21 October 2022

BSA COMMENTS ON DRAFT PRUDENTIAL STANDARD CPS 230 ON OPERATIONAL RISK MANAGEMENT

Submitted Electronically to the Australia Prudential Regulatory Authority

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide input to the Australia Prudential Regulatory Authority's (**APRA**) draft Prudential Standard on operational risk management for the financial sector (**CPS 230**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members create the technology products and services that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. Many of our members provide services across the financial services sector and thus have unique insights into the opportunities and risk management challenges associated with cloud adoption in this sector.

BSA and its members support the overall objective of increasing operational resilience of APRA's entities to protect the integrity of the Australian financial system. However, certain areas of the proposal should be adjusted to best achieve the desired objectives. These include the following:

1. Defining and narrowing the scope of "core technology services";
2. Making clear the requirements on risk assessments and reporting of "operational risk incidents";
3. Reviewing the proposed contractual requirements between APRA-regulated entities and third-party service providers; and
4. Reviewing the notification requirement for offshoring agreements.

Define and narrow the scope of "core technology services"

Paragraph 48 requires APRA-regulated entities to identify and maintain a register of its "material service providers" and manage the material risks associated with using these providers.[2] Such

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] CPS 230, paragraph 48.

[redacted]

material service providers are further defined as those which the entity relies on to undertake a critical operation or that expose it to material operational risk. This would include services such as "core technology services".[3]

The term "core technology services" is undefined in CPS 230 and as such is open to interpretations which are overly broad. A technology service provider may provide a range of technology services to an APRA entity which could be loosely considered as "core technology services", but the services provided might not be considered as critical to the operation of an APRA entity (e.g., payroll services). It would therefore be disproportionate to subject that technology service provider to the CPS 230.

BSA recommends clearly defining the term "core technology services" to provide guidance for both APRA-regulated entities and their service providers. In defining "core technology services", BSA also urges APRA to adopt a narrow definition by limiting it to services that "support the effective provision of core functions provided by the APRA-regulated entity" (i.e., it directly supports the provision of the APRA-regulated entity's service to its customers, the integrity and reliability of the APRA-regulated entity, or the confidentiality of information held by the APRA-regulated entity).[4]

Make clear the requirements on risk assessment and reporting of "operational risk incidents"

Requirements on risk assessment

Paragraph 52 requires APRA-regulated entities to conduct a series of risk assessments prior to entering or renewing an arrangement with a material service provider. While the intention of such a provision may be to reduce risks posed to the system, it could unintentionally lead to operational complexity and uncertainty for APRA-regulated entities which might not be best placed to evaluate "risks associated with geographic location" and whether the provider is "systematically important in Australia".[5]

Furthermore, requiring risk assessments based on the service provider's "geographic location" could also restrict the number of products available for use by APRA-regulated entities and might even dissuade APRA-regulated entities from using overseas third-party providers and subcontractors, despite the quality and commercial benefits of their services. This could have negative consequences to such entities' global competitiveness.

The vague definition of "geographic location" risk is also open to broad interpretation and may result in inconsistencies across different entities, causing challenges in compliance. For instance, it could be interpreted as requiring the data or service to be deployed across geographically-diverse data centers, or that the service must reside in Australia. Existing geographic risk-based guidance such as the Financial Action Task Force (**FATF**) high risk jurisdictions and those subject to increased monitoring[6], and the Australian Transaction Reports and Analysis Centre (**AUSTRAC**) prescribed

[3] CPS 230, paragraph 49.

[4] This suggestion is based on guidance material provided by Australia's Cyber and Infrastructure Security Centre (**CISC**) on critical infrastructure assets. See Register of Critical Infrastructure Assets Guidance, September 2022, p. 2, https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/register-critical-infrastructure-assets.pdf

[5] CPS 230, paragraph 52 (b)-(c).

[6] FATF, Jurisdictions under Increased Monitoring, June 2022, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2022.html

foreign countries[7] focus on risks such as money laundering, terrorism financing, and tax havens. These risks are not necessarily relevant for all cloud delivered or outsourced services. It is unclear whether the applicability of such "lists" is appropriate.

As such, BSA recommends that APRA provide further guidance on and definition of the following:

a) **risks based on geographic location relevant to nature of the cloud service or business operations being provided;**

b) **the types of financial and non-financial risks from using a material service provider;**

c) **what would constitute a "systemically important" provider in Australia;**

d) **The "reasonable steps" for APRA-regulated entities to assess whether a provider is "systemically important in Australia", and the actions they should take after making this assessment.**

Requirements on reporting of "operational risk assessments"

Paragraph 32 requires APRA-regulated entities to notify APRA of certain operational risk incidents. The footnote to paragraph 32 references *Prudential Standard CPS 234 Information Security* (**CPS 234**), stating that "a notification of an information security incident reported under CPS 234 does not need to be separately reported under [CPS 230]".

