Members Health Fund Alliance

Submission on APRA's proposed *Prudential Standard CPS230 Operational Risk Management*, October 2022.

Members Health FUND ALLIANCE

Putting members' health before profit

Members Health
FUND ALLIANCE

21 October 2022

[redacted]
General Manager, Policy
Policy and Advice Division
Australian Prudential Regulation Authority

By email: policydevelopment@apra.gov.au

Dear [redacted]

Consultation on APRA's proposed Prudential Standard CPS230 Operational Risk Management

Members Health Fund Alliance (Members Health) welcomes the opportunity to provide its comments on issues raised in the Australian Prudential Regulation Authority's Discussion Paper: *Strengthening operational risk management* and on its proposed *Prudential Standard CPS230 Operational Risk Management* (CPS 230).

Our Alliance of 26 not for profit and member-owned funds represents more than 35 per cent of the private health insurance (PHI) market. Members Health supports a robust and fit-for-purpose prudential framework that ensures appropriately structured and systematic approaches are in place to identify and manage operational risk.

The PHI industry has, along with other APRA-regulated industries, experienced a number of disruptive events over the past few years (such as Covid-19), however not only has it been resilient, it has also achieved greater consumer confidence as evidenced by rising participation in taking up private health insurance.

Members Health is facilitating a joint response led by our Governance, Risk and Compliance Committee on behalf of its participating funds to raise a number of concerns in relation to the practical implementation of the proposed prudential requirements.

The key areas for concern relate to:

1. When specifying a requirement, the use of 'absolute' terms does not allow for an entity's compliance to be commensurate with its size, business mix or complexity.
   Recommendation: incorporate the feedback provided in Attachment A

2. Learnings have not been incorporated from implementing past standards where the ambiguous use of specific terms were open to interpretation and therefore difficult for auditors to assess whether an entity was compliant.
   Recommendation: incorporate the feedback provided in Attachment B

3. The implementation date falls outside an ordinary compliance cycle where CPS-220 requires entities to submit a declaration that they are compliant with a standard between 1 July – 30 June each year. If the new standard is implemented in January it would mean entities will be required to conduct their annual reviews of the efficacy of their operational resilience within six months after adoption of the standard.

   We would also like to draw attention to the significant effort for PHI insurers to implement CPS-230 compared to other industries that are already compliant with the higher compliance thresholds of CPS-231 and CPS-232.

   Recommendation: extend the implementation date to 1 July 2024

With consideration of the substantive increase in compliance obligations for PHI insurers, compared to other APRA-regulated industries, Members Health offers a detailed breakdown of proposed strategies to address concerns with specific prudential requirements. These have been provided in Attachment B and include:

1. Exempting non-SFIs from particular requirements that are not considered to be proportionate for a non-SFI entity considering the lesser risk to the stability of the financial system should an entity fail to manage their operational risk effectively.

2. Amending requirements to allow for a PHI entity's discretion in implementing internal controls that are commensurate with the industry's risk profile, the scale and complexity of an entity's operations, the nuances of running a not-for-profit[1] organisation, the severity and extent of a potential threat, and the targets and tolerances of an entity's risk appetite.

3. Identifying requirements that would benefit from additional guidance to assist with uplifting a PHI entity's capabilities and implementation of CPS-230.

Members Health appreciates the complexity of combining multiple Prudential Standards into a single cross-industry Standard and welcomes the opportunity for further consultation, before finalising the Standard, to ensure the new requirements represent sensible business practice and accommodate the diversity of private health insurers in the market.

Once again, Members Health thanks APRA for the opportunity to participate in this consultation and we are available to discuss the issues that are outlined in our submission.

Yours sincerely,

[redacted]

[redacted]

CEO, Members Health Fund Alliance

[1] Noting that the 26 funds that Members Health represents are member-owned, not-for-profit organisations which are recognised for protecting their members' interests by prudently managing expenditure to ensure more benefits go back to their members through lower premiums, improved health programs and generous benefits supporting health and wellbeing.

