Ms Heidi Richards
General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
GPO BOX 9836
SYDNEY NSW 2001

Email: PolicyDevelopment@apra.gov.au

12 June 2018

Dear Ms Richards

CPS 234 INFORMATION SECURITY (CPS 234)

The Insurance Council of Australia[1] (Insurance Council) welcomes the opportunity to comment on the proposals outlined in APRA's Discussion Paper for a new cross-industry prudential framework for the management of information security (Discussion Paper) and the associated draft Prudential Standard CPS 234 Information Security (CPS 234).

The Insurance Council is broadly supportive of APRA's proposals. The decision to establish a Prudential Standard introducing new principles and minimum requirements for the management of information security across APRA regulated entities' will assist to strengthen our members' resilience to cyber risks across the extended business environment. The Insurance Council considers, however, the clarity of the requirements in CPS 234 could be improved and greater recognition of the complexity of implementation.

In particular, the Insurance Council advocates greater consistency between APRA's requirements and other regimes around data and privacy breaches; adequate time for implementation, especially in regard to renegotiation of third party arrangements; and a satisfactory intermeshing between CPS 234 and other prudential standards, particularly CPS 220 and 231.

The key issues for Insurance Council members are detailed in the following attachments:

- Role of the Board (Attachment A);
- Notification (Attachment B);
- Assessment of Third Party Information Security Capability (Attachment C);
- Groups (Attachment D);
- Implementation period (Attachment E); and

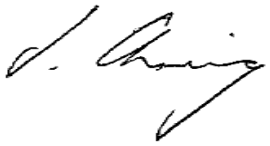
[1] The Insurance Council of Australia is the representative body of the general insurance industry in Australia. Our members represent more than 90 percent of total premium income written by private sector general insurers. Insurance Council members, both insurers and reinsurers, are a significant part of the financial services system. December 2017 Australian Prudential Regulation Authority statistics show that the private sector insurance industry generates gross written premium of $44.9 billion per annum and has total assets of $118.6 billion. The industry employs approximately 60,000 people and on average pays out about $132 million in claims each working day.

- General approach (Attachment F).

I have included some specific drafting suggestions in Attachment G.

If you have any questions or comments in relation to our submission, please contact John Anning, the Insurance Council's General Manager Policy, Regulation Directorate, on (02) 9253 5121 or janning@insurancecouncil.com.au.

Yours sincerely



for
Robert Whelan
Executive Director & CEO

ATTACHMENT A

ROLE OF THE BOARD

Paragraph 12 sets out the responsibility of the Board, including reference to the Board "… ensuring that the entity maintains the information security ...". This drafting could be interpreted as suggesting that the Board has some level of operational responsibility for information security management, rather than oversight of it.

The Insurance Council suggests that the drafting of CPS 234 be more closely aligned with CPS 220, paragraph 9, which states the Board is "ultimately responsible for the institution's risk management framework and is responsible for the oversight of its operation by management". CPS 234 could be reworded along the lines that the Board is "ultimately responsible for the entity's information security capability commensurate with the size and extent of threats to its information assets, and is responsible for the oversight of its operation by management".

If, however, APRA's preference is to retain the term "ensuring" in paragraph 12, in order to ensure consistency of interpretation it should be defined as per Prudential Standard GPS 001 *Definitions* in line with other prudential standards, including CPS 220.

Paragraph 28 sets out a requirement for escalation and reporting to the Board or senior management on testing results in certain circumstances. Whilst reporting to the Board in certain circumstances is appropriate, the Board's responsibility to "respond" should be in regard to remediation plans as proposed by management. This should be better reflected in the drafting.

ATTACHMENT B

NOTIFICATION

APRA Notification

34. An APRA-regulated entity must notify APRA as soon as possible, and no later than 24 hours, after experiencing an information security incident that:

> *(a) materially affected, or had the potential to materially affect, financially or no-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers (referred to in this submission as "stakeholders")*
>
> *(b) has been notified to other regulators, either in Australia or other jurisdictions.*

35. An APRA-regulated entity must notify APRA soon as possible and no later than five business days after identifying a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.

The notification requirements set out in paragraph 34 present a range of practical issues and do not align with related mandatory data breach laws in Australia. There are also potentially international implications as it is not clear if the application is solely to stakeholders[2] in Australia (consistent with APRA's mandate) or extends to those outside Australia.

An "information security event" will not always involve a data breach (for example, denial of service, malware or phishing incidents) and in such cases the incident would only affect the interests of the "entity". Unlike many business continuity events, an information security incident may not be as immediately identifiable and the extent of impact or potential impact is likely to require analysis and investigation.

