SUBMISSION

Submission to APRA – CPG 230 *Operational Risk Management*

13 October 2023

The Association of Superannuation Funds of Australia Limited
Level 11, 77 Castlereagh Street
Sydney NSW 2000

PO Box 1485
Sydney NSW 2001

T +61 2 9264 9300
1800 812 798 (outside Sydney)
F 1300 926 484
W www.superannuation.asn.au

ABN 29 002 786 290 CAN 002 786 290

File: 2023/32

Mr Gideon Holland

General Manager, Policy

APRA

Via email: PolicyDevelopment@apra.gov.au

13 October 2023

Dear Mr Holland

Draft Prudential Practice Guide CPG 230 *Operational Risk Management*

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to APRA's consultation on draft CPG 230 *Operational Risk Management*.

About ASFA

ASFA is a non-profit, non-partisan national organisation whose mission is to continuously improve the superannuation system, so all Australians can enjoy a comfortable and dignified retirement. We focus on the issues that affect the entire Australian superannuation system and its $3.5 trillion in retirement savings. Our membership is across all parts of the industry, including corporate, public sector, industry and retail superannuation funds, and associated service providers, representing almost 90 per cent of the 17 million Australians with superannuation.

*****

If you have any queries or comments in relation to the content of our submission, please contact Julia Stannard, Senior Policy Advisor, on (02) 8079 0819 or by email jstannard@superannuation.asn.au.

Yours sincerely

Julian Cabarrus

Director – Policy Operations, Member Engagement & External Relations

General comments and executive summary

ASFA is pleased to provide this submission on APRA's draft version of CPG 230, which has been prepared following extensive consultation with our members – registrable superannuation entities (RSEs) and their service providers. Our members appreciated the opportunity to discuss the draft guidance with key APRA staff, and that dialogue has informed our submission.

ASFA wishes to acknowledge the constructive approach APRA took to its consultation on the prudential standard CPS 230, which is reflected in the final version of the standard. Several key amendments align with recommendations made by ASFA in our submission on the draft version of CPS 230.

In particular, ASFA welcomes:

- the deferred commencement date, which will help regulated entities to implement the new requirements in a measured way.
- APRA's statement of milestones regulated entities should work toward during the implementation period for CPS 230, which clearly articulates APRA's expectations.
- provisions allowing a regulated entity to classify a prescribed operation as not critical, or to classify a prescribed service provider as not material, if it can provide satisfactory justification for those decisions. This is a practical and sensible approach and will be of particular assistance to RSEs who might, for example, utilise multiple providers to deliver the same type of service. ASFA's members are highly cognisant of a broad range of risks, and remain mindful that risk is a necessary component of providing the best possible financial outcomes for beneficiaries. To that end, we specifically note that conscious risk decisions enable sound outcomes, within the bounds of each RSE's enterprise risk management system. That said, we consider that some additional clarification is required to provide comfort to regulated entities when making an assessment that a prescribed operation is not critical, or a prescribed service provider is not material.

ASFA was also pleased with APRA's recognition of the need for transitional arrangements for existing material service provider arrangements, a point we highlighted in our earlier submission. Ideally, transition arrangements will help to minimise unnecessary cost and bottlenecks which are likely to occur if the many APRA-regulated entities attempt to simultaneously renegotiate contracts with common service providers. As noted below, however, we have some concerns around how the transition arrangements for material service provider agreements will operate in practice, as well as the absence of any provisions to smooth the transition from SPS 231 and 232 to CPS 230 for RSEs.

The following sections of our submission highlight a number of areas where ASFA members have requested clarification of APRA's expectations.

Some of the issues with interpretation of CPS/CPG 230 reflect the challenges of applying generically drafted provisions in a cross-industry standard and guidance to specific situations arising in one particular sector. We would welcome the inclusion of more sector-specific examples throughout CPG 230, and do not consider the cross-industry nature of the guidance an impediment to APRA including areas of guidance and/or expectation that are focussed on particular sectors.

Comments in relation to specific aspects of CPS/CPG 230

Areas for clarification – pre-commencement phase of CPS/CPG 230

CPS/CPG 230 will replace a number of existing cross-industry and sector-specific prudential standards and guidance notes – of particular relevance to RSEs, this includes SPS/SPG 231 *Outsourcing* and SPS/SPG 232 *Business continuity management*.

