DISCUSSION PAPER

Risk management prudential standard for private health insurers

December 2016

Disclaimer and Copyright

Preamble

This discussion paper seeks submissions on the extent to which features of the private health insurance (PHI) industry warrant different prudential requirements to those mandated for other APRA-regulated institutions under *Prudential Standard CPS 220 Risk Management* (CPS 220).

To facilitate consultation, the draft version of CPS 220 released with this paper has proposed specific PHI adjustments highlighted.[1] Beyond these adjustments, it is APRA's view that the general requirements of CPS 220 should apply to all PHIs.

The draft versions of the *Prudential Practice Guide CPG 220 Risk Management* (CPG 220) and *Prudential Standard HPS 001 Definitions* (HPS 001) also released with this discussion paper have been updated to include references to the PHI industry and definitions contained in CPS 220. Read in conjunction with the proposed amended version of CPS 220, these documents will assist private health insurers to understand the core principles and requirements of CPS 220.

APRA welcomes submissions on any aspect of the proposed amendments to CPS 220, CPG 220 and HPS 001, but is particularly interested in views on:

- whether there are any features of the PHI industry which warrant different treatment to the requirements set out in the version of CPS 220 released with this paper;
- the proposed transition period if CPS 220 is to be applied to private health insurers; and
- any new material costs a private health insurer may face complying with the standard.

Written submissions should be forwarded to APRA, preferably by email, by 15 April 2017 to: insurance.policy@apra.gov.au.

Submissions should be addressed to:

General Manager
Policy Development
Australian Prudential Regulation Authority

[1] APRA released a new version of CPS 220 on 8 August 2016 (media release 16.24) which will become effective from 1 July 2017. This is the version of CPS 220 relied upon for this consultation process. It can be found at www.apra.gov.au/CrossIndustry/Pages/Supervision-of-conglomerate-groups-L3-august-2016.aspx.

Important disclosure notice – publication of submissions

All information in submissions will be made available to the public on the APRA website unless a respondent expressly requests that all or part of the submission is to remain in-confidence.

Automatically generated confidentiality statements in emails will not suffice for this purpose.

Respondents who would like part of their submission to remain in-confidence should provide this information marked as confidential in a separate attachment.

Submissions may be the subject of a request for access made under the *Freedom of Information Act 1982* (FOI Act).

APRA will determine such requests, if any, in accordance with the provisions of the FOI Act. Information in the submission about any APRA-regulated institution which is not in the public domain and which is identified as confidential will be protected by section 56 of the *Australian Prudential Regulation Authority Act 1998* and will be ordinarily exempt from production under the FOI Act.

Executive summary

Strong and active risk management is fundamentally important to the prudential management of an institution in tandem with sound governance and capital management. Risk management underpins the achievement of both organisational performance and prudential soundness. APRA considers it essential that all private health insurers employ a structured and systematic approach to the identification and management of risk given the complexity of the PHI operational environment.

An effective, enterprise-wide risk management framework supports the board and management of a private health insurer to perform their respective roles. Such a framework provides a critical tool for identifying, assessing and monitoring risks with the potential to materially affect a private health insurer's ability to meet its strategic, business and operational objectives, and to assess a private health insurer's overall risk of failure.

Past reviews of the risk management practices of private health insurers conducted by the Private Health Insurance Administration Council (PHIAC) observed a range of practices – some good and some weaker. Although not systemic, instances of weaker practice included limited board review of risk, low levels of staff awareness and limited use of risk management processes. APRA's current risk management thematic review is confirming that many of these issues remain.

Given the above, APRA is proposing the introduction of risk management requirements for private health insurers in line with those applicable to other APRA-regulated industries with the objective of clearly setting out minimum expectations for how private health insurers should manage risk. In developing the draft CPS 220 attached to this discussion paper, APRA has carefully considered whether each requirement is appropriate for the PHI industry.

Key elements of this discussion paper include:

- a discussion of core principles and requirements of CPS 220;
- an opportunity for the industry to identify if there are any elements of the standard which may not be applicable to the PHI industry; and
- quantification of any additional material costs private health insurers may face in complying with the requirements of CPS 220.

