in its CPG, set out its expectations of what an entity would reasonably do to prudently manage fourth parties. Additionally, the definition of MSP includes the concept of 'relying': *as those which the entity 'relies' on to undertake a critical operation or that expose it to a material operational risk*. Industry seeks guidance on the threshold of what constitutes 'reliance' to help regulated entities identify when a service provider would be considered as 'material' under CPS 230. An

example, it is unclear if CPS 230 would capture a supplier that is used for a small part of a critical operation but is not considered to expose a regulated entity to material operational risk. Also, APRA's expectation regarding aggregation of services from service providers and related entities is also unclear, for example should this be limited to only like services?

Further, the definition of MSPs as set out in paragraphs 48 – 50 will potentially capture a large number of third party and related service providers that generally would not considered to be undertaking a critical operation or exposing the APRA-regulated entities to material operational risk. The ABA suggests APRA provide clarification that the materiality test for a service provider which is set out in paragraph 48, be applied to each service provider relationship captured by the list in paragraph 49, so as to allow the APRA-regulated entity to determine materiality on a case-by-case basis according to their own risk assessment of both the critical operations and the specific service arrangement(s) which support these critical operations.

The ABA recommends the definition of MSP is amended to ensure that it does not unintentionally capture the following arrangements, which generally would not considered as supplying goods or services for consumption by a regulated entity:

- counterparty arrangements which may often be appointed by the underlying customer, e.g. mortgage brokers and financial planners;
- financial market infrastructure arrangements; typically participant or member style arrangements which whilst arguably critical to operations, are used industry wide and are typically regulated entities in their own right, or perform a regulatory oversight function. e.g., payment systems, central securities depositories, securities settlement systems, central counterparties and trade repositories (as defined by IOSCO).

These types of third-party arrangement would not meet the current test for outsourcing under CPS 231, and the ABA notes the ability to negotiate regulatory contractual clauses, impose performance metrics or tender for this particular subset of third parties would be extremely difficult for industry to achieve.

Additionally, industry has serious concerns about the link in the definition of MSP to CPS 234 – in industry's view not all CPS 234 service providers regulated under CPS234 are material. There is also no criteria for information assets being "*classified as critical or sensitive under CPS 234*." If APRA is thinking about for example any "*sensitive data*" for instance, the definition would be extraordinarily broad and catch hundreds of suppliers.

The ABA notes that other jurisdictions include a list of service providers which are exempt from requirements similar to those in draft CPS 230, for example the EBA's Guidelines on outsourcing. Adopting a similar approach in Australia appears reasonable to industry and could assist in focusing banks' activities while reducing regulatory burden. Accordingly, industry suggests that paragraph 50 of CPS 230 be amended to take into consideration the volume and sensitivity of information handled by the suppliers and the level of material operational risk posed to the regulated entity.

Indemnity and fourth parties

Additionally, MSP, like current material outsourcing providers, are required to indemnify the ADI against actions of a subcontractor, as if they were its own. This sets up strong incentives for the MSP to manage fourth parties properly. Most agreements exert some client control over changes of significant subcontractors, and dependence on them would be accounted for in a good business continuity plan. To require ADI investigation of subcontractors would depend in practice on the service provider and mostly replicate their controls. To have some knowledge and control is useful, but it will be difficult to improve on the incentives given by the indemnity requirement. Some clarity or guidance in relation to this would be useful including where APRA sees the additional requirements providing benefits beyond those realised by the indemnity agreements.

Pragmatic implementation

Furthermore, the requirement to re-assess the materiality for current suppliers under proposed new definitions on the 'backbook' of service providers is unachievable within the proposed timeframe. A pragmatic approach would be for these assessments be performed in alignment with the contract

renewal cycle with a 'hard' compliance date as suggested in the cover letter above. Practically, this is when banks, particularly smaller banks, are in the best position to negotiate the terms in line with the standard. In other words, there may be a suite of contracts in place that are not aligned to the standard on the effective date, as these arrangements are yet to fall due for renewal.

Maintaining banks' ability to respond quickly

Concerningly, CPS 230 does not contain an equivalent paragraph to paragraph 33 from CPS 231. APRA regulated entities need to be able to enter into new service provider agreements at short notice in the event of an extreme event or sudden failure – which may not allow the entity to notify APRA within the normal periods of time. The draft CPS also contains requirements for service providers to notify APRA-regulated entities of their use of material service providers. We query how that assessment should be carried out and what the APRA-regulated entity needs to do with that information.

