briefing note 385 Jan 2019

CPS 234: Will you comply? Information Security standard for APRA regulated organisations

By Denny Wan[1] and Tahiry Rabehaja[2]

Synopsis

In November 2018, the Australian Prudential Regulation Authority (APRA) released Prudential Standard CPS 234 making the board of regulated entities accountable for ensuring the adequacy and sustainability of their information security program. APRA's standard was published 9 months after the Notifiable Data Breach scheme[3] came into effect in the first quarter of 2018. The CPS 234 comes into full force in July 2019 with a 12 month extension for third party supplier contracts until July 2020.

Prudential Practice Guide CPG 234, expected to be updated in the first half of 2019, is the primary guidance for the implementation of this prudential standard. However, APRA has confirmed that it will not provide guidance or method for the classification of the materiality of an information asset. A structured approach to cyber risk quantification similar to the now mature natural catastrophe risk modelling or operational risk management is important to ensure the impartiality of the classification methods.

What is CPS 234

The goals of CPS 234, as stated in the policy release announcement[4], are to:

shore up APRA-regulated entities' resilience against information security incidents (including cyber-attacks), and their ability to respond swiftly and effectively in the event of a breach

ensure all regulated entities develop and maintain information security capabilities that reflect the importance of the data they hold, and the significance of the threats they face

---

[1] Denny Wan is the principal consultant of Security Express and a postgraduate researcher at the Optus Macquarie University Cyber Security Hub. He has deep expertise in cyber risk quantification. His research focuses on applying cyber insurance concepts to supply chain risk management. He is the chair of the Sydney Chapter for the Open Group FAIR cyber risk framework.

[2] Dr. Tahiry Rabehaja is a Software Engineer at Risk Frontiers and a Research Fellow at the Optus Macquarie University Cyber Security Hub with expertise in probabilistic modelling and Information Security.

[3] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

[4]https://www.apra.gov.au/media-centre/media-releases/apra-finalises-prudential-standard-aimed-combating-threat-cyber-attacks

Regulated entities are required to:

- ***clearly define information-security related roles and responsibilities;***
- ***maintain an information security capability commensurate with the size and extent of threats to their information assets;***
- ***implement controls to protect information assets and undertake regular testing and assurance of the effectiveness of controls; and***
- ***promptly notify APRA of material information security incidents.***

To ensure compliance, clause 13 explicitly makes the board of the regulated entities be ultimately accountable:

13. The Board[4] of an APRA-regulated entity (Board) is ultimately responsible for the information security of the entity. The Board must ensure that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.[5]

Information security is a business problem

APRA has made it clear in its response to the submission to the draft CPS 234[5] that it intentionally makes the boards accountable for information security. This clearly means that information security is a business problem and not just an IT challenge. In its response, APRA explained that some submissions sought clarification on the "materiality rules". Page 7 of the response gives one example of such a request:

various requests for the application of a materiality threshold in relation to certain requirements in CPS 234 as the basis for determining the need to apply requirements or the degree of work required in applying certain requirements in the standard. For example, some submissions argued for a materiality threshold to apply in relation to testing the effectiveness of information security controls, and in determining the need to escalate and report testing results to the Board or senior management where security control deficiencies are identified that cannot be remediated in a timely manner;

The following emphasis is further stated on page 8 under the section "APRA Response":

This reflects the fact that ensuring the information security of all information assets remains the responsibility of the regulated entity and that the Board is ultimately responsible for the information security of the regulated entity.

[5]https://www.apra.gov.au/sites/default/files/response_to_submissions_-_information_security_cross-industry_prudential_standard.pdf

A reasonable interpretation of APRA's response is that the board is responsible for determining the materiality of information risk and adequacy of the controls. This interpretation is echoed by several commentators [6] [7] [8].

How to comply with CPS 234

A key challenge in preparing for compliance with CPS 234 is the lack of prescriptive compliance guidelines. This concern is discussed by other commentators [9] and was also echoed in some submissions. APRA noted on page 8 in its response to the submission regarding the materiality of an information asset:

CPS 234 prescribes neither the classification method nor the level of granularity — these are left to the regulated entity to determine, as appropriate for the entity's size and complexity

The standard identifies nine compliance areas:

1. ***Roles and responsibilities (clause 13 - 14)***
2. ***Information security capability (clause 15 - 17)***
3. ***Policy framework (clause 18 - 19)***
4. ***Information asset identification and classification (clause 20)***
5. ***Implementation of controls (clause 21 - 22)***
6. ***Incident management (clause 23 - 26)***
7. ***Testing control effectiveness (clause 27 - 31)***
8. ***Internal audit (clause 32 - 34)***
9. ***APRA notification (clause 35 - 36)***

CPG 234 released in May 2013 is the practice guide referenced in CPS 234 covering most of these areas except information security capability (clause 15 - 17). APRA is expected to release a revised CPG 234 in the first half of 2019 to provide guidance on the implementation of CPS 234. However, it is clear from APRA's response to the submission that the update to CPG 234 will not provide specific guidance on classification method nor the level of granularity in determining the materiality of an information asset. This can potentially create a challenge to comply with clause 15:

[6] https://www.ey.com/Publication/vwLUAssets/ey-CPS-234/$FILE/ey-CPS-234.pdf

[7] https://www.minterellison.com/articles/apra-prudential-standard-cps-234-information-security-has-been-released

[8] https://www2.deloitte.com/au/en/pages/risk/articles/apra-cps-234.html#

[9] https://blog.compliancecouncil.com.au/blog/what-are-the-information-security-requirements-of-cps-234

15. An APRA-regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.

As a result, the absence of a national cyber security standard or metric prompts the board to be responsible for eyeballing the materiality criteria and assess the sufficiency of their information security program under clause 13 and 15.

This is where a structured cyber risk quantification approach is important to provide an objective and quantifiable implementation of the compliance program. Currently, Risk Frontiers is partnering with the Optus Macquarie University Cyber Security Hub to develop a model for cyber security risk, parallel to its extensive work in natural catastrophe and rare event modelling. The cyber model aims at forecasting potential losses from tangible cyber-attacks given the profile of the victim. Such a model would provide the required metric to assess the potential severities of Information Security breaches for the underlying company.