21 October 2022

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

By email: [redacted]

Dear General Manager

Discussion paper - Strengthening Operational Risk Management:
Proposed Prudential Standard CPS 230 Operational Risk Management

The Australian Financial Markets Association (AFMA) welcomes the opportunity to make comment on APRA's above-referenced discussion paper. We commend APRA for its endeavours to introduce a principles-based approach to operational risk management that is outcomes-focussed, while also consolidating existing standards — this having the potential to introduce efficiencies for industry and regulators alike.

More generally AFMA strongly supports APRA's program to modernise the prudential architecture. We see this as a very worthwhile initiative, well aligned with the national interest and supporting good regulatory outcomes.

AFMA is concerned, however, that the draft standard may not be optimally calibrated in terms of its additional level of prescription and so may create excessive costs. We are concerned that if the modernisation program continues in the direction of CPS 234 and the draft CPS 230 there will continue to be inefficient increases in costs and losses in connectivity to international standards as APRA locks industry into a particular approaches to various aspects of risk management.

The excess of prescription in the draft operational risk standard would result in two related issues for different types of ADIs. For domestic firms it will require well-designed (and independently assessed) operational risk schemes to be substantially reworked at great cost to fit with the particular approach to operational risk that APRA has selected.

For foreign ADIs the level of prescription will mean that, unless carve-outs are made, it may not be possible to continue to use often advanced head office compatible

approaches to operational risk, even where these align with the BCBS Principles. This would be an inefficient outcome that may not be compatible with the aims of APRA's simplification program.

We suggest APRA might be better to retain more flexibility in operational risk management for firms and the professional services firms that advise them as long as their processes are justifiable and consistent with sound evolving practices in the space.

There is a risk that if APRA is too prescriptive it may risk locking firms into an approach to operational risk that might quickly become out of date. In relation to APRA's Information Security Standard CPS 234, this is a relatively static standard compared to the continually evolving international standards such as NIST. For example, NIST has evolved cloud specific extensions since CPS 234 was established.

Rather than chasing international standards and evolving international practice, it is perhaps preferable to more fully leverage these standards such as ISO 31000 and NIST. We note that ASIC has kept its requirements for information security intentionally high level and compatible with NIST. Firms are encouraged by the ASIC approach to use international standards such as ISO and NIST but the exact implementation is left up to firms without detailed prescription from the regulator. This enables and encourages firms to stay up to date with the latest developments. In contrast, to support firms work with CPS 234 AFMA is working with international bodies to map CPS 234 to NIST, the additional local standard creates an unnecessary layer of complexity and cost.

For foreign ADIs AFMA holds that foreign ADI branches should be allowed to rely on the head office protocols satisfying the home regulator, i.e., that APRA accepts the head office requirements as substituted compliance for these branches. We note the benefit in continuing to codify the applicability to foreign ADIs of the proportional application, given the very specific attributes of foreign ADI structures.

For all ADIs including domestics, the variation from existing standard operational risk practices mean implementation costs are expected to be substantial. We estimate in the order of $400 million across the ADI sector. This estimate may be conservative as a lack of guidance is limiting some ADIs' ability to accurately understand the totality of the increased requirements and the associated oversight and cost burden. We expect APRA will receive submissions including this one noting various variances from existing or standard practice and while these points are important the underlying issue is that the standard is too prescriptive. For example, the requirements around which providers to capture force a large increase including non-material providers required to be captured, rather than allowing firms to take their own risk-adjusted approach.

We would expect that a less prescriptive approach would significantly reduce these costs without compromising operational risk and resilience standards.

APRA has indicated it intends an uplift in operational resilience measures and the industry supports this aim. We seek to work with APRA to find efficiencies where possible while maintaining an uplift in operational resilience.

In terms of the consultation process we would encourage APRA to engage more at the conceptual stage rather than the draft stage where strategic change is much more difficult, and inertia tends to be more of an issue.

Given the scale of the industry project, it is important that sufficient time is allowed for implementation. APRA should consider a phased implementation, with final implementation no earlier than 1 January 2026.

For foreign ADI branches, where home jurisdictions are also undertaking work on operational resilience, APRA should endeavour to ensure its program coordinates well with this work. Implementation would be greatly assisted by published regulatory guidance including the topics and areas mentioned in this submission at a minimum one year prior to effective date.

Table 7 of the consultation lists eight key questions intended to identify specific areas for feedback that would assist APRA in finalising the requirements. AFMA's response to these areas follows this letter.

Issues where clarification is sought by our constituents, and other matters raised, are listed in the 'Specific questions' section at the end of our submission.