APRA engagement with MSPs will be required

Finally, it would be useful for APRA to communicate its expectations and the requirements in CPS 230 directly to service providers who are or are likely to become MSPs. Initial conversations that ABA members have had with some large service providers reflect a lack of awareness and / or emerging concerns about the new requirements.

Practical example: Fourth Party Relationship

Context: Genpact, a material supplier, is predominantly used by a bank across a range of divisions. CPS 230 seeks to impose sharing of information related to the supplier's business relationships (fourth parties). The bank is required to maintain a policy on these fourth parties as well as detail the use of said fourth parties within formal agreements.

Practical Impact:

- Assess arrangement with supplier on which party will take responsibility of managing risks and governance associated with fourth parties.
- List and risk assess all fourth party suppliers which Genpact are dependent upon, including but not limited to:
    - Data and Data Protection – IBM/Amazon Web Services;
    - Network Providers – CISCO;
    - Cybersecurity – CISCO/Fortinet/IBM;
    - Hardware Providers – Hewlett-Packard/Dell/Microsoft; and
    - Screening Services – First Advantage/ Xref /Equifax.
- Uplift at an MSA level to include references and updated policies with respect to fourth parties.
- Supplier arrangements with fourth parties may include confidentiality requirements which prevent discussion with the bank.

Australian Banking Association

Appendix B: Other thematic observations

Implementation timeline

The ABA is broadly supportive of the proposed CPS 230 but notes its implementation will require significant work on behalf of banks at a time of ongoing heightened regulatory change particularly in the prudential space. The proposed effective date will be less than one year from the publication of a final standard and less time from the release of the final guidance. CPS 230 also relates to and has implications for other APRA requirements that are currently being developed. It is difficult, or impossible, for banks to accurately determine the burden of implementation and realism of the proposed timeline with the concurrent development of related requirements.

In light of this, it may not be possible for banks to meet the proposed implementation timeline. The ABA notes that other jurisdictions have allowed longer implementation timelines for similar regimes, for example the UK which had a transition period of several years (1 year to implement but up to 3 years to show they could stay within tolerance levels). Some examples of items that will need a transition / phased implementation are:

- Commercial agreements with MSPs, especially APRA access rights – a possible solution is to adopt an approach similar to CPS 234, which had the earlier of contract renewal or a set date. An alternative approach is to apply CPS 230 to:
    - new MSP contracts from 24 months after finalisation of CPS 230 and CPG 230; and
    - existing MSP contracts from 1 January 2026.

  In addition, APRA support to get key terms understood and agreed may be beneficial, in particular for providers from non-APRA regulated industries;
- Business resilience – establishing tolerances and scenario analysis;
- E2E mapping of Critical Operations and their dependencies in a consistent and maintainable way; and
- Development of BCPs for Critical Operations, setting effective tolerance levels and completing annual business continuity exercise in line with the systemic testing plan.

Industry suggests that a minimum of 24 months from finalisation of the CPS 230 and CPG 230 should be allowed for entities to implement the new requirements; plus an additional transitional period for certain elements, including those noted above.

The ABA is supportive of the proportionality options included in the proposal and strongly encourages APRA to consider the timing of implementation of these reforms, given the various other reforms currently being developed and implemented. Notwithstanding this, the ABA notes that implementation challenges related to MSP management are likely to be more intense for medium and small banks. In some cases, it would be extremely difficult or impossible for these banks to apply sufficient pressure on (large and international) service providers to change their practices, procedures or contracts. In light of these challenges, that ABA recommends:

- As suggested below, that APRA proactively engage with MSPs to articulate APRA's intent and the new standard's specific requirements; and
- Implementation for medium and small banks to trail the implementation for larger banks by 12 months, at least for new MSP contracts.

Associated guide

Given CPS 230 is principles based, it is difficult to fully analyse and understand its impact and implications of the standard without the associated guidance. Optimally, this guidance would provide further detail and reference to the other standards that link into resilience, for example, CPS 190 Financial Contingency Planning and CPS 900 Resolution Planning (**CPS 900**) and how the new

standard works in with these areas, as well as how it will align with a refresh of the Cloud Paper and contemplate a similar "whitelist" concept as New Zealand Reserve Bank's BS11 Standard.

