CUSTOMER OWNED BANKING ASSOCIATION

www.customerownedbanking.asn.au

SUITE 403, LEVEL 4, 151 CASTLEREAGH STREET, SYDNEY NSW 2000 GPO BOX 4686, SYDNEY NSW 2001

6 June 2018

Ms Heidi Richards
General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority

via email: PolicyDevelopment@apra.gov.au

Dear Ms Richards

APRA Consultation on Information Security Requirements

The Customer Owned Banking Association (COBA) welcomes the opportunity to comment on APRA's Discussion Paper on proposals to implement a cross industry framework for the management of information security (Discussion Paper) and the associated draft Prudential Standard CPS 234 Information Security (draft CPS 234).

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has $110 billion in assets, 10 per cent of the household deposits market and 4 million customers.

COBA agrees with APRA's Discussion Paper that effective information security is critical as cyber-attacks are becoming increasingly frequent, sophisticated and having a larger impact on affected organisations and the economy more broadly. COBA recognises that APRA's proposals respond to the rapidly evolving nature of information security threats.

COBA understands that the proposals also respond to APRA's 2015-16 cyber security surveys, which revealed weaknesses in the information security management practices of certain APRA-regulated entities operating across different industries.

As APRA would be aware, a significant number of COBA members rely heavily on third-party service providers for their core banking system and information technology service requirements. In this regard, COBA is pleased that APRA is consulting on this matter and particularly appreciates how the Discussion Paper and draft CPS 234 also focus on risk exposures associated with information assets managed by third parties.

While COBA supports the intent of APRA's proposals, COBA is concerned with various aspects of the planned changes – particularly:

- the proposed transition timeframe
- related or third-party control assurance
- scope of application
- Board responsibility
- notification requirements, and
- interaction with established standards or requirements.

COBA stresses that APRA's proposed implementation timeframe is insufficient for our member ADIs, chiefly given the sector's significant reliance on third-party service providers and that the implementation costs associated with APRA's proposals will fall more heavily on smaller ADIs.

Feedback received from our members is that implementing APRA's proposals would involve a number of critical stages (such as a gap assessment, policy framework development, asset classification, security assurance review and contractual changes with third party service suppliers). A number of these stages would take a minimum of 12 months to complete, while the proposals concerning related or third party control assurance, in particular, would take *at least* a further 12 months.

On this basis, COBA considers that it would be more realistic for the final CPS 234 to take effect *at least* 24 months from its release date, assuming that the necessary refinements are made to the draft CPS 234 to address COBA's other concerns.

COBA emphasises that a number of APRA's proposed requirements – such as the proposed notification and auditing obligations, for example – would place significant resourcing pressure on smaller ADIs. Feedback from our members is that many of APRA's proposed requirements are cost-prohibitive and would need to be outsourced.

As APRA would appreciate, mutual ADIs do not have the scale of information security resources compared to larger ADIs and other APRA-regulated entities operating in different industries. In this context, the final CPS 234 should not inadvertently disadvantage mutual ADIs, as this would only operate to further exacerbate the competitive imbalance between mutual ADIs and larger ADIs.

The Appendix of this submission elaborates on COBA's feedback to APRA's proposals.

COBA looks forward to working closely with APRA on refining the draft CPS 234 to facilitate a smooth and efficient transition to the new environment. Please do not hesitate to contact Tommy Kiang, Senior Policy Manager, if you wish to discuss any aspect of this submission.

Yours sincerely

LUKE LAWLER
Director - Policy

APPENDIX

Alignment with existing mandatory information security standards

COBA notes from the Discussion Paper that, in developing draft CPS 234, APRA has considered the work of other Australian government agencies and industry-accepted standards to ensure that industry-accepted practices and language are leveraged where appropriate.

COBA considers that it is critical for APRA to ensure that the final version of CPS 234 is appropriately aligned with existing requirements of other Australian government agencies and key international information security standards, such as the *Payment Card Industry Data Security Standard* (PCI DSS) and the International Organization for Standardization's *ISO 27001* and *ISO 27002*[1].

COBA has outlined further below, under 'Incident Notification Requirements', member concerns regarding the interaction of APRA's proposed 24 hour reporting requirement with other existing obligations relating to information security incident notification.

Audit, Controls and Testing

Related or third party control assurance

COBA notes that draft CPS 234 would require an entity to test the effectiveness of their information security controls through a systematic testing program. COBA also notes that this would include where information assets are managed by a related party or a third party, and the entity is reliant on that party's information security control testing.