For more information or if you have questions in relation to this letter please contact [redacted]

Yours sincerely

Murray Regan

Director Policy and Markets

Overall Design

1. *Is a single cross-industry standard for operational risk management supported?*

AFMA supports a single cross-industry standard. The key operational risks referenced in the proposed principles-based Standard (legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, reputational risk and change management risk) are common across the industries and are without doubt, a complex path to navigate. Accordingly, it is eminently sensible to 'translate' and aggregate the existing five cross-industry standards into a single standard.

There are advantages in a reduction in complexity for both firms and APRA itself, and an increase in commonality of requirements for firms interacting with firms from different financial sectors.

As outlined in the discussion paper, accompanying the aggregation process is the introduction of CPS 230 is intended to strengthen the management of operational risk and raise standards. We support this aim but have concerns around the approach being used and excessive costs it entails.

AFMA's submission notes areas where greater proportionality is appropriate on a risk adjusted basis, and where sectoral differentiation, albeit framed within the common standard, would continue to support efficiency.

Care must be taken to ensure that sensible industry-specific refinements currently embodied in the existing standards are not lost in the translation to a single standard, e.g. for foreign ADI branches this would include home jurisdiction outsourcing arrangements and other concessions recognised in CPS 231 and CPS 232. These refinements can create efficiencies for the industry and regulator; and ultimately the investing public.

2. *Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?*

Key areas where concerns were raised and/or clarifications sought are listed in the Specific Questions section at the end of this submission.

In addition to these, we note that the creation of guidelines (CPG 230), will be essential in fully assessing materiality, systemic importance, risk tolerances, and assisting with implementation.

3. *How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs?*

The consensus view of foreign ADIs in our membership is that they would strongly support the more explicit approach to scaling down or exclusion from certain requirements in

APRA standards for non-SFIs and the subcategory of foreign ADIs. This is consistent with our response to consultations on (1) APRA's post-implementation review of LCR and NSFR; (2) Proportionality and SFIs; and (3) APRA's Strengthening crisis preparedness discussion paper.

There are efficiencies for firms in ensuring the application of the standard is risk-based. It would also assist in ensuring APRA's resources are applied in an appropriately way to the risk landscape.

Beyond these explicit exclusions and scaling there should of course remain scope for proportionate application of the standard requirements that are not explicitly excluded or scaled down for non-SFIs and the subcategory foreign ADIs.

Inclusion of foreign ADI subcategory

AFMA recommends retaining a foreign ADI sub-category in this and other prudential standards as a separate category of non-SFIs. We note this would be consistent with existing standards. Maintaining use of the foreign ADI category through APRA's modernisation and simplification of the prudential architecture program will maintain clarity around what is applicable to these entities.

Foreign ADIs are a recognised category of ADI in the Banking Act for which various exclusions apply. APRA also recognises in its definition of an SFI that foreign ADIs are generally to be excluded. These limitations recognise that a foreign ADI branch forms part of the same legal entity as its head office and is largely supervised by the prudential regulator in the home country. Foreign ADI branch operations including risk management must be, and will be, supported by the head office.

While the SFI vs non-SFI distinction is supported as sensible, further enhancement of proportionality could be achieved with respect to the prudential obligations through the use of a foreign ADI subcategory and suitably calibrated requirements.

CPS 230 Operational risk management

Under the draft CPS 230, ultimate responsibility for a foreign ADI branch operational risk profile is assigned to the Senior Officer Outside of Australia (SOOA). This person or group is part of the head office operational risk management group and will be required to implement the head office standards.

APRA notes it has had regard in designing the new standard to the BCBS' recently released Principles for Operational Resilience and Principles for the Sound Management of Operational Risk. This is supported as it contributes to global consistency.

Where the head office of a foreign ADI operates or intends to operate under these principles (or similar principles in the relevant jurisdiction), the Australian branch will also be required to operate under these principles.

Imposing additional or different risk management protocols that are bespoke to Australia on a foreign ADI branch already operating under a BCBS compatible regime is duplicative and redundant. In our view it would be an unnecessary burden on the branch, its SOOA and on the head office without an accompanying gain in operational risk outcomes. We would suggest this would be unlikely to align with APRA's intentions for its project to simplify and modernise the policy frameworks.

More generally, ensuring that home jurisdiction requirements, where comparable and consistent with international standards and principles, are recognised consistently across all relevant APRA prudential standards should be an important outcome of modernisation of the prudential architecture.

The recognition of head office substituted compliance is already acknowledged by APRA in some prudential standards e.g. APS 221 (Large Exposures)- with exclusion of foreign ADI's subject to consolidated supervision by their home country supervisors; and CPS 226 (Margining and risk mitigation for non-centrally cleared derivatives) – para 67 which allows foreign ADI's to rely on home jurisdiction margin and risk mitigation requirements.