Considering the importance of the guidance, the ABA encourages APRA to consult on the associated guidance before finalising CPS 230 and to ensure that this is process and timeline is taken into account when determining implementation dates.

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, the ABA notes APRA's intention expressed to the ABA and member banks in the recent workshop that this Paper would be aligned to the requirements of CPS 230. Industry seeks confirmation on the application of the existing Cloud Paper until this alignment is undertaken.

If the Cloud Paper remains relevant, industry would welcome:

- Consideration of whether it may be efficient to consolidate the requirements of the Cloud Paper into CPG.
- Clarity is sought with regards to 'Consultation' and corresponding 'No Objection' requirements for Heightened and Extreme risk cloud material workloads given paragraph 58 of CPS 230 refers to 'Notification' requirements

Approach to operational risk management

Feedback to industry suggests that the intent of the proposed standard is a holistic, almost strategic, shift to include broader resilience principles. If a step shift in resilience is the intention with the view to have an E2E approach tied to strategy and appetite, the segregation of areas within the standard (Operational risk management, Business continuity and Management of service provider arrangements) seems to detract from this intent.

A possible approach is to address this through a more explicit overarching principle/ approach, prior to covering specific topics. This could be better highlighted in the objectives and key principles of the standard, through the guidance, as well as linked through to the expectations outlined in the CPS 220 Risk Management Standard (**CPS 220**).

In addition, CPS 230 materially expands the scope of APRA requirements in relation to operational risk including explicitly expanding and/or amending the scope of current requirements. In particular, the requirements set out in paragraph 26(b) are expected to generate a significant amount of work.

Head of Group considerations

The burden and complexity of the proposed reforms could be reduced by including a "Head of Group" statement, similar to that in other standards. The preamble to CPS 510 Governance provides such an example (see extract below):

> *Where an APRA-regulated institution is the Head of a group, this Prudential Standard requires that the group has in place governance arrangements appropriate to the nature and scale of the group's operations, and the provisions of this Prudential Standard are applied appropriately throughout the group, including in relation to institutions that are not APRA-regulated….*

Such a statement would reduce duplication of requirements and allow for a more proportional adoption.

Business continuity

APRA is silent on their expectations on the continuity of the types of BCPs developed under CPS 232 – this could be read as APRA expecting all of that work to cease now. Clarity from APRA on this point is requested. If all those BCPs continue, then does APRA expect all the CPS 230 requirements applying to each BCP for example, notification of BCP activation?

Critical operations

Industry seeks clarification from APRA on what it means by 'critical operation'. There may be intent to cover this in the guidance, however, industry seeks to clarify the scope for critical operations by providing a broad description, consistent to the level of detail provided across industry referred to as the Banking and Finance Sector Group Essential Functions 1-17. From these broad descriptions it is anticipated to have several sub-processes. Industry appreciates that the intent with a principles-based approach is to self-define. However, it would be useful to have 'guardrails' or indicia of what might be considered a critical operation, and clarity of what constitutes minimum acceptable practice. This would help support the tiering of processes across the organisation.

Examples provided in CPS 230 are more internally focused than that of other jurisdictions. Industry encourages the use of further examples that have more of the customer-impact focus that it understands APRA is intending, for example the ability to validate account balances, or make purchases with credit / debit cards. Industry would welcome examples of critical operations and tolerance levels illustrated for each APRA-regulated industry by way of examples in the CPG.

Additionally, further clarity in its application and scope will be beneficial particularly in the context of:

(i) What is considered as a 'Critical Operation' as a defined term under CPS 230 including the E2E process documentation underpinning each of them to identify obligations, risks, controls, dependencies & exposures (including downstream impacts and 3rd/4th party dependencies).