COBA is concerned that APRA's proposed controls testing obligations would impose significant compliance costs that will fall more heavily on mutual ADIs, chiefly as these ADIs typically rely on third parties to manage their information assets. Additionally, smaller ADIs usually outsource technical assurance requirements to external auditors, given the specialised nature of this work and the generally prohibitive costs for smaller ADIs of maintaining an internal capability. COBA emphasises that it is critical for APRA to carefully take this into account in finalising CPS 234 and revising its *Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology* (CPG 234).

To satisfy APRA's proposed requirements concerning related or third party control assurance, smaller ADIs would need to negotiate cooperation from *all* related or third parties, which typically will require renegotiating service contracts. As APRA would appreciate, smaller ADIs may have myriad contracts with different third party service providers, many of which have contract periods of 1 or 2 years.

It is important for APRA to recognise that resolution of any third party contractual re-negotiations may not be within the control of smaller ADIs, particularly in a situation where a number of smaller ADIs rely on a single service provider (such as for a core banking system). For example, while existing service contracts may not allow access to information security, any new contracts may need to explicitly accommodate an internal audit review of information security policies and frameworks.

This is a key reason why COBA submits that providing at least a 24 month transition timeframe would be more realistic. Additionally, COBA notes that third party service

[1] *ISO/IEC 27001*: Information Technology Security Techniques, Information security management systems-requirements and *ISO/IEC 27002*: Information Technology Security Techniques, Code of practice for information security controls.

contracts may again need to be negotiated once APRA finalises its prudential standards for business continuity, outsourcing/service provision, and operational risk[2].
With that said, COBA stresses that implementation by smaller ADIs of the related or third party control assurance proposals would be on a 'best endeavours basis' only. In this regard, it is likely that APRA may in future need to reassess the transition timeframe for these requirements, on an entity-by-entity basis (e.g. reassessment at 24 months after the release of the final version of CPS 234).

Indeed, given the inherent complexities associated with third party contract renegotiations, APRA may wish to explore, together with other government agencies, whether there is merit in developing guidelines or requirements for third party information asset/security service providers, to also help facilitate their smooth transition to the new regulatory environment. For example, APRA may wish to consider the specific requirements for shared service providers under the latest *Payment Card Industry (PCI) Data Security Standard*[3].

Furthermore, external auditors presently used by smaller ADIs typically would not have a sufficient technical capacity to assess compliance with draft CPS 234. Consequently, smaller ADIs may need to pay for the audit services of either a specialised information security controls auditor or a major auditor. As APRA would appreciate, this would exacerbate the already significant compliance costs of APRA's proposals for smaller ADIs.

COBA's view is that APRA's proposed systematic testing requirements should be targeted. COBA submits that it would be more appropriate for these requirements to apply only to those controls identified as key security controls.

COBA would also appreciate confirmation from APRA that any party used by an APRA-regulated entity for controls testing would not need to be specifically certified (for example, ISO certification).

Definitions

COBA would appreciate clarification from APRA on the intent of paragraph 20(c) of draft CPS 234. COBA is unaware of any scenarios within retail banking where an asset lifecycle stage would influence the level of control applied to an information asset.

- As APRA would appreciate, information assets typically retain their sensitivity over time and there are strict legislative obligations to destroy data after a set period of time or in certain circumstances.

COBA notes that paragraph 21 of draft CPS 234 would require that where information assets are managed by a third party, an entity "…must evaluate the design and operating effectiveness of that party's information security controls". COBA submits that this proposed requirement should be clarified to:

- include only those controls that apply to the entity's assets, *not* the entire control environment of the third party, and
- remove upstream or downstream providers to the third party from the scope of this requirement (noting that arrangements would typically already be in place in a third party vendor's own 'third party management program').

COBA notes that paragraph 26(d) of draft CPS 234 introduces a concept of exposure to untrusted environments and how exposure may impede an entity's ability to enforce its information security policy. COBA would appreciate APRA, in revising its CPG 234, providing further guidance on this concept and associated examples of 'untrusted environments' together with how an assessment of an environment is to be made.

[2] APRA Information Paper, '*APRA's policy priorities*', released 31 January 2018. Page 15 refers.
[3] Payment Card Industry (PCI) Data Security Standard, Version 3.2.1 May 2018. Appendix A1 refers.

