Amstelveen Pty Ltd
ABN: 54 615 045 531
Level 11, 570 George St
Sydney NSW 2000

19 October 2022

General Manager – Policy
Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001
Australia

By email: [redacted]

APRA Policy Team,

Re: Response to Discussion Paper – Strengthening Operational Risk Management

Amstelveen welcomes the opportunity to provide feedback on APRA's Draft Prudential Standard CPS 230 Operational Risk.

Amstelveen is a specialist risk and compliance consultancy which operates across Australia and New Zealand. Our clients include organisations in the banking, insurance, payments, funds management and superannuation industries.

In this submission we have identified five observations which we believe are worthy of consideration, including that:

1. The proposed structure of operational risk prudential standards is reasonable;
2. The new definition of a material service provider should be clarified;
3. The minimum set of operational risks defined in the new standard should include 'process execution risk';
4. The defined approach to operational risk profiling should require consideration of emerging risks; and
5. Requirements for Internal Audit controls testing should be streamlined.

We describe these considerations in further detail below.

1. The proposed structure of operational risk prudential standards is reasonable

The new draft prudential standard CPS 230 serves to address operational risk as a whole and to consolidate existing standards for business continuity and management of service provider arrangements. This is a sensible approach which reduces duplication and allows for the application of common principles across various operational risk areas.

A notable exception to this consolidation is CPS 234 Information Security. Information security is a subset of technology risk, which is a type of operational risk. Given the high degree of industry and Board interest in information security, the specific nature of controls prescribed by CPS 234 and the relatively recent introduction of the standard, it is reasonable that information security co-exists as an operational risk area with a specific prudential standard.

2. The new definition of a material service provider should be clarified

CPS 231 Outsourcing notes that "*This prudential standard only applies to the outsourcing of a material business activity*". The standard provided a number of considerations relevant to the classification of a service provider as a material outsourcing provider.

Draft CPS 230 removes the specific reference to 'outsourcing' and modifies this to state that:

> *48. Material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk.*
>
> *49. Material service providers include, but are not limited to, those that provide the following services to an APRA-regulated entity: risk management, core technology services, internal audit, credit assessment, funding and liquidity management, mortgage brokerage, underwriting, claims management, insurance brokerage, reinsurance, fund administration, custodial services, investment management and arrangements with promoters and financial planners.*
>
> *50. Material service providers also include providers that manage information assets classified as critical or sensitive under CPS 234.*

The inclusion of s49 could be interpreted in two ways:

a. Any service provider involvement in the activities listed in s49 requires a supplier to be categorised as a material service provider; or
b. The listed activities are those that APRA considers to be a "critical operation" in s48 and material reliance on providers for these services should result in a supplier being classified as material.

The standard is unclear as to which of these interpretations APRA has intended, however the accompanying discussion paper implies that it is the latter.

This would be the more prudent interpretation, as the first interpretation would have the effect of seeing a large number of relatively immaterial suppliers being classified as material. From a competitive perspective, this could result in a concentration of sourcing from existing, larger suppliers, since performing even small amounts of work with a new supplier would necessitate their inclusion as a

material service provider and increase administrative overheads for both the regulated entity and the provider. This is not desirable for regulated entities, as it would concentrate activity and risk in a fewer number of vendors.

APRA should clarify s49 in favour of the second interpretation above. This could be achieved by modifying the clause from:

> *49. Material service providers include, but are not limited to, those that provide the following services to an APRA-regulated entity:* [..]

To:

> *49. Critical operations include, but are not limited to, the following:* [..]

3. The minimum set of operational risks defined in the new standard should include 'process execution risk'

The draft prudential standard has established a minimum set of operational risks to be managed by an APRA-regulated entity at s23. These include "*legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, reputation risk and change management risk*". A notable operational risk which is absence from this list is 'process execution risk', which is the risk that losses arise due to failed, erroneous or anomalous processes or transactions.

While the business continuity provisions of draft CPS 230 cover the process failure and continuity elements of this risk, considerations relating to process output errors are not currently covered.

