Sydney

Level 2, 5 Martin Place
Sydney NSW 2000 Australia
GPO Box 3698
Sydney NSW 2001
www.challenger.com.au

Telephone 02 9994 7000
Facsimile 02 9994 7777

21 October 2022

General Manager, Policy
Policy and Advice Division
Australian Prudential Regulation Authority
Level 12
1 Martin Place
Sydney NSW 2000

Sent via email to: PolicyDevelopment@apra.gov.au

Dear Sir / Madam

Thank you for the opportunity to comment on APRA's draft prudential standard CPS 230 *Operational Risk Management* (CPS 230). This submission is made on behalf of Challenger Limited, Challenger Life Company Limited, Challenger Retirement and Investment Services Limited, and Challenger Bank Limited (Challenger).

We agree that operational resilience is critical for ensuring that financial institutions operate effectively to meet the commitments made to individuals, whether they are policyholders, beneficiaries, or customers. Challenger supports the important initiative by APRA to review, strengthen and streamline regulatory requirements concerning operational risk management, business continuity planning and third-party risk management, and welcomes the opportunity to provide our feedback on the framework's design and its implementation.

Overall, the proposals, although principles based, will require a significant uplift in practices for operational risk management and in doing so APRA's proposals have the potential to impose increased compliance costs on the industry. In particular, we would like to bring to APRA's attention that setting risk framework requirements at a low and granular level may have unintended consequences and hinder the ability of the Board of Directors and Senior Management to appropriately focus on material risks and issues. We do not believe this was APRA's intention and in response to your questions below we seek to bring these areas of concern to your attention.

Responses to Key Questions in the Discussion Paper:

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

Challenger is supportive of a single cross-industry standard for operational risk management. The draft CPS 230 however significantly uplifts expectations on operational risk management, and although the concept of proportionality applies, some of the increased requirements may result in significant increases in compliance costs.

For example, at present, Challenger Limited (and its consolidated entities) has approximately 290 'critical business operations' as defined in CPS 232 *Business Continuity Management* (CPS 232). Challenger seeks clarification as to whether the definition of critical operation in CPS 230 is proposed to be set at a similar level as 'critical business operations' in CPS 232.

Challenger Limited ABN 85 106 842 371 Challenger Group Services Pty Limited ABN 91 085 657 307
Challenger Life Company Limited ABN 44 072 486 938 AFSL 234670
Challenger Investment Partners Limited ABN 29 092 382 842 AFSL 234 678
Challenger Retirement and Investment Services Limited ABN 80 115 534 453 AFSL295642 RSE Licence No. L0001304
Challenger Mortgage Management Pty Ltd ABN 72 087 271 109 Challenger Securitisation Management Pty Ltd ABN 56 100 346 898 AFSL 244593
Challenger Investment Solutions Management Pty Ltd ABN 63 130 035 353 AFSL 487354

Although Challenger's critical business operations are covered by documented business continuity plans, the Challenger operational risk framework (for example, the processes, risks, controls and material service providers) have not been defined at such a low operational business level.

The requirement, per paragraph 26(b) of CPS 230, requires the 'APRA regulated entity to identify and document the processes, and resources needed to deliver critical operations including people, technology, information, facilities and service providers, the interdependencies across them and the associated risks, obligations, key data and controls'. While Challenger captures these elements across the organisation, applying this definition to 290 critical business operations would require significant re-work of our operational risk framework to ensure all of the processes, risks, controls and material service providers are captured and documented at this detailed level. Utilising this definition of critical operation would also increase the list of material service providers that are required to be captured, and therefore materially increase both business and management time required to monitor these service providers.

We do not expect it was APRA's intention to require the construction of the operational risk register and the material service providers at such a granular level. We would therefore appreciate if APRA could provide further guidance clarifying the level that a critical operation is to be defined for the purposes of the operational risk framework, and would recommend that this is set at a higher level than that currently defined in CPS 232.

In taking a single cross-industry standard approach, we would appreciate if APRA could consider incorporating the requirements of the 2018 Information Paper on Outsourcing Involving Cloud Computing Services (APRA Cloud Paper) into CPS 230. At present although the Discussion Paper references the growing use of cloud-based services, there are no specific requirements for cloud-based arrangements in CPS 230. Incorporating the APRA Cloud Paper requirements into CPS 230 would clarify APRA's expectations for cloud-based arrangements, and streamline the compliance requirements for APRA-regulated entities.

