Australian Institute of Company Directors

[redacted]

21 October 2022

Mr [redacted]
General Manager, Policy
Policy and Advice Division
Australian Prudential Regulation Authority

via: [redacted]

Dear Mr [redacted]

Strengthening operational risk management – Discussion Paper

Thank you for the opportunity to comment on the Discussion Paper (the **Discussion Paper**) regarding the proposed *Prudential Standard CPS 230 Operational Risk Management* (**CPS 230**).

The Australian Institute of Company Directors' (**AICD**) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership of more than 49,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits, large and small businesses and the government sector.

The AICD's policy positions on CPS 230 have been informed by engagement with our members who sit on the boards of Australian Prudential Regulation Authority (**APRA**) regulated entities (**APRA entities**), including from the AICD's standing policy committee - the APRA Regulated Entities Forum, as well as additional discussion with industry.

1. Executive Summary

The AICD supports APRA's objectives with CPS 230 to enhance the operational resilience of APRA entities and position them to respond to changes in technology and the risk environment.

The AICD strongly supports APRA's outcomes focused approach to the drafting of CPS 230 and replacing five existing prudential standards across the regulated industries with one cross-industry standard in CPS 230. This approach represents a welcomed harmonisation and modernisation of existing prudential requirements and appropriately reflects that all APRA entities should have a consistent governance and management focus on operational risk and business continuity planning.

Our key points on the Discussion Paper and draft CPS 230 are:

1. The AICD supports the 'Role of the Board' provisions in CPS 230 noting that the board being 'ultimately accountable' and setting the roles and responsibilities of senior managers reflects existing governance practices at APRA entities. We encourage APRA to resolve any misalignment with the proposed Financial Accountability Regime (**FAR**) through minor drafting changes or guidance.
2. The AICD recommends that the Board should be able to delegate some of its responsibilities in respect of business continuity planning and material service providers to the Board Risk Committee.

3. A proportionate model to application of the material service provider arrangements, based on the Significant Financial Institution (**SFI**) distinction, would appropriately reflect the scope of the proposed obligations, the resource intensive nature of meeting the obligations in an ongoing manner and the relative limited bargaining position of non-SFIs.
4. APRA's expectations for 'fourth party risk management' are unclear and there is a limit to what an APRA entity can reasonably have oversight and influence on beyond the primary or principal material service provider arrangement.
5. The commencement timeline for CPS 230 should be extended to at least 18 months - 2 years from finalisation of the standard and guidance. Additionally, a transition period and/or grandfathering of existing service arrangements would recognise the significant industry disruption and resource burden that will be placed on entities to renegotiate contracts with material service providers.
6. Comprehensive practical guidance will be key to assisting APRA entities meet the intent of the proposed obligations under CPS 230 and promote improvements in operational risk and business continuity practices across all APRA regulated industries.

2. The role of the Board

This section responds to the 'Role of the Board' provisions at paragraphs 19 – 22 of draft CPS 230.

The AICD considers that the drafting of paragraphs 19 and 20 broadly reflects the existing oversight role of the board of an APRA entity. AICD members have noted that in practice the board is already accountable for the operational risk and business continuity practices of an entity. Further, the boards of APRA entities, particularly authorised deposit-taking institutions (**ADIs**) subject to Banking Executive Accountability Regime (**BEAR**), have existing processes to allocate responsibilities to senior management.

Alignment with the FAR

The FAR is currently before Parliament and appears likely to pass before the end of 2022 with a resulting commencement for ADIs in the middle of 2023 with all other APRA entities to follow in 2024. As with the BEAR, the FAR places obligations on the entity itself and each individual accountable person, including each director. It does not explicitly convey a joint or collective accountability on the board of the APRA entity.

The use of 'ultimately accountable' at paragraph 19 may create some uncertainty or misalignment with the FAR obligations in that it does convey a collective prudential 'accountability' obligation on the board. The AICD expects that in most cases this distinction is unlikely to be meaningful. However, there may be rare instances where APRA is examining whether a director has taken reasonable steps under the FAR in respect of operational risk matters and the potential for there to be tension with the collective accountability under CPS 230. The AICD encourages APRA to assess whether a minor amendment to this drafting could be made to clarify interaction with the BEAR/FAR or alternatively this could be addressed in prudential guidance.

