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

13 October 2023

Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001

Via email: PolicyDevelopment@apra.gov.au

Consultation on draft Prudential Practice Guide CPG 230 Operational Risk Management

Amazon Web Services Australia Pty Ltd (**AWS**) welcomes the opportunity to comment on the Australian Prudential Regulation Authority's (**APRA**) draft Prudential Practice Guide CPG 230 Operational Risk Management (**CPG 230**).

AWS is generally supportive of the proposed guidance, and we appreciate that some important issues raised in the consultation on the accompanying Prudential Standard CPS 230 Operational Risk Management (**CPS 230**) have been reflected in CPG 230.

However, we believe enhancing CPG 230 in a small number of key areas will assist APRA-regulated entities to interpret and apply the principles in CPS 230 to make the best decisions for their organisations. In particular, we would welcome APRA clarifying that concentration and offshore geographic location of service providers (i) are not necessarily higher risk than the alternatives, (ii) in the case of cloud, may actually enhance cybersecurity and resilience, and (iii) do not necessarily require an APRA-regulated entity to pursue a 'multi-cloud' strategy to mitigate. We also suggest some clarification of guidance in respect to service provider agreements.

Key issues

Concentration risk assessment

Paragraph 53(b) of CPS 230 contains a direction for APRA-regulated entities to assess risks associated with concentration of service providers before entering into or materially modifying a material arrangement, but paragraphs 98-100 of CPG 230 do not elaborate on (i) what concentration risk means, (ii) how an entity should conduct this analysis, (iii) examples where concentration may be beneficial, nor (iv) what – if any – actions are required to mitigate such risk. AWS recommends APRA provide expanded guidance on this requirement to assist APRA-regulated entities make the required assessment.

Our understanding is that the concentration risk provision in paragraph 53(b) of CPS 230 is intended to ensure that APRA-regulated entities develop an awareness of the level of concentration across their entire service provider portfolio (regardless of whether a material arrangement exists). Paragraph 53(b) does not require APRA-regulated entities to undertake unnecessary mitigation actions.

However, it has been our experience that regardless of APRA-regulated entities' capability and maturity using cloud, many entities are over-interpreting APRA's direction to *assess* concentration as an automatic requirement to implement mitigations, such as 'multi-cloud' strategies. Of particular concern is the erroneous belief that APRA-regulated entities must run critical systems (i.e. systems of heightened and extreme inherent risk) in an "active-active" configuration[1] across two different cloud platforms.

In some circumstances, vendor diversity may reduce some risks involved with concentration of service providers. However, in the area of cloud, increasing vendor diversity through multi-cloud strategies may also give rise to other, arguably greater, risks. These include reduced resilience or potentially increased exposure to a security incident as entities with limited resources attempt to build and manage platforms across two vendors rather than building expertise in one service provider's technology stack. Our customers' experiences to date have found maintaining an IT workload across multiple cloud providers is generally 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. The US Department of Treasury found that "No financial institution reported the capability to do so for more complex use cases, such as running core operations on multiple public clouds. Running an application across multiple CSPs[2] at the same time may also be less desirable, given the costs, staffing, and complexity involved in doing so, particularly given the complexity associated with identifying and managing risk across multiple cloud environments."[3] Some AWS customers – even those with deep cloud expertise – have found that the additional expense and effort in people, process and tools (collectively known as an 'operating model') is many multiples of what it would cost to run a single provider strategy, and resulted in weakened resilience and recovery time, and recovery point objectives unable to be met. We believe that pursuing multi-cloud strategies should be done in an extremely cautious and controlled manner, with a focus on overall net risk position.

We also contend that concentration is not always inherently a risk, and in many circumstances may be beneficial to the overall risk profile of an APRA-regulated entity. Cloud service providers offer access to necessary skills and expertise which may reduce an entity's cyber risk, particularly for smaller entities with limited resources to invest in cybersecurity technology and personnel about which APRA has recently expressed concern.[4] Hyperscale 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.[5] Hyperscale cloud providers are also able to make investments in security and

[1] Running a single workload across two different cloud providers, with the expectation that in the event of an outage at one provider, operations will fail over without interruption and continue at the other provider with near-zero downtime and data loss.

