17 May 2019

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

By email: PolicyDevelopment@apra.gov.au

Dear Sir/Madam

CPG 234 Information Security

The Australian Financial Markets Association (AFMA) is a member-driven and policy-focused industry body that represents participants in Australia's financial markets and providers of wholesale banking services. AFMA's membership reflects the spectrum of industry participants including banks, stockbrokers, dealers, market makers, market infrastructure providers and treasury corporations. AFMA counts many APRA regulated entities within its membership and the proposed guidance will have significant implications for these members.

AFMA welcomes the opportunity to comment on APRA's consultation on Prudential Practice Guide CPG 234 Information Security (the "guidance").

AFMA supports APRA's prudential standard on information security CPS 234 as a well-developed standard that is likely to bring increased consistency to information security practices. While this and our previous submission outline some suggestions for fine-tuning the standard, these should be taken in the context that overall we believe it is a high quality standard that reaches the right balance in most areas.

We encourage APRA to build on this strong foundation and to work through the Council of Financial Regulators Information Security Working Group to ensure that there is a coordinated approach to ADI information security regulation.

We note in this regard that the ACCC has recently proposed an information security standard as part of its Open Banking Rules Exposure Draft that could place a second information security standard on ADIs participating in the scheme as Data Recipients that

would apply in parallel and with a different regulator to some of the work ADIs do in relation to Open Banking.

A single standard, and we would recommend CPS 234 be that standard, should apply to ADIs in all their areas of activity. We have suggested in our submission to the consultation that it is appropriate for ACCC to recognise through a substituted compliance arrangement the validity of APRA's information security standard for all Open Banking related activities.

Further, we note that as the Open Banking standard proposes a reduced version of CPS 234 that does not include CPG 234, which Data Recipients under the scheme other than ADIs would be subject to a lower information security standard. Given that a failure of information security under the scheme would be difficult for consumers to differentiate as not relating to ADIs there are prudential considerations that accompany this approach.

Consultation practices

While there is no doubting the quality of the work that has gone into CPS 234 and CPG 234, consistent with our submission to the APRA Capability Review, we would encourage APRA to consider earlier and more empowered engagement with the regulated community in the design and construction of its policies.

By the time APRA presented both CPS 234 and CPG 234 for consultation there were significant policy commitments and approaches embedded in the documents that could not be subject to ready revision by consultation. Earlier engagement with the regulated community during the ideas or concept phase could leverage the willing involvement of the regulated community.

We would encourage APRA to consider the work of Archon Fung in the influential 2006 article *Varieties of Participation in Complex Governance*[1]. Fung offers a taxonomy to assess the inclusiveness of consultation processes along three axes of a 'democracy cube'.

At present Australian regulatory processes, including those of APRA, tend to fall towards the left on Fung's axes. There is a significant reservoir of relevant knowledge and experience that could be drawn upon to benefit the quality of regulatory outcomes. These can assist, *inter alia,* with ensuring outcomes are fully cognisant of the practical challenges of implementation.

Timing

A significant challenge in relation to the CPS 234 implementation for affected firms relates to the timings that APRA has created.

[1] Fung, Archon (2006), 'Varieties of participation in complex governance', *Public Administration Review*, 66 (S1), 66–75. http://faculty.fiu.edu/~revellk/pad3003/Fung.pdf Revisited in 2015 in Fung, Archon. "Putting the Public Back into Governance: The Challenges of Citizen Participation and Its Future." *Public Administration Review* 75.4 (July/August 2015): 513–522. http://archonfung.net/docs/articles/2015/Fung.PAR2015.pdf

The draft guidance was released on March 25, 2019 yet full compliance is required by July 1, 2019. The guidance is a fairly comprehensive rewrite of the previous CPG 234. CPS 234 itself has only been out in final form since November 2018. The commencement of the new requirements on 1 July allows an inadequate amount of time for implementation of the standard and guidance.

Full compliance with the guidance by July 1 would be entirely unachievable for any firm starting from scratch in information security. Fortunately, AFMA members report they are well advanced as they already comply with various international information security and process standards.

We understand from our discussions that APRA regulated firms beyond our membership share common concerns about the timing requirements around the standard.

It should be noted that even conducting an exercise to confirm that an existing information security program that conforms to an international standard is compliant with the new standard and guidance is a substantial undertaking. Nuanced differences in the approaches of the different standards can lead to functional gaps that will need to be addressed by remediation programs.

For a large firm the project to check for such gaps can take months to implement. This could be followed by multiple remediation programs that also may take months to implement.

Sufficient time should be allowed to implement the guidance from the time the final guidance is issued. For such a significant program we would suggest 18 months would be an appropriate timeframe to allow firms to implement a comprehensive conformance program.

We note that an earlier and more comprehensive consultation program as we have suggested above would have alerted APRA to the realities around implementation timing at an early stage and allowed for more appropriate implementation schedules.

Scaling

CPG 234 describes what a mature information security program designed to meet CPS 234 for a large firm might look like. This is entirely appropriate given that as guidance it should provide information about regulatory expectations for firms of all sizes with programs at all levels of maturity.

We understand from our interaction with the wider financial sector outside the financial markets that compliance with the guidance is likely to mature over time, with some firms aiming to continue to improve the depth of their programs beyond the initial July 1 target. AFMA believes this is a sensible aim and supports APRA setting its expectations for the depth of programs supporting compliance with the standard to continue along a path that increases maturity over time.