Members Health FUND ALLIANCE

Attachment A – Response to Key Questions

The following responses are intended to provide feedback for specific areas that APRA has identified would assist APRA in finalising the requirements. Additional information is provided in Attachment B.

Overall Design	
A key area of concern with the overall design of the Standard is the use of 'absolute' terms, when specifying a requirement, which does not allow for an entity's compliance to be commensurate with its size, business mix or complexity.	
1.	**Is a single cross-industry standard for operational risk management supported?** Members Health supports a single cross-industry standard for operational risk management, contingent on amending the Standard so its implementation is commensurate with an entity's size, business mix and complexity, and in particular acknowledges the different risks posed to the stability of the financial system by differentiating between SFI and non-SFI entities. Consultation should be extended to accommodate the differences between the finance and private health insurance industries. In terms of protecting the best interests of policyholders, the funds are already prudently managing operational risk under CPS-220, with capital contingencies under HPS-110. While CPS-230 may improve the efficacy of an entity's internal controls, introducing the new requirements as a cross-industry standard without acknowledging the difference between the prudential obligations of financial institutions and private health insurers will introduce an undue compliance burden on PHI insurers that does not allow for sensible business practice commensurate with their scale or complexity.
2.	**Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?** Attachment B includes extensive feedback on specific topics that would benefit from guidance to assist in implementation. While the guidance will be an important element to help entities meet their compliance obligations, ultimately clarifying the prudential requirements in the Standard before it is finalised will add the greatest value for ensuring an effective implementation.
3.	**How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs?**

Overall Design	
	Members Health supports that there is merit in differentiating requirements for SFIs and non-SFIs where the obligations should be proportional with setting prudential requirements that are not overly complex, and are relative to what is needed to ensure the financial safety and operational resilience of smaller non-SFI entities. This was demonstrated in the recently finalised new capital standard for PHI. We are of the view that APRA should take a similar prudent approach with the new PHI capital standard in differentiating and taking into consideration the size and complexity of an entity's risk and operational profile (i.e. SFI and non-SFI). Rather than adopting the approach embedded in the existing CPS-231 and CPS-232 (neither of which apply to PHI), Members Health recommends a more explicit approach where smaller, less complex entities that are deemed to be non-SFI are exempt from specific requirements, or at least the requirement specifies whether it would allow discretion to meet the requirements in a proportionate manner commensurate with the scale and complexity of an entity's business. Members Health notes that only two of the prudential requirements in CPS-230 currently allow for proportionality, despite the objective of the Standard stating that the "entity's approach to operational risk management must be appropriate to its size, business mix and complexity".
4.	**What are the estimated compliance costs and impacts to meet the new and enhanced requirements?** While Members Health has not conducted a formal impact analysis to understand the estimated compliance costs, funds are anticipating there will be a substantive increase in management expenses, where additional resources with highly specialist skill sets will be required to increase capacity for the internal audit function, procurement function and quality control function. At a minimum, the smaller funds are anticipating management expenses could increase by at least $300k to allow for: • an additional internal audit function specialising in contracts, • a procurement team to run tenders, assess risk for third and fourth parties, and negotiate contracts (new, renewed and material changes), • a quality control team dedicated to maintaining the documentation of processes, conducting health checks and testing BCP scenarios, • fit-for-purpose technology support and systems. Should the prudential requirements be revised to reduce the compliance obligations for a non-SFI, compared to a SFI (per the recommendations in Attachment B), the cost estimates are expected to decrease accordingly.

