asia cloud computing association

The Asia Cloud Computing Association (ACCA) is the apex industry association for Asia Pacific stakeholders in the cloud computing ecosystem. We represent a vendor-neutral voice of the private sector to government and other stakeholders, with the mission to accelerate the adoption of cloud computing through Asia Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for cloud computing products and services.

aws

DIGITAL REALTY

EQUINIX

Google Cloud

HSBC

Microsoft

ORACLE

salesforce

Renée Roberts
Executive Director, Policy & Advice
Australian Prudential Regulation Authority
Level 12, 1 Martin Place
Sydney NSW 2000

21 October 2022

Comments submitted via email [redacted].

Dear [redacted],

Re: Asia Cloud Computing Association (ACCA) Comments on Australian Prudential Regulation Authority (ARPA)'s Consultation on New Prudential Standard CPS 230 Operational Risk Management

I hope this letter finds you well. On behalf of the Asia Cloud Computing Association (ACCA), we would like to thank the Australian Prudential Regulation Authority (ARPA) for the opportunity to comment on the New Prudential Standard CPS 230 on Operational Risk Management ("CPS 230").

We welcome APRA's consultative approach on the new cross-industry prudential standard CPS 230 Operational Risk Management, which provides a set of minimum standards for managing operational risks in the banking, insurance, and other industries in the financial sector. This aligns with the APRA's priorities for 2022 to modernise Australia's prudential architecture and support the growth of digital innovation in financial institutions. As the new standard will replace the existing five standards related to outsourcing (CPS 231), business continuity (CPS 232), as well as others, many entities including service providers will be affected by the new requirements. We would like to take this opportunity to share our feedback and comments included below.

Overall, we encourage APRA to provide greater clarity in the Draft Prudential Standard CPS 230. We also hope to have a dialogue with APRA in November to provide further clarification of the above issues.

As the apex industry association, the ACCA's mission is to accelerate the adoption of cloud computing through Asia-Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for cloud computing products and services. Thank you for your consideration.

Best regards,
Sim Xin Yi
Secretariat
Asia Cloud Computing Association
[redacted]

Feedback on APRA's New Prudential Standard CPS 230 on Operational Risk Management

1. Service Provider Agreements

Article 52(b) requires APRA-regulated entities to assess the financial and non-financial risks from dependence on material service providers, including those (subcontracted) service providers that the service provider depends on for the provision of that service.

Similar to how the requirements focus on material service providers servicing the regulated entities, the requirements for subcontracted service providers should also include a materiality threshold.

Recommended revisions

Article 52(b) "Before entering into, renewing or materially modifying an arrangement with a material service provider, an APRA-regulated entity must:... (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 materially relies upon in providing the service; and…"

Article 52(c) requires APRA-regulated entities to assess whether the service provider is "systematically important in Australia" before entering into a third-party arrangement.

We appreciate the good intent of this policy to mitigate the risks posed by third parties to the financial system. However, it is impractical for a single APRA-regulated entity to assess the systemic importance of the provider in a meaningful way on its own. Regulated entities are not best placed to address systemic risks as they do not have visibility over what service providers that other entities use. Instead, this systemic risk assessment would be best done by the relevant authorities in collaboration with the financial services industry, given that the authorities have oversight of the industry and the broader ecosystem. We therefore recommend removing this requirement.

Alternatively, we encourage APRA to provide guidance and clarity on the definition of "systemically important" and examples of "reasonable steps" that APRA-regulated entities are expected to take. In implementing this requirement, we also suggest that APRA provide APRA-regulated entities with relevant information to facilitate this assessment.

2. Critical Operations and Tolerance Levels

Article 38 requires an APRA-regulated entity to review and change its tolerance levels for a critical operation. APRA may also set tolerance levels for an APRA-regulated entity.

There is, however, no clarity on how APRA will exercise its discretion to change or set tolerance levels. There is also a lack of consultation with APRA-regulated entity before the changes.

We recommend that APRA set tolerance levels that are commensurate with the criticality of the operation, and that APRA consult with APRA-regulated entities before making any changes to ensure that there is clarity among all parties on the impact of the proposed changes.