During this consultation round, it is not APRA's intention to open up for review the content or the language of CPS 220 more broadly. The applicability of the standard to the PHI industry is the focus of the consultation round.

APRA's current intention is to finalise any revisions to CPS 220 during 2017, so that the requirements for private health insurers will come into effect from 1 January 2018.

Chapter 1 - Background

As part of its consideration of the introduction of a risk management standard to the PHI industry, APRA has sought to reach an appropriate balance between the objectives of financial safety and efficiency, competition, contestability and competitive neutrality, whilst promoting financial stability.[2]

APRA considers the proposals in this discussion paper will meaningfully enhance the financial safety of individual entities by strengthening their resilience through the adoption of more structured risk management practices. Efficiencies will be realised through the adoption of consistent terminology. The supporting guidance material will clarify APRA's expectations. Costs will be minimised by implementing the standard in a manner appropriate to the size, business mix and complexity of each private health insurer. Adopting a principles-based approach will accommodate the diversity of private health insurers in the market, so as not to alter the competitive balance.

Application of CPS 220

In undertaking the current review, APRA has adopted as its starting point the cross-industry risk management prudential standard CPS 220. Introduced in January 2015, this standard reflects APRA's expectations of sound prudential practice. CPS 220 has been informed by APRA's experience supervising institutions in multiple financial industries over a number of years, observations of better practice within those industries and domestic and international developments.

In APRA's experience, CPS 220 is effective both when applied to large institutions and to smaller institutions. CPS 220 also provides an effective framework for institutions that are part of a wider corporate group, as the standard provides consistency in terminology and expectations.

APRA's initial assessment is that the core principles of CPS 220 are appropriate for the PHI industry. On that basis, this discussion paper proposes that CPS 220 will be applied to the PHI industry. Should sound arguments be raised during consultation that certain requirements of CPS 220 are not relevant, or do not fully reflect circumstances in the PHI industry, APRA will consider modified requirements.

If the amount of change necessary to CPS 220 to properly accommodate the specific circumstances of the PHI industry is significant, APRA will consider a separate PHI risk management standard. At this stage, APRA has not identified any issues that would necessitate a separate standard.

The cross-industry risk management prudential practice guide CPG 220 has been designed to assist APRA-regulated institutions to understand the core principles and requirements of CPS 220. It outlines APRA's view of how the prudential requirements can be met and provides information on good practice. CPG 220 also references other APRA guidance materials which

[2] Section 8(2) of the *Australian Prudential Regulation Authority Act 1998* refers.

may assist private health insurers to understand APRA's expectations of regulated institutions. These include:

- *Prudential Practice Guide CPG 235 Managing data risk;*
- *Prudential Practice Guide PPG 511 Remuneration;* and
- *Aid for Directors of ADIs and insurers*.

Private health insurers are encouraged to familiarise themselves with these documents as part of building their understanding of APRA's approach to prudential supervision.

Previous consultations on risk management

Following the introduction in 2009 of the PHI governance standard (now *Prudential Standard HPS 510 Governance* (HPS 510)), private health insurers have been subjected to periodic review of the effectiveness of their risk management frameworks and practices through a variety of supervisory methods.

Over that period, while many good practices have been identified in the industry, instances of weaker practice have also been identified which, in APRA's view, need to be addressed. These have included:

- limited board oversight of risk management;
- limited application of risk management as a governance mechanism or a business process;
- poor quality risk data going to the board;
- inconsistent training of staff in risk management; and
- few independent reviews of the effectiveness of the risk management practices of private health insurers.

In January 2013, private health insurers were invited by PHIAC to comment on three approaches to improving the effectiveness of risk management practices in the industry. The options considered were:

Option 1: no change to the existing arrangements;

Option 2: release of non-binding guidance material; or

Option 3: development of a prudential standard requiring all private health insurers adopt effective risk management practices.

