Mercer

welcome to brighter

Mercer (Australia) Pty Ltd
ABN 32 005 315 917
Collins Square
727 Collins Street
Melbourne, VIC Australia 3008
GPO Box 9946 Melbourne VIC 3001
T +61 3 9623 5464
www.mercer.com.au

[redacted]
General Manager, Policy
Australian Prudential Regulation Authority

Via email: policydevelopment@apra.gov.au

21 October 2022

Subject: **Strengthening operational risk management**

Dear [redacted]

Thank you for the opportunity to provide feedback in response to APRA's discussion paper *Strengthening operational risk management* (**Discussion Paper**) and the draft Cross Prudential Standard CPS 230 *Operational Risk Management* (**CPS 230** or **Standard**).

***Executive Summary***

In a time of rapidly evolving technology and increasing risk and complexity, the sound operational risk management and operational resilience of APRA-regulated entities is a key priority. Mercer welcomes APRA's initiative to consolidate and enhance operational risk requirements in this context.

In considering APRA's Discussion Paper and draft CPS 230 from the superannuation industry perspective, two key questions arose – What is the actual impact of these reforms? How will they benefit member outcomes? Undoubtedly, a proactive, accountable and mature approach to operational risk and resilience is beneficial to member outcomes. However, while APRA has identified that it expects the reforms in CPS 230, as outlined in the Discussion Paper will have "no material impact" on the efficiency of APRA-regulated bodies, in reality, the CPS 230 reforms are substantive. Mercer is concerned that the new Standard will result in a significantly increased compliance burden both in the implementation stage and ongoing business as usual, which will lead to additional costs and decreased efficiency for superannuation funds and their service providers. This, ultimately, will adversely impact member outcomes.

We have identified the following key issues arising from the proposed new CPS 230:

- *Guidance* – clear industry-specific guidance will be critical to better ensure CPS 230 is properly interpreted, implemented and embedded within organisations across the various APRA-regulated entities. In particular, considered guidance is needed with regards to the key definitions of 'critical operations' and 'material service providers', as well as the relationship between CPS 230 and other prudential standards as they relate to risk. From Mercer's perspective, we believe there are some critical differences between superannuation funds and say, banking or insurance.

- *Material service providers and fourth party providers* – the definition of 'material service provider' is so broad as to potentially encompass all providers of critical operations. This will significantly increase the burden on compliance, risk, legal and procurement functions to manage implementation of CPS 230 and ongoing business as usual. Mercer recommends a materiality threshold be applied.

  In addition, further guidance is needed regarding fourth party provider requirements and APRA's minimum expectations.

- *Commencement date and transition period* – the lack of a transition period will put a significant strain on organisations at a time when there are other significant reforms in train, most notably the Financial Accountability Regime (which also has a "hard" start date of 1 January 2024); this is the case for both RSE licensees and service providers.

  APRA-regulated entities will need time to review all existing service providers against the broader definition of 'material service provider' (this list will likely be significantly longer under that definition), and then renegotiate service provider agreement terms for compliance with CPS 230. This will substantially impact governance, risk and compliance, legal and procurement resources.

  Service providers will also be impacted by the lack of transition period; for example, superannuation fund administrators with large numbers of superannuation fund clients, all seeking to renegotiate service agreements over the 6 - 8 month period prior to 1 January 2024. This will place severe pressure on service providers and will likely result in a bottleneck as providers seek to work with clients on any necessary changes. There is also the potential scenario for non-APRA regulated service providers to refuse accommodating the additional provisions in legal agreements, which may trigger a need to consider alternate arrangements.

- *Costs* – having regard to the points above, there will likely be significant implementation and ongoing costs to superannuation funds and their services providers, which is likely to lead to increased fees for superannuation members. It is difficult to quantify a financial cost at this stage but costs will flow from impact on legal, risk and compliance functions, as well as procurement.

***Responses to specific questions from the Discussion Paper***

Our responses to the specific questions raised in the Discussion Paper are set out in the Appendix.

***About Mercer***

Mercer believes in building brighter futures by redefining the world of work, reshaping retirement and investment outcomes, and unlocking real health and well-being. Mercer's approximately 25,000 employees are based in 43 countries and the firm operates in 130 countries. Mercer is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people, with 83,000 colleagues and annual revenue of over $20 billion. Through its market-leading businesses including Marsh, Guy Carpenter and Oliver Wyman, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment.