In contrast, an "information security incident" affecting the interests of stakeholders is most likely to involve, and be intrinsically linked to, a data privacy incident and/or breach and therefore needs to be considered together with the notifiable data breach obligations in this area.

Under the *Privacy Act 1988* (Cth) (Privacy Act), a data breach is "eligible" if it is likely to result in "serious harm" to any of the individuals to whom the information relates. An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds;
2. this is likely to result in serious harm to one or more individuals; and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

The Office of the Australian Information Commissioner (OAIC) has issued substantial guidance in each of these areas: *Data breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1998 (Cth)*, February 2018.

[2] This submission uses "stakeholders" to refer to "depositors, policyholders, beneficiaries, or other customers.

APRA's concept of "materially affected, or had the potential to materially affect, financially or non-financially" introduces an additional criteria that has the potential to be inconsistent, adds complexity and is less specific than the criteria established under the Privacy Act. This creates an added cost and burden for the industry and the associated benefits are not clear, especially as they relate to the stakeholders affected or potentially affected given the specific nature of the Privacy Act requirements.

Notification to the OAIC in accordance with the Privacy Act is required "promptly" if an entity is aware of reasonable grounds to "believe that there has been" an eligible data breach. If the entity only has reason to "suspect that there may have been" a serious breach, it needs to undertake an assessment within thirty (30) calendar days. Once the entity is aware that there are reasonable grounds to believe that there has been an eligible data breach (during the assessment or when the assessment is complete), prompt notification to OAIC is required.

Providing entities with a reasonable timeframe in which to undertake an assessment is likely to facilitate greater clarity in relation to an incident, including the extent of the impacts. Regulators are accordingly provided with more complete information, rather than notifications relating to matters which, once investigated, may not be assessed as material in nature.

The Insurance Council strongly recommends that APRA consider aligning its reporting criteria with those established under the Privacy Act. In summary:

For information security incidents:

a) affecting stakeholders *in Australia* – reporting should be aligned with the Privacy Act such that entities would be required to notify APRA within 24 hours of notifying the OAIC of a data breach, with no additional materiality criteria for reporting to apply;

   An alternative that would be less burdensome for entities would be for APRA to be provided with these notifications direct from the OAIC;

b) affecting stakeholders *outside Australia* – reporting should be aligned with local privacy/data laws such that entities would be required to notify APRA where notification has been made to other regulators, within five (5) business days of that notification (the longer timeframe allowing for time differences and internal reporting processes). This would help avoid conflicting obligations for groups operating in multiple jurisdictions; and

c) affecting an "entity" (including an entity forming part of a group) *in and outside of Australia* – reporting should remain based on APRA's proposed materiality criteria but with a timeframe consistent with the Privacy Act (promptly or within 30 days) that commences upon the entity "becoming aware" of the incident, not from when the incident was "experienced" (as there may be a time delay between the two) to provide a reasonable time for the entity to investigate the incident. (See discussion below on this point.)

   An alternative could be to provide a reporting timeframe of at least ten (10) business days upon the entity becoming aware of the incident.

For information security control weaknesses:

d) Paragraph 35 would be deleted and information security control weaknesses would be reported to APRA in accordance with CPS 220 (paragraphs 53 and 49-51) and the associated reporting timeframe of ten (10) business days.

Suggested amendments to CPS 234 to reflect the above approach are:

1) Paragraph 34(a) would remove reference to "depositors, policyholders, beneficiaries, or other customers" and be limited in application to "entities", with the timeframe extended from 24 hours to "promptly or within 30 days" (or alternatively to a minimum 10 business days);

2) Paragraph 34(b) would include reference to "depositors, policyholders, beneficiaries, or other customers", and where affecting overseas stakeholders, the timeframe would be extended to five (5) business days (for notifications to other Australian regulators the timeframe would remain as 24 hours); and

3) Paragraph 35 would be deleted and information security control weaknesses would be reported to APRA in accordance with CPS 220.

There may be circumstances where an information security incident also meets the criteria for notification to APRA as a major disruption under CPS 232. In such circumstances, the CPS 232 reporting timeframe should prevail (if APRA extends the reporting timeframes under CPS 234). However, the Insurance Council would encourage APRA to consider alignment upon review of CPS 232 during 2018.