4. *What are the estimated compliance costs and impacts to meet the new and enhanced requirements?*

Based on the figures we have received; we estimate total ADI costs to be in the order of $400 million in project costs, particularly should APRA significantly expand the type and number of service providers potentially in scope as outsourced as drafted.

Our ADI members may individually respond with cost estimates relative to their entity.

Specific requirements

5. *How could APRA improve the definitions of critical operations, tolerance levels and material service providers?*

<u>Definitions</u>

As APRA seeks to rationalise definitions in prudential standards, we suggest these should mirror BCBS definitions as far as possible to promote international consistency. Increased international consistency can reduce complexity for global institutions seeking to implement a consistent global framework.

AFMA also notes that local definitions should, as far as possible, support international practice. For example, foreign ADIs report that tolerance levels can be set to specific times such as the next market open rather than periods of time.

APRA may wish to consider adding a definitions section to ensure all defined terms are in one place rather than throughout the Standard or standards, and that the definitions of criticality and sensitivity in both CPS 230 and CPS 234 are consistent.

Critical Operations

AFMA supports APRA not providing a prescribed list of critical operations. We note that UK regulators intentionally did not provide a list. Regulated firms were tasked with determining what would constitute a critical operation ('Important Business Service').

To assist firms in identifying these services the UK regulators provided thresholds e.g. could a disruption/outage of any given service threaten a firm's safety and soundness or threaten financial stability. Under the UK guidance a business service needs to be a service that is delivered to an external end-user, that is understood by the end-user and is a single service rather than a collection of services.

The combination of clear guidance on Important Business Services and Impact Tolerances enables firms to identify their critical operations and understand what is needed on top of classic business continuity planning to limit prudential harm to themselves or the economy. Incident management and business continuity should sufficiently cover all other scenarios.

APRA could consider a similar approach to the criteria firms should consider when making a determination that an operation is a Critical Operation. More guidance on the principles, tests and materiality thresholds would assist firms in identifying critical operations.

We suggest that the operations listed in para 35 be reframed as typical examples rather than a minimum list. Different firms will have different critical operations given their business activities in the jurisdiction and having examples would better reflect this state of affairs.

Material service providers

As drafted CPS 230 appears to significantly expand the type and number of service providers potentially in scope as outsourcing.

We note the proposed test in para 49:

> "Material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk"

A qualitative threshold approach as outlined above may better serve the wide range of entities that will be subject to the regulatory obligations of CPS230.

We note that fourth parties relied upon by material service providers will often not be APRA regulated entities. The requirement to manage risks associated with fourth party service providers may endeavour to create requirements for non-APRA regulated entities by proxy. This type of indirect regulation has natural limits to which it can be implemented, and substantial costs for all parties. It is not an optimal solution and imposes increasingly challenging requirements for ADIs to look back through long service channel provision chains. It may not be an economically efficient approach to increasing operational resilience to create liabilities for long supply chains.

Further comments in relation to material service providers are provided under Question 6 below.

6. *What additions or amendments should be made to the lists of specified critical operations and material service providers?*

APRA may wish to explicitly list material service providers which are outside the scope of the Standard, this would be consistent with the EU approach. For example, such a list could include services and systems usage mandated by ASX, Austraclear, RITS, PEXA. etc.

Such a list should assist in reducing duplication of assessment requirements and thereby increase the efficiency of ensuring operational resilience in relation to these systems.

AFMA seeks to understand whether APRA sees Tier 1 banks in Auspaynet's hierarchy as part of the financial market infrastructure.

AFMA sees the potential for more flexibility to be introduced for industry in relation to prescribed critical operations. The critical operations prescribed are by nature broad and will differ from institution to institution.

We note APRA is using language consistent with that the BCBS Principles in referring to 'critical operations'.

Current drafting of the list of specified critical operations may impose unnecessary requirements placed on a regulated entity for non-material services it receives from a "material service provider". Examples: i) the entity hosts its payments technology with a cloud provider, it would have "payments" as a material service, and therefore the cloud provider as a material service provider; ii) the regulated entity may also have other services delivered from the cloud provider e.g. an employee benefits web portal offering retail discounts from partner organisations. The latter is in no way material, yet given it is delivered by a material service provider, greater clarification is required as to whether non-material services would be caught by the proposed contractual requirements in CPS 230.

7. *Are the notification requirements and the time periods reasonable?*

Notification timeframes

Members advise that the new requirement to notify APRA within 72 hours after becoming aware of an operational risk incident is likely to have a material financial impact or

material impact to meet the timelines. See also our comments in relation to para 32 below.

Members report that CPS230 as drafted would require significant changes in terms of incidents response arrangements that require immediate tracking and real-time understanding of incidents. The notification schedule - 72 hours max to (1) identify (2) assess (3) escalate, (3) record, (4) address and notify APRA is tight. As such, it will be important for APRA to clarify how materiality is to be determined and to clarify the reporting granularity required in the report notified. We suggest reports should be high level and considered indicative only.