[2] Cloud Service Providers

[3] U.S. Department of the Treasury, The Financial Services Sector's Adoption of Cloud Services, February 2023

[4] APRA Member Therese McCarthy Hockey - GRC2023, 'From fires to firewalls: the evolution of operational risk', August 2023

[5] For example, the Zen Bleed vulnerability, which may have allowed attackers to potentially access sensitive information on systems running specific processors, did not affect AWS customers because of the investments AWS has made in its custom-designed infrastructure.

resilience which exceed that which individual entities or even industry sectors may be able to make. Data obtained from operating at scale also allows development of better security. For example, using artificial intelligence and machine learning (**AI/ML**) techniques, heuristics and pattern-matching on the traffic attempting to enter our networks allows AWS to pre-emptively mitigate distributed denial-of-service (**DDoS**) attacks and scrub malicious traffic before they reach customer systems running on AWS. Hyperscale cloud providers are also able to respond at speed and at scale to new and emerging threats such as "zero-day" exploits, where hardware or software vulnerabilities are discovered by attackers before the vendor has become aware, so no patch or other counter-measure is available.[6]

Hyperscale cloud providers proactively mitigate potential concentration risks by offering services via physically separate locations and logically segregated IT systems. 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.

Recommendation:

AWS recommends that paragraphs 98-100 of CPG 230 be strengthened by:

- providing guidance as to how concentration is defined and how APRA-regulated entities should assess for it;
- stating that concentration is not inherently negative and may indeed be beneficial in certain circumstances (such as the case of hyperscale cloud providers as highlighted above);
- acknowledging that accepting the concentration risk associated with a single-provider strategy will often lead to an overall lower net risk position than pursuing a multi-provider strategy;
- explicitly stating that running workloads in an active-active configuration across two different cloud providers is extremely technically complex, and that even for extreme inherent risk workloads, is not an approach required or recommended by APRA;
- confirming that the intent of paragraph 53(b) of CPS 230 is for APRA-regulated entities to be *aware* of the level of concentration among their service providers, and to only take mitigating actions where the entity considers it necessary in a way that will not increase the entities' overall net risk position; and
- explicitly stating that APRA-regulated entities should contact their APRA supervision team if they have any questions.

[6] The Log4J vulnerability, discovered at the end of 2021, can be considered as one of the most critical vulnerabilities in recent years, potentially affecting millions of servers worldwide. Within 72 hours of the exploit being announced, AWS engineers had developed a hotfix and patched all AWS Services, and also made the patch available to the public via Github. This protected customers, as well as the general public, at far greater speed than would have likely been possible at an individual level.

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

Geographic location

Paragraph 53(b) of CPS 230 contains a direction to assess risks associated with geographic location of service providers before entering into or materially modifying a material arrangement, and paragraph 100 of CPG 230 provides some guidance as to the types of risks envisaged when engaging service providers in another jurisdiction.

Paragraph 59 of CPS 230 also includes prior notification/consultation reporting requirements for offshoring agreements, for which no guidance is provided in CPG 230.

These two requirements may 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 services.

However, in certain circumstances, services provided from another jurisdiction may actually reduce operational risk and increase resilience and security. For example, storing data offshore often facilitates greater redundancy in terms of increased geographic spread and the reduced risks that come with that.

CPS 230 and CPG 230 should not discourage APRA-regulated entities from utilising services provided from other jurisdictions where those services may reduce their overall operational risk and increase resilience.

Recommendation:

AWS recommends that APRA include guidance in CPG 230 in relation to paragraph 53(b) of CPS 230 to clarify that services delivered from another jurisdiction are not inherently riskier, and that diverse geographic locations of service provision may reduce operational risk and increase resilience and security which APRA-regulated entities should focus on when conducting their assessments.