Given the extended implementation period for CPS 230, this raises the question of the approach APRA will take to SPS 231 and 232 through to 1 July 2025. ASFA members would appreciate clarification in relation to APRA's approach and/or expectations, during the pre-commencement period, in relation to:

1. The requirements for compliance processes and frameworks

   ASFA understands that APRA expects RSEs to maintain SPS 231 and 232 compliant processes and frameworks through to a hard cutover to CPS 230 compliant processes and frameworks on 1 July 2025. This will prevent RSEs from progressively adopting CPS 230 compliant processes and frameworks, unnecessarily complicating the transition and adding to the cost and workload associated with implementation of CPS 230. We request that APRA reconsiders this stance and permits regulated entities to move progressively toward CPS 230 compliance during the pre-commencement phase.

2. Outsourcing/material service provider agreements

   Currently, SPS 231 is in force and prescribes matters that must be addressed in each outsourcing agreement. CPS 230 will commence on 1 July 2025 and will prescribe minimum content for formal agreements. There are differences between the two standards.

   APRA's *Response paper – Operational Risk Management* states: "APRA-regulated entities will have until the earlier of 1 July 2026 or the next renewal date of an existing agreement to ensure the agreement complies with CPS 230. That said, contracts with material service providers should be updated as soon as possible given their importance to critical operations and operational risk."

   It is unclear whether, before 1 July 2025, an RSE licensee entering into a formal agreement for a material arrangement that is also an outsourcing agreement (that is, SPS 231 applies and CPS 230 will apply later) can choose to comply early with CPS 230, rather than SPS 231 and 232. If RSEs are unable to do so, this will require them to incur cost and work to update agreements that is, in ASFA's view, unnecessary – and may contribute to the creation of bottlenecks with service providers that industry had hoped would be avoided by the granting of transition arrangements.

We urge APRA to provide a 'no action' position in relation to non-compliance with SPS 231 and 232, where a regulated entity complies early with CPS 230.

Key principles

As noted throughout the following sections of our submission, the concepts of materiality (of service provider arrangements) and criticality (of business operations) are key to understanding the intended scope of CPS and CPG 230. They will also have a very direct impact on the implementation effort and cost, and the ongoing compliance arrangements, for the standard. ASFA encourages APRA to consider providing further commentary on these concepts, whether within or separate to CPG 230, including on a sector-specific basis.

We note that CPS/CPG 230 also makes some parallels between the size of a regulated entity and the complexity of its business operations. This approach may not be appropriate in all cases, as a small entity will not necessarily be non-complex and conversely a large entity may not be highly complex.

Paragraph 4 refers to the level of granularity expected in assessing the operational risk profile of a smaller entity, including identifying and documenting processes, resources and scenario analysis. ASFA requests that additional guidance is included in CPG 230 giving similar information about the level of granularity expected of larger entities.

'Better practice' statements

ASFA requests greater clarity around the status of the 'better practice' statements outlined in the draft CPG 230.

In particular, ASFA seeks to understand whether APRA views these as 'better practice' over and above the minimum that is necessary to comply with an entity's obligations, potentially likely to be achieved by entities that are larger and more highly resourced and/or more complex. Alternatively, will APRA, in future compliance reviews, treat the 'better practice' statements as standards that a prudent entity would meet – effectively as quasi-requirements for all entities? ASFA members have reported a tendency for matters described as 'guidance' to be treated as 'expected' in reviews conducted by APRA in relation to other regulated areas, and for some variation in application of guidance/expectations as between different APRA offices. If APRA expects entities to achieve what it has outlined as 'better practice', it is important that this is made clear from the outset so regulated entities can plan their CPS 230 implementation accordingly and avoid costly and time-consuming rework at a later time.

We note that there is likely to be a spectrum across the industry in terms of sophistication of operational risk management architecture. Some entities are very large in scale and will have a significantly higher level of human and technical/infrastructure resources devoted to risk management, while others are smaller in scale. The 'better practice' statements set out in the draft guidance may be readily achievable for some entities (and potentially already in place for some) but represent targets for others to achieve as their risk management architecture continues to evolve. In ASFA's view, some of the better practice statements appear to impose an additional layer on top of what may be reasonable for an entity given its size, business mix and complexity. It is likely, given the level of cost and/or compliance burden involved in achieving some of the better practice statements, that some entities may choose, following a cost-benefit analysis, not to adopt them.

Risk management framework

Paragraph 10 of CPG 230 states that "where an entity has identified material weaknesses in its operational risk management, APRA expects that the entity would keep it informed of the progress of its remediation."

We note that this wording does not align with the wording used in paragraph 19 of CPS 230. That paragraph refers to actions that APRA may take – including requiring development of a remediation program – where *APRA* (rather than the entity) considers that a regulated entity's operational risk management has material weaknesses. We recommend that paragraph 10 is amended to refer to *APRA* having identified material weaknesses, rather than the entity. The alternative interpretation is that paragraph 10 is intended to convey an additional, proactive expectation on regulated entities that is not sourced from a requirement imposed by CPS 230 – if that is the case, ASFA requests that this be made more explicit in CPG 230.