Drafting suggestion: "Experiencing"

Paragraph 34(a) and (b) refer to the entity '*experiencing* an information security incident'. The expression 'experiencing' is a key concept in the reporting obligations set out in paragraphs 34(a) and (b), but its technical meaning is unclear and doesn't provide an effective trigger for notification. For example, there may be a time gap between an entity's information security framework being affected by or 'experiencing' an issue and the actual identification of the issue. By contrast, the trigger for notification under draft paragraph 35 is the entity '***identifying*** a material information security control weakness'. We recommend that the concept of 'identification' is used as the common trigger across all reporting requirements in CPS 234.

ATTACHMENT C

ASSESSMENT OF THIRD PARTY INFORMATION SECURITY CAPABILITY

15. Where information assets are managed by a related party or third party, the APRA–regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.

Given the broad definition of "information assets" it is likely that almost all entities providing services to an insurance group's operations (including for example claims processing and loss adjusting, IT services and professional services) are likely to "manage information assets" in some capacity.

When considering the extent of the obligation created by this provision, it is unclear whether:

a) an assessment of information security capability is to be undertaken for all service providers which manage information assets and if the assessment is to be "commensurate with the potential consequences of an information security incident"; or

b) an assessment of each service provider which manages information assets should be undertaken "commensurate with the potential consequences of an information security incident" and the assessment of information security capability is then undertaken for those service providers where the potential impact of a security incident has been assessed as material.

If the intention is the interpretation in (a), then a transitional arrangement of at least two years should apply in respect of all non-material service providers. This would provide a more reasonable period of time for entities to assess all of their service providers and to review and amend contractual arrangements where required. (See Attachment E, Implementation Period.)

In addition, if this is the intended interpretation, the Insurance Council would appreciate clarification in relation to the application of these requirements to a group's overseas operations as the impact of applying these requirements to all service providers globally is likely to be extensive.

If the interpretation in (b) is the intention, then the Insurance Council considers that this could be more clearly applied within the context of CPS 231, where the potential consequences of an information security incident could be included as a criteria in determining the materiality of a service provider. It would then follow that the additional requirements relating to the assessment of a service provider's information security capability be addressed within CPS 231. A co-ordinated implementation date would be appropriate in this context. (See Attachment F, General Approach.)

ATTACHMENT D

GROUPS

No need to specifically extend obligations to service providers part of the same group

Consistent with the approach of other prudential standards (including CPS 220 Risk Management), it is appropriate to extend CPS 234 to groups. However, in order to avoid duplication of requirements, the Insurance Council suggests that the specific application of certain provisions to "related parties" which are service providers managing information assets (paragraphs 15, 21, 27 and 33) should not extend to those service providers that are part of a Level 2 or Level 3 Group. Such related entities would naturally fall within the scope of a group's compliance with CPS 234.

Implications for the use of group resources

On a literal reading of CPS 234, an APRA-regulated entity must itself comply with each of the obligations. However, in practical terms, there should scope for the obligations in paragraphs 14, 16, 17, 20, 22, 23, 24, 26, 30 and 31 to be met (either wholly or partly depending on the obligation) by the APRA-regulated entity's group resources.

For example, where an APRA-regulated entity is part of a global international group headquartered offshore, the entity may work in conjunction with global or regional technology services companies or other dedicated IT resources located offshore to fully address the requirements of these clauses. In these circumstances, an entity's information security framework will consist of a number of layers or levels of defence, some of which are arranged globally or regionally. This provides for centralisation of expertise and efficiency while ensuring cost effectiveness.

For example, paragraph 26 of CPS 234 includes a requirement to test the effectiveness of information security controls through a systematic testing program. Whilst the ultimate accountability for this testing process should rest with the APRA–regulated entity and its Board, this requirement will be met using dedicated resources within the group but which are external to the APRA regulated entity.

ATTACHMENT E

IMPLEMENTATION PERIOD

APRA has recognised the need to provide supplemental guidance to support this standard in CPG 234 and the intention is to finalise CPS 234 and CPG 234 in the second half of 2018 with a proposed commencement date of 1 July 2019. This will be challenging for regulated entities as it does not provide sufficient time to take a strategic approach to implementing required changes, especially those that relate to third parties.

In determining the commencement date of CPS 234 and CPG 234, the Insurance Council suggests that APRA takes a staggered implementation timeframe, with considerably more time allowed for those obligations with third party considerations given the time needed to renegotiate those arrangements. In this regard, it is worth noting the approach adopted by the New York State Department of Financial Services (NY DFS) in 23 NYCRR Part 500, a regulation establishing cybersecurity requirements for financial services companies.

