General Manager, Policy
Australian Prudential Regulatory Authority

Via email: PolicyDevelopment@apra.gov.au

Dear General Manager,

Submission – Draft Prudential Standard CPS 230 Operational Risk Management

Thank you for the opportunity to provide feedback on the draft cross-industry Prudential Standard CPS 230.

FinTech Australia is the peak industry body for financial technology businesses and represents over 400 fintech Startups, Hubs, Accelerators and Venture Capital Funds across the nation. Our membership includes payment providers, digital banks, Insurtechs, Regtechs, Wealthtechs and other service providers. Some of our members are directly regulated by APRA ("regulated entities"). Others will be indirectly impacted by CPS 230 as material service providers to regulated entities.

FinTech Australia members affected by the draft CPS 230 can be broadly categorised as:

- Regulated entities, including Authorised Deposit-taking Institutions ("ADIs").
- Companies that are material service providers to regulated entities. These fintechs which partner with banks will be indirectly impacted by the requirements in CPS 230 flowing from regulated entities.
- Fourth parties, on which material service providers rely. These entities will also be impacted by requirements flowing from regulated entities.

We agree with the general approach taken in the draft CPS 230 to consolidate operational risk concepts into a single standard. However, the anticipated impacts of CPS 230 differ between our members. For members that are ADIs, the new requirements in CPS 230 will materially increase the compliance burden. We support the use of proportionality measures, to stagger the implementation for non-SFIs. It is not yet clear what the requirements will be from the service-provider perspective. Regulated entities may differ in their approaches to identifying material service providers. The draft CPS 230 does not ensure adequate consistency in the requirements under contractual arrangements between regulated entities and service providers.

The successful implementation of CPS 230 to improve operational risk management, without imposing undue burden on material service providers, will depend on effective guidance. FinTech Australia encourages APRA to develop the CPS 230 Prudential Practice Guide ("PPG") with comprehensive guidance regarding the threshold for critical operations and material service providers. We look forward to working closely with APRA as this guidance is developed to ensure fintechs understand the new requirements and how it will impact their relationship with ADIs.

Please see below answers to specific questions from the Discussion Paper:

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

FinTech Australia supports simplifying and streamlining the existing requirements into a single standard. Members note that a single standard simplifies the compliance burden.

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

FinTech Australia members are concerned that the expectations on service providers are not clear enough as a result of the proposed changes to CPS 230 and that there should be more guidance provided to service providers. This would assist fintech service providers as they provide services to regulated entities.

Some FinTech Australia members believe that it would be helpful if APRA develops guidance (which could be in the PPG) which summarises how the proposed CPS 230 changes would impact service providers specifically. This would drive greater consistency in how these obligations are implemented and, as a result, would greatly assist service providers to understand their indirect obligations. Increased consistency would greatly reduce the compliance burden on those impacted by these proposed changes.

Some FinTech Australia members also believe there should be more clarity and consistency in relation to the expectations of regulated entities on fintech service providers. For example, if a fintech service provider served multiple ADIs, it is likely that each ADI would have their own materiality thresholds, or definitions of what their critical functions are and which service providers may be captured. As a consequence, fintech service providers would have to spend a large amount of time and resources trying to accommodate multiple different requirements from different ADIs, due to the lack of clarity and consistency across the definitions of critical operations, material service providers and tolerance levels.

Additionally, some FinTech Australia members believe that there should be more specific guidance around what is meant by a "disruption" to business operations. Disruptions can vary in terms of severity. Some disruptions can render critical operations completely unavailable, whereas there may be many disruptions which may impact a material service but only in an insignificant way. FinTech Australia encourages APRA to provide more

guidance and clarity as to what specific disruptions it is targeting in its proposed changes to CPS 230. There may be immaterial disruptions to critical operations that do not materially impact the continued operation of critical systems and functions, yet the proposed changes may require a regulated entity to report such a disruption, and there will be a need to document such disruptions in BCPs. Some FinTech Australia members believe APRA should provide more clarity as to the level of disruptions that is being contemplated in the proposed changes to CPS 230, otherwise there may be unintended yet significant and burdensome requirements that may be imposed on APRA-regulated entities.

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

FinTech Australia supports the distinction between SFIs and non-SFIs and considers that it may be appropriate for non-SFIs to be exempt from specific requirements.

FinTech Australia believes that this approach would provide greater certainty and clarity. If, on the contrary, the requirements are ambiguous or unclear, different regulated entities may each have different views as to whether particular requirements apply, which will increase the regulatory and compliance burden on these service providers and will cause great confusion and uncertainty amongst the industry.

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

Compliance Costs

There are differing views between members as to the likely compliance cost of CPS 230. Some members note that CPS 231 has presented a manageable compliance burden. Assuming the proportionality approach is similar under the final CPS 230 (with lesser reporting requirements for non-SFIs), the requirements under CPS 230 for regulated entities appear practicable.

From a service provider perspective, the magnitude of these compliance costs will depend on contractual arrangements with regulated entities. Costs could be exacerbated by a

divergence in requirements between partners, under service provider management policies.

Some members anticipate they will need to significantly uplift their operational risk staff and capabilities. Third party service providers will need to be engaged to map third and fourth party dependencies, and to obtain risk management testing capabilities.