Management of service provider arrangements

a) Mandated changes to service provider agreements

Paragraph 57 of CPS 230 states that "APRA may require an APRA-regulated entity to review and make changes to a service provider arrangement where it identifies heightened prudential concerns." There is no specific guidance on this requirement in CPG 230.

Recommendation:

AWS recommends that APRA include guidance on this requirement that (i) defines or provides examples of "heightened prudential concerns", and (ii) confirms that APRA would use its other consultative measures and powers prior to enforcing paragraph 57 as a last resort.

b) "Material modification" of material agreements

Paragraph 53 of CPS 230 outlines requirements APRA-regulated entities must undertake "before entering into or materially modifying a material agreement." Paragraph 59 of CPS 230 provides notification requirements on "materially changing an agreement" and "when there is a significant change proposed to the arrangement." CPG 230 does not provide guidance in respect of the types of changes that may trigger these requirements.

In the absence of guidance as to what "material modification" means, APRA-regulated entities may over-burden internal resources trying to comply with this provision when making simple changes to their contractual arrangements. We do not believe this is APRA's intention.

Recommendation:

AWS recommends that APRA clarify that a "material modification" to an existing agreement would only occur when there is a fundamental change to the scope or purpose of the agreement (e.g. 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.

c) Service provider agreements

Paragraph 54 of CPS 230 states the following:

> *54. For all material arrangements, an APRA-regulated entity must maintain a formal legally binding agreement (formal agreement). The formal agreement must, at a minimum:*
>
> *(a) specify the services covered by the agreement and associated service levels;*
>
> *(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, dispute resolution, audit access, liability and indemnity;*
>
> *(c) include provisions to ensure the ability of the entity to meet its legal and compliance obligations;*
>
> *(d) require notification by the service provider of its use of other material service providers that it materially relies upon in providing the service to the APRA-regulated entity through subcontracting or other arrangements;*
>
> *(e) require the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider;*
>
> *(f) include a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event; and*
>
> *(g) termination provisions including, but not limited to, the right to terminate both the arrangement in its entirety or parts of the arrangement. For an RSE licensee, 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 (refer to subsection 52(2)(c) of the SIS Act).

Recommendation:

AWS recommends the following clarifications be included in CPG 230 on these requirements.

- (Paragraph 54(a)) Clarify that services do not need to be listed in the agreement, but can be listed on a website referenced in the agreement.
- (Paragraph 54(b)) Clarify that 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. In this instance – an entity can read 'ownership' as 'control' or only apply this provision when applicable.
- (Paragraph 53(c)) Clarify that the material service provider and the APRA-regulated entity must comply with their own legal and compliance obligations and are not responsible for ensuring that the other party meets all of its legal and compliance obligations.
- (Paragraph 54(d)) 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.
- (Paragraph 54(g)) Clarify that the right to terminate "parts of the arrangement" 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.

d) Liability in agreements

With reference to paragraph 54(e) of CPS 230, paragraph 103 of CPG 230 states that, "The agreement would typically specify the extent of liability of each party and, in particular, whether liability for negligence is limited."

Limiting liability for negligence is not appropriate in all outsourcing agreements. Negligence is a tort, not a cause of action under contract. Breaches of agreements are either caused by negligence or are intentional. The remedy for this breach is a claim for breach of contract, not negligence. If a customer wants to bring a claim for negligence, the customer should sue the service provider for the negligence tort. This approach is industry standard.

Recommendation:

AWS recommends removing the guidance that outsourcing agreements should outline whether liability for negligence is limited because it is not appropriate in all outsourcing agreements.

e) Termination provisions

With reference to paragraph 54(e) of CPS 230, paragraph 104 of CPG 230 states that "termination provisions would typically detail transition arrangements as well as ownership and access to documents, data, intellectual property and other assets."

Recommendation:

AWS recommends that APRA delete "as well as ownership and access to documents, data, intellectual property and other assets" as this is not relevant in all outsourcing agreements and could lead to customer confusion.

f) Access to information and on-site visits

Paragraph 55 of CPS 230 requires formal service provider agreements to include provisions to allow APRA access to documentation and information, the right to conduct an on-site visit to the service provider, and ensure the service provider agrees not to impede APRA in fulfilling its duties. CPG 230 only provides guidance in relation to APRA typically notifying service providers before seeking information or an on-site visit.

