Amazon Web Services Australia Pty Ltd ▪ Level 37, 2 Park Street ▪ Sydney, Australia 2000

21 October 2022

Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001

Via email: [redacted]

Consultation on draft Prudential Standard CPS 230 Operational Risk Management (CPS 230)

Amazon Web Services (AWS) welcomes the opportunity to comment on APRA's draft Prudential Standard CPS230 Operational Risk Management (CPS 230).

AWS is supportive of APRA's principles-based approach to setting prudential standards, which we believe works well for APRA-regulated entities and their service providers. We also endorse APRA's approach in streamlining the prudential standards with CPS 230 replacing and superseding five existing standards, and believe the draft standard strikes a good and workable balance, subject to our suggested changes below.

However, clear and detailed supporting guidance is crucial for regulated entities to interpret and apply the principles in CPS 230, particularly as it is replacing existing standards. AWS believes that publishing detailed draft guidance concurrently with the draft standard enables a more comprehensive consultation and feedback process, and ensures APRA-regulated entities seeking to prepare ahead of the implementation of the standard are making more informed decisions. We have suggested some areas where we believe such guidance is crucial, and look forward to contributing further to the consultation on draft guidance for CPS 230 scheduled for early 2023.

Key issues

Threshold requirements for contracting with service providers (paragraphs 52 and 58)

AWS is concerned that APRA-regulated entities may interpret certain provisions in CPS 230 as indicating that using hyper-scale cloud providers rather than smaller-scale solutions, using international service providers rather than domestic service providers, and using a single cloud service provider rather than a multi-cloud solution, or storing data offshore is inherently risky, or riskier, than alternatives. This would limit APRA-regulated entities' ability to use the most appropriate IT infrastructure and services for their needs, and we understand this is not APRA's intention. The provisions of concern are: the requirement to assess the geographic location or concentration risks of service providers (paragraph 52(b)); the requirement to assess whether a provider is systemically important in Australia (paragraph 52(c)); and more onerous notification requirements for offshoring arrangements (paragraph 58(b)).

APRA-regulated entities might interpret both the requirement to assess risks associated with the geographic location or concentration of service providers, and the more onerous notification requirements for offshoring arrangements, as encouraging them to avoid or be wary of storing data

offshore or of using hyper-scale cloud providers, international service providers, or only a single cloud provider. This would be counterproductive for several reasons:

- First, hyper-scale cloud providers typically have substantially more secure and resilient IT infrastructure than alternatives such as smaller-scale infrastructure owned and managed by an APRA-regulated entity itself.
- Second, cloud providers proactively mitigate potential geographic and concentration risks by offering services via physically separate locations and logically segregated IT systems. For example, AWS's Cloud infrastructure is built around AWS Regions, which are separate physical locations with multiple Availability Zones. AWS Availability Zones consist of one or more discrete data centres, each with redundant power, networking, and connectivity, housed in separate facilities that offer customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data centre. AWS currently has 27 Regions around the world, comprising a total of 87 availability zones. The AWS Sydney region, with 3 Availability Zones, has been running since 2012, and the Melbourne region – also with 3 Availability Zones – will launch shortly.
- Third, storing data offshore often facilitates greater redundancy in terms of increased geographic spread and the reduced risks that come with that.
- Fourth, our customers' experiences to date have found maintaining an IT workload across multiple cloud providers is often not worth the intended risk/reward outcome. Spanning workloads across multiple cloud providers is technically very difficult, operationally more complex, and may negatively impact security and operational resilience. This is primarily because multi-cloud forces customers to attempt to standardise on the lowest common denominator services between cloud providers, which may vary significantly in maturity and capability. For example, some AWS customers have found that the additional expense and effort in people, process and tools (collectively known as an 'operating model') is anywhere between 1.25 and 2+ times the cost of a single provider strategy with no tangible improvement in operational resilience.
- Finally, even if multiple APRA-regulated entities exclusively use the same cloud provider, this would not create a problematic concentration risk so long as that service provider's infrastructure and services are offered via physically separate locations and are designed to be highly secure and resilient. For example, AWS mitigates this as every customer's workload deployment on AWS is different, which means that no two customers are exposed to the same set of technology, or exactly the same geography.

Similarly, APRA-regulated entities might interpret the requirement to determine whether a material service provider is "systemically important in Australia" as discouraging them from using hyper-scale cloud providers. This would be counterproductive for the same reasons as above. In our view, well-architected cloud frameworks like AWS's are net reducers of systemic risk. Cloud technology can help APRA-regulated entities achieve better operational resilience, improve security, better identify and address threats, and increase stability of the overall financial system.

