Microsoft Submission in response to the proposed Prudential Standard CPS 230

Submission to the consultation process run by the Australian Prudential Regulation Authority

October 2022

1. Introduction

1.1. Microsoft welcomes the opportunity to present this submission to the Australian Prudential Regulation Authority (**APRA**) in relation to the proposed cross-industry Prudential Standard CPS 230 relating to operational risk management (the **Draft Standard**).

1.2. As a major provider of cloud services, software and other technology solutions to many APRA-regulated entities, Microsoft understands the importance of Prudential Standards in maintaining the stability and security of Australia's financial system, as well as our role in supporting operational resilience in our APRA-regulated customers.

1.3. In preparing this submission, Microsoft has performed a comprehensive review of the Draft Standard, as well as APRA's accompanying *'Discussion Paper: Strengthening operational risk management'* (**Discussion Paper**). Microsoft is broadly supportive of the Draft Standard and view it as a sensible proposal to update and streamline several interrelated, but presently distinct, Prudential Standards.

1.4. This submission identifies areas where Microsoft welcomes further clarity from APRA or where we envisage potential challenges stemming from the Draft Standard as presently drafted, along with related recommendations for your consideration. Our submission covers the following areas:

a) the treatment of material service providers with respect to non-critical services; and

b) the management of service provider arrangements, including:

i. the due diligence requirements in paragraph 52 of the Draft Standard; and

ii. the contractual requirements in paragraphs 53 and 54 of the Draft Standard.

2. Material service providers and non-critical services

2.1. Microsoft understands that a core focus of the Draft Standard is the management of operational risks as they relate to, and are impacted by, material service providers. In our view, the descriptions of 'material service provider' in the Draft Standard appropriately balance clarity and flexibility:

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

b) *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.*

c) *Material service providers also include providers that manage information assets classified as critical or sensitive under CPS 234.*[1]

2.2. A matter that remains less clear is whether service providers that are deemed to be a material service provider of an APRA-regulated entity retain such a classification with respect to all services they provide to the entity, or only those that are material.

2.3. For example, a service provider may provide a service that manages critical or sensitive information assets under CPS 234 for an APRA-regulated entity (**Service A**), but also separately provide a service that is used to undertake a non-critical operation with low or no exposure to operational risk (**Service B**). The service provider will be deemed a material service provider on account of Service A, and the APRA-regulated entity will have several relevant obligations to consider under the Draft Standard on this basis. However, it is unclear whether the same service provider will also be treated as material with respect to a separate engagement for Service B.

2.4. Given the not-insubstantial requirements placed on APRA-regulated entities by the Draft Standard with respect to material service providers, service providers should only be treated as material service providers with respect to those services that attracted the classification, and not to other, non-critical services that may be separately provided.

2.5. Microsoft recommends that this be clarified in guidance developed for the Draft Standard.

3. Management of service provider arrangements (Due diligence)

3.1. Paragraph 52 of the Draft Standard would require APRA-regulated entities to take specified steps before entering into, renewing or materially modifying an arrangement with a material service provider. The term 'arrangement' is undefined but would presumably adopt a wider meaning than just formal 'agreements', which is referenced elsewhere in the Draft Standard.

3.2. Such specified steps include that APRA-regulated entities must:

a) *undertake appropriate due diligence, including an appropriate tender and selection process and an assessment of the ability of the service provider to provide the service on an ongoing basis;*

b) *assess the financial and non-financial risks from reliance on a particular service provider, including risks associated with geographic location or concentration of the service provider(s) or parties the service provider relies upon in providing the service; and*

c) *take reasonable steps to assess whether the provider is systemically important in Australia.*[2]

Entering into, renewing or materially modifying an arrangement

3.3. While some of the specified steps may be reasonable in the context of **entering into** initial master agreements with material service providers, Microsoft suggests that the existing drafting does not adequately consider how the requirement would function in the context of framework agreements and other forms of contracting structures.

[1] Draft Standard, paragraphs 48 – 50.
[2] Draft Standard, Paragraph 52.