Additional guidance would also be appreciated in relation to the interaction of CPS 230 paragraph 19(c) with the existing Operational Risk Financial Requirement imposed on trustees under SPS 114, which we acknowledge is currently under review by APRA. ASFA is of the view there should not be any duplication of requirements or powers, nor any inconsistency between, the two standards. We note that additional guidance appears to have been provided for ADIs and insurers (in paragraph 9 of CPG 230), but not RSE licensees.

Roles and responsibilities

In our submission on the draft version of CPS 230, we noted our concerns that it sought to place on the Board responsibilities that should, in industry's view, sit with management. We welcome the confirmation, in APRA's 'response paper' for the consultation, that the intent of CPS 230 is not to impose management functions on the Board and that the intent is not for the Board to play a role in day-to-day operational risk management.

However, as there were no substantive changes made to that section of CPS 230, it is important that the guidance provided in CPG 230 makes very clear the respective roles of the Board, its Board or management committees, and senior management. ASFA notes it is also important that this is co-ordinated and aligned with the requirements and expectations under the Financial Accountability Regime (FAR).

We understand it is APRA's view that the responsibilities of the Board sit with the Board and cannot be delegated, even to a committee of the Board – that is, the role of a Board committee is to provide recommendations for the Board's consideration. We recommend that this is reflected more directly within CPG 230. ASFA further requests that APRA provide further clarity, within CPG 230, on:

- The expectation, in paragraph 16(c), that a Board will take a deep dive into any areas of 'significant weakness' – it is unclear how (or if) 'significant weakness' is intended to differ from 'material weakness' (a term used in paragraphs 19, 31 and 39 of CPS 230 and paragraphs 9 and 10 of CPG 230).
- What is intended, in subparagraph 16(d), by the Board paying "particular attention" to significant new ventures that may give rise to material or novel operational risk. What would "particular attention" involve in practice?
- Whether paragraph 18 is in effect referring to the entity's risk appetite statement, albeit using different terminology. If so, we recommend that this paragraph is redrafted to improve clarity.
- How the examples in CPG 230 of senior management setting tolerance levels would interact with the Board's role (paragraphs 18 and 19).

  Paragraph 18 notes that the board is responsible for setting the entity's overall tolerance levels, with senior management able to set more granular tolerance levels and indicators that are consistent with (and do not undermine) the Board-approved levels. Paragraph 19 provides examples, including one of relevance to superannuation. It states that "more granular tolerances may be set for parts of the investment and fund administration processes, such as for the timely investment of contributions and any payments that may have a direct impact on members (such as retirement benefits or early release payments for severe financial hardship and processing of rollovers)." ASFA members have noted that what is described in this paragraph as 'granular' actually appears to be quite fundamental and high level. We would appreciate further explanation from APRA around the distinction between the levels that can be set by the Board as opposed to senior management.

Operational risk management

ASFA members have queried whether APRA is intending to imply that regulated entities are required to have a specific architecture for management of operational risk. We note that entities will typically manage types of risk in a standardised and consistent manner – although a possible exception might be investment related risks, which tend to have more detailed and different practices and specific guidance applied to them. As a result, it is important to ensure that the controls implemented are adequate and appropriate for managing *all* risk categories, not only operational risk.

ASFA members would appreciate greater clarity around APRA's expectations in relation to end-to-end business process mapping (paragraph 22-53 of draft CPG 230, particularly paragraph 24). We note that mapping of all end-to-end processes, as suggested in paragraph 36(b), by the 1 July 2025 commencement date for CPS 230 will be a significant task for many regulated entities.

Areas where ASFA members have requested greater clarity or additional guidance include:

- What level of mapping is required (paragraph 24) - is this limited to critical business operations, or potentially to the next layer of supporting business processes, or does APRA expect this to extend further?
- In paragraph 39, what does APRA mean by *'sufficiently stressed'* – does this mean stressed to failure?
- As part of an example in which an entity has suffered a high-rated fraud incident which is deemed material, subparagraph 53(d) states that an entity could "consider business process mapping" to support its reassessment of fraud risk, reassessment of controls linked to the fraud risk and the conduct of a root cause analysis. It is unclear whether APRA is referring here to business mapping the risk event or the incident process. In this context, ASFA presumes that "consider business process mapping" should be interpreted to mean the entity could review and revalidate its business process mapping, to ensure all relevant processes and controls are accurately captured.
- The use of varied terminology including:
    - CPS 230, paragraph 27(c), which relates to operational risk, refers to 'severe operational risk events'. CPS 230 paragraphs 16(e) and 43, which relate to business continuity planning, refer to 'severe but plausible scenarios'. Guidance would be appreciated to confirm whether these are intended to be the same, or different scenarios.
    - the meaning of 'operational risk incidents and near misses' as referred to in CPS 230 paragraphs 32-33 – to ensure a consistent approach is applied across the industry.