The majority of private health insurers (by total number as well as market share) expressed a preference to formalise risk management prudential requirements. In November 2013, when private health insurers were invited by PHIAC to comment on a draft risk management prudential standard, the majority of respondents supported introduction of the standard.

In developing this consultation paper, APRA has taken into account the feedback received in response to those earlier consultations. In particular, that:

- prudential requirements should not be set too low;

- terminology should be kept broadly consistent with that of the existing APRA standard for consistency, clarity of messaging and for private health insurers in group structures; and
- guidance material should be provided to support the prudential standard.

This paper also considers the findings of the PHI risk management thematic review program commenced by APRA in late 2015 to assess individual private health insurer's risk governance and operational risk management arrangements. This program of reviews, which is scheduled to conclude in early 2017, indicates that whilst there has been improvement in the practices of some private health insurers, the introduction of a risk management standard and guidance material clearly setting out APRA's expectations will assist all private health insurers to strengthen the effectiveness of their risk management practices.

Harmonisation across APRA-regulated industries

Since its establishment, APRA has sought, where appropriate, to take a consistent approach to the setting of prudential requirements for APRA-regulated institutions in areas such as governance, fitness and propriety, outsourcing, business continuity management and risk management, where the fundamental principles of good practice do not materially vary across industries. Good practice in these areas is not industry-specific.

Whilst harmonising with the requirements applying in other industries is not APRA's main goal, applying APRA's cross-industry risk management prudential standard to the PHI industry would result in like risks being treated in a like manner, utilising a common language across APRA-regulated institutions and simplifying compliance obligations, particularly for those private health insurers operating in group structures with other APRA-regulated institutions.

Consultation process

Interested parties have until 15 April 2017 to comment on this discussion paper and the versions of CPS 220, CPG 220 and HPS 001 released with this paper.

Following consideration of submissions, APRA expects to issue a further paper setting out APRA's response to the key questions and concerns raised, identifying any changes to the proposed approach. If appropriate, that paper will also include an amended standard and practice guide. If significant changes are necessary, a further round of consultations may be undertaken to ensure all matters have been fully considered prior to finalising the prudential standard.

Chapter 2 - Specific Proposals

Role of the board

The board plays a critical role in the prudential management of all APRA-regulated institutions. It sets standards and expectations that have a strong influence on the management and culture of the business and on the quality of its governance.

In explicitly stating that the board of an APRA-regulated institution is ultimately responsible for the institution's risk management framework and oversight of its operations by management, CPS 220 makes it clear APRA expects the board of every private health insurer to provide direction and leadership on the institution's approach to risk management.

CPS 220 requires the board to:

- set a clearly articulated risk appetite so that the boundaries within which management may operate are clear;[3]
- oversee the implementation and ongoing operation of a robust and effective risk management strategy;
- form a view of the risk culture within the private health insurer and the extent to which the risk culture supports the ability of the institution to operate consistently within the board's risk appetite;
- approve a business plan that sets out the approach for the implementation of the strategic objectives of the private health insurer; and
- make an annual risk management declaration to APRA.

APRA expects boards to be able to demonstrate their commitment to the establishment of a strong risk management framework through robust challenge and oversight of key policies and processes implemented by management to identify and effectively manage key risks.

APRA's *Aid for Directors of ADIs and Insurers* (2014) provides further guidance about APRA's expectations of board members.

Risk culture

The establishment and maintenance of a strong risk management culture is essential to the ongoing effectiveness of an institution's risk management framework. APRA has observed that in institutions with a sound risk culture, emerging risks or risk-taking activities are more likely to be recognised, assessed, escalated and addressed in a timely manner.

CPS 220 requires boards to form a view of the risk culture in the institution, the extent to which that culture supports the ability of the institution to operate consistently within its risk

[3] The risk appetite is captured in a formal risk appetite statement. Amongst other things, this must convey the degree of risk that the institution is prepared to accept in pursuit of its strategic objectives and business plan, giving consideration to the interests of depositors and/or policy holders.

appetite, to identify any desirable changes to the risk culture and to ensure steps are taken to address those changes. It is up to individual boards how they meet these obligations and demonstrate to APRA that they are proactively involved in monitoring and influencing the risk culture of the institution.