For example, an agreement between an APRA-regulated entity (as a customer) and a material service provider may be governed by a master services agreement where the parties have agreed that numerous different services may be procured over the term in response to customer need. These separate procurements may take the form of order forms, statements of work or service contracts subordinate to, but governed by, the master services agreement. Given that the general term 'arrangement' is used in this requirement, these subordinate documents are likely covered.

In such scenarios, Microsoft suggests that carrying out each of the steps specified in paragraph 52 of the Draft Standard would, more often than not, be unpracticable for the parties and, we submit, not necessarily add to the resilience of the regulated entity's risk framework in such circumstances.

3.4. The ability to efficiently **renew** agreements between service providers and their customers, on terms agreed to between the parties, is key for the continuity of service expected by customers and their stakeholders. This is especially the case where shorter initial and renewal terms are agreed between the parties, which are often negotiated in this way to enable greater flexibility for customers whose business needs and external drivers are subject to change.

3.5. Similarly, parties must be able to **modify** an agreement in a straightforward and prompt manner to ensure service delivery continues in line with potentially changing expectations. While the Draft Standard conditions this to only apply in the case of 'material' modifications, it is unclear where the threshold for materiality lies, warranting the steps specified under paragraph 52.

Issues with specified steps

3.6. **Subparagraph (a)** outlines certain prescriptive due diligence requirements that must be undertaken by APRA-regulated entities. While due diligence is appropriate when procuring material services, what due diligence should involve will vary depending on the nature of any given procurement.

The Draft Standard's specification of minimum due diligence requirements risks oversimplifying the diverse nature of contracting by APRA-regulated entities and assumes that activities such as tender and selection processes necessarily enhance risk outcomes for APRA-regulated entities. Depending on the nature of the procurement, mandated tenders may end up stalling the remediation of issues that themselves create operational risk.

The requirement to undertake an appropriate tender and selection process is also practicably incompatible with the renewal or variation of existing agreements, especially in circumstances where the circumstances of the service provider and/or regulated entity, or the nature of the arrangement, has not materially changed.

3.7. **Subparagraph (b)** requires APRA-regulated entities to assess risks arising from reliance on a particular service provider, including concentration risks associated with that provider or its associated supply chains. This requirement may be particularly burdensome on APRA-regulated entities depending on the frequency and volume of renewals and modifications.

Should this subparagraph be maintained, we suggest that the nature of the concentration risk be clarified so that APRA-regulated entities understand whether they are being asked to assess macro or micro concentration risk (or both).

Microsoft has published a **White Paper** exploring the regulation of concentration risk and the important distinctions between micro and macro risks. Micro concentration risks involve overreliance on a particular provider within an entity's own ecosystem, and the vulnerability created by a 'single point of failure'. Macro concentration risks contemplate similar concerns, but on a collective level with respect to a given market or infrastructural sector.

APRA-regulated entities are best-placed to consider their own *micro* concentration risks. While doing this can, in turn, contribute to better collective outcomes, we caution against tasking each APRA-regulated entity with assessing macro concentration in each procurement decision it makes.

3.8. The specified step in **subparagraph (c)** requires APRA-regulated entities to take reasonable steps to assess whether the provider is systemically important to Australia. In addition to our comments above regarding the appropriateness of this obligation in several of the contractual settings currently contemplated by the Draft Standard, we also more generally query whether the requirements in subparagraph (c) are reasonably practicable.

It is unclear how APRA-regulated entities should be assessing service providers for systemic national importance, and how associated outcomes are to be factored into arrangements with material service providers.

3.9. We also query the utility of various APRA-regulated entities subjectively assessing factors related to macro concentration risk in the context of assessing a provider's "systematic importance" at a national level. Centralised assessments from APRA regarding macro concentration risks and systemic national importance would provide greater value and certainty.

3.10. Microsoft appreciates the policy intention behind the proposal and the need for APRA-regulated entities to approach supplier due diligence as an ongoing concern. However, in many ways we view this policy intention as being appropriately captured by paragraph 55 of the Draft Standard.