- While the ABA notes APRA has specified certain Critical Operations that must be included for the banking industry to drive consistency:
  - In industry's view, each of the specified Critical Operations are still very broad in their own right and industry would welcome further guidance on what aspects of an operation may be considered as critical or otherwise. For example, for Payments, payroll may be considered critical while transfers to own account may not be. As another example, how would the APRA deposit book example translate into a critical operation - would that relate to deposit taking, the security of deposits, or ability to withdraw?;
  - Clarity on how these specified Critical Operations are anticipated to overlap with and/or differ from the Critical Infrastructure lists as required by SOCI (both for banking assets and also third party / fourth party service providers who may also fall within the SOCI regime directly) and/or align to industry defined Essential Services. In the absence of this there may be a risk of inconsistent interpretation and application of these regulations across the industry.

    Industry recommends that consideration be given to whether suppliers that may be directly regulated under the new SOCI regime (for example, data storage / processing entities) should still come within the full remit of CPS 230 as MSPs, to avoid duplication, overlap of regulatory effort, and/or conflict of requirements. In addition, some material suppliers may be of national significance and so better designated under the SOCI regime instead of dealt with by 'contractual proxy' under CPS 230. This is also of relevance to the identification of identify MSPs that are 'Systemically Important to Australia' in paragraph 52c.

- Preliminary work of mapping the E2E process, show this to be a large and complex task with key dependencies and overhead (for example, systems support, changes to frameworks, data quality and service taxonomy) to operationalise at scale and achieve the desired outcomes. The breath, depth, and extent to which it is carried out will depend on how it is looked at. For example, the holistic process of Payments Operations at high level (L1); each subprocess individually and/or in aggregate supporting the Payments Operations (L2); and/or the next level down (L3). This will then need to be applied across all Critical Operations of the entity. As such, guidance on the appropriateness level of granularity will be beneficial.

- Noting that CPS 230 and CPS 900 do include cross reference to each other, further guidance is required on differentiation and overlap between critical operations (in CPS 230) and critical functions (in CPS 900)

(ii) In addition to clarity sought under paragraph 1(a)(i), guidance will be welcomed on key considerations that are required to be considered by regulated entities when setting approved tolerance levels including factors such as[1]:

- As noted above, to what extent do tolerances need to be mapped to each and every critical operation and related subprocesses given its complexity;
- Critical Operations provided to multiple customer segments;
- Prioritisation of different tolerances for different operational objectives (for example, restoring service availability vs data security);
- Measurement, monitoring and reporting requirements to Board and Senior Management;
- Level of benchmarking required (including benchmark across the industry, and against regulatory and customer expectations);
- Ability for a regulated entity to justify the tolerances set which may differ from its peers; and
- Guidance on how to set data loss tolerance levels as required under paragraph 37 (b).

(iii) Guidance / clarity on the systemic testing program and related compliance requirements: frequency, scope, test type including types of severe plausible scenarios that are required to be considered. Noting that testing of some scenarios may require significant time, infrastructure, investment, and coordination across participants in the Critical Operation chain.

(iv) Guidance on DR planning requirements (as referenced in paragraph 33(c))

(v) Further guidance would be helpful on the level of granularity to undertake scenario analysis in testing operational resilience, as an example, over a 3-year period versus annually, focusing on material operational risks for the bank, and use of customer data to inform the severity.

(vi) What is APRA's expectations and guidance on management of non-critical operations given that this will still represent a significant proportion of an entity's operation?

(vii) It is unclear if the operations listed in paragraph 35 in scope regardless of the test in paragraph 34?

Practical example: Business Continuity

Context: Taking an example of a critical operation (Customer enquiries), as defined by APRA, a preliminary mapping has been performed. This has highlighted areas of challenge and uplift which will need to be addressed as part of the implementation to successfully complete this activity, noted below.

Practical Impact:

- The current Value Chain work needs to be extended to cover additional Geographies
- The BIAs are not informed by the Value Chain work, and are therefore not clearly aligned (e.g., one to many or many to many relationships). In addition, the consistency and depth are varied, which will result in gaps when mapped which must be addressed
- The existing BIA's have not been required to define impact tolerances. Work will need to be completed to develop a methodology for setting these and applying to the critical operations

[1] An example of this working well is the Bank of England's Supervisory Statement on Impact tolerance for important business services.

- Technology assets are inconsistently captured in the BIA, and the information contained within our systems will need to be correctly mapped out for Critical Operations.
- The approach to Disaster Recovery will need to be reviewed to confirm coverage of critical operations and may need to be refined.