In the Pacific region, Mercer Australia is a trusted adviser and guardian to our clients and members. We look after the superannuation benefits of over two million members in over 30 corporate stand-alone, public sector funds and industry funds and in the Mercer Super Trust (which includes approximately 230 corporate clients). We provide customised administration, technology and total benefits outsourcing solutions to our clients, and our expertise in administering and managing the investments of diverse, complex superannuation benefit designs is well recognised. Our clients include some of the world's leading organisations in both the public and private sectors, as well as many smaller rapidly growing organisations seeking best practices in order to gain competitive advantage.

We would be happy to discuss this submission in more detail at your convenience. Please do not hesitate to contact me to arrange.

Yours sincerely,

**Senior Partner**

# APPENDIX

## Feedback responses

### *1. Is the single cross-industry standard for operational risk management supported?*

The cross industry standard approach taken for CPS 230 is consistent with the Australian Prudential Regulation Authority's (**APRA**) strategic initiative to modernise its prudential framework. Mercer generally supports this initiative and the application of a cross-industry standard where there is commonality across sectors, as is the case with requirements for risk management, business continuity planning and management, and service provider risk management.

However, the consolidation of a number of existing prudential standards into a single cross-industry standard means that, overall, CPS 230 is more principles-based than the existing standards. In practice, this may present implementation challenges, having regard to the distinct functions and activities of, and legal frameworks supporting, each sector – for example, a Responsible Superannuation Entity (**RSE**) licensee is likely to have more complex outsourcing arrangements as compared to a friendly society, whilst an insurer is likely to be significantly more affected by a business disruption impacting underwriting than a RSE licensee. Much will depend on the guidance issued by APRA to support CPS 230 and the level of sector-specific detail to ensure that CPS 230 can be properly interpreted, implemented and embedded into organisations.

To address this issue, Mercer recommends that APRA delays issuing CPS 230 until it has consulted on the draft guidance or, preferably, until it is in a position to publish the Standard and accompanying guidance, relevant for each industry.

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

As noted above, industry-specific guidance will be critical to ensure APRA-regulated entities properly apply and comply with the requirements of the new Standard. The guidance should contain sufficient detail, including industry-specific case studies and examples, without being overly granular or prescriptive.

Specific areas or topics for guidance may include:

- *Interaction with existing prudential standards and other relevant regulatory requirements*

The Discussion Paper touches only briefly on the relationship between CPS 230 and other APRA prudential standards and guidance.[1]

Mercer recommends that APRA provide further guidance on the interaction between CPS 230 and the other prudential standards and guidance that relate to risk management.

In this regard, we note table 2 on page 13 of the Discussion Paper sets out APRA's proposed new "framework for operational resilience":

| Operational resilience | Prudential Standard | Guidance |
|---|---|---|
| Operational risk management | CPS 230 | CPG 230<br>CPG 233 *Pandemic Planning*<br>CPG 235 *Data management*<br>SPG 223 *Fraud risk management – Superannuation only* |
| Information security | CPS 234 *Information Security* | CPG 234 |

We submit that for RSE licensees, the following standards are also relevant in the context of operational risk and resilience, and should be considered as forming part of the framework:

- SPS 220 *Risk Management*;
- SPS 114 *Operational Risk Financial Requirements*;
- CPS 190 *Financial Contingency Planning*[2];
- SPS 515 *Strategic Planning and Member Outcomes;*
- SPS 520 *Fit and Proper;*
- SPS 521 *Conflicts of Interest.*

APRA has also recently conducted consultation with the superannuation industry with respect to strengthening financial resilience and the importance of having adequate financial resources to fund their business operations. The Discussion Paper and CPS 230 are silent on the intersection between financial resilience and operational risk management (and operational resilience).

In Mercer's view, without clear guidance, overlap between CPS 230 and other prudential standards may create confusion for entities, particularly if there are actual or apparent inconsistencies between the standards and guidance.

[1] CPS 230 itself refers to the requirements for operational risk in SPS 220 *Risk Management*, SPS 114 *Operational Risk Management* and APRA's powers to increase the target amount in certain circumstances, and the requirements for information security in CPS 234 *Information Security*.