ASFA members have noted a need for greater clarity in the guidance regarding requirements to regularly monitor, review and test controls for design effectiveness (DE) ***and*** operating effectiveness (OE). The guidance (at CPS 230 paragraph 30 and CPG 230 paragraphs 40-48) could be read as requiring review of *all* controls for all material risk categories or alternatively requiring independent review for only key controls.

We note that most organisations will have thousands of controls, which may be documented at a high or low level. The guidance is silent on whether testing of controls should be 'independent'. Comfort that a control is designed or operating effectively can be achieved in a number of ways, including:

- monitoring of OE using key indicators
- self-attestation - an attestation or negative assurance ('nothing has come to my attention')
- self-attestation - an attestation with some evidence to support the assurance

- self-assessment designed against best practice standards, to ensure design manages the risk (DE) with sample-based testing (for OE) - ASFA members have indicated that, in their experience, the cost to test a single control for DE and OE is, on average, $10,000 (or 10 business days work effort)
- independent assessment – an assessment of DE and OE performed by someone other than the control owner, whether this is second line, third line, or a third party – with third party assessment involving significantly higher cost, typically two to three times the cost of self-assessment (first line assessment).

The cost and compliance burden involved with the approaches noted above will obviously differ substantially. Further, ASFA considers it important that industry is working toward a common understanding to ensure consistency of approach.

Paragraph 31 of CPG 230 states that "Better practice is for information systems to enable real time and aggregated reporting and integrate risk data across different components of the framework, for example: risks, obligations and key data (including controls, issues, incidents and breaches)." We note that ADIs have been subject to real time reporting type requirements for some time and should be well placed to achieve the better practice outlined in this paragraph. This is understandable give the real time nature of transactions in the banking sector. It is likely that entities in other regulated sectors, including RSEs, will not currently have this level of functionality in place. The cost of implementing this is likely to be substantial, and may not be supported based on the outcome of cost-benefit analysis (particularly given the time to payment is typically slower in superannuation as compared to banking, with assets held for longer duration). Potentially, RSEs will need to move toward achieving real time reporting as they continue to evolve their risk management infrastructure. For this reason, we support APRA's description of this as 'better practice' rather than stipulating it as a requirement or expectation.

ASFA presumes that APRA's better practice statement in paragraph 45 is limited to capturing the key controls relied on to mitigate the majority of risk in the entity's critical operations, and is not intended to apply to every control implemented by an entity.

Business continuity

ASFA members would appreciate clarity as to APRA's expectations where a service provider refuses to adopt the regulated entity's approach to business continuity management (BCM).

Paragraph 56 notes that better practice is for business continuity management to be approached across the whole of the business, irrespective of organisational structure or "whether an operation is performed internally or by another party." However, there will be situations where a service provider, which is not itself regulated by APRA, might simply refuse to accept terms and conditions a regulated entity might seek to impose, including in relation to BCM. While it is possible to interpret paragraph 56 as suggesting it might be 'better practice' for a regulated entity not to use that service provider, where the provider is of large scale with few competitors – for example, providers of software – that interpretation may not reflect the commercial reality of the situation. It may also decrease the potential for innovation and broader practical improvements within the industry.

With regard to identifying critical operations, paragraph 58 sets out five factors that a prudent entity would consider. We request that APRA provide clarification as to whether these factors are to be considered independently, or in isolation. That is, is satisfaction of only one factor sufficient to determine characterisation as a critical operation?

As noted earlier, ASFA members appreciate that APRA has acknowledged that the operations prescribed as 'critical' in paragraph 36 of CPS 230 might not be a critical operation for every regulated entity. While we welcome the ability for entities to assess that a prescribed operation is not critical, we question the requirement to review that assessment "on at least an annual basis" (CPG 230, paragraph 60). We suggest it should be adequate for entities to review that assessment on a triennial basis or sooner if there is a fundamental change in the entity's business model. In the absence of a significant change in the entity's business operations, it appears unlikely that the criticality of an operation would change from one year to the next.

APRA requires RSE licensees to capture 'investment management', 'fund administration' and 'customer enquiries' as critical operations under paragraph 36 of CPS 230. While this is a good starting point for identification of critical operations, these are broad umbrella terms which may be interpreted differently across the superannuation industry, leading to differences in the way the standard is applied.