Separately, we note that none of the draft FAR prescribed responsibilities specifically cover operational risk management, business continuity or the management of service provider arrangements.[1] We would expect it would be acceptable for a senior manager or executive who is an accountable person under the FAR to be allocated responsibility for operational risk matters under CPS 230. For example, the

[1] Exposure Draft, Financial Accountability Regime Minister Rules 2022, September 2022

accountable person with responsibility for 'overall risk management arrangements'.[2] Again, we encourage APRA to provide guidance that is clear that an APRA entity can utilise the FAR prescribed responsibilities for meeting the CPS 230 obligations.

Delegation to the Board Risk Committee

The AICD recommends that APRA enable the Board to delegate to a board committee, such as the Board Risk Committee, elements of the obligations under paragraph 21.

Consistent with the existing standards the AICD supports the Board having overall responsibility for approving the Business Continuity Plan (**BCP**) and service provider management policy. However, our view is that the following obligations would appropriately sit within the scope of the Board Risk Committee:

- review the results of BCP testing and oversee the execution of any findings; and
- review risk and performance reporting on material service provider arrangements.

Enabling delegation to the Board Risk Committee would be consistent with the approach under *Prudential Standard CPS 220 Risk Management* (**CPS 220**)(e.g. reporting on the review of the Risk Management Framework). As CPS 230 will result in a significant expansion of material service providers it would have a significant time impost on the Board to review performance reporting on every arrangement. Delegation would maintain director oversight, be consistent with the important role of the Board Risk Committee and importantly ensure that the strategic and oversight function of the Board is not undermined through unnecessary and overwhelming reporting.

3. Material service providers

The AICD supports APRA's approach to broadening the concept of service providers from that under the existing *Prudential Standard CPS/SPS 230 Outsourcing*. The AICD recognises the increasing importance of third parties in providing critical services to all APRA entities.

Proportionality

The definition of material service providers and list of services in draft CPS 230 is very broad in scope and will result in a significant resource burden on entities to not just meet the obligations from commencement but also in an ongoing manner. APRA entities have provided feedback that it will likely require significant technological change and expansion in the staff needed to monitor and review the material service provider arrangements. Small APRA entities will face significant challenges, due to their size and bargaining position with service providers, in meeting these obligations in an ongoing manner.

APRA contemplates in the Discussion Paper that one model of proportionality is where Significant Financial Institutions (**SFIs**) face heightened obligations as compared to non-SFIs. The AICD recommends that APRA explore whether proportionality based on the SFI distinction can be built into management of service provider arrangements under CPS 230.

One option to reduce the burden on non-SFIs would be to remove the requirement that for a *renewal or material modification* of an arrangement that a non-SFI has to undergo the steps at paragraph 52, for instance running a tender process. Non-SFIs often face bargaining challenges that are not shared by

[2] Ibid, 5(2)(b)

larger APRA entities and will regularly be in a 'take or leave' position with large service providers, for instance cloud computing providers. It is not apparent that requiring these entities to go through an intensive process for each renewal or modification will result in any improvement in operational risk outcomes.

Were APRA concerned that such an exception would result in open ended contracts or arrangements it could seek to place an overall time limit on any extended arrangements, for instance six years.

Fourth party risk management

Draft CPS 230 proposes to enhance the existing obligations under existing CPS 230 related to an APRA entity's oversight of the use of sub-contractors or fourth parties. The Discussion Paper adds additional context that APRA expects that the entity would have visibility of the risks associated with downstream providers.

Our view is that this is a key area requiring extensive APRA guidance as currently it is unclear how an APRA entity is expected to meet this obligation under the proposed service provider management policy requirements. As reflected by APRA in the Discussion Paper, increasingly service provision, particularly of critical business functions, often involve very complex supply chains with multiple organisations providing key inputs to the primary contractor or service provider.

While in-principle an APRA entity should have oversight of the risks in these supply chains this ignores the reality that frequently an APRA entity will have limited visibility of any risks that may exist and importantly limited leverage to influence changes in how fourth parties provide services to the primary contractor.