Accordingly, AWS encourages APRA to revise CPS 230 and publish supporting guidance to ensure that APRA-regulated entities focus on the security and resilience of services offered by different service providers, more so than their concentration, systemic importance, or geographic location. This will empower APRA-regulated entities to use the most appropriate infrastructure and services for their needs, and will reduce systemic risk.

Mandated changes to service provider arrangements (paragraph 56)

Paragraph 56 of CPS 230 introduces uncertainty into all agreements between APRA-regulated entities and material service providers, as they could be subject to changes mandated by APRA at any time. Introducing a unilateral right for an APRA-regulated entity to amend an agreement may lead to the disruption or unavailability of services, and increased operational risk, because some material service providers may be unable to accept or operationalise certain terms for some or all services.

As such, AWS recommends deleting paragraph 56 of CPS 230. Paragraphs 53 and 54 of CPS 230 already require APRA-regulated entities to have appropriate terms and protections in their contracts with material service providers. If APRA identifies additional requirements for agreements between an APRA-regulated entity and a material service provider, these should be addressed at an industry level rather than mandated to a specific regulated entity or its service provider, and should be included in revisions to paragraphs 53 and 54 of CPS 230.

Terms of service provider agreements (paragraphs 53-54)

AWS recommends explicitly stating in CPS 230 that paragraphs 53 and 54 contain the only provisions that APRA-regulated entities must include in their agreements with material service providers. This will address any confusion resulting from CPS 230's consolidation of multiple separate prudential standards relating to agreements with material service providers.

In addition, AWS recommends specific sections in paragraphs 53 and 54 be redrafted or clarified in order to minimise uncertainty and inconsistency. These recommendations, along with other recommendations on specific paragraphs of CPS 230, are outlined below.

Additional comments on specific paragraphs of CPS 230

Threshold requirements for contracting with service providers (paragraphs 52 and 58)

> *52. Before entering into, renewing or materially modifying an arrangement with a material service provider, an APRA-regulated entity must:*

APRA-regulated entities frequently update existing agreements with material service providers (e.g., to adjust pricing terms, extend the duration of a contract, or procure supplementary services). It would be unnecessarily onerous for APRA-regulated entities to carry out the steps, processes and assessments in paragraph 52 each time an agreement is updated. AWS recommends that APRA amend paragraph 52 to apply only when an APRA-regulated entity enters into a new arrangement with a material service provider. Alternatively, AWS recommends that APRA replace the lead-in to paragraph 52 with the relevant text in Prudential Standard CPS 231 Outsourcing (CPS 231), which requires an APRA-regulated entity to perform relevant assessments only when "assessing the options for outsourcing a material business activity."

> *52 (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;*

APRA-regulated entities might interpret "an appropriate tender ***and*** selection process" to require a tender process in every instance, which may create unnecessary operational burden for APRA-regulated entities, limit their ability to improve their existing contractual terms due to the resource-intensive nature of a tender, and in many cases have no positive impact on security or resilience. In CPS 231, APRA-regulated entities are required to "[undertake] a tender ***or*** other selection process for selecting the service," providing them greater flexibility to employ a selection process appropriate to the circumstances. AWS recommends paragraph 52 (a) be amended in line with CPS 231, as follows:

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

> *52 (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;*

As outlined on pages 1 and 2 above, APRA-regulated entities might interpret the requirement to assess risks associated with the geographic location or concentration of service providers as encouraging them to avoid or be wary of storing data offshore, or of using hyper-scale cloud providers, international service providers, or only a single cloud provider. This would be counterproductive for the reasons detailed above, and may discourage APRA-regulated entities from choosing the most appropriate infrastructure and services for their needs and hence unintentionally increase systemic risk.

Accordingly, AWS recommends deleting the words "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 supplementing paragraph 52(b) with guidance recommending that APRA-regulated entities focus on assessing the security and resilience of services offered by different service providers.

> *52 (c) take reasonable steps to assess whether the provider is systemically important in Australia.*

Similarly, paragraph 52(c) creates uncertainty about what systemic importance means, how an APRA-regulated entity should assess whether a provider is systemically important, whether an individual APRA-regulated entity is best-placed to make that assessment, and how that assessment should influence an entity's use of different service providers. For example, an entity might reasonably conclude that using a systemically important provider is (a) preferable because the provider is likely subjected to a higher degree of testing and scrutiny and expected to meet the highest bar of security and resilience (e.g. via the federal government's Security of Critical Infrastructure framework), or (b) riskier for some reason relating to its systemic importance. Without clear guidance, this paragraph risks influencing APRA-regulated entities' choices in unintended ways.