Members Health
FUND ALLIANCE

Specific Requirements	
5.	**How could APRA improve the definitions of critical operations, tolerance levels and material service providers?** **Critical Operations** Members Health supports that the definition of 'critical operations' as stated in clause 34 sufficiently describes the baseline for identifying a critical operation, however seeks more guidance in relation to clause 36 (please refer to our comments in Attachment B) **Tolerance Levels** Members Health supports the definition of 'tolerance levels' as stated in clause 37, however seeks more guidance in relation to clause 38 (please refer to our comments in Attachment B). **Material Service Providers** Members Health supports the definition of a 'material service provider' as stated in clause 48, however has some concerns in relation to clauses 50, 51, 52, 54 and 56 (please refer to our comments in Attachment B). Guidance would be helpful to provide some practical examples for each term.
6.	**What additions or amendments should be made to the lists of specified critical operations and material service providers?** **Lists of Critical Operations** The current list of critical operations is specific to the finance industry – for example – deposit-taking and management, custody, settlements, and clearing are unique to financial institutions. As a cross-industry standard, the list should either apply to all industries, or a list should be created that is relevant to a specific industry. For example – clause 35 could say "For the purposes of this Prudential Standard, critical operations include, but are not limited to: (a) for financial institutions – payments, deposit-taking, clearing, etc. (b) for super funds – payments, custody, fund administration, etc. (c) for general insurers – payments, claims, enquiries, etc. (d) for private health insurers – a management function, an HR function, a claims processing service, a service relating to the negotiation of contracts for hospital treatment and general treatment, and an internal audit function. Further guidance would be helpful to understand what aspect of a critical operation is deemed to be critical by APRA – for example for 'enquiries' would the entire call centre be considered a critical operation or only aspects of being able to take and respond to a call from a policyholder?

Specific Requirements	
	Lists of Material Service Providers The current list of material service providers is specific to the finance industry – for example – credit assessment, funding and liquidity management, mortgage brokerage, custodial services, financial planners are unique to financial institutions. As above, clause 49 could include a breakdown of material service providers that is relevant to a particular industry. HPS-231 currently refers to the *material business activities* of a private health insurer which include – a management function, an HR function, a claims processing service, a service relating to the negotiation of contracts for hospital treatment and general treatment, and an internal audit function.
7.	**Are the notification requirements and the time periods reasonable?** Members Health supports that the 'notification requirements' as stated in clause 57 and 58 are reasonable, however seeks more guidance in relation to clause 41 (please refer to our comments in Attachment B)
8.	**What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers (if required)?** The timeframe needed to renegotiate contracts with existing service providers will depend on how many contracts need to be negotiated at any time, the complexity of the arrangements to be negotiated (types, criticality and extent of services), the number of counterparties, the timeliness of the counterparties to reach mutual agreement and finalise the contracts. Given the Standard will introduce new requirements that need to be incorporated into the existing contracts, renegotiating the conditions of an existing contract could take anywhere between eight weeks to 12 months (considering the above dependencies). The negotiation will also be dependent on whether the contract is due for renewal (end of life) or if APRA requires entities to break a contract and renegotiate it within the first 12 months of the new Standard being adopted. Contracts with existing service providers may have extended service periods (e.g. three year terms) or may be continual agreements (e.g. the fee is increased each year but otherwise the agreement continues to rollover indefinitely as long as all parties are meeting their commitments). If a contract was not due for renewal within the first 12 months of adopting the new Standard, or if it was unlikely that the renegotiation would be settled

Specific Requirements	
	within the first 12 months, Members Health recommends that a transitional arrangement allows for PHI entities to request either an exemption from the prudential requirement or an extension, depending on the circumstances. For a non-SFI, the expectation to renegotiate all existing service provider contracts (particularly if they are not due for renewal) is not considered to be proportionate with the threat of a contract failing to meet the compliance threshold for CPS-230 where the provider has otherwise been meeting its performance objectives, and the contract is compliant under HPS-231. More information relating to Members Health's recommendations for transition timeframes, exemptions and extensions can be found in Attachment B against the corresponding prudential requirement.

Members Health
FUND ALLIANCE

Attachment B – Clause-by-clause feedback

Members Health has compiled specific clause-by-clause feedback in the table below.

