Australian Banking Association

17 May 2019

Ms Heidi Richards
General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
Email: PolicyDevelopment@apra.gov.au

Dear Ms Richards

Consultation on Prudential Practice Guide CPG 234 Information Security

Thank you for the opportunity to make a submission on the draft prudential practice guide *Prudential Guidance* CPG 234 Information Security (**CPG 234**).

With the active participation of its members, the ABA provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services. The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

The ABA found the ABA/APRA workshop held on 2 May 2019 in Sydney for members very useful. Members considered that the workshop was very constructive and informative. The ABA understands that APRA wants its guidance principle based and this submission addresses those issues that remain outstanding from that discussion. The ABA's has specific comments on the following chapters:

- Third parties and related parties
- Implementation of controls
- Internal audit
- Attachment B: Training and awareness
- Attachment C: Identity and access

Each of the chapters is discussed below.

Third parties and related parties

Capability of third parties and related parties (paragraph 17)

The ABA recommends new wording for paragraph 17 (see suggested wording below). The current paragraph 17 needs to be simplified to make it easier to understand and recommends separating the different duties into separate paragraphs. The ABA suggests the following wording to replace the current paragraph 17.

> *APRA – regulated entities often place reliance on informational security capabilities of third parties and related parties to provide a targeted information security capability, or as part of a wider service – provision arrangement. Accordingly, entities would have a view as to the sufficiency of resources, skills and controls of third parties and related parties. This includes consideration of sub-contracting and on-sourcing arrangement. Assurance could be achieved through a combination of interview, service reporting, control testing, certifications, attestations, referrals and independent assessments.*

Any capability gaps identified would be addressed in a timely manner. An APRA – regulated entity should consider the scope, depth and independence of certifications, attestations and assurance provided and take steps to address any limitations identified.

Where services are being provided by third parties and related parties, who are regulated by APRA and are subject to this standard, then APRA related entities could place reliance on the information security capabilities of the third party or related party.

The intent of the additional sentence at the end of paragraph 17 is to address the concern the ABA raised during the consultation meeting, that ABA members are starting to see the rise of a costly "industry" of requests by other APRA regulated entities asking for an attestation of compliance to *Prudential Standard* CPS 234 Information Security (**CPS 234**). We would be appreciative of any guidance that APRA were able to provide that demonstrated how a consistent, efficient and sustainable approach (or alternative) to these requests could be adopted across both the industry and APRA's regulated population.

In addition, it would be helpful if APRA could provide some further guidance on 'consideration of subcontracting and on-sourcing arrangements' as mentioned in paragraph 17. Specifically, the ABA would welcome written guidance on APRA's expectations of a regulated entity to assess the information security capabilities of a fourth party, with which a third party has entered into a sub-contracting or on-sourcing arrangement.

Similarly, with regard to paragraph 60, it would be helpful if APRA could provide guidance on the extent to which it expects regulated entities to evaluate the capabilities and design of controls operated by fourth parties.

Notifications

The ABA would like the guidance to clarify the notification requirements so only information security matters are reportable. This would ensure that other types of breaches, such as privacy related data breaches, would have no bearing on the regulated entities security systems. For example, a data breach involving a loss of a physical artefact, such as employee name and contact lists, which may be reportable as a personal data breach impacting on an individual under privacy regulation but not reportable under CPS 234.

In terms of making notifications to APRA under Prudential Standard CPS 234 Information Security, It would be helpful if the guidance provided to members at the workshop on the comprehensiveness of reporting to APRA was added to paragraphs 84 and 85 of the Guide. Specifically, it would be helpful to underline that an entity should notify APRA, even in the absence of all of the information set out in paragraph 84 or 85. Further, it would be helpful if APRA would confirm that it would be acceptable, for example, if an Incident notification made within 72 hours of discovery with partial information (the "what we know now" scenario) was followed up with prompt clarification / further information outside the 72 hour notification period.

The ABA would also like to see further clarification on the format and content required for breach notifications. In particular, providing more information on whether breach notification will be via APRA XtraNet for reporting or if a separate reporting form will be needed would be of assistance.

Implementation of Controls

The ABA looks forward for the final version of the guidance to be reflect its consideration on developer access to productions practice. As part of the recent workshop, APRA agreed to consider whether it's position on developer access to production environments aligns to DevOps practice, and whether some refinement is required in CPG 234 to account for this, whilst maintaining that Secure Code Review, Privileged Access Management and IT Change Management controls applicable to production environments are effective.

Australian Banking Association

Data leakage

As part of the ABA/APRA workshop discussion, the ABA considered it better to amend the wording of paragraph 48 to replace the word “use” with “misuse” to better meet the intention of the guidance. Following the amendment, the paragraph would read as follows:

> *Controls, commensurate with the sensitivity and criticality of the data, would typically be implemented where sensitive data is at risk of leakage. Examples of data leakage methods include the ~~use~~ misuse of portable computing devices…*

Board and internal audit

The ABA agrees that assurance reports can be an important vehicle by which the Board can be informed about the status information security. However, where an assessment of a third parties assurances identifies deficiencies, or no assurance is available, the ABA would expect that only material issues be typically raised with the Board for its consideration. What is material (such as a materiality test) would need to be established by the entity as part of its internal reporting processes. The ABA suggests that the guidance be changed to reflect a materiality requirement before reporting issues regarding third party assurances to the Board.

As part of the clarification of materiality, it would be useful if APRA could indicate whether banks should use the definition of material consistent with *Prudential Standard* CPS 231Outsourcing or if another definition is more appropriate.

Further, it would be useful if APRA could provide some guidance and examples of the types of evidence it would expect to see to determine that the Board is effectively discharging its responsibilities of oversight, seeking assurance, and challenging management. For example, how should regulated entities demonstrate that the Board is discharging its responsibilities around ensuring the policy framework meets its expectations; or that the board is appropriately seeking assurance and challenging management on reporting regarding the effectiveness of the information security control environment.

Attachment B: Training and awareness

As part of the workshop discussion, the ABA considered that referring to all non-staff personnel as contractors is more aligned with the intent of the guidance. The amended wording would be as follows:

> *An APRA-regulated entity could benefit from developing a training and information security awareness program. This would typically communicate to personnel (staff and ~~,and~~ contractors ~~and third parties~~) regarding information security practices, policies and other expectations as well as providing material to assist the Board and other governing bodies to execute their duties. Sound practice would involve tracking training undertaken and testing the understanding of relevant information security policies, both on commencement and periodically. An APRA-regulated entity would regularly educate users, including both internal staff and contractors ~~third party staff~~, as to their responsibilities regarding securing information assets.*

Attachment C: Identity and access

The ABA is concerned that section 7(c) which prohibits sharing of accounts and passwords (including generic accounts) would require a significant change in current process and standard industry practice for essential generic accounts. At present, generic accounts are used by teams when it is functionally necessary and unavoidable. Banks limit the access and use of generic accounts as part of their internal

controls and consider these a credential of last resort. The ABA recommends that 7(c) be amended to reflect the operational necessity of shared generic accounts subject to appropriate internal controls.

Yours faithfully

Karen O'Brien
Policy Director