Recommended revisions

Article 38

"APRA may require an APRA-regulated entity to review and change its tolerance levels for a critical operation so that they are commensurate with the criticality of the operation. APRA may set tolerance levels commensurate with the criticality of the operation for an APRA-regulated entity, or a class of APRA-regulated entities, where it identifies a heightened risk or material weakness. Before exercising its powers in this section, APRA will consult the impacted APRA-regulated entities on the impact of the proposed tolerance levels."

3. Cyber Risk Incident Reporting

Article 32 requires service providers to report cyber incidents to their customer APRA-regulated entity no later than 72 hours, after determining that the operational risk incident is likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations.

We applaud the APRA for matching the cyber-incident reporting timeline of 72 hours with international best practices such as the EU's General Data Protection Regulation. This will allow sufficient time for APRA-regulated entities to assess the security problem and rule out false positives while ensuring that incidents are reported without delay.

That said, we recommend the APRA to include a clear definition of operational risk incidents, especially if certain operational risk incidents are required to be reported. The absence of such a definition could lead to varying interpretations by APRA-regulated entities.

4. Material Service Providers

Article 47(d) currently uses the term “fourth parties” in a very broad manner. To align it with similar provisions in the draft, such as Article 53(d) on subcontracting, this provision should focus only on material fourth parties.

Recommended revisions

Article 47(d):

“The policy must include: …

(d) the entity's approach to managing the risks associated with any material fourth parties that material service providers rely on.”

Article 49 provides a broad scope of the definition of “material service providers”. Beyond third parties and related parties deemed material, material service providers include core technology services and others that manage information assets classified as critical or sensitive under CPS 234. APRA may also classify a service provider, or type of service provider, as material.

While we acknowledge the imperative of addressing third-party risks, the definition of “core technology service” is broadly worded. A technology service provider may be providing a range of services to an APRA regulated entity but only a sub-set of its services might be considered “core”. Hence, this broad interpretation could lead to a disproportionate impact on technology service providers.

We encourage APRA to better define the scope of requirements and replace the term “core technology services” with a definition specifically limiting to critical services deemed material for enhanced clarity.

Recommended revisions

Article 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~~ technology services for critical functions…”

Similarly, with respect to Article 51, we recommend that greater clarity be provided on how APRA intends to exercise its discretion in requiring regulated entities to submit their register of material service providers.

Prior consultation should be sought with the regulated entities before classifying a service provider as material.

Recommended revisions

Article 51

"An APRA-regulated entity must submit its register of material service providers to APRA on an annual basis. APRA may require an APRA-regulated entity, or a class of APRA-regulated entities, to classify a service provider, or type of service provider, as material based on the definition in Paragraph 48 and after consultation with the APRA-regulated entity."

5. Flexibility in Notification of Business Continuity Plan.

APRA-regulated entities are required to notify APRA within 24 hours if it has activated its Business Continuity Plan (BCP). The notification covers a range of information including the nature of the disruption, the likely impact on the entity's business operations and the timeframe for returning to normal operations.

While we recognize the importance of the BCP, the timeframe of 24 hours for the notification of BCP is too short. Given the nature of business continuity events, not all of the required information may be available within the 24-hour period. It may be challenging for some APRA-regulated entities to accurately predict the full impact on their business operations or the timeframe for returning to normal operations within 24 hours. In the worst-case scenario, this short timeframe could lead to inaccuracies in the reporting.

We recommend providing some flexibility in the information required.

Recommended revisions

Article 41:

"An APRA-regulated entity must notify APRA as soon as possible, and no later than 24 hours, if it has activated its BCP. The notification must cover, to the extent the information is available at the time of notification, the nature of the disruption, the action being taken, the likely impact on the entity's business operations and the timeframe for returning to normal operations."

6. Monitoring, notifications and review

Article 58 requires APRA-regulated entities to notify APRA prior to entering any third-party arrangements with a material service provider or when there is a significant change proposed to the agreement.

We would like to caution against the use of prescriptive language as this requirement could be interpreted as a form of regulatory approval, which may in turn dissuade regulated entities from proceeding with the arrangements with service providers. In this regard, we encourage APRA to provide greater certainty for businesses while ensuring that APRA retains its supervisory authority.

Recommended revisions

Article 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) not fewer than 20 business days prior to entering into any offshoring agreement with a material service provider, or ~~when there is~~ making a significant change ~~proposed~~ to the agreement, including in circumstances where data or personnel relevant to the service being provided will be located offshore, and shall proceed with the agreement only if it does not receive a letter of objection from APRA within the said period."