COBA notes that paragraph 28 of draft CPS 234 would require the Board or senior management of an entity to be advised of "…information security control deficiencies that cannot be remediated in a timely manner". COBA considers that this should be amended so that only deficiencies in *key* security controls would be in scope.

- COBA also suggests the removal of "…to enable an assessment and potential response by the Board or senior management to mitigate the exposure, as appropriate" in paragraph 28, as different mutual ADIs typically have different internal processes to respond to and mitigate exposures.

COBA notes that paragraph 29 of draft CPS 234 would require that testing "…must be conducted by appropriately skilled and functionally independent specialists". COBA considers that APRA should amend this proposal to remove the requirement for testers to be functionally independent.

COBA notes that paragraph 31 of draft CPS 234 would require an entity's internal audit function to review "…the design and operating effectiveness of information security controls, including those maintained by related parties and third parties". COBA submits that this proposal should be amended to only apply to those controls used by the third party to directly safeguard an entity's information assets.

Broad Scope of Application

General comments

COBA notes from the Discussion Paper that draft CPS 234 would extend to "an assessment of the information security capability of **all other** outsourcing providers"[4] [emphasis added], not just the outsourcing of material business activities.

COBA is very concerned with the broad scope of draft CPS 234, as mutual ADIs rely heavily on third-party service providers. This would unfairly impose significant administrative and compliance costs on smaller ADIs on the basis that they do not have the scale to manage information assets internally.

Put another way, the broad scope of draft CPS 234 would operate to **penalise smaller ADIs** for relying more heavily on third-party service providers. COBA considers that the final version of CPS 234 should only apply to the outsourcing of material business activities (e.g. core banking systems).

Definitions

COBA notes that paragraph 11(e) of draft CPS 234 defines an information security incident as a "…confirmed or potential compromise of information security". As with any other internet-connected organisation, ADIs are subject to ongoing cyber probes and attacks, all of which have varying degrees of potential to cause damage.

- COBA emphasises that ADIs may encounter several thousand potential information security incidents every day. On this basis, COBA submits that APRA should amend the definition to cover only *confirmed* information security compromises.

COBA notes that paragraph 18 of draft CPS 234 would require an entity's security policy framework to "...provide direction on the responsibilities of all parties who have an obligation to maintain information security". Footnote 6 at paragraph 18 identifies "related parties" and "customers" as within the scope of the policy framework. COBA submits that footnote 6 should be amended to remove customers and members.

- COBA would also appreciate clarification from APRA in terms of what an entity would be required to do in terms of providing, within an information security

[4] APRA Discussion Paper: Information security management: A new cross-industry prudential standard. Page 8 refers.

policy, "direction on the responsibilities". COBA suggests that further guidance could be set out in the revised CPG 234.

Classification of Information Assets

General comments

COBA supports in principle the proposed requirement to classify information assets.

COBA notes that draft CPS 234 does not prescribe the information asset classification method and granularity, leaving an entity to determine the appropriate scaling. COBA urges APRA to carefully consider the complex challenges that would be faced by smaller ADIs with asset classification, chiefly in terms of:

- their potential inability to gain full visibility of all information assets of their third party service provider(s), and
- potentially not having sufficient technical capacity to determine the criticality or sensitivity of information assets (e.g. information technology server infrastructure and hard or soft copies of different information assets).

To help reduce uncertainty, minimise compliance costs and facilitate a more consistent approach to information asset classification, COBA supports APRA's intention to provide further guidance on the classification of information assets in the revised CPG 234.

Definitions

COBA encourages the consistent use of terminology across different prudential standards, where possible. In this context, COBA would appreciate further clarity from APRA on the definitions of 'criticality' and 'sensitivity' (as also used in APRA's Information Paper on outsourcing shared computing services[5]).

COBA also supports the consistent application of terminology between different regulatory regimes, where appropriate. COBA considers that there may be merit in ensuring that the use of the term 'sensitivity' under the final CPS 234 is broadly aligned with the use of 'sensitive information' under the *Privacy Act 1988*[6] (Cth) and 'sensitivity' in the context of the Government's *Notifiable Data Breaches Scheme*[7].