Members agree that the 24-hour requirement to notify APRA of BCP activation is reasonable but hold that the notification report should be on a best endeavours basis. APRA notification is unlikely to assist system recovery, and resources should be directed primarily at that aim.

Implementation timeframe

The timeline for implementation of the Standard, i.e. January 2024, is overly ambitious given i) the complexity, and size of implementation projects required to meet the proposed standard, ii) the current lack of guidance and iii) other regulatory programs utilising scarce resources.

APRA's proposed implementation date coincides with those of a variety of other standards, e.g. CPS 511 Remuneration (for non-SFIs), CPS 190 Financial Contingency Planning, and CPS 900 Resolution Planning. In addition to this, the Financial Accountability Regime (FAR) will also be implemented during the 2023 period.

All regulatory changes require a significant transition period following the final release of the Standard and its guidance. Furthermore, successful implementation is dependent upon ADIs receiving adequate time to design, document, test, ratify and apply the key requirements as outlined in the final guidance; in the case of CPS 230 this assumes the latter can be provided within the first half of 2023 to meet the proposed 1 Jan 2024 date.

A more reasonable and practical path towards successful implementation would be to postpone implementation until January 2026 at the earliest, and that entities (to which this Standard is clarified as applicable), apply the additional time afforded by this to the formalisation of internal protocols while prioritising the mitigation of the key risks in a manner that provides ongoing surety of operational resilience.

It should be noted that some of APRA's initiatives mirror other regulators who are also implementing regulatory initiatives to enhance operational resilience. Some consideration to provide flexibility in implementation timelines should be given to Foreign ADIs who may have global rollout timelines dictated by home regulators.

8. *What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers (if required)?*

Any contract negotiation and/or renegotiation, be it with existing service providers or in relation to outsourcing arrangements, can be a lengthy process. It will invariably be subject to review, amendment and acceptance by both parties operational and legal divisions. Refreshed agreements may in the first instance be subject to further, timely negotiations.

EU guidelines on outsourcing note the challenges faced by institutions when updating assessments and documentation within a one-year period. This minimum timeframe should also apply in Australia.

Specific industry questions on draft CPS 230

Foreign ADI branch concessions

Important concessions appear to have been discarded during the consolidation process. This has raised concerns for foreign ADI branches particularly around home jurisdiction outsourcing arrangements and other concessions recognised in CPS 231 and CPS 232, e.g. Group reliance, outsourcing and other intra-group arrangements.

CPS 231 (para 5) and CPS 232 (para 6) each contain language that allows reliance on board-approved global policies. CPS 231 (para 32) also provides that where a foreign ADI enters into an outsourcing arrangement with its head office, an outsourcing agreement is not required. However, these critical provisions have not carried over into CPS 230, and should be inserted in recognition that:

a) the branch is part of the same legal entity as the parent (making binding legal agreements between the two not possible).

b) the branch and its parent will be relying on the same operational infrastructure to run critical business functions.

c) the branch should not be expected to have any material input in the oversight of fourth party providers to a head office outsourcing arrangement.

d) the branch operations are necessarily dependent on those of the overseas bank as a whole.

e) it is inefficient to require foreign ADI branches to have bespoke policies and procedures at a time where entities generally are actively working to centrally align these as the means to mitigate regionally idiosyncratic risk profiles.

Specific topics or areas on which guidance would be particularly useful to assist in implementation

Application and Commencement, key principles

Para 2: We suggest foreign ADIs should be allowed to use substituted compliance with home jurisdiction regulatory frameworks and policies where these are compatible with international standards.

Para 3: AFMA notes the potential for indirect impacts on the head office and affiliate branches of the Australia branch due to the inclusion of obligations attached to offshored processes and suppliers.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7955 Fax: +61 2 9776 4488
Email: info@afma.com.au Web: www.afma.com.au

Para 11a: This draft introduces requirements around appropriate standards for conduct and compliance. We seek to understand more around the inclusion of these areas within an operational risk standard as these would typically be dealt with separately.

We note that in the conduct space many APRA regulated entities are also regulated by ASIC who oversee market conduct requirements.

Para 13: More information is sought in relation to the concept of "practicable" both generally and especially in relation to the prevention of disruption to critical operations.

Para 14: The requirement for an ADI to 'not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks', may not fully take into account the interdependent nature of Australia's financial system and the dependency of a local branch of a foreign ADI to the head or regional office.