Practical example: Critical Operation

Context: There is currently uncertainty on what constitutes a 'Critical Operation', and this is likely to lead to an increase in number of material suppliers.

Adobe, currently considered as a moderate supplier, is utilised by a bank for a range of data analytics and content management services. Adobe Analytics and Adobe Campaign are used to perform digital reporting, tracking customer interactions and email outbound messaging. Adobe Experience Manager is used to manage the bank's public websites and media across digital channels which imposes Potential risk of Personal Identifying Information, Customer Information/Data, Business Continuity.

Practical Impact:

- Assess the criticality and impact to the Critical Operations within the bank in the event of an outage by the supplier:
    - What customer-facing and internal websites would be affected?
    - Impact on customers who receive outbound messaging/marketing materials, how is customer data protected by the supplier?

The outcome would likely classify the supplier as material. This would require the bank to:

- Understand what systems Adobe are dependent upon for their services. For instance, strategic partnership with Microsoft Azure for Cloud based services vs On-Premises risks.
- Examine additional fourth party services relied upon by the supplier.
- Uplift the MSA and SOW to incorporate governance, enhanced business continuity requirements and improved operational resilience. This will increase spend/costs.

Australian Banking Association

Appendix C: Specific observations on CPS 230

Key Principles

Paragraph 11

Paragraph 11 states that APRA-regulated entities must "*maintain appropriate standards for conduct and compliance*". The ABA assumes "*conduct and compliance*" in this context is relevant only in that it relates to operational risk and that, via CPS 230, APRA is not looking to create holistic, entity-wide governance requirements for 'conduct and compliance'.

Risk management framework

Paragraph 15 (b)

Paragraph 12 advises "operational risk is inherent in all products, activities, processes and systems". However, paragraph 15(b) discusses "defined risk appetite supported by … limits". In industry's view, it would be preferable to express paragraph 15(b) in terms of a 'tolerance' rather than a "limit".

Paragraph 15 (f)

This requirement seems to industry very wide. Industry seeks further clarity regarding APRA's expectations for the "*processes for the management of services provider arrangements*".

Role of the board

Industry asks that APRA:

- Provide greater clarity regarding the tolerance levels and level of detail provided to Boards, the frequency of Board approval and how these requirements align to CPS 220; and
- Consider on matters where it may be appropriate to delegate Board accountabilities to Senior Management in line the BEAR / FAR regimes and commensurate to the level of operational risk posed to the entity.

Paragraph 21:

Industry seeks APRA's guidance on how the requirements under paragraph 21 would be achieved.

Paragraph 21 (b) and (c):

The current drafting of paragraph 21 (b) and (c) has the potential to blur the boundaries between the Board and management with regards to requirements on "*reviewing the results of (BCP) testing and oversee execution of any findings*" and "*review risk and performance reporting on material service provider arrangements*". Industry seeks APRA's guidance on how a Board would be expected to approve all of the actions required by 21 (b) and (c) and the distinction to management. Consideration should be given to allowing delegated authority, like in current CPS 230.

Paragraph 21 (c):

For clarity, and consistency with previous requirements, industry suggests the inclusion of a paragraph similar to CPS 231, paragraph 5:

"Nothing in this Prudential Standard prevents an APRA-regulated institution from adopting and applying a group policy used by a related body corporate, provided that the policy has been approved by the Board and meets the requirements of this Prudential Standard."

Paragraph 22:

Industry seeks guidance on APRA's expectations regarding how this would be practically governed and evidenced in regards to the scope of the requirements. Industry contends that "*comprehensive information*" in this context may be too detailed for the Board. Rather, the principle should be for senior

management to provide 'sufficient information' to the Board for it to assess the probably impacts to critical services when make decisions that could affect those services.

Operational risk management

Paragraph 23:

Paragraph 23 lists a number of risks of which some may be considered impacts rather than causes or events. Given the variation of risk taxonomies across organisations, the ABA suggests paragraph 23 allow for controls that reflect the business models and risk management frameworks of the organisation, provided these address the key risks listed by APRA in the draft standard.

Additionally, not all of the risks listed in paragraph 23 as operational risks are necessarily causes of risk or risk events, for which banks would put in place controls, for example, 'reputational risk'. Does APRA take a prescriptive approach and require controls for each risk listed?