Implementation Timeframe

COBA is very concerned with APRA's proposed implementation timeframe – this would be insufficient for mutual ADIs, given their significant reliance on third-party service providers. To help provide APRA with some guidance on the significant level of work that would be involved with implementation, provided below is a basic outline of a possible implementation approach that may be adopted by a mutual ADI:

- internal business case, board and management discussion
- gap assessment
- develop policy framework
- information classification
- develop and conduct security assurance
- incident response plan and exercise, and
- contractual renegotiations with all third party vendor(s) and obtain security information.

[5] APRA Information Paper: Outsourcing Involving Shared Computing Services (Including Cloud). Page 5 refers.
[6] *Privacy Act 1988 (Cth)* s 6(1).
[7] Office of the Australian Information Commissioner, '*Identifying eligible data breaches*', December 2017.

Feedback received from our members is that the main costs associated with implementation and maintenance would be in the areas of:

- sourcing additional information security specialists and auditors to assist in managing third parties, testing and reporting
- major modifications to systems architecture (e.g. encryption of data, which would involve significant internal and/or external resources)
- developing and updating an information asset register, including hiring the personnel required to maintain such a register and
- evaluation of and through-the-life management of third parties.

COBA considers that it would be more realistic for the final version of CPS 234 to take effect *at least* 24 months from its release date, to enable smaller ADIs to appropriately budget and implement the final requirements. COBA notes from the Discussion Paper that the final CPS 234 is expected to be released during the fourth quarter of 2018.

Additional time for ADIs to formally comply with CPS 234 will not weaken information security defences because all ADIs have a strong internal incentive to have effective measures in place, given the severe reputational risk posed by information security incidents.

Incident Management

Definitions

COBA notes that paragraphs 22 and 23 of draft CPS 234 contain similar drafting and that there appears to be overlap in relation to incident response. COBA would appreciate confirmation from APRA that paragraph 22 relates to *detection* capability and that paragraph 23 relates to *response* capability. COBA also suggests that APRA provides a definition, such as in the revised CPG 234, of an 'information security response plan' and what this would need to capture – COBA would suggest a similar approach as used under paragraph 26 of *Prudential Standard CPS 231 Outsourcing*.

Incident Notification Requirements

General comments – 24 hour notification

COBA notes that draft CPS 234 would require an APRA-regulated entity to notify APRA as soon as possible, and no later than 24 hours, of an information security incident that materially impacted or had the potential to cause a material impact.

While this would broadly align with APRA's *Prudential Standard CPS 232 Business Continuity Management*, COBA *objects* to this proposal as it would be inappropriate in the context of an information security incident for the following key reasons:

- Information security incidents may not be as readily identifiable as a Business Continuity Management event. A 'material' information security incident may not be able to be identified within a 24 hour period.
- In the event of an information security incident, an ADI would first need to focus on determining the impact of the incident and responding to any impact (e.g. to resolve the incident or reduce its impact), which may take days or weeks depending on the scale of the incident.
    - As APRA would appreciate, a quick response to an information security incident can reduce the likelihood of affected customers suffering harm and lessen any financial damage to the ADI that experienced the incident.
    - Requiring an ADI to instead focus *first* on an APRA reporting obligation instead of incident response and recovery may operate to exacerbate the impact of an incident.

- Indeed, requiring an ADI to prioritise an APRA reporting obligation over incident response and recovery would appear to conflict with the core objective of the standard – that is to protect the interests of depositors.

Additionally, COBA emphasises that APRA should also carefully consider the potential interaction of the proposed 24 hour reporting requirement with other existing obligations relating to information security incident notification.

- As APRA would be aware, mutual ADIs (as credit providers) already have extensive obligations under the *Privacy Act 1988* (Cth) to secure personal information and comply with the Notifiable Data Breaches Scheme[8], which, among other things, requires mutual ADIs to notify individuals and the Office of the Australian Information Commissioner (OAIC) about eligible data breaches.
  - COBA notes that the OAIC permits entities up to 30 days to make an assessment regarding a potential breach of personal identifiable information.
  - COBA considers that APRA should restrict notification requirements to actual disruptions or material incidents and that it would be more realistic to adopt a 30-day reporting timeframe, so that it would be consistent with the OAIC and allow entities an appropriate amount of time to assess impact.
- Additionally, there are other key agencies that have similar information security incident notification regimes in place, such as CERT Australia (Australia's national computer emergency response department) and the Payment Card Industry Security Standards Council, which administers the Payment Card Industry Data Security Standard (PCI DSS).
  - The PCI DSS, for example, is a set of security standards designed to ensure that all companies (such as mutual ADIs) that accept, process, store or transmit credit card information maintain a secure operating environment.
  - COBA believes that there may be merit in APRA working closely with CERT Australia to develop a coordinated approach to assisting an ADI respond to a material information security incident. This would particularly benefit smaller ADIs that do not have a complex internal incident response capability.