As such, we recommend CPG 230 provide clarity that RSE licensees may determine which facets of 'fund administration', 'investment management' and 'customer enquiries' it considers to be 'critical operations for RSE licensees for CPS 230 purposes. That is, we seek confirmation that it is up to RSE licensees to apply the principles set out in paragraph 35 of CPS 230 and paragraphs 57-59 of CPG 230. For example, when applying the principles of CPS 230 to the 'fund administration' critical operation scope, an RSE licensee may determine that its critical operations include fundamental and high-volume functions such as contributions, rollovers and payments, but might exclude lower volume functions such as family law and departing Australia superannuation payments. This reflects the intent of the 'critical operation' concept under CPS 230, with a focus on core business continuity as opposed to the delivery of every operational process.

Finally, we note that paragraph 64 of CPG 230 refers to reputational risk considerations in setting tolerance levels. There are also other references or inferences to 'reputational risk' across the guidance (including in paragraph 58(b) and 65). These would appear to conflict with the explicit removal of 'reputational risk' from the range of 'operational risks' that an entity is required, by CPS 230 paragraph 24, to manage.

Management of service provider arrangements

As a general matter, in some of the clauses in this section of CPG 230 it is unclear whether the intended reference is to material service providers or to service providers more broadly. It appears from the relevant clauses of CPS 230 that the references are to material service providers, however it would be useful for APRA to make this explicit in the guidance.

We note that paragraphs 84(a) and 97 refer to obligations on an 'accountable person'. This term is not defined within the guidance and nor does it reference an existing definition. We anticipate it is intended to reference the definition introduced under the FAR and suggest that this should be clarified within the guidance.

Determination of what is a 'material service provider'

The concept of 'materiality', when determining an entity's material service providers, continues to be a key area of concern for ASFA members, given its importance to understanding the scope of the obligations imposed under CPS/CPG 230.

ASFA members have queried whether, when assessing the 'materiality' of arrangements, APRA considers there to be any nuance based on the type of industry an entity operates in, or whether it views all entities (and industries) through a common lens.

As noted in our submission in relation to CPS 230, ASFA members are heavily focussed on the concept of materiality because outsourced service providers are used to a far greater extent by the superannuation industry than many of APRA's other regulated sectors. It is imperative to ensure that the 'material service provider' concept is clearly – and consistently – understood by all regulated entities and is scoped appropriately. The broader the approach taken to identification of material service providers, the greater the cost and the operational due diligence burden that will be borne by the entity. In the case of RSEs, those costs will ultimately be borne by their members – Australian superannuants.

We note that paragraph 49 of CPS 230 defines 'material service providers' as "those on which the entity *relies to undertake a critical operation* or that expose it to a material operational risk." This conveys that *all* service providers relied on to undertake the critical operation would be considered to be material service providers – the words do not apply a test of materiality, but one of *reliance*. Further, it does not appear necessary for there to be *material reliance*.

Paragraph 49 goes on to define 'material arrangements' in similar fashion as being "those on which the entity *relies to undertake a critical operation* or that expose it to material operational risk." This raises a similar issue – 'relies' would best be understood to include *all* service providers relied on, without any scope for the application or materiality.

Paragraph 50 of CPS 230 then sets out a prescribed list of service providers that a regulated entity must, at a minimum, classify as 'material service providers' unless the entity can justify otherwise. This ability to justify otherwise, which APRA has noted it expects to apply only in exceptional circumstances, sits somewhat awkwardly with the emphasis on reliance in paragraph 49.

While draft CPG 230 seeks to elaborate on the process for determining whether a provider is a material service provider, ASFA members have found paragraphs 93-94 somewhat ambiguous and have requested greater clarity in drafting – especially if, as it appears, APRA considers that determining reliance involves a test of materiality.

For example, while ASFA accepts that investment management as a function would be considered a critical business operation for an RSE, it does not follow that every provider of investment management services is genuinely 'material' for the RSE – some managers may hold an amount that is financially immaterial given the overall size of the RSE's investments, and in practice many managers will be relied upon to support the critical business operation of investment management.

On this basis, an RSE might consider it can justify that those financially immaterial managers are not material service providers, applying the qualification in paragraph 50 of CPS 230. We understand from discussions with APRA staff that this is consistent with APRA's intention as to how paragraph 50 might be applied. However, the repeated references to 'reliance' in paragraph 49 of CPS 230 have caused significant concern amongst ASFA members, especially when taken together with subparagraph 94(a) of CPG 230.

That subparagraph lists, as one of the factors an entity would consider in determining which service providers are material, "whether the service supports a critical business operation". The subparagraph again focuses on the mere fact of an entity's reliance, on a service provider, not on the extent of its reliance. We understand from discussions with APRA staff that the factors listed in subparagraphs 94(a)-(e) are intended to provide additional guidance beyond the position stated in paragraph 49 of CPS 230 about determination of an entity's material service providers, and are to be considered holistically. That is, in ASFA's view, the correct approach – any requirement to treat a provider as 'material' based on any of those factors in isolation would, for an RSE, lead to an outcome where a very large number of providers are deemed to be material service providers, regardless of whether they are in fact material for the RSE.