The current PHI risk management thematic review program is providing an opportunity for private health insurers to discuss APRA's expectations on an individual basis. In these reviews, APRA has sought to understand the private health insurer's attitude to risk awareness, risk taking and risk management, and how each private health insurer is currently monitoring risk culture. CPG 220 provides guidance as to how the board and the senior management of an institution can fulfil their responsibilities in relation to risk culture.

Board risk committee

An independent board risk committee, separate from the board audit committee, provides a board with an objective non-executive oversight of, and advice on, the appropriateness of an institution's risk management framework and assurance that management are appropriately implementing the board's strategy for managing risk. Separate committees for audit and for risk, and separate meetings, can increase the ability of the board to give due focus to risk management matters.

The current PHI prudential standards do not mandate the establishment of a board risk committee. HPS 510 provides that private health insurers have a board audit committee which must include amongst its functions:

> *"an objective, non-executive review of the effectiveness of the private health insurer's risk management framework, unless there is another board committee undertaking this function"*[4]

APRA does not propose to revise HPS 510 prior to its planned review in 2017/18.[5] At that time, APRA will invite comment from the industry on establishing separate sub-committees for audit and risk management. In the meantime, private health insurers are encouraged to consider the merits of establishing a board risk committee.

A number of private health insurers already have a board risk committee in place. APRA encourages those insurers to review the charter of the committee against the requirements of CPS 220.

Group risk management

CPS 220 enables private health insurers that are part of a broader corporate group to meet their risk management obligations on a group basis provided the board of each private health insurer within the group structure can be satisfied that it continues to meet its individual risk management requirements under CPS 220.

To be effective, a group-wide risk management framework must co-ordinate, identify, measure, evaluate, report and control or mitigate all material risks across the group that

[4] Sections 33 and 34 of *Prudential Standard HPS 510 Governance* refer.

[5] APRA's letter to the industry on the prudential policy outlook (4 August 2016) refers.

have the potential to impact any private health insurers within the group structure, not just those risks directly attributable to private health insurers within the group.

APRA proposes to retain the ability to require private health insurers in group structures to meet their risk management requirements on a separate basis to the group where APRA determines that the requirements of CPS 220 are not being met in relation to the private health insurer.

Risk management function

CPS 220 recognises the importance of a structured and systematic approach to the identification and management of risk and requires every APRA-regulated institution have a designated risk management function.

CPS 220 requires the risk management function to be appropriate to the size, business mix and complexity of the APRA-regulated institution. The risk management function is required to be operationally independent and resourced by staff with clearly defined responsibilities, capable of providing effective challenge to activities and decisions which may materially affect the risk profile of the APRA-regulated institution. The risk management function is also to be capable of providing technical support to the board, its sub-committees and senior management on the risk management framework and any significant breaches of, or material deviation from it. APRA proposes to extend these requirements to private health insurers.

Chief risk officer

A critical element of an entity's risk management function is its designated Chief Risk Officer (CRO). CPS 220 formalises this designation. APRA expects the CRO to be of sufficient seniority and independence to be able to effectively challenge decisions and activities which may materially affect the risk profile of the institution. The CRO is to be independent from business lines, other revenue-generating responsibilities and the finance function of the private health insurer, to have a direct reporting line to the Chief Executive Officer and unfettered access to the board and its sub-committees.

APRA does not envisage the CRO assuming responsibility for the key risks of a private health insurer. Rather the CRO is to be responsible for effective risk management in the organisation and implementing the necessary mechanisms to achieve this. For example, some of the CRO's responsibilities might include the training of staff in the identification and management of key risks, facilitating risk assessments, the issue of guidance material, coordination of risk reporting, and assisting with the development, review and maintenance of a private health insurer's risk management framework. The CRO can have a range of other functions, provided they are consistent with the independence requirements set out in CPS 220.