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

Please see below for a list of areas where guidance would be useful:

- APRA could clarify whether an arrangement with a related body corporate is intended to be captured by all of the requirements of CPS 230. Paragraph 27 of CPS 231 Outsourcing (CPS 231) includes a reduced set of requirements for related body corporate arrangements, taking into consideration that some of the steps required under paragraph 26 of CPS 231 may be unnecessary, such as the need to prepare a business case, undertake a tender process and perform due diligence. CPS 230 has no such exclusions for related body corporate arrangements. Challenger has several related body corporate arrangements, which are due to the functional nature of our business, and the remuneration of our staff by two entities in the group. Therefore, we request that APRA excludes related body corporate arrangements from some of the requirements in CPS 230, and in particular the requirement to prepare a business case, undertake a tender process and perform due diligence.
- APRA could provide guidance and examples on what would be considered to be a reportable operational risk incident and the examples of the format and information APRA would like to be included in the notification? Please see our response to Question 7 for further information.

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

We do not have any feedback regarding proportionality as it is addressed in the standard, other than as mentioned in the response to Question 1.

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

As per our response to some of APRA's other questions, the compliance costs will be dependent on the final standard, their interpretation, and whether feedback provided by Challenger, other APRA-regulated entities and the industry are incorporated into these requirements.

If the standard is implemented in its current form the compliance costs would be significant for Challenger and would include the following key activities:

1. Undertaking a project to identify and document all of the processes, service providers, risks and controls to support the critical operations.
2. Revisiting all of the critical business operations to ensure that the tolerance levels meet the requirements of paragraph 37 of CPS 230.
3. Building a new Board and Senior management governance approach for the oversight of control gaps, weaknesses, and risk and performance reporting on material service provider arrangements.
4. Increasing the length of the Board meetings with supporting workshops to take the Board through all of the tolerance levels that have been set across the critical operations.
5. Setting up new arrangements with existing service providers that meet the threshold for a material service provider. We expect this will be an extensive exercise, and is further explained in response to APRA's Question 8.
6. Developing a material service provider policy and supporting processes. Significant effort will need to go into building frameworks and requirements for assessing fourth party service providers if this is required.
7. Reviewing and updating all other relevant policies such as the Incident Management Policy and BCM Policy to align to the CPS 230 requirements.

If APRA addresses some or all of the feedback we have provided then the compliance effort and cost will be materially reduced.

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

Critical Operations

As per our response to Question 1, the level that critical operations are defined is important and has follow-on effects to the definition of material service provider, the requirements for inclusion in the operational risk framework and the business continuity requirements. We would recommend that APRA seeks to clarify this definition and we suggest that a separate definition of critical operation is used to support the operational risk framework and material service provider requirements from the definition used to underpin the business continuity requirements which should be at a more granular level.

Material Service Provider

There are two points that we would appreciate APRA considers in its definition of material service provider.

Point 1 – Applying a materiality level to a material service provider

APRA has defined a material service provider as 'those on which the entity relies on to undertake a critical operation or that expose it to a material operational risk'. APRA has not (similar to CPS 231 para 14(a)-(f)) defined the factors that should be considered when making this determination. This may unintendedly require an APRA regulated entity to define service providers as material, albeit the service they are performing may not materially impact a critical operation. For example, Paragraph 49 of CPS 230 states that material service providers include investment management. An investment manager may be managing a very small / immaterial amount, and be providing a service that is easily transferable and as such may have previously been considered as not a material outsourcing arrangement under CPS 231. Under CPS 230 it appears that this same service would automatically be considered material.

In addition, the list of material service providers articulated in Paragraph 49 of CPS 230 does not utilise a materiality threshold and therefore would benefit from the insertion of 'may' to state 'Material service providers may include…'.

Point 2 – Potential exclusions

The proposed definition of material service providers in CPS 230 does not clarify whether it is intended to capture several types of arrangements which were excluded from CPS 231 as stated in PPG 231, including:

- Short-term arrangements where the agreement is less than 12 months old; and
- Contractor relationships, such as utility services, legal services, advertising, recruitment, printing services and software licencing arrangements.

We request that APRA provides further guidance and clarity on its intentions, but would recommend that the types of arrangements noted above remain excluded from the requirements, otherwise this would create additional compliance costs where the underlying service may be easily replaced.

