19 October 2022

General Manager, Policy
Policy and Advice Division
Australian Prudential Regulation Authority

By email: policydevelopment@apra.gov.au

Discussion Paper: Strengthening Operational Risk Management – Tyro Submission

Dear Sir/Madam,

Tyro Payments Limited (**Tyro**) welcomes the opportunity to provide a submission in response to the Australian Prudential Regulation Authority (**APRA**) discussion paper – *Strengthening Operational Risk Management*.

About Tyro

Founded in 2003, Tyro is a technology-focused and values-driven company providing Australian businesses with payment solutions and value-adding business banking products. We provide simple, flexible, and reliable payments solutions as a merchant acquirer, along with complementary business banking products.

Tyro was issued an Australian Financial Services Licence and became an Authorised Deposit-Taking Institution (**ADI**) in 2015, making us, at that time, the first new domestic banking licensee in over a decade. We are now Australia's fifth largest merchant acquiring bank by number of terminals in the market, serving over 63,000 merchants.

Notwithstanding Tyro's growth in the merchant acquiring market, Tyro's operations as an ADI are still relatively modest, with Tyro's banking business operations contributing less than 2% of Tyro's overall annual revenue. Further, by virtue of our size, Tyro is considered to be a *'Non-significant financial institution (**non-SFI**)*' as defined in under ARPA's Prudential Standard APS 001.

Overview

The proposed Prudential Standard CPS 230 *Operational Risk Management* (**CPS 230**) seeks to strengthen the management of risk, in this case operational risk, across the banking, insurance and superannuation industries. Whilst Tyro supports the overall intent of CPS 230, we are concerned that without proper regard being given to the size and scale of the APRA-regulated entities to which this prudential standard applies, the impact of CPS230 could have a disproportionate effect on smaller entities, which could ultimately hinder competition in the sector.

In providing scalability, this will better enable smaller entities the ability to manage the associated compliance costs and administrative burden, whilst continuing to remain compliant and competitive against larger APRA-regulated entities. This is crucial for entities such as Tyro, whose existence depends on staying competitive against existing larger providers, particularly in the small business banking segment.

Specific Feedback

We have taken this opportunity to address the following questions as raised in the discussion paper:

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

Whilst we agree that a cross-industry standard for operational risk management should be implemented, as stated above, a balanced approach should be taken when implementing reforms to minimise complexity for smaller entities.

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

To help entities better understand the application of CPS 230, we believe that guidance on the following would be required:

- Additional clarification on the definition of *'material service provider'*. In particular:
  - terms such as *'core technology service'* are included in the definition, however they themselves are not defined;
- *Service provider agreements* within CPS 230 (paragraphs 52-56) requires an APRA-regulated entity to take reasonable steps to assess whether a provider is 'systemically important' in Australia. We believe that guidance regarding what APRA would consider to be a *'systemically important'* provider is important for smaller entities, noting that a given APRA-regulated entity may not have the requisite industry-wide perspective to assess 'systemic importance'.

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

With the increased complexity and growing cost of compliance, Tyro advocates proportionality and increasing simplicity for non-SFIs to allow them to remain competitive.

<u>Service Provider Management</u>

As described above, the current wording of paragraph 50 suggests that material services providers also include providers that manage information assets classified as critical or sensitive under CPS 234. We consider that this potentially captures an extraordinarily broad number of agreements under CPS 230, which would then require additional steps to be taken in relation to many of those agreements. This would likely require complex negotiations and be a time-consuming process which, for non-SFIs, would require significant additional resources to be applied to meet that requirement, which seems disproportionate to the objectives of CPS 230.

Accordingly, to reduce complexity for non-SFIs, we are of the view that CPS 230 should be structured such that non-SFI's are not subject to all obligations within this section of CPS230. A key example is the current paragraph 52(a), which appears to require an APRA-regulated entity to undertake a tender and selection process in relation to all material service providers (which would include all third-party service providers that are in scope for the purposes of CPS 234). This is particularly onerous in circumstances where the obligation to undertake a tender and selection process seems to apply even where the arrangement is only being renewed or materially modified.