Draft CPS 230 provides examples of the types of critical operations for which this risk is relevant, in the context of business continuity, at s35; "*payments, deposit-taking and management, custody, settlements, clearing, claims processing, investment management, fund administration, customer enquiries and the systems and infrastructure needed to support these operations*".

The draft prudential standard should be updated to include 'process execution risk' specifically in the minimum set of operational risks to be managed by an APRA-regulated entity at s23. This aligns with APRA's broader intent around the standard, as articulated in s12; "*An APRA regulated entity must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems.*".

Flexibility should be provided for financial institutions to focus this risk type differently depending on their core business, as this is current practice. For example, some current uses of this in industry within Risk Taxonomies include "Transaction execution and processing risk", "Process Management Risk" and "Process or payments execution risk".

4. The defined approach to operational risk profiling should require consideration of emerging risks

The draft standard indicates a number of considerations which are required as part of the assessment of the operational risk profile at s26. These do not currently include a requirement to consider emerging risks and their impact on the risk profile. Consideration of such risks enables response activity to address

potential uncertainties before they become incidents and prevents risk profiling from being a superficial or rote activity.

This requirement could be incorporated into the draft CPS 230 standard through inclusion of the following within s26:

> *(d) identify, consider and document any emerging risks impacting the operational risk profile, and the need for any new or modified controls or other mitigation strategies.*

5. Requirements for Internal Audit controls testing should be streamlined

Through this draft standard and existing prudential standards, an entity's Internal Audit function will have a series of obligations to perform controls testing for operational risks. This includes a requirement to:

- CPS 230, s45: "*Periodically review the entity's BCP and provide assurance to the Board that the BCP sets out a credible plan for how the entity would maintain its critical operations within tolerance levels through severe disruptions and that testing procedures are adequate and have been conducted satisfactorily.*"
- CPS 230, s59: "*Review any proposed outsourcing arrangement with a material service provider for a critical operation, and regularly report to the Board or Board Audit Committee on compliance with the entity's service provider management policy for such arrangements.*"
- CPS 234 Information Security, s32: "*Review [..] the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance).*"
- APS 310 Audit and Related Matters, s22: "*Review [..] the policies, processes and controls put in place by management to ensure compliance with APRA's prudential requirements*" (this is applicable to Authorised Deposit-taking Institutions only).

As is evident, prudential requirements covering the scope of Internal Audit controls testing are currently fragmented. It may be preferable to consolidate these into a single set of Internal Audit operational risk controls testing requirements. These four provisions could be consolidated into CPS 230 per the below:

> *X. An APRA-regulated entity's internal audit activities must include a periodic review of the design and operating effectiveness of key controls that the entity uses to manage operational risks. This must include, at a minimum, key controls relating to information security, business continuity planning, relationships with service providers and compliance with prudential obligations.*
>
> *Y. An APRA-regulated entity's Internal Audit function must review any proposed outsourcing arrangement with a material service provider for a critical operation, and regularly report to the Board or Board Audit Committee on compliance with the entity's service provider management policy for such arrangements.*

This draft text could also be updated to include other operational risk and control areas worthy of mandated Internal Audit attention. General internal audit provisions in CPS 234 relating to using

appropriately skilled personnel (s33), and reliance on third-party controls testing (s34) should also be moved into the broader draft CPS 230 prudential standard as they are relevant to all internal audit controls testing activities, rather than just information security.

Alternatively, draft CPS 230 requires testing of controls (s29), presumably by Management. An addition requiring Internal Audit to perform similar control testing could be appended, as follows:

> *30. An APRA-regulated entity's internal audit function must establish, at least annually, an opinion on the effectiveness of the entity's control environment relating to operational risk. This opinion must be supported by independent control testing covering key operational risk areas, including at a minimum information security, business continuity, relationships with service providers and compliance with prudential obligations.*

Conclusion

Thank you for providing us with the opportunity to provide input into the draft prudential standard CPS 230. Please feel free to contact us to discuss any of these items in further detail.

Sincerely,

David van Gogh
Managing Director
Amstelveen

[redacted]