AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY
1 Martin Place (Level 12), Sydney, NSW 2000
GPO Box 9836, Sydney, NSW 2001
T 02 9210 3000 | W www.apra.gov.au

25 June 2019

TO: ALL APRA-REGULATED ENTITIES

Response to Submissions – Prudential Practice Guide CPG 234 Information Security

In March this year, APRA released for comment a draft update to cross-industry *Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology* renamed as *Prudential Practice Guide CPG 234 Information Security* (CPG 234). Five submissions were received in response. Overall, responses supported the guidance and comments generally sought clarification on certain aspects of the guidance. This response letter details the more substantive matters raised in submissions and APRA's responses. In addition, APRA has made a number of minor changes to CPG 234 as part of the final review process.

The guidance in CPG 234 should assist APRA-regulated entities in complying with *Prudential Standard CPS 234 Information Security* (CPS 234) which takes effect on 1 July, as well as addressing common areas of weakness that APRA has noted as part of its supervisory activities. The following material issues were raised by submissions.

Assessing information security capability of third-parties

Two submissions queried the need for an APRA-regulated entity to assess the information security capability of a third party where that third party is:

- already subject to regulation by APRA (i.e. other APRA-regulated entities); or
- subject to another regulator's requirements (e.g. energy companies, securities exchanges).

APRA expects that a regulated entity will assess the information security capability of **all** third parties that manage information assets on its behalf, commensurate with the potential consequences of an information security incident affecting those assets. APRA does not consider it sufficient for a regulated entity to rely on the fact that a third party may be subject to some form of regulatory oversight as being an indicator that the information security capability of that third party is automatically commensurate with the size and extent of threats to an entity's information assets, and would therefore enable the continued sound operation of the entity.

Assessing information security capability of downstream service providers

One submission queried whether an APRA-regulated entity would need to assess the information security capability of other service providers engaged by the third party that manages the information assets of the regulated entity.

Under CPS 234, where information assets are managed by a third party, an APRA-regulated entity must assess the information security capability of the third party commensurate with the potential consequences of an information security incident affecting its information assets.

When the third party engages another service provider to deliver an end-to-end service, additional vulnerabilities and threats are introduced. Under such circumstances, APRA's expectation is that an APRA-regulated entity would take reasonable steps to satisfy itself that the third party has sufficient information security capability to manage the additional threats and vulnerabilities resulting from such arrangements. APRA will further consider this matter more broadly as part of the upcoming review of *Prudential Standard CPS 231 Outsourcing*.

Assessment of classification of information assets

APRA has clarified its expectation of the timing of classification of information security assets in CPG 234. In order to maintain the classification of its information assets, an APRA-regulated entity would benefit from implementing a process which identifies where the classification of information assets requires change as well as allowing for the classification of new information assets. This would normally be undertaken at least annually, or when there is a material change to the regulated entity's information assets or business environment.

Other matters

With the 1 July start date for CPS 234 imminent, it is important that all APRA-regulated entities have assessed their level of compliance with the standard and taken appropriate steps to address any gaps. APRA recognises that the new information security requirements materially raise the bar across the industry and will take time to be fully effective. If an entity assesses that it will not be able to fully comply with the new standard from 1 July, it should immediately contact its APRA supervisor.

CPS 234 requires an APRA-regulated entity to notify APRA of certain information security incidents and material information security control weaknesses. Notifications are to be made via the notification link on the APRA website at:

Information security incident notification under paragraph 35 of CPS 234

https://apra.au1.qualtrics.com/jfe/form/SV_5cL51HPlmtGWr8V

Material information security control weakness notification under paragraph 36 of CPS 234

https://apra.au1.qualtrics.com/jfe/form/SV_5mYAnSiYR8tovNr.

The final prudential practice guide can be found at: https://www.apra.gov.au/information-security-requirements-all-apra-regulated-entities.

Yours sincerely,

Pat Brennan
Executive General Manager
Policy and Advice Division