Operational Risk Management

The draft Standard sets out new requirements for regulated entities in relation to managing operational risk. Whilst Tyro acknowledged that the management of operational risk is important, we are concerned that the draft Standard does not appropriately balance obligations based on the nature and size of regulated entities. Our view, is that the clauses [26]-[30] which set out the requirements to implement, design and embed internal operational risk controls and testing across all products, activities, processes and systems are particularly onerous for smaller entities and will again require significant resources in order to uplift and implement these requirements and a more proportionate approach should be considered.

4. ***What are the estimated compliance costs and impact to meet the new and enhanced requirements?***

We anticipate that the new and enhanced requirements will have a significant impact on compliance costs. For example:

- smaller APRA-regulated entities, like Tyro, will be required to update and uplift contracts with existing providers to meet the new contractual obligations. This process may require complex negotiations with little commercial outcome;
- the requirements for managing operational risk controls and testing will require significant investment in human capital, in an already tight talent market;
- entities may require new software or planning tools to assist in meeting the enhanced obligations; and
- the internal, regular monitoring and reporting to senior management on material service provider arrangements is likely to entail significant costs.

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

Industry specific examples that support the definitions would enable regulated entities to fully understand APRA expectations of what would meet the definition of a 'critical operation', appropriate 'tolerance level' and 'material service provider' relevant to their respective industry. Further guidance by way of practical examples would be beneficial in relation to the following terms:

- 'Material adverse impact'
- 'Material financial impact'
- 'Minimum service level'

6. ***What additions or amendments should be made to the lists of specified critical operations and material service providers?***

Please refer to our response to questions 2 & 5.

We add that, in our view, paragraph 50 of CPS 220 should be deleted for the following reasons:

- specifying under paragraph 50 of draft CPS 230 that 'material service providers' includes all providers that manage critical or sensitive information assets potentially leads to a

disproportionate regulatory outcome (as described in our responses to questions 2 and 3 above); and

- the existing general definition of a material service provider (ie those upon which an entity relies to undertake a critical operation or that expose it to material operational risk) is independently sufficient, where relevant, to capture any service providers that manage critical or sensitive information assets.

7. Are the notification requirements and the time periods reasonable?

Greater clarity on the reporting timeframes is requested, particularly whether entities will be required to submit and report against CPS 230 activities to APRA as at 1 January 2024. We would also appreciate clarity on whether APRA expects regulated entities to submit BCP plans to APRA on an annual basis. APRA has suggested in the Discussion Paper that regulated entities will be required to submit BCP plans to APRA on an annual basis, this requirement however does not seem to appear in the draft CPS 230.

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

As currently drafted, we expect contracts with existing providers will require update and uplift to meet the new contractual requirements under CPS 230. As mentioned previously, this is a complex and time-consuming process, which is often highly dependent on the specific service provider (and their appetite to negotiate amendments to contracts, which is often low in the context of non-SFIs dealing with technology providers that operate on a global scale). The proposed CPS 230 requirements may lead to prolonged and difficult negotiations with many providers, noting that the minimum requirements deal with issues that are generally the most contentious aspects of contracts, such as liability, indemnity, ownership and control of data and termination provisions. Smaller APRA-regulated entities are at a distinct disadvantage as opposed to larger APRA-regulated entities with significantly more market power.

Noting the above and that the practical guidance for CPS 230 is yet to be finalised and is not expected until mid-2023, the anticipated timing for commencement of the Standard leaves organisations with a limited opportunity to fully appreciate its application. With this is mind, we ask that APRA take this into consideration when finalising the timeframe for commencement of CPS 230. Noting that the proposed CPS 230 requirements are broader and more complex than those under CPS 234 (for which there was a 12-month transition period), we suggest, at minimum, an 18 to 24-month transition period.

Tyro would welcome the opportunity to participate in further consultations as the Prudential Standard is developed.

Yours sincerely,

[redacted]
Head of Compliance