Industry also asks for clarification on whether APRA intends that 'change management risk' includes delivered risk *and* delivery risk. Also, more detail on the senior management responsibility requirement, particularly what 'E2E' requires would assist.

Paragraph 25:

Paragraph 25 requires assessment of the impact of business and strategic decisions on operational risk profile as part of its business and strategic planning processes. However, the second part of the paragraph requires this to include impact of new products, services, etcetera on risk profile which is at a much more granular level than the strategic planning process. These type of impacts are generally managed through risk in changes process including new product approval ones. Industry suggests the standard clarify a materiality threshold for needing to assess "*new products, services, geographies and technologies*".

Paragraph 26:

Industry seeks guidance on the expectation on the scope and breadth from APRA regarding the comprehensive assessment of operational risk profiles**.** It is industry's view that operational risk management should maintain a degree of 'risk sensitivity' rather than a blanket requirement for all (potential) risks, regardless of the (potential) scale, scope and impact of those risks.

Paragraph 26 (C):

Industry seeks guidance on the definition of 'severe' in "*assess the potential impact of severe operational risk events…*" and propose to amend to "assess the potential impact of severe *but plausible* operational risk events…".

Paragraph 27:

Industry asks for clarification on who is responsible to assess the materiality of the service, is this the provider or the recipient of the material service? Given this paragraph is stating that banks are providing a material service to another entity – will this be in the supporting CPG? The recipient of the service may not be a regulated entity under CPS 230, can APRA clarify if this would this negate the requirement?

Furthermore, needing to conduct a comprehensive risk assessment every time a service is offered will increase the cost of that service. This may have a disproportionate effect on smaller players and new entrants. A more pragmatic and less burdensome approach would be to require a periodic comprehensive risk assessment for a service or group of services.

Business continuity

Industry would welcome clarity on APRA's expectations in relation to current BCP frameworks under CPS 232 – whereby banks have numerous BCPs at Group, business unit, and support unit levels. It would be welcomed if APRA provided direction on whether all those BCPs should continue; and which

CPS 230 requirements would apply – particularly where a BCP does not materially support a Critical Operation.

Clarity may be provided by differentiating between BCP as the overarching business continuity framework of the organisation and BCP as the business continuity plan of a specific critical business operation or department. Industry would expect some requirements within the standard to sit at the framework level and others at the individual plan level. A suggested approach would be to refer to the framework as Business Resilience Framework, or just framework, and plans as BCP.

Paragraph 32:

Further guidance on the definition of material impact within the new standard would assist industry, due to the more explicit testing requirements.

Industry recommends that timeframes start from the point of the event being identified as material, as distinct from when the event was identified to have occurred.

Industry asks for clarification on the overlap between the notification requirements in paragraph 32 and paragraph 41 of CPS 230 and how that would work in practice. For example, assuming that clause 32 relates to a "*creeping incident*" such as an evolving privacy or supplier incident – for example, tape destruction or the need to shift to a new supplier? That is, at what point does it shift from being an operational risk / privacy incident into a crisis management activation?

Paragraphs 32 and 41:

There is discrepancy of notification timelines on reportable events between 72 hours (paragraph 32) and 24 hours (paragraph 41). Industry contends that aligning to 72 hours for consistency is most appropriate.

Paragraph 33:

As noted above, industry seeks clarification from APRA on what they mean by BCP in CPS 230 – for example, is it only BCPs for critical operations? What about the role of the dozens of individual BU BCPs? What is a 'credible' BCP? How should tolerance levels be determined?

Paragraph 37:

Can APRA clarify whether tolerance levels must be recorded in the Critical Operations Register?

Additionally, guidance is required on the definition of 'data loss'.

Paragraph 38:

Paragraph 38 states that "*APRA may set tolerance levels for an APRA-related entity, or class of APRA-related entities…".* As stated above, industry would welcome greater clarity regarding tolerance levels.

Paragraph 42:

Industry seeks further clarity from APRA regarding paragraph 42. This paragraph could be interpreted to mean that all critical operations must be tested against all scenarios identified, and potentially annually. The ABA understands this is not APRA intent.

Clarifying APRA's intent in the CPS or CPG would be useful as applying such an approach would be a significant exercise and would add material effort and cost. Additionally, it is likely that not all scenarios will be relevant to all critical operations and that one single annual exercise will not cover all critical operations. A better approach may be to risk assess and rotate testing.