The AICD recommends that any guidance recognises this tension and limits expectations for what fourth party risk management practices an APRA entity can influence. For instance, reporting from the service provider on fourth party risk moray be appropriate however there will ultimately be a limit to how much visibility an APRA entity will be able to have on the supply chain.

4. Commencement and transition

This section responds to question 8 from Chapter 5.

AICD members, industry bodies and APRA entities have been consistent in providing feedback to us that the proposed commencement date of 1 January 2024 is unreasonable and does not reflect the operational and contractual changes that will be required under draft CPS 230. The Discussion Paper notes that CPS 230 will not be finalised until early 2023 with accompanying guidance at a later date. This will provide less than a year for implementation. Further, as discussed below, guidance will be key to understanding the obligations and meeting APRA's expectations and APRA entities should have the guidance in place for a sufficient period of time.

APRA entities, particularly smaller entities, will struggle to implement the obligations from the start of 2024, particularly as they relate to material service providers. CPS 230 as drafted will require wholesale contract renegotiation across all APRA industries. At the same time as entities are implementing CPS 230, they will also be implementing the FAR and a suite of other regulatory changes, for instance *Prudential Standard CPS 511 Remuneration*.

The AICD recommends that commencement is a minimum 18 months – 2 years from finalisation. For instance, if CPS 230 and the accompanying guidance are not final until the first half of next year the

obligations should commence at the earliest at the start of 2025. The AICD also strongly supports a transition period, and/or grandfathering arrangements, as detailed below.

Transition and grandfathering

The AICD recommends a transition period where APRA entities can allow existing service provider arrangements to run to the end of the contractual term before they have to meet the CPS 230 requirements. An alternative to transition would be to enable the grandfathering of existing arrangements.

A form of transition or grandfathering over a number of years would appropriately recognise the complexity and challenges in APRA entities meeting the proposed obligations. CPS 230 will require all APRA entities to enter into some form of contract renegotiation or renewal of a high number and diverse range of services. This will take time and for smaller entities in a limited bargaining position may result in the renegotiation of terms and price to their detriment.

Further, there is a real risk that in effect requiring all APRA entities to undertake tenders in the relevant markets at the same time will result in unintended consequences for the level of competition. It may incentivise service providers with a strong bargaining position to offer a standard contract or terms of conditions, including potentially price.

Transition and/or grandfathering is an area where APRA can apply a proportionality model. For example, SFIs could have a two-year transition period from commencement while non-SFIs would have three years. This would reflect the resource level of non-SFIs and their limited bargaining position relative to SFIs.

As an alternative to transition would be grandfathering where all arrangements in place at a determined date, for example 1 January 2023, could run until the end of their contractual term. Again, were APRA concerned this would be result in long open-ended arrangements it could limit renewals or contracts beyond a certain timeframe.

5. Guidance

The AICD encourages APRA to develop comprehensive guidance on the proposed obligations under CPS 230. Industry consultation will be key in ensuring the guidance reflects best practice and accounts for differences in the sizes, complexity and industry of APRA entities.

Areas we have identified that warrant guidance include:

- alignment with FAR, including confirmation that an entity may utilise the FAR prescribed responsibilities to allocate CPS 230 responsibilities;
- expectations for Board review of material service provider reporting and business continuity testing;
- detail the application and scope of the material service provider definition, including what constitutes a 'critical operation' and whether this is applied on a provider-by-provider basis or to a class of providers (i.e. all providers that provider a particular service or product);
- interaction with existing prudential standards, such as CPS 220 and *Prudential Standard CPS 234 Information Security*, and the degree to which processes and controls under those standards can be relied upon to meet the obligations under CPS 230; and

- expectations for fourth party risk management, including monitoring.

Comprehensive practical guidance will assist APRA entities meet the intent of the proposed obligations under CPS 230 and promote improvements in operational risk and business continuity practices across all APRA regulated industries.

6. Next Steps

We hope our submission will be of assistance. If you would like to discuss any aspects further, please contact [redacted]

Yours sincerely,

Louise Petschler GAICD
General Manager, Governance & Policy Leadership