The NY DFS has recognised the time it will take to implement each of the requirements set out in its regulations will vary, depending on its nature. Critically, the NY DFS has recognised that the policies and procedures designed to ensure the security of information systems that are accessible or held by third party service providers are likely to require the most time to implement, and they have granted an additional 24 months for entities to implement these requirements on top of the initial 180-day implementation period.

The NY DFS third party requirements echo many of the requirements set out by APRA in draft CPS 234, including the identification and risk assessment of third party service providers, minimum cybersecurity practices required to be met by third parties, due diligence processes to evaluate the adequacy of cybersecurity practices of third parties, and periodic assessment of third party providers to ensure continued adequacy of their cybersecurity practices.

Consequently, the Insurance Council recommends that APRA consider a similarly staggered implementation timeframe for certain CPS 234 obligations, particularly the requirements with third-party considerations. For the paragraphs listed below, the Insurance Council proposes a 24 month implementation period:

- Paragraph 15: which requires where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party;
- Paragraph 19: which requires that an APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity;
- Paragraph 20: which requires that an APRA regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner;
- Paragraph 21: which requires that where information assets are managed by a related party or third party, an APRA-regulated entity must evaluate the design and operating effectiveness of that party's information security controls;

- Paragraph 27: which requires that where information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, an entity must assess whether that testing is commensurate with the requirements in paragraph 26(a)-(e);
- Paragraph 31: which requires that an APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties; and
- Paragraph 33: which requires that where information assets are managed by a related party or third party, internal audit must assess the information security control assurance provided by that party where an information security incident affecting those information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers.

For all other requirements in CPS 234, the Insurance Council recommends that APRA provides a 12 month period to achieve compliance dating from the publication of finalised versions of CPS 234 and CPG 234 for topics other than those related to third party arrangements.

ATTACHMENT F

GENERAL APPROACH

The Discussion Paper canvassed three options for enhancing the framework for the qualitative management of operational risk:

e) Option 1: status quo;

f) Option 2: stepped approach;

g) Option 3: simultaneous approach.

APRA's preferred approach is option 2: the stepped approach as implementation of the full proposal in two stages would allow industry to focus attention on information security; and area which APRA considers to be an industry weakness. Not having APRA's sector wide perspective, the Insurance Council defers to APRA's judgement in identifying matters of industry weakness. However, we agree with APRA's decision to make action on information security a priority.

In doing so, the Insurance Council suggests that requirements relating to service providers would be better placed in Prudential Standard CPS 231 *Outsourcing* (CPS 231). Including requirements in CPS 234, as well as CPS 231 and also other prudential standards, such as CPS 220 and Prudential Standard CPS 232 *Business Continuity* (CPS 232), makes it difficult to readily grasp a coherent, comprehensive view of prudential requirements. Given that APRA has stated it is also reviewing CPS 231 and 232 during 2018, there is an opportunity to ensure these standards operate seamlessly and practically together.

While pursuing this, the Insurance Council would encourage APRA to consider aligning the compliance date for obligations related to third party arrangements with the implementation of revised Prudential Standard *CPS 231 – Outsourcing*. On the basis of the arguments in Attachment E Implementation Period, the Insurance Council suggests a common compliance date of two years from final issue of CPS 234 and related guidance.

A number of footnotes in CPS 234 state that certain of its paragraphs are not applicable if related or third parties are 'captured as service providers of outsourced material business activities' under CPS 231, Outsourcing (CPS 231). The Insurance Council suggests that this be reviewed as the footnotes in CPS 234 could be read as raising questions as to how outsourced providers, as defined in CPS 231, would comply with the various information security obligations under CPS 234.

INSURANCE COUNCIL OF AUSTRALIA

ATTACHMENT G

DRAFTING SUGGESTIONS

The Insurance council suggests that the comprehension of CPS 234 could be made easier by a number of drafting improvements.

Information security capability

Paragraph 14 requires an entity to "establish an information security capability that meets the requirements of paragraph 12". However paragraph 12 sets out the Board's responsibility in relation to information security management.

The Insurance Council queries whether the intention is that the information security capability should be "commensurate with the size and extent of threats to those assets, and which enables the continued sound operation of the entity" rather than a reference to the Board's role. If so, this may be better expressed by a specific repeat of this in paragraph 14 and perhaps a reference to the definition of an information security capability, as set out in paragraph 11(c).

