Grant Thornton

Cyber Security

Business Risk

Financial Services

Renewed focus on APRA's Prudential Standard CPS 234 Information Security

November 2020 saw APRA announce their 4 year strategy with a focus to increase the rigor of compliance with the CPS 234: *Information Security*.

Historically CPS 234, which as been effective since 2019, has not required independent verification of compliance to APRA – until now.

APRA has commenced a pilot series of tripartite audits, requiring the Board of regulated entities to engage third party independent auditors to undertake a thorough CPS 234 compliance audit with results reported not only to the Board, but also directly to APRA.

Why the increased focus?

- Recognition that the strength of the security environment is only as strong as the weakest link. APRA directly supervises around 680 entities, however noted that there is a financial eco-system of an estimated 17,000 entities to support these entities. Any weakness within these 17,000 points can expose the APRA regulated entity to cyber risk. Hence the **inclusion of third party cyber security practices** to meet CPS 234 compliance.
- APRA monitoring since CPS 234 has come into effect, has highlighted there are still a number of security "hygiene" issues that expose entities to significant cyber risk.

What do you need to do now?

Prepare for CPS 234 compliance independent audits. APRA have announced a limited number of tripartite independent cyber security reviews, focusing on larger institutions. The results of these reviews are expected to inform further reviews across the regulated sectors.

- Ensure your organisation has the right level of focus on cyber security, including your third party providers and internal audit function.
- Engage an independent auditor to undertake a CPS 234 audit.

What does this mean for you?

As an **APRA regulated entity** you will be subject to independent compliance audits in the near future.

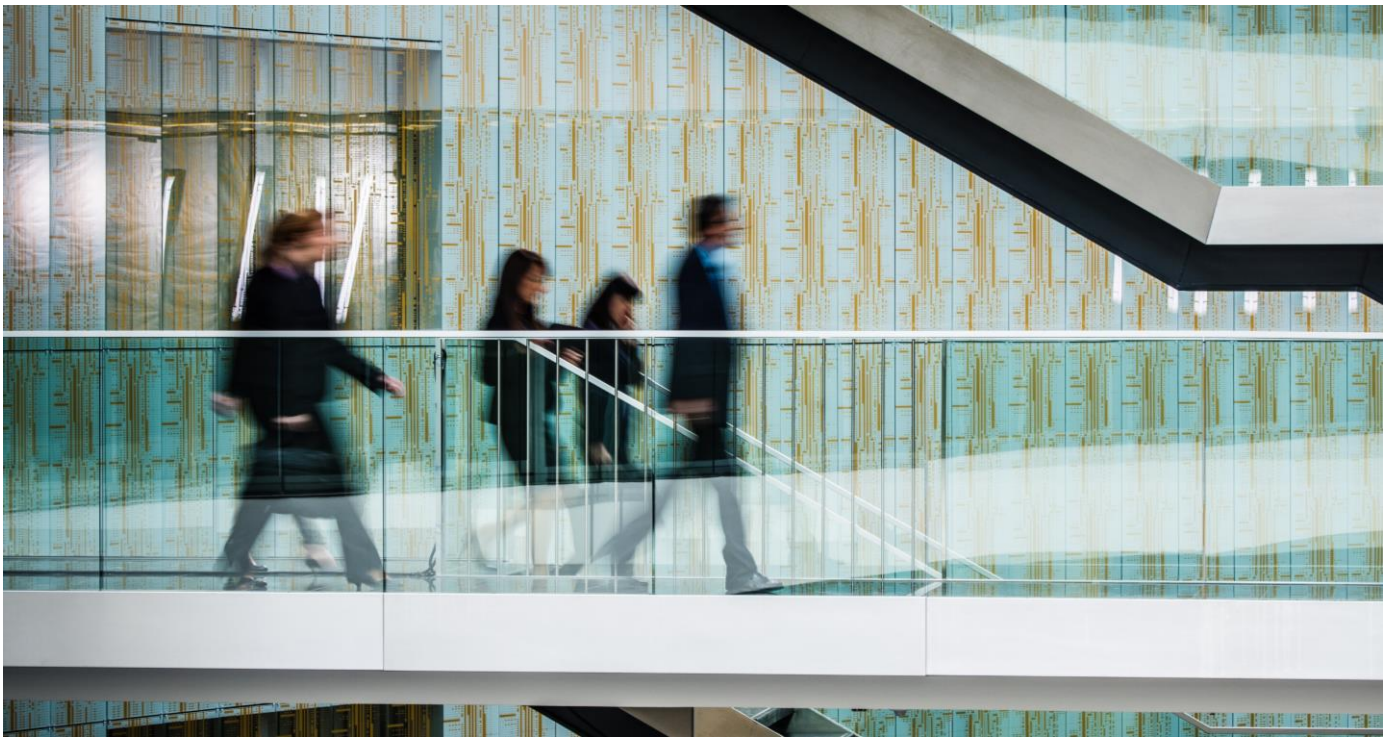
As an **organisation providing services** to an APRA regulated entity you also may be subject to independent compliance audits.

APRA have advised non compliance to CPS 234 could lead to entities required to issue a breach notice and rectification plan or being subject to formal enforcement action by APRA.

1 July 2019
- CPS 234 Effective and APRA regulated entities must comply with the standard

1 January 2021
- End of transition period for third party providers
- All APRA regulated entities compliance must include any third party operations.

Starting 2021
- Boards required to engage external audit firm to assess CPS 234 compliance



How we can help

Our Risk Consulting team can provide assistance in developing and enhancing your approach to information security in order to be prepared against cyber threats and the meet the changing regulatory requirements.

We will work with you to assess your information security maturity against the APRA CPS 234 requirements, including the maturity of your third party providers. Working across a range of industries and organisations, we appreciate every organisation is different and there is no one size fits all to information security. We use the CPS 234 requirements as the baseline of good information security control that need to be met whilst ensuring these are commensurate with the size and nature of your organisation.

Get in touch

Matt Green
Partner – Risk Consulting
T +61 3 8663 6168
E matthew.green@au.gt.com

Daniel Farthing
Director – Risk Consulting
T +61 2 8297 2650
E Daniel.farthing@au.gt.com

Grant Thornton