We consider there would be value in APRA:

- more clearly stating the relevance of 'reliance' when an entity is determining whether a provider is a material service provider
- amending subparagraph 94(a) to refer to "*the extent to which* the service supports a critical business operation"
- clarifying, whether the factors in paragraph 94 are intended to apply to all assessments by an entity of whether a service provider is a material service provider, or only where the entity is considering a service provider that is not of a type prescribed in paragraph 50 of CPS 230
- providing additional examples (beyond those provided in CPS 230 paragraph 50) of the types of providers that it would consider to be material service providers for specific regulated industries. In particular, our members have requested a specific industry-based scenario as an example under subparagraph 94(d), which relates to assessing the degree of difficulty in the existing service provider arrangement and transitioning delivery of services to another provider or bringing it in-house.

With regard to paragraph 99, ASFA members would appreciate further clarity around the requirement for a regulated entity, when selecting and assessing a service provider for material arrangements, to consider, against its risk appetite, 'concentration risk'. In particular, is concentration risk to be considered in relation to the entity itself (for example, where the entity has selected a service provider to provide a number of services) or at an industry level (for example, where there are a number of regulated entities using the same provider), and at the RSE (or entity) level or the supplier level?

Finally, ASFA members would appreciate APRA's confirmation that obligations imposed under CPS/CPG 230 relating to material service providers apply in respect of *material arrangements*. That is, where an agreement or arrangement with a material service provider includes both material and non-material arrangements or services, the prudential requirements are intended to apply to the extent the entity relies on the arrangements or services to undertake a critical operation or that expose it to material operational risk, rather than to all services or arrangements.

Monitoring of risks associated with service providers

ASFA members request additional guidance on APRA's expectations in relation to monitoring of risks managed by fourth parties (paragraphs 90-92). The broader the monitoring requirement, the greater the operational ramifications and costs are likely to be for the regulated entity, therefore it is important to ensure there is clarity around the extent of monitoring that APRA will require, or consider to be 'better practice'.

While draft CPG 230 uses the terminology 'fourth parties', we note that paragraph 91(a) refers to conducting due diligence to identify material fourth parties "and, where feasible, other downstream providers that could materially impact the performance of the service". ASFA requests that APRA provides:

- further guidance on how deep into the service provider chain regulated entities are expected to go – that is, how many levels beyond 'fourth parties'
- confirmation that risk management in relation to 'fourth' and 'downstream' parties should be limited to the impact such parties may have on a regulated entity's critical operations (that is, on material arrangements with the relevant third party service provider and not in relation to the provision of broader services).

Further, we note that many 'fourth parties' will likely be entities that are not themselves regulated by APRA and may be unwilling to facilitate the level of due diligence envisaged in CPG 230. We request clarification of APRA's expectations should that be the case – specifically, we seek confirmation of whether APRA expects a regulated entity to avoid or stop using that provider.

With regard to paragraph 96 (management of operational risk associated with cohorts of service providers), ASFA members have queried:

- whether there is a nuance associated with the size of the operation; and
- if there are sub-outsourcing arrangements, whether entities are required to capture only material service providers or all the sub-agreements associated with a material service provider.

Additionally, ASFA members request further guidance on how oversight of service providers and 'fourth parties' – including their risk management practices – is expected to work in practice. For example, we note that some of the more detailed information requirements may be commercially sensitive and many service providers located in different jurisdictions, and not subject to APRA regulation, may be unwilling to comply. This could result in a potentially harmful impact on regulated entities, as it may force them to cease using reputable providers – who in practice provide a high standard of service, but are unwilling to provide due diligence materials for legitimate security reasons or because it will disclose highly sensitive commercial information – and move to providers who may not provide such a high standard of service, but are more open to providing due diligence materials (for example, smaller providers with less market power).

Requirements for a formal legally binding agreement

Paragraph 101 notes that the formal legally binding agreement required under CPS 230 "would typically be sufficiently flexible to accommodate changes". With respect, ASFA finds this wording somewhat curious, as it could be seen as implying a party to the agreement has the power to unilaterally vary the agreement. ASFA would not expect to see scope for flexibility in a formal agreement. An agreement would typically have an amendment power, or in the absence of an amendment power it would be possible for the parties to agree to amend the contract. It would be appreciated if APRA could provide additional clarity regarding its expectations in this area.