APRA is aware that some of the smaller private health insurers are concerned at the cost involved in having a dedicated CRO. Paragraph 41 of CPS 220 provides scope for smaller, less complex private health insurers to propose alternative arrangements to APRA where a case can be made for different treatment based on their individual circumstances.

Under CPS 220, APRA has considered on a case-by-case basis, institution-specific alternative arrangements to the CRO requirement where an institution could demonstrate that the requirement to have a designated CRO was not cost effective. A number of alternative arrangements, such as a management committee acting as the CRO, dual-hatting with another role, or outsourcing the role have been approved. Typically, these arrangements are for smaller, less complex institutions where the institution has demonstrated that potential conflicts of interest between roles have been identified and can be appropriately managed. APRA anticipates adopting a similar approach in the PHI industry.

Management information system

The establishment and maintenance of an effective management information system (MIS) is a key part of any risk management framework. The design and operation should facilitate the recording, analysis and reporting of information needed to make informed and timely decisions about financial condition, operating performance and key risks.

The MIS should be supported by a robust data framework capable of measuring, assessing and reporting on all material risks across the institution. It should enable the aggregation of exposures and risk measures across business lines, the prompt reporting of limit breaches, forward-looking scenario analysis and stress testing.

APRA is aware that a number of the smaller private health insurers expressed concern in 2013 at the cost of establishing such systems. The recent thematic reviews have identified that there has been some progress towards purchasing off-the-shelf, or developing in-house, systems capable of monitoring key material risks in normal circumstances. There has been less progress on the prompt reporting of limit breaches or stress testing capabilities.

It is a matter for individual private health insurers to determine the design and operation of their MIS and processes. APRA's expectation is that the system adopted will be commensurate with the size, business mix and complexity of the private health insurer and its risk profile. It is also critical that the system be capable of providing the board with timely and accurate reports on financial condition, operating performance, key risks and limit breaches.

For smaller institutions, relatively basic systems to capture and record information may suffice. Larger institutions will be expected to have more sophisticated systems to support robust management of a more complex set of risks. In all instances, reporting to the board should be sufficient to provide the board with assurance regarding the comprehensiveness of the identification of risks facing the institution and the effectiveness of the controls in place to manage those risks.

Periodic reviews

CPS 220 requires two types of periodic review of the risk management framework:

- an annual review that covers compliance with and effectiveness of the risk management framework, by internal and/or external audit; and

- a three-yearly comprehensive review of the appropriateness, effectiveness and adequacy of the framework, by an operationally independent expert.

The key difference between the two types of reviews is the depth and scope of the assessments.

The annual review is to focus on the current state of the risk management framework and assess the effectiveness of and compliance with individual components of the framework in accordance with a rolling audit plan.

APRA is currently reviewing the role of the Appointed Actuary across all insurance industries.[6] APRA's life insurance and general insurance frameworks currently require that the Appointed Actuary include in the annual Financial Condition Report an assessment of the suitability and adequacy of the insurer's risk management framework. APRA is currently considering that requirement in the context of the review of the role of the Appointed Actuary and has proposed some changes. APRA has yet to reach a decision on how the outcomes of that review will apply in relation to private health insurers.

The three-yearly reviews of the risk management framework are intended to provide a holistic, institution-wide view of the ongoing effectiveness of the risk management framework, including interaction of its key elements. This review should also provide an assessment of, and recommendations on the appropriateness of the risk management framework going forward. APRA's requirements as to the content of these reviews is clearly set out in CPS 220 and CPG 220.

In the 2013 PHI risk management consultations, a number of private health insurers expressed concern at the potential cost of five-year independent reviews, noting that they did not expect such reviews would produce outcomes dissimilar to internal audit reviews. APRA sees considerable value in periodic, operationally independent reviews of a risk management framework. In other regulated industries, such reviews have meaningfully contributed to enhancing the quality of the risk management framework. On that basis, APRA proposes to apply the three-year review requirement to the PHI industry.