Accordingly, AWS recommends deleting this paragraph. Alternatively, AWS recommends that APRA provides guidance clarifying that entities which are "systemically important in Australia" will likely have robust (and potentially industry leading) security and resilience standards due to being subject to a higher and continuous degree of scrutiny and testing.

> *58. An APRA-regulated entity must notify APRA:*
>
> *(a) as soon as possible and not more than 20 business days after entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation; and*
>
> *(b) prior to entering into any offshoring agreement with a material service provider, or when there is a significant change proposed to the agreement, including in circumstances where data or personnel relevant to the service being provided will be located offshore.*

As outlined above, the more onerous requirements for offshoring agreements in paragraph 58 imply that offshoring is inherently riskier and may encourage APRA-regulated entities to use domestic providers instead of international providers, even when doing so may lead to less secure and resilient outcomes. For these reasons, AWS recommends deleting paragraph 58(b) so that there is no distinction between notification requirements applicable to domestic vs. offshore material service agreements. If APRA wants to create differing notification requirements to distinguish different levels of risk, this should be based on the criticality of a service, rather than the location from which a service is delivered.

We also recommend that the notification requirements in paragraph 58 only apply when an APRA-regulated entity enters into a new material service agreement, but not when changes are made to an existing agreement. Alternatively, we recommend that APRA clarify that a "material" (or "significant") change to an existing agreement would only occur when there is a fundamental change to the scope or purpose of the agreement (for example, converting a software licensing agreement into a cloud services agreement), but not when there are changes to the commercial, operational, liability and other terms of the agreement. This will avoid uncertainty and ensure that the contracting parties can quickly and efficiently update agreements when needed.

Further, AWS recommends that APRA clarify that paragraph 58 of CPS 230 will supersede the notification and consultation directions in APRA's 2018 Cloud Information Paper, or if not, clarify why cloud is subject to a higher level of regulatory scrutiny than other similarly critical service provision arrangements.

Terms of service provider agreements (paragraphs 53-54)

> *53. For all material service provider arrangements, an APRA-regulated entity must maintain a formal legally binding agreement. The formal agreement must, at a minimum:*
>
> *(a) specify the services covered by the agreement and associated service levels;*

Material service providers could offer many services to their customers, not all of which will have service levels or be used by any individual customer. APRA-regulated entities might misinterpret paragraph 53(a) as requiring every service to be explicitly listed in their agreements, and service levels to be included for every service. To avoid this confusion, AWS recommends that APRA replace paragraph 53(a) with the existing text in paragraphs 29(a) and 29(e) of CPS 231, which are already well-understood and applied by APRA-regulated entities and their material service providers:

> "(a) the scope of the arrangement and services to be supplied; […]
>
> (e) service levels and performance requirements;"

53 (b) set out the rights, responsibilities and expectations of each party to the agreement, including in relation to the ownership of assets, ownership and control of data;

Ownership of assets will often not be relevant to the services provided by a material service provider, and in many cases operational ***control*** of assets is more relevant than ownership. Accordingly, AWS recommends amending paragraph 53 (b) as follows:

> "set out the rights, responsibilities and expectations of each party to the agreement, including, **if relevant**, in relation to the ownership **or control** of assets, **and** ownership and control of data."

53 (c) include provisions to ensure the ability of the entity to meet its legal and compliance obligations;

It is unclear what types of provisions are envisaged by this paragraph, and which legal and compliance obligations are intended to be addressed. To address this lack of clarity and ensure that each contracting party is only responsible for what it can reasonably control, AWS recommends redrafting this paragraph as follows, or supplementing it with guidance to clarify that the material service provider and the APRA-regulated entity must each meet its own legal and compliance obligations, but is not responsible for ensuring that the other party meets all of its legal and compliance obligations.

> "53 (c) include provisions to ensure **that each party** ~~the ability of the entity to meet its legal and compliance obligations~~ **agrees to comply with laws and regulations that are applicable to that party's obligations under the agreement**."

53 (d) require notification by the service provider of its use of other material service providers, through sub-contracting or other arrangements;

AWS suggests APRA clarify that notification is only required after a material service provider engages another material service provider. Prior notification is unlikely to be feasible and could cause operational disruption if there is a need to quickly engage another material service provider to address unforeseen circumstances.

53 (g) termination provisions including, but not limited to, the right to terminate both the arrangement in its entirety or parts of the arrangement. […]

We recommend APRA clarify in the guidance that the right to terminate "parts of the arrangement" in paragraph 53(g) means that an APRA-regulated entity should have the ability to terminate or cease using a particular service in agreed circumstances, but not a unilateral right to terminate discrete terms or parts of an agreement that was negotiated and agreed as a whole.