Clause	Prudential Standard CPS 230 Operational Risk Management – Section
A key area of concern with the proposed implementation of the Standard is that lessons learned from implementing past standards have not been incorporated where the ambiguous use of specific terms (such as 'periodical') were open to interpretation and therefore difficult for auditors to assess whether an entity was compliant, particularly where different funds have implemented different approaches. For example – 'periodical' means occasional or regular. This can be interpreted as something that needs to be monitored occasionally (e.g. every 2 years), or regularly (every 2 weeks). For the sake of compliance audits, it would be preferable to note that the frequency can be determined at the discretion of the entity (depending on whether they are an SFI or non-SFI). The feedback provided against each of the relevant clauses below is intended to draw attention to particular wording or obligations that are considered to be ambiguous, overly complex or are not considered to be relative to what is needed to ensure the financial safety and operational resilience of a private health insurer – and recommend whether clarifying the clause, and / or providing additional information in a prudential practice guide would assist in implementing the Standard.	
	Objectives
0.	Despite the objectives stating that the entity's approach to operational risk must be appropriate to its size, business mix and complexity, the language used in the requirements is very prescriptive and does not allow for scale or complexity. None of the requirements allows for proportionality.
	Key Principles
14.	It is not clear whether the requirements stated in clause 14 correlate to the requirements stated in clause 47(d) where there is an additional obligation on entities to effectively manage the risks of both third and fourth parties. We seek clarification for whether "must not rely on a service provider" extends to "and fourth parties relied on by a service provider"? Should the requirement extend to fourth parties, we do not consider this to be proportionate for a non-SFI, and would request that non-SFIs are exempt from this requirement, or the wording is amended to allow for an entity's discretion in whether their assessment of fourth-party risk exposure is sufficient that they have addressed it in their entity's risk appetite.

Clause	Prudential Standard CPS 230 Operational Risk Management – Section
	Risk Management framework
16.	It is not clear whether the requirements stated in clause 16 require the review of the operational risk management to be included as part of CPS-220's annual review of the risk management framework or the triennial comprehensive review of the risk management framework. We seek clarification for whether the review is intended to be annual or triennial, noting that CPG-220 states that "APRA will accept annual reviews that explore particular elements of the risk management framework on a rotational basis … all elements of the framework subject to review at least every three years".
18.	It is not clear what would constitute a material weakness. We seek clarification as to whether the requirement to hold additional capital (under 18c) would be in addition to the requirement under HPS-110 to hold additional capital to mitigate operational risk? Additional guidance for 'material weaknesses' would be helpful.
Clause	Role of the Board
21.(b)	It is not clear how the Board can avoid becoming overly involved in operational matters. Additional guidance for 'the role of the Board vs management' would be helpful.
21.(c)	Additional guidance for developing a 'service provider management policy' would be helpful (noting that this requirement correlates to clause 47 which provides a high-level breakdown of the policy structure).
Clause	Operational Risk Management
26.	Additional guidance for 'maintaining a comprehensive assessment of an operational risk profile' would be helpful.
Clause	Business continuity
35.	The list of critical operations is specific to the financial industry and includes operations that are not relevant to the PHI industry (such as deposit-taking, custody, settlements, and clearing). As this is intended to be a cross-industry standard, we suggest the list is either tailored for the relevant industries, or updated to include examples of critical operations that are applicable to PHI.

Clause	Prudential Standard CPS 230 Operational Risk Management – Section
	Additional guidance for 'examples of critical operations' that are specific to PHI would be helpful.
36.	It is not clear how clause 34 correlates with clause 36, where clause 34 gives a baseline for defining a 'critical operation' and clause 36 states that APRA may require an entity to classify a business operation a critical operation. We seek clarification for what criteria APRA might use to re-classify a business operation as a critical operation? Additional guidance for 'classifying a business operation as a critical operation' would be helpful.
38.	It is not clear how clause 37 correlates with clause 38, where clause 37 gives a baseline for describing how a Board should establish 'tolerance levels' for a critical operation and clause 36 states that APRA may require an entity to change its tolerance levels. We seek clarification on what grounds APRA might have to override a Board's established tolerance levels for critical operations, considering these are operational decisions made with respect to operating a business within the Board's risk appetite, and in accordance with the PHI industry's risk profile, while clause 38 states APRA may require an entity to review and change its tolerance levels? Should the requirement intend for APRA to manage risk on behalf of its regulated entities, we do not consider this to be proportionate for a non-SFI PHI entity. Additional guidance for 'how APRA would determine a 'heightened risk or material weakness' would be helpful.
41.	It is not clear whether the notification, that an entity has activated its BCP, is required for every possible business disruption regardless of the incident's severity, extent, outage duration, intermittent outages, or whether the outage was in relation to a critical operation or an ordinary business operation. We seek clarification for whether APRA requires notification for each incident of business disruption, noting that clause 15(e) states that a BCP is not exclusive to critical operations, and therefore may apply to a scenario where there has been a brief power outage or multiple intermittent power outages throughout the day. Should the requirement intend to cover every possible business disruption, regardless of the severity and extent, we do not consider this to be proportionate for a non-SFI.