CPS 220 provides that the three-year reviews are to be conducted by persons identified as operationally independent of the APRA-regulated institution. Whilst in many cases APRA-regulated institutions use an external consultant to undertake this review, there is no requirement that these reviews be undertaken by an external party. An internal party or current service provider employed by a private health insurer will be able to undertake the comprehensive review provided they have appropriate expertise and operational independence.

Annual risk management declaration

In addition to requiring annual and three-year reviews of the risk management framework, CPS 220 requires confirmation that there are systems in place to ensure compliance with

[6] The discussion paper: *The role of the Appointed Actuary and actuarial advice within insurers* (June 2016) is available on the APRA website.

legislative and prudential requirements, and that the board has satisfied itself as to the adequacy of, and compliance with the risk management framework. The annual review is likely to be key to this attestation.

Attachment A to CPS 220 sets out the minimum statement which the board must make to APRA each year in the form of an annual risk management declaration. There is no APRA approved form for completing this annual declaration, leaving it open to boards to provide additional information in the annual declaration should they wish to do so. For example, if there have been significant breaches of, or material deviations from, the risk management framework during the year, this additional information would be expected to be included in the annual declaration together with what actions have been employed to mitigate any issues or minimise such breaches in the future.

In signing the annual declaration, APRA expects the board to have obtained reasonable assurance and, if necessary, considered independent advice on the matters covered by the declaration prior to it being signed.

Material risks

A key difference between CPS 220 and the draft 2013 PHI risk management standard released by PHIAC is that CPS 220 puts the onus on each private health insurer to identify, measure, monitor and report on its material risks. APRA defines material risks in a principles-based way, as those risks that could have a material impact, both financially and non-financially, on the institution, or on the interests of policy holders. CPS 220 is therefore less prescriptive than the draft 2013 PHI risk management standard. For example, while paragraph 26 of CPS 220 lists core material risks to APRA-regulated institutions, it is the responsibility of each APRA-regulated institution to determine whether all those risks are material to its operations. The list is not intended to be exhaustive, and, where a listed risk is found to not be material to an institution's operations, there is no expectation by APRA that it be considered in detail.

Similarly, for breach reporting purposes, under CPS 220 it is the responsibility of each APRA-regulated institution to determine the threshold for the reporting of significant breaches of, or material deviations from the risk management framework, based on its risk appetite, risk profile and risk tolerance. APRA considers this to be another significant difference from the 2013 PHI risk management standard issued by PHIAC, which required private health insurers report all breaches of the standard.

Capital management policy

Under *Prudential Standard HPS 110 Capital Adequacy* (HPS 110), private health insurers are required to have a board endorsed capital management policy. CPS 220 requires APRA-regulated institutions in other industries to include an Internal Capital Adequacy Assessment Process (ICAAP) as part of their risk management framework. A capital management policy and an ICAAP are fundamentally similar. However, in its current form, APRA considers the PHI capital management policy to be less explicit on the identification, monitoring and management of key risks and the capital held against such risks than the ICAAP process.

As APRA is not proposing to review HPS 110 until 2018/19, unless a prudential issues or other change arises which warrants an earlier review, APRA does not propose to require private health insurers develop an ICAAP in the interim. Private health insurers can continue to rely on the capital management policy as set out in HPS 110 until APRA reconsiders this issue in the context of the broader PHI capital standards review of 2018/19.

Aspects of CPS 220 that are not relevant to PHIs

Under CPS 220 some industry-specific requirements for risk management are necessary or appropriate, particularly where there are underlying differences in the legislative framework applying to a particular industry. In such areas, industry-specific requirements are included in CPS 220 and are clearly expressed as such.