[2] As CPS 190 is a cross industry standard it should form part of the "framework for operational resilience" for all APRA-regulated entities.

Finally, we note that guidance on the interaction of notification requirements with breach reporting and other notification requirements, taking into consideration consistency of terminology / interpretation; timeframes and, where possible, possibilities for "deemed notification". We have considered this further below in relation to Question 7.

- *Service provider requirements*

  In our view, further detail is required regarding APRA's expectations with respect to management of material service providers and fourth party providers, particularly addressing the following matters:

  - The statement in CPS 230 that a regulated entity must not rely on a service provider unless it can ensure it can continue to meet prudential obligations in full and effectively manage associated risks. This statement is extremely broad and appears to extend beyond the critical operations and material service provider concepts in the Standard. In our view, this should be limited in application to providers of critical operations.
  - How an APRA-related entity is to assess whether a service provider is "systemically important in Australia".
  - Fourth party providers – to what extent are APRA-regulated entities and their service providers to look down the supply chain? Also, what are the obligations on APRA-regulated entities where a material service provide will not, or cannot (because of confidentiality requirements in their own agreements, or lack of adequate governance arrangements), provide the details of a fourth party provider?

    Mercer is concerned that the time and cost associated with seeking information on fourth party providers (and their service providers, and so on) and applying the requirements as envisaged under CPS 230, will outweigh the benefit of the exercise. A third-party service provider may rely upon numerous service providers to provide the service, with varying degrees of relevance and materiality to the services ultimately provided to the APRA-regulated entity.

    Mercer recommends APRA provide guidance on its minimum expectations with respect to fourth party service providers and management of fourth party risk. We consider that a pragmatic approach is needed in this respect. For example, managing this risk via contractual arrangements regarding third-party service provider liability for subcontractors / service providers (as per paragraph 53(e) of the Standard), or limiting the requirements in CPS 230 to fourth-party providers and only to the extent that failure of that fourth party would have a material adverse impact on the APRA-regulated entity or the third-party service provider's ability to provide the service to the APRA-regulated entity.

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

Mercer welcomes APRA's intention to strengthen operational risk management requirements in a proportionate manner. Taking a proportional approach reduces the compliance burden for smaller and less complex entities.

However, we note that the principles of proportionality are not always borne out in CPS 230. While certain elements of the Standard are high-level and principles-based, the Standard also contains certain prescriptive requirements and granular detail appearing to apply regardless of size, business mix or complexity of the entity – for example, the prescribed critical operations at paragraph 35 and material service providers at paragraphs 49 and 50; also with regards to setting tolerance levels. We therefore recommend that the Standard use explicit language around proportionality of requirements when finalising the Standard (rather than relying on the overarching statement currently found in the *Objectives and key requirements* section at the beginning of the Standard).

Mercer is of the view that CPS 230 should apply to all APRA-regulated entities, irrespective of whether they are SFIs or non-SFIs, provided it is clear in the Standard that the requirements must be implemented having regard to the size, business mix and complexity of the relevant entity.

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

The Discussion Paper states that APRA expects there will be "no material change" on the efficiency of APRA-regulated entities. Mercer disagrees. We anticipate that the proposed reforms in CPS 230 have the potential to impose significant costs on industry (both for regulated-entities and service providers) – which will ultimately be borne by members and impact member outcomes. Without guidance indicating the degree of granularity that APRA expects for compliance, it is difficult at this stage to quantify the financial costs to APRA-regulated entities and service providers as a result of complying with the enhanced requirements. However, we expect costs and impacts in the following areas:

- *Resource costs*
  - Implementation – the reforms will impact legal and procurement resources, as well as management and enterprise risk and compliance, noting APRA-regulated entities will have to, among other things:
    - identify 'material service providers' and fourth party providers and create a register to be provided to APRA – this list will likely be longer than previously identified, given the significantly expanded definition of 'material service provider' in CPS 230;
    - review and renegotiate service provider agreements by the proposed commencement date of 1 January 2024;
    - update and uplift policies and governance documents, and processes, particularly in the areas of compliance and risk, outsourcing and procurement.