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

We believe the list of services to be appropriately set where the level a critical operation should be defined.

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

The notification requirements for an Operational Risk incident of 72 hours may be challenging to meet, depending on the level of information that APRA requires to be included in the incident notification. Comparatively ASIC's revised breach reporting requirements for AFS and credit licensees requires notification within 30 calendar days from identification of the reportable situation. We request that APRA considers extending the incident notification timeframe to align to that introduced by ASIC. We would also like to request further guidance and examples on what APRA would considers is a reportable operational risk incident and what information APRA would like to be included in the notification.

The requirement to notify APRA as soon as possible and no later than 24 hours, if it has activated its BCP is reasonable.

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

The timeframes required to renegotiate contracts with existing service providers will depend on the quantity of service providers that are required to be captured under definition of material service provider. As per our response to Question 1, this will be dependent on on the level that a critical operation is set.

At present, Challenger has 23 material outsourced service provider arrangements (noting some of these are internal arrangements). As the contractual term requirements between CPS 231 and CPS 230 for material arrangements are similar, we recommend that APRA allows these arrangements to be grandfathered, until they are revisited at their scheduled next renewal date at which point the arrangements can be transitioned to comply with CPS 230.

The transition of other material service provider arrangements that have previously not been captured under CPS 231 will be an extensive exercise. In all of these cases, the contracts will need to be renegotiated, APRA required terms included and additional risk assessment steps conducted. We recommend that APRA allows APRA-regulated entities at least 24 months to transition these arrangements.

<u>Additional points for APRA's consideration</u>

A. Role of the Board

Challenger supports the Board having accountability of the overall operational risk framework, however we believe APRA should provide APRA-regulated entities with discretion to delegate elements to management, particularly those activities that are more operational in nature. At Challenger we believe in providing the Board with timely and appropriate information to allow the Board to effectively discharge their responsibilities and have strong governance and oversight of the Challenger group's operations, strategies and risks.

CPS 230 seeks to introduce specific and detailed requirements for the Board, for example, to approve tolerance levels for disruptions to critical operations. It is our view that such detailed activity should be delegated to management rather than be required to be performed by the Board. Challenger's business continuity plans (BCPs) and tolerance levels are documented at a granular level and the requirement for the Board to approve all tolerance levels would require a greater involvement by the the Board and may restrict or distract the Board from undertaking their other duties and identifying other material risks and issues.

B. Fourth-Party risk management

We note the new requirement for APRA-regulated entities to manage the risks associated with any fourth parties that support the delivery of a material service. Challenger's third-party service providers may utilise multiple fourth parties to deliver their services. We believe the consequences associated with a failure of a fourth party are already considered and addressed by paragraph 53(e) of CPS 230 which requires the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider. To require APRA-regulated entities to look through to fourth parties will be an extensive exercise, particularly if we have not had any experience or exposure with that fourth party. The look through will likely require a full risk assessment which could be particularly onerous if the third-party service provider is not regulated by APRA, and therefore does not maintain a register or make assessments of material service providers. We would recommend that APRA considers removing this requirement.

C. Service provider agreements

Paragraph 52 of CPS 230 states that an APRA-regulated entity must undertake an appropriate tender and selection process before entering into, renewing or materially modifying an arrangement. We agree that an APRA-regulated entity should undertake an appropriate tender and selection process before entering into a new material service provider arrangement, but would like to raise that this may not be appropriate for renewing or materially modifying an existing arrangement, particularly if the service provider has been performing well, meeting all of their service levels, and there is no material change to the financial and non-financial risks associated with the service provider, as already covered by the assessment in section 52(b) of CPS 230.

Additionally, we do not agree that an APRA-regulated entity should be required to assess whether the provider is systemically important in Australia, as required by paragraph 52(c) of CPS 230. It may not be possible for an APRA-regulated entity to be able to perform this assessment, considering we may not have information from the service provider regarding their other clients, and the nature and criticality of those services provided. We would suggest that APRA obtains this information from the collection of each APRA-regulated entity's register of material service providers.

Final words

Thank you for giving Challenger the opportunity to comment on the proposed standard. Should you have any questions in relation to the items raised, please contact me.

Yours faithfully

[redacted]

Chief Risk Officer
Challenger Limited