To improve certainty for service providers, we encourage APRA to include further guidance and clarity in the PPG regarding the flow of requirements along the supply chain. If regulated entities clearly set out their requirements in contract negotiations with service providers, this will alleviate some of the uncertainty. It is expected that partnering with regulated entities will result in additional reporting requirements and complexity. The overall impact of CPS 230 will depend on the types of requirements regulated entities will mandate under contractual arrangements with service providers.

Anticipated impacts of draft CPS 230

The new requirements may make it more difficult for some members to provide services to regulated entities. Challenges may arise where a fintech provides services to multiple ADIs with different sets of requirements based off CPS 230. Juggling differing requirements associated with different partners may become cumbersome (as discussed above, at Question 2). However, larger fintech service providers with well-established compliance teams are better placed to manage the compliance burden. Additional teams will need to be involved in supporting the vendor relationship with a regulated entity (to ensure comfort regarding adequate risk management controls). This will impact internal stakeholders, who will require additional resources to manage the new requirements.

Additionally, regulated entities that are non-SFIs are likely to face challenges negotiating with relatively larger service providers (for example, cloud service providers). It will be difficult for these relatively smaller entities to negotiate the risk mitigation mechanisms contemplated by CPS 230 in service provider arrangements.

5 How could APRA improve the definitions of critical operations, tolerance levels and material service providers?

Members note that the materiality threshold lacks clarity. What is material to one regulated entity may not be for another. There is a risk of lack of consistency, due to different interpretations of CPS 230 (as discussed above, at Question 2). We note that under CPS 230, related parties and third parties that manage critical information assets for the purpose of CPS 234 (“Information Security”) are deemed material.

We encourage APRA to provide additional prescriptive guidance in the PPG regarding whether a service provider is material or non-material (beyond the guidance in the Discussion Paper). Members note that list of service providers that APRA considers non-material would be helpful in this respect.

Additionally, it would be helpful to clarify the types of impacts on critical operations (for example, with regards to the ORX impact taxonomy) that would be considered material.

Furthermore, greater clarity regarding critical operations, would be useful (beyond the specified critical operations in the CPS 230 Discussion Paper, and the associated term "critical business operations" in CPS 232). Members note that setting tolerance levels is complex, and not entirely captured by the three data points currently set out in draft CPS 230 (namely, maximum time-period, maximum extent of data loss and minimum service levels to maintain during a disruption). Consequently, members welcome further guidance around "disruption" (as discussed above at Question 2).

We note that under the new requirements, senior management of regulated entities are responsible for "operational risk management across the end-to-end process for all business operations". We welcome further guidance as to what is meant by "end-to-end" and encourage the use of proportionality measures to ease the compliance burden associated with mapping the prescribed operations.

8 What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers (if required)?

FinTech Australia expects that an extended transition period would be appropriate, as it may take some time for APRA-regulated entities and their service providers to negotiate the necessary updates. FinTech Australia and its members believe that fintechs will have to allocate a significant amount of resources to deal with the impacts of the proposed changes to CPS 230 and update contracts.

We support at least a similar transition process to CPS 234. Under CPS 234, the transition period was the earlier of one year post commencement of the new standard, or the next contract renewal date.

Further feedback for APRA

Managing risks associated with fourth parties

Members expressed concern regarding the "management of service provider arrangements" with respect to fourth parties. Members acknowledge the importance of uncovering hidden concentrations in the supply chain and managing the associated risks. We support further guidance for regulated entities on the expectations around supply chain visibility. Our members note that the ability of regulated entities to identify and influence parties diminishes further along the supply chain.

Concentrations of material service providers at points along the supply chain may require an industry solution to both identify the parties at these concentration points and to manage the associated operational risks. It may be difficult for a single regulated entity or service provider to manage these complex supply chain risks, through the mechanisms proposed in the draft CPS 230.

This lack of clarity also impacts service providers. To identify and manage the risks associated with service providers, regulated entities may impose cumbersome requirements. This could negatively impact the competitiveness of service providers.

A fintech's reliance on third parties may be far greater than large and established SFIs. Some members consider freelancers to be included in the assessment of operational risk management as employees. Complexity arises further down the supply chain. A fintech may use several third-party contractors. A third party provider to a fintech, may be caught by the fourth party requirements under CPS 230. Currently there is no certainty as to how a given regulated entity will decide to manage the risks associated with fourth parties.

We anticipate this will require amending contracts with service providers, to allow for the obligations of regulated entities to flow on to fourth parties. It may be burdensome if a fintech is required to provide a regulated entity with extensive information regarding their service providers.

This may be less burdensome for larger regulated entities that are major customers of upstream providers and possess substantial bargaining power. However, many fintech are minor customers, with relatively less bargaining power. Consequently, they may face greater challenges in renegotiating downstream contracts including additional requirements from regulated entities.

Outcome-focused approach

FinTech Australia urges APRA to ensure that the changes to CPS 230 are outcome-focused. Some FinTech Australia members consider that the requirements for detailed documentation and processes under CPS 230 may be overly burdensome for some service providers, when considered in light of the relative risk involved in the underlying service. Ensuring the burden is commensurate with the risk will encourage and not stifle the participation of service providers in the industry.

About this Submission

This document was created by FinTech Australia in consultation with its members.

In developing this submission, our Members participated in a roundtable to discuss key issues relating to this submission.

We also particularly acknowledge the support and contribution of King & Wood Mallesons and K&L Gates to the topics explored in this submission.