The implementation of CPS 230 will come at a time when there are other significant reforms in train for RSE licensees, most notably the Financial Accountability Regime (**FAR**) which, we note, comes into effect on 1 January 2024 with no transition period. Similar impacts will be felt for service providers who service numerous APRA-regulated entities; for example fund administrators providing superannuation fund administration services to fund trustees.

*Example: Mercer Outsourcing (Australia) Limited (**Mercer Outsourcing**) currently services 21 administration clients – having regard to CPS 230 in its current form (in particular, noting there are no transition requirements) Mercer Outsourcing may be required to renegotiate all administration client contracts within a 6 month period leading up to 1 January 2024. This will have a significant impact on legal and procurement resources and will likely result in a "bottleneck" as Mercer Outsourcing seeks to work with clients to amend the agreements as required. Other administrators are likely to be under similar pressure.*

- Ongoing – there is likely to also be ongoing legal and procurement, and risk and compliance, resourcing pressure and costs. These arise primarily as a result of the enhanced operational risk management obligations which will apply to a larger number of service providers, and also due to the requirement for APRA-regulated entities to undertake an appropriate tender and selection process before entering into, renewing or materially modifying an arrangement with a material service provider.

  In this respect, Mercer recommends APRA reconsider the prescribed tender requirements and instead leave this to the discretion of the APRA-regulated entity, having regard to the context of the outsourcing arrangement, and the size, business mix and complexity of the entity. In our view, undertaking a tender process may not always be practical or appropriate, noting the costs (for both the trustee and tendering parties) and timeframes associated with the tender process.

  Mercer recommends that CPS 230 specifically address use of benchmarking exercises as an acceptable approach for trustees to assess member value from outsourcing arrangements. This aligns with observations recently published by APRA on the thematic review of the management of outsourcing arrangements.

- *Audit & Assurance costs*

It is expected that CPS 230 will trigger a significant increase in audit and assurance costs, where RSEs seek deeper levels of assurance across operational risk management – e.g. information technology controls; compliance and governance controls; monitoring third and fourth parties. While existing audit and assurance practices (e.g. GS007) play an important role, their coverage is generally broad and not deep.

Additionally, this is likely to present a significant issue for Mercer Outsourcing and other fund administrators; the volume of client (RSE) initiated audit activity could increase to the extent that it materially affects operating efficiency and effectiveness of administration services. Responding

to multiple audit requests has the potential to divert key resources away from servicing member outcomes.

Through the sheer volume of assurance activity to be performed across Financial Services due to the CPS 230 mandate (as currently drafted), exponential demand for assurance providers will increase assurance pricing, with costs ultimately borne by members.

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

We have considered this question as part of our response to question 6 below.

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

Mercer is of the view that more clarity is required regarding the concepts of 'critical operations' and 'material service providers', as set out below. In addition, the specified critical operations and material service providers listed at paragraphs 35, 49 and 50 respectively should be expressed as examples, rather than prescribed operations and services to better reflect APRA's stated intention that CPS 230 be applied proportionately, and having regard to the different operating models, business and strategic objectives and legal frameworks across the various APRA-regulated sectors.

- *Critical operations*

  The definition of 'critical operations' is located at paragraph 34 of the Standard as:

  > "*processes undertaken by an APRA-related entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system*".

  This is slightly different from the concepts of 'critical business operations' and 'material business activities' in SPS 232 *Business Continuity Management* and SPS 231 *Outsourcing* respectively, both of which are limited in context to *business.* The definition of 'critical operations' in CPS 230 is broader, capturing a wider range of operations and activities and potentially extending beyond the scope of 'business' to areas such as software licensing, facilities management, utilities and resourcing. It is not clear whether this is APRA's intention; it would be beneficial if the definition could be clarified. For example, using industry-specific examples in accompanying guidance material. APRA could also consider specifying which operations or activities are *excluded* from the definition (rather than prescribing certain operations and activities).

- *Material Service Providers*

  CPS 230 includes a significantly broader definition of 'material service providers' at paragraph 48. Potentially, the definition is so broad as to capture <u>any</u> service provider on which the entity relies to undertake a critical operation or a part of a critical operation. Mercer recommends APRA introduces a materiality threshold to ensure that the requirements only capture service providers

that are relied on substantively for critical operations. This would better align with the principles of proportionality and ease the compliance burden on APRA-regulated entities both in terms of implementation and ongoing compliance.