3.11. We suggest that APRA's aims could be achieved in a more proportionate way by amending the specified steps in paragraph 52 so that:

- the end of the first sentence is adjusted to read "*, an APRA-regulated entity must have appropriate regard to:";*
- subparagraph (a) only requires entities to "*~~undertake~~ any appropriate due diligence considerations, which may include ~~including~~ an appropriate tender and selection process and assessment of the ability of the service provider to provide the service on an ongoing basis*";
- subparagraph (b) is supported by guidance that clarifies concentration risk should be considered in the micro sense; and
- subparagraph (c) is removed entirely, particularly as supplier viability and concentration risks at a national level are arguably more appropriate for a regulator to consider.

3.12. Microsoft also recommends providing clarity, such as in associated guidance, about how APRA-related entities should handle paragraph 52 requirements in the context of framework contracting approaches.

4. Management of service provider arrangements (Contractual requirements)

4.1. Paragraphs 53 and 54 of the Draft Standard would require APRA-regulated entities to maintain formal, legally-binding agreements with material service providers that, at a minimum, include certain prescribed provisions. For the most part, Microsoft view these prescribed provisions as sensible and in-keeping with market practice.

Force majeure

4.2. Subparagraph (f) outlines that formal agreements must include a **force majeure** provision indicating those parts of the contract that would continue in the case of a force majeure event. While the intention of this subparagraph appears focused on clarifying which provisions continue in the event of a force majeure event, it also has the implication of mandating that a force majeure provision is included in the first place.

4.3. While reasonably common risk-mitigation mechanisms in contracts, force majeure clauses are not universally included in agreements between APRA-regulated entities and their service providers. Generally speaking, force majeure clauses have the potential to provide balanced benefit where both parties have substantive performance obligations under the contract. However, in a customer relationship, where the service provider bears the bulk of the obligations, force majeure clauses will generally only benefit the service provider.

In the case of Microsoft, and we would imagine in other cloud services contexts, force majeure provisions are not included in our standard terms. Our customers generally do not raise this as an issue, particularly given that a force majeure clause in this context primarily benefit the supplier and are of little utility to the customer.

If this requirement is included in the finalised CPS 230, Microsoft would be required to repaper many agreements in a manner that does not provide a practical benefit for APRA-regulated entities, nor necessarily improve their operational risk profile.

4.4. Given the breadth of material service providers and arrangements potentially covered by the Draft Standard, we understand that force majeure provisions may be necessary in other contexts. We also understand that where force majeure provisions are included, it should be made clear that they only apply to services and obligations actually impacted by a force majeure event, and not to the service provision as a whole (where relevant).

4.5. We recommend that subparagraph (f) be amended to read, for example: "where a force majeure provision is included, specify that it has effect only with respect to those obligations impacted by a relevant force majeure event, or outline which obligations would continue in the case of a force majeure event".

4.6. Alternatively, the Draft Standard could require APRA-regulated entities to consider whether any force majeure provision places undue and unacceptable risk on operational security vis-à-vis the material service provider.

Termination

4.7. Subparagraph (g) outlines that formal agreements must include **termination** provisions that include the right to terminate both the arrangement in its entirety or parts of the arrangement. Further, with respect to a registerable superannuation entity (**RSE**) licensees, termination provisions must include the ability for the RSE licensee to terminate the arrangement where to continue the arrangement would be inconsistent with the RSE licensee's duty to act in the best financial interests of beneficiaries.

4.8. Microsoft is of the opinion that it is commercially reasonable (and common) for service providers to limit the circumstances in which customers may terminate an agreement, and to resist the inclusion of broad termination for convenience clauses.

4.9. As such, while Microsoft sees the more general termination requirement at the beginning of subparagraph (g) as generally reasonable, we suggest that narrowing it to termination for breach (or similar concepts) would be more balanced for APRA-regulated entities and their material service providers.

4.10. Beyond this, the drafting of termination requirements under the Draft Standard or any related guidance should avoid layering-on additional expectations regarding termination provisions that unduly limit the ability of service providers to condition termination provisions. For example, it is commonplace for termination for cause provisions to be couched within reasonable notice and process requirements.