Some of the examples given, for instance in Attachment H of the guidance, provide extremely detailed suggestions about the sort of metrics and measures that a firm might use to achieve compliance with CPS 234. We support the framing of these as suggestions in the context of guidance as APRA has done. Firms may have approaches that differ in achieving the requirements of the standard appropriate for a firm of their size.

We note APRA's comments in relation to Board delegation. Firms may take a view that some of the metrics and measures suggested by the guidance may not suitable for review by the Board directly but rather might be more appropriate for senior management.

It is important that Boards maintain their proper roles as providers of governance and not as providers of management to firms. Some firms may take the view that some of the day-to-day reporting and response envisaged by the guidance, for example reviewing the "Systems with out of vendor support components (by type, count, coverage %)" or "User access review (by role, privilege, ageing, coverage %)"[2], may be best dealt with at the management level under governance oversight. Where senior management identifies significant issues it may of course be appropriate that these are raised directly with the Board. AFMA notes there is a risk that if too much low-level information is provided to Boards then technical detail may overwhelm the larger strategic questions that are more critical to questions of governance.

Classification Methodology

AFMA supports the guidance around firms consistently using their own *classification methodology* for assessing criticality and sensitivity. Concerns were raised in relation to the use of these terms in the standard but these have been addressed by the proposed methodology approach. Firms will be able to create methodologies that will enable the factors that will be considered when assessing information assets against these criteria and we believe this will create an appropriately flexible and responsive regime.

Third parties

The arrangements required around third parties may require substantial work programs by individual firms and the industry as a whole.

We understand from communications from APRA that third parties include infrastructure providers such as exchanges. There is the potential, as we understand has occurred in other markets, of collective assessments providing some savings in this area to avoid each of the many firms that use a particular infrastructure provider undertaking their own assessment of that provider's information security arrangements.

AFMA will investigate the potential for such an approach but note that these type of arrangements may take some time to complete.

AFMA supports the guidance methodology at paragraph 83 which appears compatible with the approach of large cloud computing providers with regard to assurance reports.

[2] CPG 234 Draft Appendix H, p. 43.

International Reporting

We understand from APRA's communications that for foreign ADIs, the regulated entity is the domestic branch and not the parent entity for the purposes of reporting material weaknesses and breaches under CPS 234 paragraph 35 (a).

APRA has indicated it expects that where there is an issue within the broader parent entity of which the branch is a part, and that issue could potentially affect the Australian branch operation, then APRA would also expect to be notified of such matters.

The coordination of responses from other branches and head office for reporting requirements in Australia is difficult.

For example:

> If an information security incident or potential incident happened in the London branch, that branch may take time to identify what the issue is and also to judge whether they should make a report to Head Office in New York or the regulator. Once the London branch notified an incident to Head Office, then Head Office would assess whether the incident causes a material impact to customers or not, and also whether the incident causes a material impact to other overseas branches including the Australian branch.

Consistent with the wording in the standard AFMA supports the time period for reporting commencing from the time the Australian branch becomes aware of the issue.

The limitation, as APRA's commentary may suggest, of reporting of incidents originating outside of the local ADI to those that could potentially affect and not those have already been addressed and can no longer affect the local entity by the time the local entity becomes aware of them, also contributes to making these reporting requirements more workable.

AFMA would support further discussion of expectations around these requirements.

Other

The Guidance states that "An APRA-regulated entity's information security policy framework would typically be consistent with other entity frameworks such as risk management, service provider management and project management."

AFMA supports this principle, these frameworks should integrate in a consistent manner, noting they may be conducted in different ways. Project management in particular typically has different implementation methodologies, noting it should appropriately consider information security policy outcomes.

Due to the interconnectedness of networks, the guidance's requirements around the need to consider assets "which are not intrinsically critical or sensitive but could be used to compromise information assets which are" suggests a very broad scope.

A firm's global computer networks while not intrinsically critical or sensitive to the local entity could be at risk in theory of being used to compromise the local network and assets. We note that the guidance suggests that entities "could benefit from considering the interrelationships between" such assets. This is appropriate as it would be impractical to require a classification process to analyse the entirety of such related networks. In practice we expect some firms to ensure risks are managed will rely on baseline requirements for such assets and network security such as the use of secure configuration standards, monitoring to identify deviations, defensive security and detection tools.

We also note in relation to Section 53 (e) of the guidance that there are limitations in the extent to which firms can benchmark against peers given the nature of the often proprietary and confidential information security controls.

Encryption

The guidance suggests that "In order to minimise the risk of compromise, an end-to-end approach would typically be adopted, where encryption is applied from the point-of-entry to final destination."

AFMA supports this conclusion but notes that in different circumstances 'point-of-entry' could be interpreted in a number of ways, for example external facing firewalls, DMZ gateways, internal gateways, message routing infrastructure. Likewise the term 'end-point' could mean internal gateways, message routing infrastructure, applications or application components. We also note that in certain situations, for example, a gateway component can legitimately terminate an external TLS connection and then re-transmit internally on a different TLS session to the end-application. This is not full end-to-end encryption from end-user to application processing but is required to perform other security processing.

Conclusion

AFMA supports APRA's work in relation to CPS and CPG 234. We encourage APRA to build on this work to ensure ADIs face this single standard in relation to information security and avoid a multiplicity of inconsistent standards from multiple regulators.

In relation to the process used to create the standard and guidance we have noted that improvements could have resulted in more realistic timing.

We are supportive of the flexible approach APRA has taken in relation to the standard and note our support for the classification methodology approach.

Yours sincerely

Damian Jeffree

Director of Policy