Furthermore, it is unclear what level of maturity and scale of testing APRA considers appropriate. Industry foresees that in some instances a table-top exercise may suffice and in others a live simulation/activation may be preferred. The ABA recommends that banks be able to make this determination.

To articulate the potential effort required to test critical operations from E2E, one major bank conducts one annual exercise to demonstrate recovery from E2E. The 2022 exercise took 4 months to plan and approximately 70 colleagues across multiple stakeholder groups to design, execute and review. The

required effort would multiply substantially under CPS 230 due to the number of critical operations identified and the scenarios that must be applied to them.

Management of service provider arrangements

The ABA notes that APRA's proposed approach focuses on material service providers, over material outsourcing arrangements. The ABA recommends APRA consider focusing on arrangements with service providers that are material, rather than the providers as a whole. It is likely that not all arrangements with all MSPs are individually material. Allowing banks to focus on those arrangements that are material would likely reduce the adverse impacts of CPS 230.

CPS 231 paragraph 33:

Industry is concerned that CPS 230 does not contain an equivalent paragraph to paragraph 33 from CPS 231. APRA regulated entities need to be able to enter into new service provider agreements at short notice in the event of an extreme event or sudden failure – which may not allow the entity to notify APRA within the normal periods of time.

Paragraph 43:

Guidance on 'range' and 'severe' to aiding scoping of assurance activities would assist industry. This is particularly pertinent for some smaller banks who are potentially going to need to pay for external SME's engagement to aid this dependent on expectations.

Paragraph 45:

Industry seeks clarification whether compliance to CPS 230 requires a proven ability to maintain critical operations within tolerance levels through severe but plausible scenarios?

Paragraph 46:

It is industry's view that the management of arrangement with providers will depend on the nature of the providers and that this level of detail should not be included in a policy; rather, it should be included in a standard or management desk procedure.

Paragraph 47:

Policy itself should not be required to be included in the register, but the Policy should require the register to be in place. Such a register is a living document and should be an artefact that supports the policy rather within the Policy.

Paragraph 47(d):

The ABA recommends a threshold be introduced for fourth parties rather than stating "any" fourth parties.

Paragraphs 48, 49 and 50:

Industry is concerned with the proposed definition of MSP across paragraphs 48, 49 and 50. In paragraph 48 it is a missed opportunity to define material operational risk which remains subjective.

Paragraph 49:

Industry is concerned with the Standard expressly including mortgage broking and financial planners. Mortgage brokers are not an example of a provider on which the bank relies to undertake a critical operation, as the service can be performed by proprietary lenders or other brokers / head groups. This is also applicable to financial planners, where the customer engages the planner rather than the regulated entity. Other examples which also fall in this category include: reinsurance, custodial service, claims management and risk management.

Industry suggests that 'mortgage brokerage' does not need to be explicitly in scope and can be removed.

Paragraph 48 and 49 also appear to be in conflict as 48 is principles based whereas paragraph 49 has specific direction on what can be classified. Can APRA clarify whether it intends for paragraph 49 to be guidance?

If APRA intends for the industry to use paragraph 49 as specific direction, further clarity is required on:

- defining mortgage brokerage as a process or a profession as a MSP; and
- Clarification of 4th party suppliers and if the services are treated as aggregator, what is the requirement?

The ABA notes that for some banks, if mortgage brokerage services are treated as individual, this increases the work by at least 20x.

Paragraph 50:

Industry has serious concerns about this link to CPS 234 – in industry's view not all CPS 234 service providers regulated under CPS234 are material. Draft CPS 230 does not provide a threshold and one interpretation could be that every critical or sensitive information asset managed by a service provider is deemed material regardless of actual criticality or sensitivity. If APRA is thinking about for example any "*sensitive data*" for instance, the definition would be extraordinarily broad and catch hundreds of suppliers.

Paragraph 51:

This is an additional requirement that is not in CPS 231. Industry seeks further guidance on the process/format.

Additionally, clarity is required on when APRA requires the register to be submitted each year (due date) and what details the register must include. For example, when maintaining 'registers' (such as critical operations, material service providers), should each subsidiary within the corporate group manage its own register, or should the head of the corporate group have a group-wide central register, or is that up to the group's discretion?