BSA supports ensuring that there should not be double reporting on APRA-regulated entities. **However, CPS 230 should also make clear the extent to which APRA-regulated entities are required to report security incidents occurring with their service providers, but that have no impact on the APRA-regulated entities themselves.**

In this respect, CPS 234 paragraph 35(b) requires an APRA-regulated entity to notify APRA "after becoming aware of an information security incident that has been notified to other regulators, either in Australia or other jurisdictions". It is not clear if this requirement to notify APRA extends to notifications made by a service provider of the APRA-regulated entity. This requirement may therefore be read as requiring APRA-regulated entities to notify APRA of incidents reported by their service providers in other jurisdictions, even if the incident had no impact on the APRA-regulated entities themselves.

This would lead to unnecessary and over-reporting of incidents to APRA by APRA-regulated entities, and the latter being compelled to impose similarly unnecessary requirements in their outsourcing contracts for service providers to report unrelated incidents. APRA-regulated entities and APRA may consequently face difficulties in identifying and remedying incidents that do in fact impact the APRA-regulated entities. It could also prove unworkable for the service provider – in the event of a security incident, the service provider will need to devote resources to remedying the breach and notifying affected customers; and adding a requirement for the service provider to notify unaffected customers would severely tax those resources.

BSA accordingly recommends that CPS 230 make clear that APRA-regulated entities are not required to report security incidents occurring with their service providers that have no impact

[7] AUSTRAC, High Risk countries, regions, and groups, July 2019, https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/high-risk-countries-regions-and-groups

on the APRA-regulated entities themselves; and that APRA-regulated entities are also not required to compel their service providers to report any such incidents.

Review proposed contractual requirements between APRA-regulated entities and third-party service providers

Existing relationships between cloud service providers and financial entities are based on contracts tailored to each unique scenario. CPS 230's specific contractual requirements under paragraph 53 would potentially limit the contractual freedom of companies who should be able to customize their agreements based on their specific needs and risks. **We urge APRA to issue guidelines on contractual arrangements between APRA-regulated entities and their third-party service providers instead of detailing minimum requirements as currently outlined in paragraph 53.**

Additionally, the draft provisions in paragraphs 54(a) and (b) could raise privacy and security concerns regarding, for example, personal information and business confidential information. Many third-party service providers may be contractually prohibited from accessing data on their services, or even technically be unable to access it, unless explicitly directed or allowed by their customers, a prohibition designed to increase security and privacy protections afforded to the data under the third-party service providers' control. The requirement in paragraph 54(a) to "allow APRA access to documentation, data and any other information related to the provision of the service" could be read to allow APRA direct access to specific information that might inadvertently lead a third-party service provider to be in breach of its contractual obligations to its customers.

Furthermore, many modern software-enabled services employ cloud computing and often involve one or more sub-contracting service providers. As such, the proposal in paragraph 54(b) to conduct on-site inspections and audits may not be practicable nor technically feasible, especially if there are several sub-contracting service providers involved.

As such, BSA suggests that any information access and audit requests from APRA on third-party service providers should be directed to APRA-regulated entities first. This is the guidance already contained in CPS231 (34). This would ensure that access to information processed and managed by third-party service providers are in line with their contractual obligations to their customers. APRA-regulated entities would also be in a better position to direct APRA to the right service provider. **Additionally, instead of requiring audit and on-site inspection of third party service providers, it should suffice for a service provider to demonstrate compliance based on the production of certification based on internationally recognised standards and prior audits.**

APRA should consider reiterating some existing guidance from CPS 231 mentioned above and extend guidance to allow the recognition of established international and Australian certification and audit programs.

Review notification requirement for offshoring agreements

Paragraph 58(b) requires APRA-regulated entities to notify APRA prior to entering into any offshoring agreement with a material service provider, which includes circumstances where data relevant to the service being provided will be located offshore.

BSA recognises APRA's interest in maintaining oversight of the nature and extent of service providers relied on by each industry, with a view to "identifying and responding to potential systemic issues"

(e.g., concentration risk when multiple entities are reliant on a single provider).[8] However, such notification requirements are potentially difficult for APRA to enforce and for businesses to comply with. Given the global nature of technology service providers, it is not uncommon for data to be processed or stored offshore. The location where data is located may change depending on the business needs of APRA-regulated entities, who have the final say on where they want their data to be located. Implementing notification requirements may therefore hinder cloud service providers' ability to quickly respond and adjust their services to meet customer needs, including to ensure maximum resiliency and security in a given network.

BSA therefore recommends removing the requirement for APRA-regulated entities to notify APRA prior to entering an offshoring agreement. However, if APRA maintains the notification requirement, we urge APRA to ensure that such notification requirements are minimally burdensome for APRA-regulated entities, such as by limiting the information that APRA-regulated entities are required to provide.

Conclusion

We hope that our comments will assist APRA as it moves forward on CPS 230. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

[redacted]

Tham Shen Hong

Manager, Policy – APAC

[8] APRA Discussion Paper: Strengthening operational risk management, July 2022, p.27, https://www.apra.gov.au/sites/default/files/2022-07/Discussion%20paper%20-%20Strengthening%20operational%20risk%20management.pdf.