ASFA members have also queried the interpretation of some other aspects of draft CPG 230 and CPS 230 in relation to formal legally binding agreements. To some extent, difficulties with interpretation are likely due to the challenges of applying generically drafted provisions in a cross-industry standard and guidance to specific situations arising in one particular sector. Nevertheless, additional guidance would be appreciated. For example:

- Paragraph 54(e) of CPS 230 requires the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider. We would like to clarify that this is subject to any liability regime that may be negotiated between the parties, including liability limitations and exclusions, such as for indirect loss. In the experience of ASFA's members, service providers may not accept this, and in particular will not accept liability for actions of sub-contractors to the extent that the service provider would not itself be liable to the RSE had it taken those actions itself.
- One of the required elements of a formal, legally binding agreement for a material arrangement is a termination provision that includes "the right to terminate both the arrangement in its entirety or parts of the arrangement": paragraph 54(g) of CPS 230.

A right to terminate 'part' of an arrangement is very unusual in some contexts (for example, investment management, custody). We anticipate that this wording may have been drafted in contemplation of the type of agreements that cover a menu of services where aspects can be switched on or off. However, it is difficult to understand how paragraph 54(g) could be applied to some material service provider arrangements, for example an investment management arrangement entered into by an RSE – it is generally not possible to terminate only part of the investment management function.

In addition, large technology providers generally require customers to make an upfront commitment for a subscription period (usually at least 12 months) and will only permit termination – in whole – in the event of the provider's material breach. These providers often offer pricing on the basis their customers are acquiring a full suite of services, and so will not permit partial termination. Even if these providers were willing to permit regulated entities to terminate services in part, this would likely result in the loss of cost savings that flow from bundled pricing.

ASFA members would appreciate additional guidance, in CPG 230, of how paragraph 54(g) applies to different types of material service provider arrangements. Would an ability to direct providers to cease providing specific services under the agreement be sufficient to satisfy this requirement (even if it is not formally described as a 'termination' right)?

- Further, subparagraph 54(g) requires, for an RSE licensee, termination provisions that "include the ability for the RSE licensee to terminate the arrangement where to continue the arrangement would be inconsistent with the RSE licensee's duty to act in the best financial interests of beneficiaries".

  This requirement would seem to undermine the concept of fixed-term contracting, because it suggests that an RSE licensee will then have both a right and a duty to terminate the arrangement wherever another provider can provide an equivalent service for a lower fee, after factoring in the costs and risks of transitioning to that alternative provider, or without regard to broader commercial relationships. We would appreciate clarification of whether APRA considers this places RSE licensees at a disadvantage compared to other entities such as banks and insurers, who do not need to include an equivalent termination right in their contracts? Has APRA considered the possibility that service providers will raise their prices for RSE licensees accordingly to compensate for this uncertainty, detrimentally impacting members' financial outcomes?

- Paragraph 55 of CPS 230 requires a formal agreement to also include provisions that allow APRA access to documentation, data and any other information related to the provision of the service, allow APRA the right to conduct an on-site visit to a service provider, and ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator.

  We request that APRA considers providing further guidance in CPG 230 regarding this paragraph. In particular, would it be permissible for a material service provider to impose reasonable protections to prevent APRA from accessing its privileged information, information which is subject to bona fide third party confidentiality obligations, information which cannot be provided in accordance with the laws of the service provider's jurisdiction, etc. Clarity will assist in avoiding unnecessary cost, as providers will respond to any perceived uncertainty about the scope of APRA's access under this requirement by pricing it into their contract terms or denying service.

- Paragraph 102 notes that service levels and performance are typically documented via a service-level agreement, which would normally specify the metrics by which the service provider is measured and monitored.

We note that the nature of the 'agreement' may vary depending on the type of material service provider arrangement and not all will specify service levels and performance. For example, an RSE may have an investment of a particular type, such as an unlisted trust, that it entered into pursuant to an application under a Product Disclosure Statement (or international equivalent). In such cases, there will not be an 'agreement' specifying service levels or performance, only a stipulation as to how proceeds will be disbursed during the investment and upon realisation.

- Some aspects of APRA's requirements and guidance are likely to pose challenges where the services providers the regulated entity contracts with are not themselves APRA-regulated. This will particularly be the case where, as a matter of commercial reality, a regulated entity is required to contract with very large-scale service providers that have few – or no – viable competitors for the services provided and are not themselves APRA-regulated (for example, software or cloud service providers). This issue also arises in relation to fourth parties who are not regulated entities.

  Service providers are often unwilling to negotiate their terms, either due to their market power, or the fact they have a large number of customers, or have existing controls and infrastructure in place which they deem appropriate, and will not negotiate bespoke terms. Others will only negotiate contracts if fees are over certain significant monetary thresholds, which regulated entities may not meet. These providers may nevertheless be the only option for regulated entities, or may be the most appropriate provider for a regulated entity to use (for example due to higher quality, greater security or more reliability of service than smaller service providers who may be willing to negotiate contractual terms).