Clause	Prudential Standard CPS 230 Operational Risk Management – Section
42.	It is not clear whether the annual business continuity exercise is expected to cover all critical operations included in its systematic testing program. We seek clarification for whether the annual business continuity exercise will apply to the entire program or a particular scenario. Should the requirement intend to cover the entire program, we do not consider this to be proportionate for a non-SFI. Additional guidance for 'developing a systematic testing program' would be helpful. We also seek guidance as to whether conducting an annual business continuity exercise is required where an entity has been required to activate its BCP during the year.
43.	This clause is not considered to be proportionate for a non-SFI. We seek clarification on what grounds APRA might have to require an entity to include an APRA-determined scenario in a business continuity exercise for a particular entity or a class of entities, and how would this impact the scope of the ordinary testing program in terms of requiring additional resources to test the scenario? Additional guidance for 'how APRA would determine a business continuity exercise' would be helpful.
Clause	**Management of service provider arrangements**
47.(d)	This clause is not considered to be proportionate for a non-SFI. Also this requirement is not clear as 47(d) refers to managing the risks associated with any fourth parties that material service providers rely on, however the footnote says a fourth party is a party that a service provider relies on (which could mean providers that Microsoft relies on). Managing risks associated with any fourth parties would require significant effort before any entity would be able to provide assurance that they are compliant with this requirement. The effort required for a non-SFI to conduct a risk-assessment on all fourth-parties is likely to outweigh the benefits of reducing the PHI industry's risk exposure, particularly given third-parties may be reluctant to provide details of any fourth-parties they are working with if the service they are offering is commercial-in-confidence. Members Health anticipates that the service agreement should protect a PHI entity in the event that a third-party does not comply with the terms as a result of fourth-party contagion risk. Members Health recommends this requirement should not apply to non-SFI entities.

Clause	Prudential Standard CPS 230 Operational Risk Management – Section
50.	This clause is not considered to be proportionate for a non-SFI and when read in context with CPS-234 appears to be overly complex. Under CPS-234 (clause 16), information assets may be managed by a provider (related party or third party) and not only those captured under agreements with service providers of outsourced material business activities (or under CPS-230 this would be a material service provider). The requirement under CPS-230 (clause 50) to include providers of information assets that are classified as sensitive or critical under CPS-234, that have not already been deemed material service providers, introduces a level of complexity in having to treat providers as material service providers under CPS-230. For example, under CPS-234 Microsoft might be considered a provider. Under CPS-230, Microsoft would be subject to the same requirements as a material service provider. Under clause 52, the entity must undertake "an appropriate tender and selection process" which would mean inviting Microsoft to participate in a tender process. Under clause 54, the agreement with Microsoft must include provisions that allow APRA the right to conduct an on-site visit, which would mean asking Microsoft to adapt their standard terms and conditions. The practical implementation for any APRA regulated-entity would be onerous, but more so for non-SFI where the compliance burden likely outweighs any benefits and the risk exposure would not be commensurate with a threat to the stability of the financial system. Members Health recommends this requirement should not apply to non-SFI entities.
51.	We seek clarification on what grounds APRA might have to override an entity's classification of a service provider to re-classify the service provider or type of service provider as material, considering changing the classification to a material service provider would impose a significant number of additional compliance obligations on the entity, which may not be appropriate nor commensurate with the risk exposure for a non-SFI entity? Additional guidance for 'classifying a service provider' with the PHI industry would be helpful to avoid incidents of APRA overriding an entity's classification. Additional guidance for 'submitting a register' would be helpful. Most funds are using an *Enterprise Risk Management Information System* however the export format of the contract register is likely to be different across systems, and it would be onerous for a risk manager to have to convert the report to another format if it did not meet APRA's file specifications.