Para 15: Propose the opening sentence is reworded to: *In order to fulfil its risk management framework obligations under Prudential Standard CPS 220 Risk Management (CPS220) and Prudential Standard SPS 220 Risk Management (SPS 220), an APRA-regulated entity's operational risk management framework, must, pursuant to this standard, develop and maintain*:

Risk management framework

Para 15a: (governance), 15d (monitoring, analysis etc) are more-appropriately placed in CPS 220 and kept common to all risk management practices and processes.

Para 15c: Members are interested in APRA's understanding of how 'designed and operating effectively' should be determined.

Para 15e: "Tolerance levels" and "severe but plausible scenarios" are not typically applied within BCM/BCPs. These terms are more commonly associated with an enhanced operational resilience framework.

Para 15 and 20: There appears to be the potential for interaction and linkage with the Financial Accountability Regime, more information on how these should interact is sought.

Para 17 This statement would be better placed in the CPS 220 standard.

Para 19: We note that 'Board' for foreign ADIs refers to the SOOA. We would appreciate more discussion as the standard progresses on how this should work in practice.

Para 20: The definition of 'senior management' should be clarified for across the range of ADI sizes and structures.

Para 21c: The standard needs to include a paragraph that is the equivalent of Para 5 of CSP 231, i.e.: '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.'

Para 22: "Clear and Comprehensive" are subjective terms. Comprehensive information 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 probable impacts to critical services when making decisions that could affect those services.

AFMA supports the provision in the guidance for CPS 230 of a table of examples of reporting as was done in Attachment H in CPG 234.

Operational Risk Management

Para 23: APRA is defining Operational Risk very broadly. Firms typically manage some of the risk types listed as operational risk in Para 23 as separate risk types – for example compliance risk is typically treated separately from operational risk. Consistent with this ISO has a standard for compliance management systems ISO 37301. These are often not managed as a type of operational risk. The BCBS Principles for Operational Resilience do not appear to include some of the risks suggested by APRA as operational risks including compliance and legal risk. Similarly, governance matters would be better placed in CPS 220 rather than being specific to operational risks only.

We query whether firms would be required to recast all the listed risks as operational risks under the proposed standard.

Clarification is sought on APRA's policy intent behind this where it broadened the scope of operational risk to include effectively all types of non-financial risks.

Clarification is sought on the term 'end-to-end' - does this mean across the product or service life cycle or does it mean from front office to back office?

Clarification is sought as to whether APRA intends that 'change management risk' includes delivered risk and delivery risk.

For foreign ADIs expectations around who would normally be included as 'senior managers' is requested.

Para 24: AFMA seeks more information on what would constitute the sound information and health as it relates to IT infrastructure.

In light of the reference to CPS234 both in this Para 24 and also Para 50, guidance on what constitutes "managing" information assets would be helpful, specifically is "manage" defined by a service provider having control over an information asset? - would information received solely for the purpose to perform a transaction, but the information asset is not edited in any form be considered as managed?

Operational risk profile and assessment

Para 26 AFMA seeks more information on what constitutes a comprehensive assessment of operational risk profile. Firms suggest some efficiencies can be found in cross overs with BCP testing.

Para 26a: For foreign ADIs, the information systems may be designed and managed offshore by the head office.

Para 26b: While this is in line with BCBS standards, it is not a requirement that is typically expected placed in an operational risk section.

Para 26c: We query whether it is the intention to merge operational risk scenario analysis and operational resilience scenario testing?

Foreign ADI should have discretion to determine how best to address severe operational risk events and if undertaking scenario testing is necessary relative to how the branch is structured and supported by parent organisations. In addition, current BCP requirements would address some of these material operational risk scenarios. There appears to be scope for more integration of BCP and Operational Risk Scenario testing.

Paragraph 27*:* Clarification is sought as to the where responsibility lies to assess the materiality of the service, i.e. is this with the provider or the recipient of the material service?

The requirement to perform a 'comprehensive risk assessment' every time an ADI provides a 'material service' to another party would create a cost burden on service provision, resulting in increasing the cost of providing the service to the other party.

Operational risk incidents

Para 31: Further guidance is sought in relation to current thinking in relation to 'near misses' and how it is to be factored into the operational risk profile other than for assessing systemic issues and identifying potential areas for control enhancements.

Para 32: Clarification is sought on the overlap between the notification requirements in para 32 and para 41 and how this would work in practice. Take for example, a 'creeping incident' such as an evolving privacy or supplier incident necessitating a shift to a new service provider–at what point does it shift from being an operational risk / privacy incident into a crisis management activation? This includes further guidance to determine the point from which the 72-hour period is triggered – i.e. from the point of the incident, or the point at which it is deemed to be material? The investigation into an operational

risk incident may uncover material financial impact but there may be a time lag between when the incident is first identified and becoming aware of its financial impact.

APRA may wish to consider including a section in the guidance for CPG 230 that parallels CPG 234 s88-91 to explicate notifications. A section to show the interaction between CPS 230 and CPS 234 would also be advantageous.