COBA strongly urges APRA to harmonise its final notification requirements with existing breach notification regimes, where appropriate, to ensure that the final CPS 234 does not inadvertently operate as an obstacle to efficient security incident response and remediation.

Definitions

COBA notes that paragraph 34 of draft CPS 234 would require that an entity notify APRA after 'experiencing' an information security incident. COBA considers that the term 'experiencing' is ambiguous and therefore open to interpretation. For the benefit of clarity and certainty, COBA suggests that the term 'experiencing' be replaced with 'detecting' (i.e. detection of confirmed incidents).

COBA notes that paragraph 34(b) of draft CPS 234 would require that an entity notify APRA of an information security incident if it has been "…notified to other regulators, either in Australia or other jurisdictions". Footnote 10 of paragraph 34(b) defines other regulators as including "domestic government agencies". COBA considers that the definition of other regulators should be amended to only include regulators that have clear legislated responsibilities for regulating ADIs.

COBA notes that paragraph 35 of draft CPS 234 would require an entity to notify APRA after the identification of "…a material information security control weakness". COBA would appreciate clarification from APRA on the interaction between this requirement,

[8] Australian Government Office of the Australian Information Commissioner: *Notifiable Data Breaches scheme*.

and the requirement at paragraph 28 of draft CPS 234, regarding Board and/or senior management notification.

Revisions to CPG 234

General comments

COBA is pleased that APRA plans to consult on a revised CPG 234 to reflect the final version of CPS 234. COBA also notes from the Discussion Paper that APRA will review the need to update other prudential practice guides relevant to information security, to ensure consistency with the final CPS 234 and revised CPG 234.

COBA supports the proposed topics that APRA intends to cover in its revised CPG 234, as set out in the Discussion Paper[9]. COBA emphasises that it is particularly important for the revised CPG 234 to also clarify APRA's *minimum expectations* with respect to related or third party assurance, incident notification, information asset classification and definitions of material information security control weaknesses.

COBA notes from the Discussion Paper that, in APRA's view, materiality typically requires a degree of judgement, and that techniques are not yet available for a materiality concept to be readily applied to information security. Nevertheless, COBA encourages APRA to provide guidance on assessing materiality to help ADIs develop suitable and practical materiality policies. For example, COBA notes from the Discussion Paper that APRA intends to provide guidance in relation to its expectations for the planned material internal control weakness notification requirements.

COBA considers that it would also be beneficial for APRA's revised CPG 234 to include guidance on applying the concept of 'exposure to untrusted environments' and also how APRA intends to measure a regulated entity's compliance with the final CPS 234.

Roles and Responsibilities

General comments

COBA notes that paragraph 12 of draft CPS 234 would require an entity to maintain the security of its information assets "…in a manner which is commensurate with the size and extent of threats to those assets".

As APRA would appreciate, smaller ADIs face similar threats to most other Australian retail financial organisations and would therefore need to maintain a control environment similar to that of large ADIs. COBA therefore suggests that APRA adopt a risk-based approach in the final version of CPS 234.

Role of the Board

COBA notes that draft CPS 234 states that the Board of an APRA-regulated entity is "ultimately responsible for ensuring that the entity maintains the information security of its information assets"[10]. COBA disagrees with this view.

As APRA would appreciate, there needs to be a clear delineation between the roles of the Board and senior management. The key role of the Board is to develop and set a clear strategy for their organisation, while the role of senior management is to implement the Board's strategy.

On this basis, COBA considers that the role of a Board should be more focussed on ensuring that there is an information security *capability* within an organisation.

[9] APRA Discussion Paper: Information security management: A new cross-industry prudential standard. Page 13 refers.
[10] APRA Draft Prudential Standard CPS 234 Information Security. Page 1 refers.

This would be consistent with APRA's statement in the Discussion Paper that, "…information security management necessitates the involvement of **all personnel** as well as specific roles for information security specialists"[11] [emphasis added].

[11] APRA Discussion Paper: Information security management: A new cross-industry prudential standard. Page 6 refers.