Clause	Prudential Standard CPS 230 Operational Risk Management – Section
52.(a)	This clause is not considered to be proportionate for a non-SFI. The obligation to increase the capacity of the procurement team to "undertake a tender **and** selection process" for **every** new, renewing or modified arrangement with a material service provider will introduce substantive management expenses to engage a suitably qualified and experienced procurement specialist with specific expertise in contract management to undertake due diligence, conduct tenders, negotiate (or renegotiate) contracts, and assess third and fourth party risks. Currently HPS-231 requires a PHI entity to "undertake a tender process *or other selection process*" which allows for an entity to undertake procurement activities commensurate with their complexity, the type, criticality and extent of the services, as well as the contract value. Members Health recommends this requirement should not apply to non-SFI entities, or the requirement should be adapted to allow for entities to use their discretion to meet the requirements in a proportionate manner that is commensurate with the scale and complexity of their business.
52.(c)	It is not clear how an entity would assess whether the provider is systemically important in Australia – or what the criteria is for being systemically important. We seek clarification for what is considered to be "systemically" important, and whether this requirement interacts with the requirements under the *Security of Critical Infrastructure Act 2018?* Additional guidance for what "reasonable steps" need to be taken would be helpful.
54.	The requirement to ensure all formal agreements include provisions that allow APRA the right to conduct an on-site visit to the service provider is considered to be overly complex in terms of having to negotiate with all material service providers to ensure this clause is included in the formal agreement, and renegotiate any existing contracts to include this clause. Considering this extends to providers of critical and sensitive information assets under CPS-234 (not just material service providers under CPS-230), the compliance burden for negotiating this requirement would be extensive and is unlikely to outweigh any benefits to reduce the risk exposure of a material service provider refusing to allow an on-site visit. Members Health recommends this requirement should be reviewed for all entities, and in particular PHI entities should be exempt from this requirement.
56.	This clause is not considered to be proportionate for a non-SFI.

Clause	Prudential Standard CPS 230 Operational Risk Management – Section
	We seek clarification on what grounds APRA might have to require changes to a service provider arrangement, considering changing commercial agreements where the provider has not breached the agreement or where performance has not been an issue, would impose a significant burden on the entity to re-negotiate, probably incur break costs, and which may not be appropriate nor commensurate with the risk exposure for a non-SFI entity, particularly if the higher risk is that the provider terminates the agreement rather than accepts the changes. We are also concerned about the legality of a third party, who is not a counterparty to the agreement, requiring changes to an agreement. We seek further clarification as to whether APRA would see itself as a counterparty on every service provider arrangement where it would then be able to negotiate terms of an agreement that would allow it to review and make changes where it identifies heightened prudential concerns – noting also that this requirement applies to both providers (under CPS-234) and material service providers (under CPS-230). Members Health recommends this requirement should not apply to non-SFI entities.
57.	It is not clear whether the requirements stated in clause 14 correlate to the requirements stated in clause 56 where there is an additional obligation on entities to effectively manage the risks of both third and fourth parties. We seek clarification for expectations regarding how frequently the 'regular' assessment should be conducted – monthly, quarterly, annual?
59.	This clause is not considered to be proportionate for a non-SFI. The obligation to increase the capacity of the internal audit function to "review any proposed outsourcing arrangement with a material service provider for a critical operation and regularly report to the Board or Audit Committee on compliance with the service provider management policy" will introduce substantive management expenses to engage a suitably qualified and experienced auditor with specific expertise in contract management to review **all** new, renewing or material changes to outsourcing arrangements. Further many non-SFIs have outsourced the internal audit function, and under this requirement, the internal auditor would be required to review their own outsourcing arrangement and regularly report to the Board on its own compliance. Members Health recommends this requirement should not apply to non-SFI entities.