We suggest that APRA reconsiders either whether a timeline in CPS 230 is necessary, or whether to align the proposed timeline with other existing prudential standards with similar reporting requirements. E.g. CPS220 & CPS234; as well as other legal and similar regulatory requirements [such as Corporations Law, Banking Act (s.62A - 10 days)] that substantially cover events that may have an impact on the entity being able to maintain its critical operations.

Para 33b: We will seek to understand more around what constitutes 'reasonable steps' to minimise the likelihood and impact of disruptions to critical operations.

Para 33c: i) What materiality threshold should be applied when maintaining a credible BCP, i.e. is it only for critical operations or does it extend to business units? ii) Consider replacing "credible" with "scalable" (also refer comments under Para 45).

Para 34: We would welcome further discussion on the tests and principles firms should use when determining

Para 35: AFMA suggests that the listed operations should be listed as examples but should not require these to be included necessarily as critical given the breadth of ADI models.

In the alternate we suggest removing "deposit taking" on the basis that a client can deposit funds elsewhere if an ADI is not operational. In addition, a customer enquiry does not have the potential to cause a material adverse impact as outlined under s. 34. AFMA seeks to understand what functions are intended to be included in 'client enquiries' as a critical operation. AFMA expects this should only include client service functions supporting critical functions.

Para 36: This section permits APRA to override an ADI's classification of a critical operation (e.g. where they have taken a risk-based approach to such definition). We request APRA outline the circumstances under which it may consider the need to exercise such powers and provide an example.

Para 37: Clarification is sought on where APRA expects tolerance levels to be recorded.

Para 37b: We suggest the deletion of the need to establish tolerance levels for maximum data loss. Data loss may but does not always necessarily cause disruption to an organisation – this would be dependent on what data has been corrupted and on which system. The concept of data loss has the potential to add complexity and may provide challenges in setting the appropriate impact tolerances consistent with APRA's intention i.e. is it total loss, temporary loss (which is time based), is it loss of data between systems, backup frequency, maximum recovery time of data processing (RPO's) or data inventory,

or both? APRA would also need to consider whether the expectation extend to information.

Para 38: We would seek to understand the circumstances under which APRA may intend to consider the need to exercise such powers and provide an example.

Given exercise of this clause would be a substantial intervention in the internal operational functioning of one or multiple firms we would request to understand how this would be based in APRA's legislative framework. In our view APRA should be satisfied where an ADI can effectively demonstrate compliance with the requirements.

Business continuity plan

Para 39: It may be more appropriate to frame this in terms of a critical business service rather than a critical operation as it will be easier to identify a disruption to a service than to an operation.

Para 39c - Does this include short term substitute processes?

Para 39b and **Para 39e** - We seek to understand what elements need to be included within the BCP as opposed to the crisis response plan. A communications plan may best be encapsulated in a central document rather than within individual BCPs.

The requirement to include in a plan 'triggers to identify a disruption' is unclear and does not seem practical. Where an event gives rise to a crisis management plan being invoked, a damage assessment is completed (i.e. impact assessed) regardless of a trigger resulting (or not) in a disruption.

Para 39d – We seek to understand at what level does this information need to be provided. Critical operations will logically be at the Group level. More clarity around the meaning of "assessment of the execution risks" is requested.

Para 40: An APRA-regulated entity must maintain the capabilities required to execute the BCP, including access to people, resources and technology (12). Foot note 12 refers to the Capabilities required to execute the BCP may be maintained within the APRA-regulated entity or via an agreement with another party. For the avoidance of doubt, such agreements with other parties must meet the requirements for management of service providers arrangements in this Prudential Standard.

It would be helpful if APRA can provide some examples of these capabilities in the Prudential Practice Guide – in particular clarification as to whether the APRA's focus is on the resiliency strategies that would be executed in a BC event, or the underlying components like staff skills and proficiency, capacity, access, and others needed to successfully perform the work.

Para 41: AFMA notes that firms may have multiple levels of BCP for example: Group Level BCP, the critical operation BCP, the Business Unit BCP, etc. APRA may consider allowing firms to define a risk-based approach in terms of this notification requirement, that selects key BCPs in APRA relevant units.

Please also note the comments under Para 32 with respect to the discrepancy on notification timings.

APRA may wish to consider refining the BCP notification triggers relevant for CPS 230 para 41 for foreign ADIs to only be for critical operation BCP triggers for the branch business only. Group level BCP activation trigger may not have any relevancy for the branch and ensuring awareness of branch-irrelevant matters to comply with the deadline set within the standard is an inefficient use of resources.