4.11. With regard to the more specific requirement for customers who are **RSE licensees**, we query whether it provides more subjective discretion to such customers than would be reasonably necessary in order to uphold the underlying statutory requirement. In our view, the requirement has the potential to function as unconditional termination for convenience clause in favour of these customers.

4.12. Section 52(2)(c) of the *Superannuation Industry (Supervision) Act 1993* (Cth) requires trustees to covenant that they will perform their duties and exercise their powers in the best financial interests of beneficiaries. Trustees are expected to execute this duty at all relevant times, including during all stages of material service procurement and negotiation of an agreement. During these stages, both the known and foreseeable financial interests of beneficiaries can be considered.

We appreciate that once an agreement is agreed and on foot, limited occasions may arise that cause trustees to question whether the agreement remains in the best financial interests of beneficiaries. However, fundamentally, this is a broad and highly discretionary assessment. For instance, it is foreseeable that where services being provided are no longer suitable for the RSE Licensee for any reason, and no other termination right is available, they may instead rely on the proposed right in paragraph 53(g) of the Draft Standard to assert that continuation would be against the best financial interests of beneficiaries. While contestable, the service provider is ultimately in a poor position to question the veracity of such a claim.

Any potential consequences in terms of service fees, including complying with minimum commitments, would vary on an agreement-by-agreement, provider-by-provider basis. However, given that such service fees were freely agreed between the parties, with trustees for RSE licensee customers assumedly complying with their statutory duties at the time, the payment of such service fees in line with the agreement should not be displaced on a unilateral, discretionary basis by the customer.

We also note other requirements in the Draft Standard, such as at paragraph 14, require an APRA-regulated entity to have regard to whether reliance on a service provider will prevent them from meeting its prudential obligations.

4.13. Microsoft offers customers who are APRA-regulated entities several termination rights of a permissive nature, including a right to terminate at the express direction of a regulator such as APRA, or where the customer can reasonably demonstrate that there are weaknesses regarding the management and security of customer data or information. We foresee the proposed requirement in paragraph 53(g) of the Draft Standard as it relates to RSE licensees to create unnecessary uncertainty in impacted agreements and recommend the requirement be reworked.

APRA's audit rights under service provider agreements

4.14. Paragraph 54 of the Draft Standard would require formal agreements between APRA-regulated entities and material service providers to include provisions that:

a) *allow APRA access to documentation, data and any other information related to the provision of the service;*

b) *allow APRA right to conduct an on-site visit to the service provider; and*

c) *ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator.*[3]

4.15. Microsoft's existing contractual arrangements with APRA-regulated entities satisfy the requirements laid out in paragraph 54, which we appreciate are necessary and proportionate requirements for APRA.

4.16. We understand that the Draft Standard avoids being overly prescriptive as to the exact drafting required to be included in formal agreements with service providers. In practice, this allows service providers and their APRA-regulated customers to agree upon drafting suitable in each context.

[3] Draft Standard, paragraph 54.

4.17. However, it is possible that APRA-regulated entities may interpret this approach as being incompatible with having any form of conditionality attached to required provisions. For example, a contractual ability for APRA to conduct on-site visits to a service provider's site will almost always be subject to reasonable requirements and exceptions, namely relating to safety and security considerations.

4.18. Given the extent to which the Draft Standard mandates certain minimum requirements for agreements with service providers, we recommend that APRA clarify in associated guidance that APRA-regulated entities can implement the required provisions as appropriate with service providers (including the audit requirements in paragraph 54), so long as the base requirement in the Draft Standard is being satisfied.

5. Conclusion

5.1. Microsoft thanks APRA for the opportunity to review and provide feedback on the Draft Standard. Overall, we see the Draft Standard as being a valuable consolidation and uplift for how operational risk is governed under Prudential Standards.

Microsoft hopes that the challenges and related recommendations identified in our submission are of assistance to APRA in the finalisation of CPS 230 and associated guidance. Please do not hesitate to get in touch with our team should you have any questions.