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

CPS 230 provides for the following notification requirements and timeframes:

- *Operational risk incident (paragraph 32)*: within 72 hours after becoming aware of an operational risk incident that is likely to have a material financial impact or a material impact on the entity's ability to maintain its critical operations;
- *Activation of BCP (paragraph 41)*: within 24 hours if an entity has activated its BCP;
- *Entry into or material change to service agreement for critical operation (paragraph 58(a))*: within 20 business days after entering into or materially changing an agreement for the provision of a service relied upon to undertake a critical operation;
- *Entry into or material change to offshoring agreement with material service provider (paragraph 58(b)*): prior to entering into any offshoring agreement with an MSP or when a significant change is proposed to such an agreement.

APRA regulated entities must also provide a list of material service providers to APRA "on an annual basis". We note that the timeframe for submission of the list has not been specified and recommend that a timeframe is provided for this reporting requirement (for example, within three months of 31 December of the prior year).

In isolation, the notification requirements and timeframes proposed in the Standard are reasonable. However, these obligations should be considered in the context of other notification requirements imposed on APRA-regulated entities – for example, notification requirements for superannuation fund trustees include:

- RSE licensee significant breach reporting to APRA;
- breach of risk management framework, reporting to APRA;
- Australian Financial Services (**AFS**) licensee breach reporting to the Australian Securities and Investments Commission (**ASIC**) (reportable situations);
- eligible data breach reporting requirements to the Office of the Australian Information Commissioner (**OAIC**);
- information security incident reporting to APRA under CPS 234 *Information Security*;
- suspicious matter reporting and annual compliance reporting to the Australian Transaction Reports and Analysis Centre;
- notification of changes to MySuper Product Dashboard to APRA;

- notification of prescribed matters to APRA regarding an RSE licensee's provision of insured benefits to beneficiaries under SPS 250 *Insurance in Superannuation*;
- other notification obligations under the *Superannuation Industry (Supervision) Act 1993* and the *Corporations Act 2001* (for example, notification of change in directors / responsible managers / responsible persons; changes in superannuation entity details).

*Example: An Optus like cyber breach is a definitive example that illustrates the broad notification requirements that would be triggered through multiple regulatory / legislative reporting obligations. Such an event would certainly constitute a breach under CPS 230 (as it would be classified as a material operational risk incident required to be reported to APRA, if it had not already been reported as an information security breach under CPS 234), as well as a potential reportable situation (ASIC breach of AFS licence obligations to maintain adequate compliance arrangements) and also potentially trigger reporting requirements to the OAIC.*

Mercer therefore recommends that to the extent possible, APRA aligns and streamlines the notification requirements, including considering "deemed reporting" relief such as has been flagged in the context of CPS 234 information security incident reporting.

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

Currently APRA envisages that CPS 230 will take effect from 1 January 2024 and will apply to all existing material service provider agreements, as well as agreements with service providers who qualify as material service providers. Noting that APRA has not yet commenced consultation on guidance, and does not intend to finalise the standard until 2023, this leaves a significantly condensed timeframe within which APRA-regulated entities and service providers must prepare. Without reasonable and appropriate transition requirements, Mercer considers that the implementation date of 1 January 2024 is impractical and will create pressure for APRA-regulated entities and service providers (and as noted earlier, at a time when RSE licensees are also preparing for the commencement of FAR which will also come into effect on 1 January 2024).

We have noted earlier in our submission the anticipated increase in compliance burden and impact on resources and costs to ensure the CPS 230 requirements are implemented prior to 1 January 2024. Transitional timeframes would ease this pressure and prevent bottlenecks for service providers. Mercer recommends that existing outsourcing agreement requirements under SPS 231 *Outsourcing* be held over or grandfathered until such time as the arrangements are scheduled for renewal or review, or a material amendment is proposed, with all material service provider agreements required to be updated in accordance with CPS 230 within three years of the Standard coming into effect. In our view, this timeframe is practical and reasonable having regard to the work and cost required both for APRA-regulated entities and their service providers.

With respect to the other requirements in the Standard, Mercer is of the view that a minimum of six months from the date the final CPS 230 *and* accompanying guidance is published would be required to allow entities sufficient time to properly implement the requirements under the Standard.