Para 42: AFMA suggests it be made clear that the annual business continuity exercise need not test all the regulated entity's critical operations in a single year but rather that it can be performed on a multi-year rolling or trigger driven basis. This requirement may be better served by allowing regulated entities to have a rolling testing schedule over a number of years, rather than attempting to test a disruption to every critical operation (service) every year.

We query whether end-to-end annual testing of every critical operation is the optimal approach. This will be a very significant exercise adding material effort and cost that might not strike the optimal balance between depth and coverage of testing. A better approach would be to risk-assess and rotate testing over a number of years. (In its CPG, APRA may also look to include reference to APRA's Cloud computing Information Paper and explain the relationship between that paper and the CPS.)

As noted under Para 15e, "severe but plausible scenarios" is a concept applied to operational resilience by offshore regulators (eg. BCBS, FINMA) and not BCM / BCP. APRA may wish to consider whether this concept is well suited to BCM and if so, update guidance to provide some examples of the scenarios they are expecting to be tested. If it is to be used we suggest it should be commensurate with the critical operations and tolerance levels identified and set by the Institution.

Para 43: AFMA seeks clarification of APRA's objective in relation to para 43 and under what circumstances APRA would require the inclusion of an APRA-determined scenario in a business continuity exercise for an APRA-regulated entity, or a class of APRA-regulated entities. We seek to understand if this is intended to be on a case by case basis.

Para 45: Can APRA please outline the definition of "credible" or consider replacing this word with either "feasible" or scalable" (please note the similar comment under Para 33c).

AFMA trusts that firms will be able to confirm their internal determinations of appropriate periods with APRA.

Management of service provider arrangements

CPS230 proposes a general shift in the regulatory view of service providers, moving from material outsourcing arrangements to material service providers. This may not be aligned to other jurisdiction's regulatory requirements which look specifically at the materiality of the arrangement, e.g. the recent MAS Information Paper is more focussed on the arrangements with third party service providers.

Increased consistency of terminology usage with a focus on reference to “arrangements” would be of assistance– the draft standard alternates between requirements for a material service versus a material service provider, which could lead to inconsistencies in required controls.

In addition, scope appears to include services performed by a material service provider rather than just material services, which will increase the population of services that need additional controls, oversight and notification. The scope of activities with material service providers, or any fourth parties that they rely on, should be limited to critical business services which is paramount in ensuring a risk focussed approach and an efficient use of resources. Any approach which results in an unnecessary widening of the scope of service providers would appear contradictory to APRA's objective of achieving appropriate proportionality.

Para 46: The management of arrangement with providers will depend on the nature of the providers. This level of detail should not be included in a policy; rather, it should be included in a standard or operating procedure.

Para 47: The policy should include the requirement of a register not the register itself. The latter is an operational document that would change from time to time, as providers are added and deleted.

Para 47d: refers to requirements in respect of managing ‘fourth parties’ that material service providers rely on, which may also capture sub-contracting arrangements. Guidance will be helpful in order to ascertain how far along the supply chain do APRA-regulated entities need to go in order to meet their due diligence obligations (and what level of diligence would be required).

AFMA suggests APRA consider including a materiality component in the CPS 230 definition of fourth parties in footnote 13.

To achieve a more appropriate balance of reach APRA may wish to consider revising the scope of 47d to one that is some steps closer to the outsourcing definition under the current CPS 231 plus related party or third parties who manage information assets on behalf of the regulated entity as defined by CPS 234. We suggest a dialogue with industry on these types of refinements to explore the issues.

APRA has also acknowledged the longer and more complex supply chains which often involves a reliance on cloud-based services.

APRA may wish to include a footnote to its Cloud-computing Information Paper.

Material service providers

While understanding a firm’s material service providers and the risks that are associated with them is important, the proposed approach as drafted might be more closely aligned with standard practice. The focus should predominantly be on identifying the Material Services for the register and understanding how risks are mitigated at the service level. This would:

- Closer align to how risk assessments and key controls to mitigate third party risks are performed for critical operations, such as business continuity plans, tolerance thresholds, information security assessments, geopolitical assessments. exit planning and Service Level Agreement performance monitoring all being performed at the service level and not on third parties;

- Allow more granular concentration risk analysis to be provided on the register; and

- Ensure heightened focus on material services rather than low risk services with service providers deemed material.

Para 48: It would be helpful if APRA could define a minimum expected level of content or detail to be included in the register of material service providers (APRA may consider updating the guidance to provide some examples of key data points for the purposes of maintaining an inventory register). APRA has i) advised it will be using a consolidation of industry registers to assess industry concentration; and ii) encouraged the application of a risk-based approach to capture those service providers most relevant to the continued delivery of a critical operation.

We would request guidance with respect to Footnote 14 as to whether a related party or connected party is only intended to capture an offshore related service provider or whether it would also apply to onshore related service providers e.g. a local related entity providing custodial services to another local trading entity under a prime brokerage product suite?