  For example, a regulated entity may reasonably form the view that it is in their beneficiaries' best interests to use reputable, market-leading international service providers who make significant investments in technology security and have a proven track record, even though they cannot negotiate their contractual terms, rather than a smaller provider who may be open to negotiation but has fewer resources and limited track record.

  The alternative may as a practical matter increase risk to regulated entities by requiring them to move to higher-risk, less sophisticated service providers who are willing to contractually agree to the requirements outlined in CPS 230/CPG 230, or alternatively moving the service back in house in situations where the regulated entities may not have the skills, resources or capability to perform the service themselves.

  By way of example, ASFA members envisage difficulties arising in relation to securing contractual obligations in respect of the following:

  - BCP arrangements and tolerance levels – providers may be unwilling to agree to meet a regulated entity's BCP requirements. In particular, providers contracting with multiple RSEs are likely to resist adopting a suite of granular obligations from multiple clients, including adopting a regulated entity's tolerance levels, reporting timeframes, procedures and policies. In effect, this requires a provider to adopt and comply with the risk parameters of the regulated entity with the most stringent risk controls, which will result in a cost pass through to all clients, regardless of whether they have adopted these requirements themselves.
  - Service levels (paragraph 54(a)) – providers may not agree to formal service levels separate from the terms of the agreement itself (but may for example publish service availability targets on their websites which will provide regulated entities with comfort).
  - APRA's access and audit rights (paragraph 55) –providers may not permit audits due to valid security concerns (or otherwise), and instead may only provide certain due diligence materials, RFI responses or certifications.

- Parts of the contract continuing in the case of a force majeure event (paragraph 54(f)) – providers are unlikely agree to perform obligations in circumstances where events outside their control preclude them from doing so. Generally, force majeure clauses are drafted to only excuse a service provider from performing its obligations to the extent that it is unable to do so due to a force majeure event. Accordingly, APRA's expectations in relation to paragraph 54(f) are unclear.
- Termination of part of an agreement (paragraph 54(g)) – as noted above, providers may only permit termination of the agreement "in whole" in the event of their own material breach.
- Paragraph 57 of CPS 230 provides that APRA may require a regulated entity to "review and make changes to a service provider arrangement where it identifies heightened prudential concerns". As noted above, we would not expect a formal legally binding agreement to allow one party to unilaterally make changes to the agreement, even at the behest of a regulator. ASFA requests that APRA provides, in CPG 230, some guidance around its expectations in the event APRA invokes paragraph 57 and the service provider refuses to accommodate the required changes.
- Paragraph 106 outlines better practice in relation to monitoring of key information in relation to service providers. ASFA requests that APRA provides, in CPG 230, some guidance around its expectations where a service provider is unable or unwilling to provide this information. We consider it particularly likely that service providers will baulk at the request to provide information to enable monitoring of "the ongoing viability (financial and non-financial) of the service provider and the services delivered, including strategic plans and investment in the service" (subparagraph 106(f)). This is likely to be highly confidential and commercially sensitive information that most sophisticated service providers would refuse to provide. In addition, it would be useful to have further information about what APRA means by 'non-financial' in this context.

We understand APRA may be open to taking a pragmatic view in relation to service provider compliance with CPS 230/CPG 230. ASFA members would welcome further guidance in this regard, including whether APRA would be open to regulated entities forming the view, acting reasonably, that operational risk is adequately managed through a combination of contractual obligations (to the extent available, which may include obligations on a 'reasonable endeavours' basis) as well as due diligence, monitoring and reporting in respect of risk matters, and other means.

Finally, we note that subparagraph 59(a) of CPS 230 states that a regulated entity must notify APRA "as soon as possible and not more than 20 business days after entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation".

As noted elsewhere in this submission, an entity may rely on a service to undertake a critical operation without that arrangement necessarily constituting a material service provider – for example, the provider may be one of many providing the same service to the entity or providing only a small and discrete function, the absence of which would not result in a disruption of the critical operation. There is not, in paragraph 59, any overlay of the genuine materiality or criticality of the arrangement or the service to the regulated entity. In addition, there may be changes that are material in the context of the agreement itself (for example, the fees payable or indemnities provided) but are unlikely to have any material impact on the entity's operational risk.

Finally, we request clarification from APRA, in CPG 230, about the types of changes it expects to be notified of under CPS 230 subparagraph 59(a) – in particular, whether:

- APRA only wishes to be notified of changes which are material to the entity's overall operational risk profile
- the notification requirement applies to material changes to the services provided, or material changes to clauses and obligations in the service provider agreement.