Paragraph 52 (a):

While a requirement to include a tender process is appropriate for government, it is not appropriate for private enterprise. The ABA recommends that APRA remove the requirement for a tender process on vendor selection. This is particularly relevant for arrangements between the local branch of a foreign ADI with a related entity.

Paragraph 52 (c):

The ABA has concerns with paragraph 52 (c), which requires banks to assess whether the provider is systemically important in Australia. Individual banks are not in a position to conduct this assessment; and could arrive at different conclusions for the same supplier. It is also not clear how this requirements links, or otherwise, to concepts and requirements under CPS 900. A more uniform approach might be achieved for example, if APRA was to make this assessment, such as in its resolution planning work.

Paragraph 53:

This would be a significant task for smaller entities, with further guidance required from APRA for cases – for example where an existing key supplier does not agree to a term – noting the lesser buying power smaller entities have and potential ramifications. Also, the cost/operational impact in re-contracting outside of normal review terms.

Paragraph 53 (c-f):

In paragraph 53 (c) it is unclear which "entity" is being referred to. Further, it is not possible for a provision to "ensure" an entity meet its obligations. The ABA recommends this language be modified.

Industry is concerned about paragraph 53(d) - that the agreement must require *"notification by the service provider of its use of other material service providers*". It is unclear what is the expectation on banks to act on this information once the service provider has discharged their obligation to notify. It is

also unclear how suppliers are to conduct the assessment of whether they use other material service providers (and 'material' to whom?).

The liability requirement in paragraph 53 (e) is very broad. It may be more appropriate to limit the sub-contractors liability to the services being provided by the sub-contractor.

Industry is also concerned about paragraph 53 (f), which states *"(f) include a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event*" and (g) "*termination provisions*" due to potential commercial implications for supplier - banks anticipate significant challenges with this requirement when negotiating agreements with their suppliers. Given the definition of force majeure, suppliers are unlikely to be able to pinpoint in which event they could continue to operate in.

Paragraph 55(a):

Stating that an APRA-regulated entity must identify and manage *any* risk is not consistent with a risk based assessment of risk management; namely, that the risk - reward basis of the arrangement needs to be assessed, such that those threats posing the highest risk are prioritised. If interpreted literally, this requirement would be unreasonably burdensome.

Paragraph 55(b):

It appears to industry that step-in risk and contagion risk already be addressed by APS 222. It this sub-paragraph is not removed, it would seem appropriate to provide guidance on how to identify and manage contagion risk.

Paragraph 56:

Paragraph 56 omits the word "material" service providers – industry assumes this is unintentional or else this paragraph would capture all service providers.

Industry would welcome an elaboration by APRA about what heightened prudential concerns would trigger a need to make changes to a service provider arrangement. This point is particularly important as the requirement could in effect force an ADI to breach the contract or request changes that would make it economically nonviable to continue.

Paragraph 58:

Can APRA clarify that no approval/no objections is required, given the language has changed from 'consult' (CPS 231) to 'notification' (CPS 230)?

- What is the expectation from APRA for these to be communicated? The number of notices that will be received by APRA could increase dramatically.
- What is the format? Further guidance should be provided on what APRA wants in these notices.

Paragraph 58 (b):

Clarification around the data element of this requirement would be useful. Potentially, a local branch of an APRA-regulated entity would need to notify APRA whenever its head office changes a global support arrangement related to a material service provider. Additionally, clarification around what would be considered "relevant" would assist industry.

Paragraph 59:

It is unclear to industry what APRA mean by 'outsourcing arrangement'? This term is not defined and it is the only instance of its usage in CPS 230.

Paragraph 59 also appears to be misaligned with the rest of the document, referencing Internal Audit review any 'outsourcing' arrangement (when the standard has moved away from 'outsourcing' to 'material service provider'). If in effect it is proposed to extend the definition to 'material service arrangement', this will have a significant impact on audit hours and cost spent on these arrangements, and associated Governance processes.

Additionally, it seems unnecessary to require an audit every outsourcing arrangement with a MSP for a critical operation. The need for such audits should be considered in banks' annual audit plans, which are based on annual risk assessments, with senior management and committee input and are typically approved at a very high level within an organisation.