This clause includes mention of "material operational risk". We seek further guidance on this term.

Para 49*:* On the understanding that material service providers (MSP) would be assessed at legal entity level, we query whether this would result in one provider becoming a material service provider for all business units using the provider regardless if the service received is not a critical service for that business unit?

The list of material service providers whilst helpful, does not - at face value - allow for proportionality to be considered. e.g. whilst a firm may have an arrangement with an insurance broker, the arrangement may not be material, but by a strict application of this rule, it would be.

Para 50: In light of the reference to CPS234 (para 24 & 50), and as already noted under Para 24, it would be appreciated if APRA can provide guidance on what constitutes "managing" information assets. Please provide clarification if "manage" is defined by a service provider having control over an information asset - would information received solely for the purpose to perform a transaction, but the information asset is not edited in any form be considered as managed?

Para 51: We would welcome further clarification from APRA with respect to the timing (annual due date) and format of the register submission (eg. via regulatory portal, e-mail etc).

Service Provider Agreement

Para 52: Proportionality should be considered when entering renewing or materially modifying an arrangement. The focus should be on material services rather than any service for a material service provider, this would allow resources to be focused on the services that if failed would have a material impact on the APRA Regulated Entity. Focusing on non-material services may divert attention and resources away the material services.

Para 52a: For foreign ADIs outsourcings to related bodies corporate should be excluded from the requirement to undertake a tender or selection process on the entering into, renewal or modification of a material service provider arrangement. For foreign ADIs these 'outsourcings' are often to the same legal entity in its head office entity, or are arrangements put in place by that head office.

Para 52c: There are conceptual difficulties for firms to estimate which entities have systemic importance as they are not well placed to know which other firms are using the service provider. APRA may consider removing this requirement and determine any systemic dependencies when they analyse lists of service providers/arrangements provided to them by regulated entities. APRA could then provide guidance on the determination what are 'systemically important' providers in Australia or identify those they consider are part of this category.

Para 53d: We note material service providers may not be APRA regulated and may not be aware of the 'materiality' of their own service providers unless defined by contract.

Para 54: CPS231 provided that prior to any onsite visit to a service provider APRA will normally inform the APRA-regulated institution of its intention to do so. This is no longer specified and should be re-instated.

Para 54a: We request APRA please confirm that provisions within an agreement that permit general regulatory access are sufficient, without explicit reference to APRA as a regulator.

Para 55: These requirements should be applied using a risk-based approach rather than a blanket approach for each arrangement with a material service provider, to ensure, as previously noted above, that there is heightened focus on material services rather than low risk services with service providers deemed material.

Para 55b: APRA may consider removing this requirement on the basis that this is covered by APS222 (Associations with Related Entities).

Monitoring, notifications and review

Para 58: Notification requirements relate to provision of a service however inventory register is to be on a material service provider basis (para 48). From a framework perspective this might introduce inconsistencies.

With regard to notification obligations, it could be the case that serval offshoring arrangements roll up into a single agreement with a material service provider. AFMA requests clarification on whether the notification requirements are once per material entity plus any material changes, or is the expectation at a more granular process level?

For foreign ADIs, the latter will be a significant burden for related parties. A requirement to notify APRA whenever its head office changes a global support arrangement related to a material service provider would appear excessive relative to the risks to the jurisdiction.

Under the current CPS231 (Outsourcing) prudential standard, there are carve-out provisions for the timing of the notification requirement in the event of BCP being invoked as the result of an unexpected event. We request APRA consider the same carve outs in relation to specific provisions under CPS230.

Para 58b: this obligation has been widened from the existing para 39 of CPS 231 by including any offshoring agreement with a material service provider, regardless of the risk of the service being offshored. This is quite an onerous obligation and both ADI's and APRA will benefit respectively from not utilising resources to notify and review low risk service arrangements.

Please also note that this is the only paragraph within the draft prudential standard that references "offshoring", it is otherwise referenced as "outsourcing" throughout the paper. We suggest the use of a single term if the meaning intended is the same.

Para 59: Given that ADI's employ a three lines of defence model, it would seem unnecessary to continue the in-principle requirement to conduct an audit for each and every outsourcing arrangement with a material service provider for a critical operation. Annual audit plans are based on annual risk assessments, with senior management and committee input and are typically approved at a very high level within an organisation. The audit population is covered in a risk based multi-year audit cycle with the planning, conducting, reporting and assuring individual audit engagements typically undertaken in accordance with the procedures defined in the Professional Practices Framework.

Members note that the use of the term 'outsourcing' in Para 59 should be more clearly defined such that arrangements are only captured where provided on an ongoing basis (as opposed to a temporary/short-term basis).