Paragraph 15 establishes an overarching requirement for an entity to assess the "information security capability" of service providers, where information security capability is defined in paragraph 11(c) to be "the totality of resources, skills and controls which provide the ability and capacity to maintain information security".

Paragraph 21 requires an assessment of the "design and operating effectiveness of that party's information security controls" and, where testing is relied on, paragraph 27 requires an assessment of "whether that testing is commensurate with paragraph 26(a)-(d)".

The requirements of paragraphs 21 and 27 are specific elements which would be included within the scope of paragraph 15 and duplication removed. Paragraph 15 could be expanded to incorporate the effectiveness of controls and assessment of testing as specific examples, should this be considered necessary.

Information asset identification and classification

Paragraph 19 requires an entity to classify its information assets by "criticality and sensitivity" and provides a high-level statement of "criticality and sensitivity". The Insurance Council queries whether these terms are more specifically intended to be interpreted as per the definitions in APRA's *Information Paper on Shared Computing Services (including cloud)* (July 2015) or whether it is APRA's intention that an entity define these terms in the context of its own business requirements.

The Insurance Council raises this question in light of CPG 234 Management of security risk in information and information technology paragraph 20, specifying that an "institution's IT asset classification method and granularity would normally be determined by the requirements of the business".

Implementation of controls

Paragraph 20 states that the entity itself shall have information security controls in respect of information assets held by related and third parties. When its information assets are held by a related or third party, an APRA-regulated entity will rely (at least in large part) on the information security controls of its related or third parties.

In those circumstances, it should be sufficient for the APRA-regulated entity to satisfy itself that its related or third party has information security controls of the type detailed in the draft paragraph 20.This appears to be the intention of paragraph 20 as paragraph 21 requires an APRA-regulated entity to evaluate the design and operating effectiveness of that party's information security controls.

Incident management

Paragraph 25 establishes a requirement for an entity to "annually confirm that its information security response plans are effective". More detail around APRA's expectations in relation to this confirmation needs to be included in CPS 234 to address matters such as:

- the form of the confirmation;
- responsibility for completion, approval and submission (for example, is confirmation from management to the Board or from the Board to APRA);
- alignment with the annual Risk Management Declaration as required by CPS 220; and
- the basis for confirmation (for example, internal assurance, testing and audit processes versus independent validation).

This confirmation also implies a requirement to test the information security response plans so as to be able to confirm their effectiveness. Explicit recognition of this could be included in paragraph 26 that outlines the requirements for testing of information security controls.

Testing Control Effectiveness

Paragraph 28 may benefit from some supporting guidance in CPG 234 in relation to APRA's expectations on materiality/level of risk posed by identified deficiencies, and on timeliness of remediation. For instance, deficiencies of a critical or high nature (defined in line with an entity's risk management framework) are likely to be appropriate for escalation and reporting. For timeliness, there may be deficiencies identified that require investment and change in IT systems thereby taking some time to resolve, but this should be considered in the context of the level of risk posed by the identified deficiency.

Paragraph 29 establishes a requirement for testing to be undertaken by "functionally independent specialists". Does APRA have specific expectations in relation to this? For example, where a first line business function exists, perhaps within the IT and information security function (not control owners), undertake control testing, would this be sufficient to meet the requirement, or would APRA expect this to be undertaken by second and/or third line of defence resources? Alternatively, could specialist external resources be utilised? It seems appropriate that an entity should be able to determine the appropriate resources to undertake this testing.

Paragraph 30 would benefit from additional guidance on its requirements. For instance, responsibility for reviewing the sufficiency of the testing program.

Internal audit

Paragraph 31 requires internal audit to review "the design and operating effectiveness of information security controls". As risk and compliance functions (second line of defence) may also be involved in undertaking assurance activities, these could be acknowledged, possibly in addition to third line of defence assurance.

Paragraph 31 also extends to a "review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties". **Paragraph 33** requires internal audit to "assess the information security control assurance provided by a [related or third] party" in certain circumstances.

These requirements are in addition to **paragraph 21** which requires an entity to evaluate the design and operating effectiveness of a related or third party's information security controls. Read together, a related or third party is therefore expected to provide its own assurance (this may be via a third party independent or external audit), have these subject to evaluation by an entity (possibly an information security specialist) and then also be subject to assessment by that entity's internal audit.

Where a third party provides services to multiple regulated entities, each regulated entity will be required to undertake an assessment by specialists and internal audit of the third party's controls and assurances of those controls. These requirements appear onerous and unlikely to be feasible in a range of circumstances. The Insurance Council recommends that APRA reconsider and streamline these requirements.