Are You Ready for APRA's CPS 234 Tripartite Assessment?

"We want compliance independently verified" - APRA

In November 2018, APRA released the Prudential Standard 234 for Information Security. The standard came into force on 1 July 2019. If your information assets are managed by a third party, then entities had until 1 July 2020 to be compliant.

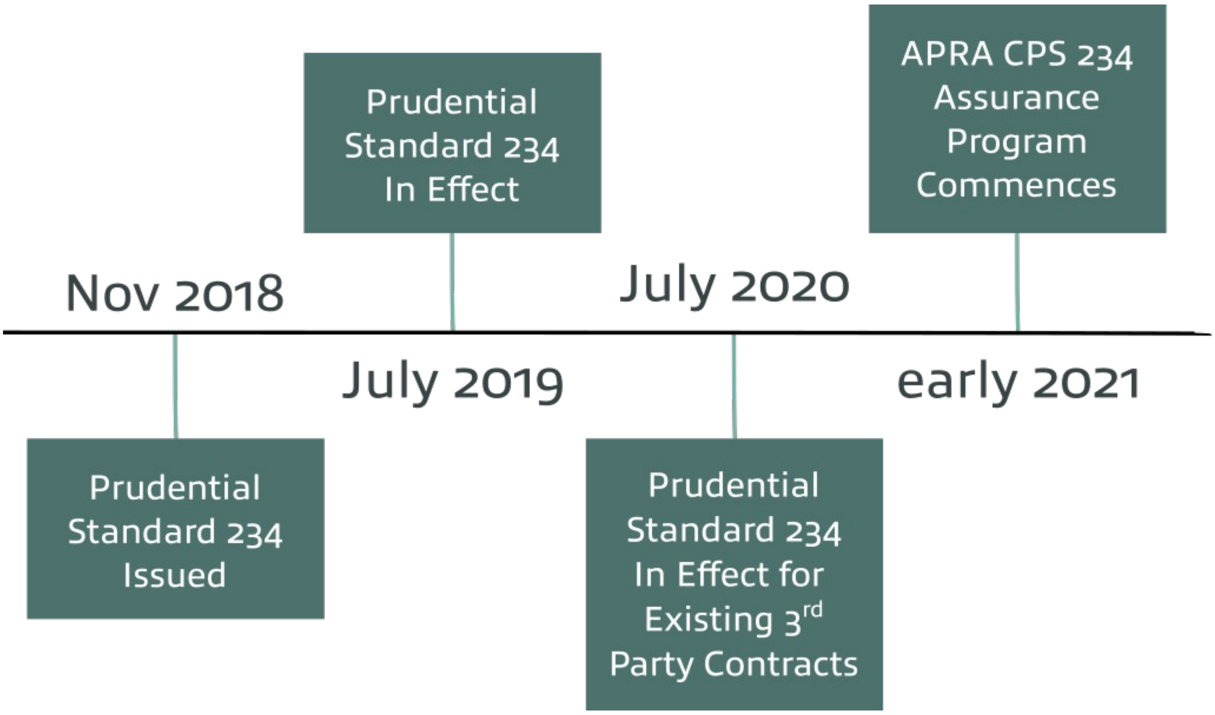
All APRA regulated entities (Banking, Insurance, Life Insurance, Health Insurance and Superannuation organisations) are required to ensure that their information security capability (resources, skills and controls) are proportionate to the size and extent of the threats to their information assets.

In a recent speech APRA has indicated that many entities who have self attested compliance have been found to be non-compliant in the following areas:

- Testing programs;
- Control environments; and
- Incident response capabilities

The speech can be viewed here: Executive Board Member Geoff Summerhayes - speech to Financial Services Assurance Forum (Thursday 26 November 2020) https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services

They have indicated that an assurance program will commence in early 2021.


Nov 2018

Prudential Standard 234 Issued

July 2019

Prudential Standard 234 In Effect

July 2020

Prudential Standard 234 In Effect for Existing 3rd Party Contracts

early 2021

APRA CPS 234 Assurance Program Commences

What is APRA planning to do?

- Prepare enhanced cyber guidance for entities in conjunction with the Australian Institute of Company Directors and other industry bodies;
- Collect and share more data on cyber security incidents between entities to enhance awareness and capability;
- Develop stronger third party assessment and assurance practices;
- Certain entities will be required to obtain independent “tripartite security reviews”; and
- Issue breach notices and require “Rectification Plans” for regulated-entities that fail to comply with CPS 234.

How Tannhauser assist’s your business in addressing CPS 234?
Cyber Risk Assessment: We perform or evaluate your cyber risk assessment in defining both the criticality and sensitivity of your information assets, as well as the size and extent of the threats faced. This includes gap analysis of existing security controls against the standard.
Internal Audit Staff Augmentation: We appreciate companies will have a challenge resourcing staff adequately to perform the internal audit requirements. Cyber security expertise may be lacking in Internal Audit teams. Our Tannhauser team will augment your existing internal audit function capability.
Independent Testing: We perform independent security control audit and testing for a variety of complex technology environments.
Cyber Resilience: Finally we help you develop incident response management plans, train staff how to respond to a cyber attack and effectively test these in real-time with simulation workshops and red team exercises.

Contact us for the latest cyber security updates to regulatory and legislative requirements for your business.

Further APRA Prudential Standard CPS 234 Information Security
guidance is located here: https://www.apra.gov.au/information-security

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Tannhauser Pty Ltd and employees do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.