> *54. The formal agreement must also include provisions that:*
>
> *(a) allow APRA access to documentation, data and any other information related to the provision of the service;*
>
> *(b) allow APRA the 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.*

AWS supports the intent of paragraph 54 and looks forward to continuing to collaborate with APRA. However, there may be a risk that APRA-regulated entities misconstrue the intent of Section 54 and ask material service providers to include terms in the agreement that undermine the security and resilience of the material service providers' services and the security and confidentiality of its other customers (who may be other APRA-regulated entities). As such, we recommend that APRA provide guidance that clarifies that these provisions can contain proportional guardrails aimed at minimising disruption to the operations of the material service provider and the security and confidentiality of its customers.

Operational risk management and risk incidents (paragraphs 24 and 36)

> *24. An APRA-regulated entity must maintain appropriate and sound information and information technology (IT) infrastructure to meet its current and projected business requirements and to support its critical operations and risk management. […]*

APRA-regulated entities, especially less sophisticated entities, might interpret this paragraph as requiring them to maintain their own physical IT infrastructure. AWS recommends amending paragraph 24 to clarify that APRA-regulated entities may source IT from service providers. Our suggested drafting is:

> "An APRA-regulated entity must maintain **or source from service providers** appropriate and sound information and information technology (IT) infrastructure **or services** to meet **the APRA-regulated entity's** current and projected business requirements and to support its critical operations and risk management."

> *32. An APRA-regulated entity must notify APRA as soon as possible, and not later than 72 hours, after becoming aware of an operational risk incident that it determines to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations.*

Paragraph 32 is similar to paragraph 35 of Prudential Standard CPS 234 Information Security (CPS 234), except that CPS 234 requires notification of an "information security incident" whereas this paragraph refers to an "operational risk incident." If this distinction is deliberate, we recommend that APRA include a definition of "operational risk incident" in CPS 230 or associated guidance to avoid confusion. If no difference is intended, we recommend deleting this paragraph and only retaining paragraph 35 in CPS 234, to avoid confusion and inconsistency in incident reporting.

In addition, in our experience many APRA-regulated entities misinterpreted paragraph 35 in CPS 234 as imposing notification obligations on service providers directly, which APRA has confirmed is not the

intention. If this paragraph remains in CPS 230, we recommend that APRA clarify in a footnote or in separate guidance that paragraph 32 of CPS 230 does not apply to material service providers.

Register of material service providers (paragraph 48)

> *48. An APRA-regulated entity must identify and maintain a register of its material service providers and manage the material risks associated with using these providers. Material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk.*

To help APRA-regulated entities efficiently comply with this obligation, AWS recommends that APRA clarify the specific information required to be maintained in the register.

APRA's key questions

AWS provides the following responses to some of the questions posed in the consultation paper.

Overall design

Q: Is a single cross-industry standard for operational risk management supported?

Yes, AWS supports this approach.

Q: Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?

APRA has unique and critically-important insights regarding areas of observed weaknesses and good practice with respect to service provider management. We encourage APRA to share as many of these insights as possible in the forthcoming guidance.

In our comments above on specific paragraphs, we have referenced several instances where we believe additional guidance will assist APRA-regulated entities to interpret and apply the provision.

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

CPS 230 sets a high standard which should be applicable to both SFIs and non-SFIs. There is a risk that setting different requirements (and associated guidance) will create inconsistency and confusion for both APRA-regulated entities and their material service providers.

Q: What are the estimated compliance costs and impacts to meet the new and enhanced requirements?

Minimising the cost of regulatory compliance has been a long-term mission for financial services regulators around the world. AWS welcomes APRA's focus on making compliance easier and more cost efficient for the regulated entities. Regulated entities store, process and report on data across a number of systems. The lack of a common financial services taxonomy contributes to the increased cost of regulatory compliance. Any guidance around adoption of a common taxonomy on regulatory reporting and ease of compliance would be welcome.

Clear guidance on CPS 230 will also avoid unnecessary confusion and misinterpretation of the standards, which will help reduce compliance costs.

Specific requirements

Q: Are the notification requirements and the time periods reasonable?

In our comments above, we have recommended there should be no difference in notification periods for domestic and offshoring arrangements in paragraph 58.

Closing

Thank you for the opportunity to contribute to this important consultation. AWS would welcome the opportunity to expand on our submission in a discussion with APRA, or to provide any further information.

Yours sincerely,

Roger Somerville
Head of Public Policy, Australia & New Zealand
Amazon Web Services
Email: [redacted]