AWS supports the intent of this paragraph and looks forward to continuing to collaborate with APRA. However, there may be a risk that APRA-regulated entities ask material service providers to include terms in the agreement that undermine the security and resilience of the material service provider's services and the security and confidentiality of its other customers (who may be other APRA-regulated entities).

Recommendation:

AWS recommends that APRA include in CPG 230 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 (e.g. allowing for a reasonable number of APRA's compliance personnel or auditors to visit each time).

g) Management of service provider arrangements

Paragraphs 89-92 of CPG 230 provides guidance on APRA's expectations for ongoing oversight of third-party service providers, as well as fourth-party/downstream providers. This guidance could be strengthened by including reference to the availability of government and industry-recognised certifications, which APRA-regulated entities can rely on for assurance over service provider control environments, including fourth-party/downstream provider management. This is applicable for both initial vendor due diligence and for ongoing oversight activities. For example, AWS currently supports 143 security standards and compliance certifications, including PCI-DSS, ISO 27001, the NIST cybersecurity framework and specific to Australia, our Strategic Hosting Provider certification under the Australian Government's Hosting Certification Framework.

Recommendation:

AWS recommends APRA include in CPS 230 reference to the availability of government and industry-recognised certifications, which APRA-regulated entities can rely on for assurance over service provider control environments, including fourth-party/downstream provider management.

Operational risk incidents

Paragraph 33 of CPS 230 requires that "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."

AWS welcomes the added footnote that a notification of an information security incident reported under CPS 234 does not need to be separately reported under the notification requirements of CPS 230.

However, in our experience many APRA-regulated entities misinterpret the similar requirement in paragraph 35 of CPS 234 as imposing notification obligations on service providers directly, which APRA has confirmed is not the intention.

Recommendation:

AWS recommends that APRA clarify in CPG 230 that paragraph 33 of CPS 230 does not apply to material service providers – the APRA-regulated entities have the obligation to act within 72 hours of becoming aware of an operational risk incident.

Offshoring

Footnote 16 in the Prudential Standard CPS 230, relevant to paragraph 59(b) regarding material offshoring arrangements, states that:

> *Material offshoring arrangement means a material arrangement where the service provided is undertaken outside Australia. Offshoring includes arrangements where the service provider is incorporated in Australia, but the physical location of the service being provided is undertaken outside Australia. Offshoring does not include arrangements where the physical location of a service is performed within Australia, but the service provider is not incorporated in Australia.*

Recommendation:

AWS recommends that APRA clarify in CPG 230 that APRA-regulated entities do not need to notify APRA if they are adding a non-Australian party to an agreement if the services will be performed outside of Australia (i.e. there will be no nexus to Australia). For example, if an APRA-regulated entity adds a Singaporean affiliate of an Australian service provider as a party to a global services agreement (that it

entered into with an Australian service provider) for the Singapore affiliate to perform work in Singapore, the APRA-regulated entity would not need to notify APRA.

Material Arrangement

Paragraph 49 of CPS 230 has introduced the concept of "material arrangements". Both "material service providers" and "material arrangements" are defined in paragraph 49 as "those on which the entity relies to undertake a critical operation or that expose it to material operational risk." In paragraph 98 of CPG 230, APRA outlines that not all arrangements with material service providers will be material to the APRA-regulated entity. It is unclear as to whether the intention of introducing "material arrangements" was to clarify that the contractual obligations in CPS 230 do not apply to agreements with material service providers that do not relate to critical operations or material operational risks.

Recommendation:

We recommend that APRA clarify in CPG 230 (i) why APRA introduced the concept of "material arrangements" in CPS 230, and (ii) whether "material arrangements" are arrangements only made with material service providers. The drafting implies that material arrangements could include arrangements made with any service provider.

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,

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