In considering the version of CPS 220 attached to this discussion paper, private health insurers need not consider provisions which relate specifically to other APRA-regulated industries. For example, references to:

- Level 2, Level 3 and Category C insurers, EFLICs and NOHCs - these terms apply to authorised deposit-taking institutions, life insurers and/or general insurers;
- Head of group references –a reference to a 'Head of group' in CPS 220 is a reference to a Level 2 Head or Level 3 Head, as relevant;
- Reinsurance management strategy or run-off insurer – terms applicable only to the general insurance industry;
- Foreign institution requirements - not applicable to the PHI industry as all registered private health insurers are required to be companies within the meaning of the *Corporations Act 2001*.[7]

Adjustments and exclusions

Paragraph 56 of CPS 220 provides APRA with the discretion to adjust or exclude the application of specific requirements contained in CPS 220 for individual APRA-regulated institutions. This provision, which is a standard feature of all APRA prudential standards, enables APRA-regulated institutions that can demonstrate that a requirement of the standard is inappropriate for their particular circumstances, to propose alternate arrangements to APRA which meet in substance the principle underlying the requirement.

Such applications will be considered on a case-by-case basis but should not form part of submissions during this first round of consultations, as the focus of this consultation round is the broad applicability of CPS 220 to the PHI industry, not individual circumstances.

Applications for an adjustment or exclusion from a requirement of CPS 220 will be considered once the final form of the standard is settled. APRA anticipates that the number of adjustments or exclusions will be relatively limited.

[7] Section 12 of the *Private Health Insurance (Prudential Supervision) Act 2015* refers.

Consequential amendments

Concurrent with APRA's review of CPS 220 for the PHI industry, APRA has reviewed *Prudential Standard HPS 001 Definitions* (HPS 001) to harmonise language, to facilitate understanding of the terminology used in CPS 220 and to resolve a number of minor typographical errors in the current document.

The amended HPS 001 has been released in draft form with this discussion paper for consultation.

Transition period

Subject to the outcomes of consultation, APRA will establish appropriate arrangements to facilitate the PHI industry's transition to CPS 220.

APRA proposes a transition period of at least six months from the date of making the prudential standard. APRA expects this will provide sufficient time for most private health insurers to be able to comply with CPS 220 as the standard is aligned to accepted, prudent business practice. Where APRA has already identified areas for improvement in a private health insurer's risk management framework through APRA's ongoing program of supervision activities, the private health insurer is already engaged in processes to meet APRA's expectations as set out in CPS 220 in the medium term.

APRA's intention is to finalise a risk management prudential standard for the PHI industry in the first half of 2017, for effect from 1 January 2018. APRA will, however, give consideration, on a case-by-case basis, to institution-specific longer transition arrangements where an insurer can demonstrate a robust plan to achieve compliance.

Chapter 3 – Next steps

Written submissions

APRA invites written comment on the proposals in this paper, in particular:

- whether there are any features of the PHI industry which warrant different treatment to the requirements set out in the version of CPS 220 released with this paper;
- the proposed transition period that would be necessary if CPS 220 is to be applied to private health insurers; and
- any material new costs a private health insurer may face in complying with the standard.[8]

Submissions can be forwarded to APRA via email by 15 April 2017 to: industry.policy@apra.gov.au marked for the attention of the General Manager, Policy Development.

APRA's response

APRA will carefully consider all submissions, update the proposals as appropriate and release a second paper responding to key questions and concerns raised. The response paper will identify any changes to the proposed approach and, if appropriate, include an amended standard and practice guide.

If significant changes are necessary, a further round of consultations may be undertaken to ensure that all matters have been fully considered prior to finalising the prudential standard. APRA's current intention is to finalise any revisions to CPS 220 during 2017, so that the new requirements for private health insurers will come into effect from 1 January 2018.

Further reviews

As noted in APRA's 4 August 2016 letter to all private health insurers discussing the prudential policy outlook for the PHI industry, once APRA's consultations on risk management are well advanced, APRA intends to commence the consultation process for business continuity, outsourcing and related matters. APRA is also looking to commence Phase 2 of its three-year systematic review of the PHI prudential framework in 2017, in particular, to consult on governance, fit and proper, disclosure and the role of the auditor.

Although APRA has not reached any decisions on the direction of those reviews, APRA anticipates that, in a similar way to APRA's review of risk management, the cross-industry *Prudential Standards CPS 231 Outsourcing*, *CPS 232 Business Continuity Management*, *CPS 510 Governance* and *CPS 520 Fit and Proper* are likely to be appropriate to the PHI industry. APRA

[8] See Chapter 4 with respect to cost-benefit information

encourages private health insurers to familiarise themselves with the requirements of those prudential standards in preparation.

Chapter 4 – Cost-benefit analysis information

To improve the quality of regulation, the Australian Government requires all proposals to undergo a preliminary assessment to establish whether it is likely that there will be business compliance costs. If a private health insurer considers that compliance costs will increase significantly as a result of the proposals in this paper, it should provide in its submission an assessment of the impact on compliance costs. In particular, APRA is interested in estimates of the compliance costs associated with:

- the establishment of a CRO position;
- establishment of a MIS system; and
- the annual and three-year independent reviews of a private health insurer's risk management framework.

Compliance costs are defined as direct costs to businesses of performing activities associated with complying with Government regulation.

Consistent with the Government's requirement, APRA will use the methodology in the Regulatory Burden Measurement Framework to assess any increase in compliance costs identified by submissions. This framework is designed to capture the relevant costs in a structured way, including a separate assessment of upfront and ongoing costs. Further information is available at: http://www.dpmc.gov.au/office-best-practice-regulation/publication/regulatory-burden-measurement-framework-guidance-note.

Private health insurers should, if possible, use this methodology to estimate any increase in compliance costs to ensure that the data supplied to APRA can be aggregated and used in an industry-wide assessment.

When submitting cost assessments to APRA, private health insurers should include any assumptions made and, where relevant, any limitations inherent in their assessment. Feedback should address any additional costs incurred as a result of complying with APRA's requirements or expectations, not activities that private health insurers would undertake regardless of regulatory requirements in their ordinary course of business.

Glossary

APRA	Australian Prudential Regulation Authority
APRA-regulated institution	an ADI under the *Banking Act 1959*, a general insurer under the *Insurance Act 1973*, a life company under the *Life Insurance Act 1995*, a private health insurer under the *Private Health Insurance (Prudential Supervision) Act 2015*, a non-operating holding company registered under the Banking Act, the Insurance Act or the Life Insurance Act and a Level 2 Head or a Level 3 Head
CRO	Chief Risk Officer
ensure	when used in relation to a responsibility of the board, means to take all reasonable steps and make all reasonable enquiries as are appropriate for a board so that the board can determine, to the best of its knowledge, that the stated matter has been properly addressed
FOI Act	*Freedom of Information Act 1982*
FSCODA	*Financial Sector (Collection of Data) Act 2001*
Level 1 insurer	an individual APRA-regulated institution
Level 2 group and Level 3 group	definitions relevant to other industries regulated by APRA. The terminology does not apply to private health insurers at present a Level 2 group is a consolidated group within a single APRA-regulated industry, headed by an authorised-deposit taking institution, general insurer or an authorised non-operating holding company a Level 3 group is a consolidated group that has been determined as a Level 3 group by APRA in writing where APRA considers that material activities are performed within the group across more than one prudentially regulated industry and/or in one or more non-prudentially regulated industries
MIS	Management information system
PHI	private health insurance
PHIAC	Private Health Insurance Administration Council (1989-2015)

private health insurer	for the purposes of this discussion paper, means a private health insurer registered under section 15 of the *Private Health Insurance (Prudential Supervision) Act 2015*
prudential requirements	includes requirements imposed by APRA on any APRA-regulated institution either through legislation, the APRA prudential standards, APRA rules, reporting standards made under FSCODA and any requirements imposed by APRA in writing
prudential standards	those made under sub-section 92(1) of the *Private Health Insurance (Prudential Supervision) Act 2015*

Prudential standard references

CPG 220	*Prudential Practice Guide CPG 220 Risk Management*
CPS 220	*Prudential Standard CPS 220 Risk Management*
HPS 001	*Prudential Standard HPS 001 Definitions*
HPS 110	*Prudential Standard HPS 110 Capital Adequacy*
HPS 510	*Prudential Standard HPS 510 Governance*

APRA