Privasec | GRC
GOVERNANCE AND INFORMATION SECURITY PARTNERS

APRA CPS 234 Compliance Assessment / Gap Assessment

> What is our methodology and typical time frames that we have seen the project completed for businesses?

Privasec adopts a pragmatic approach when assessing an organisation's compliance against the Australian Prudential Regulation (APRA) CPS 234, utilising our industry knowledge and experience with this regulatory standard. APRA recognised the threat in the digital environment and implemented the new APRA CPS 234 to ensure that APRA-regulated entities had sufficient information security protections.

At the conclusion of the assessment, Privasec will provide a set of recommendations on how to address any identified gaps against APRA CPS 234. A commentary on the current status of compliance, and any improvement opportunities to uplift and strengthen existing controls further will also be provided.

The key steps to achieving the above include, but not limited to:

1. Gathering and assessing information available
2. Reviewing existing documentation
3. Conducting interviews and workshops with relevant stakeholders
4. Consolidating our findings
5. Delivering the assessment report
6. Presenting findings to management (if required)

Depending on the size and maturity of the organisation, and the number of controls present in the environment, this will determine the total effort required to complete the assessment. Typically, in a smaller organisation setting, this could take up to two weeks; for larger and more complex organisations, it could take four or more weeks to complete the assessment.

> Any interesting/successful case studies or market observations to share?

Market observation: APRA CPS 234 started on 1July 2019; by December 2020, the level of compliance was still in its infancy across APRA regulated entities. APRA noted areas of weaknesses included testing programs, control environments and incident response capabilities.

APRA granted more than 100 requests for regulatory relief to entities struggling to meet the 1 January 2021 deadline for CPS 234 relating to third-party services, but "with consistent evidence that many entities are failing to adequately comply with CPS 234".

APRA introduced a new cyber-security strategy for 2020 to 2024 that seeks to uplift cyber-security standards and heighten accountability where companies fail to meet their legally binding requirements. Although the board's accountability is a focus of this regulatory standard, APRA has mandated further board and management accountability. Non-compliance may lead to a breach notice that requires a rectification plan, and action to be taken in a timely manner. Failure to do so may result in formal enforcement action.

APRA will request one-off, tripartite independent cyber-security reviews across all its regulated industries from 2021. It will require boards to use an external audit firm to review CPS 234 compliance and report back to both APRA and the board.

> FAQs

What is APRA CPS 234?

The Australian Prudential Regulation Authority (APRA) CPS 234 is a prudential standard that applies to all 'APRA-regulated entities'.

"APRA's CPS 234, aims to ensure that APRA-regulated entities take measures to be resilient against information security incidents by maintaining an information security capability commensurate with information security vulnerabilities and threats."

Who needs to comply?

APRA-regulated entities include:

- **Authorised deposit-taking institutions** (ADIs), including foreign ADIs, and non-operating holding companies authorised unde r the Banking Act (authorised banking NOHCs);

· **General insurers**, including Category C insurers, non-operating holding companies authorised under the Insurance Act (authorised insurance NOHCs), and parent entities of Level 2 insurance groups;

· **Life companies**, including friendly societies, eligible foreign life insurance companies (EFLICs) and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs);

· **Private health insurers** registered under the PHIPS Act; and (e) RSE licensees under the SIS Act in respect of their business operations.

What happens if your organisation is not compliant with the standard?

As indicated by the recent update from APRA, formal enforcement action may be taken for non-compliance, and potential breach notice issued for lack of timely action.

Do you operate and maintain an information security management system (ISMS) against ISO 27001? If so, you may be able to leverage this towards meeting your prudential obligations.

ISO 27001 provides a baseline to work from as it is an internationally recognised information security standard. There is a one-to-one mapping of the nine key requirements from APRA CPS 234 to the ISO 27001 information security standard.

APRA has approved your extension, where to from here?

Depending on where your gaps are, we will work with you to address the key areas of concern as a priority and devise a plan for any improvement activities required to further uplift the existing controls. Contact us and we will walk through the process with you.

Contact us via email at **info@privasec.com**,

or call us at **1800 996 001** (AU) / **+65 6610 9597** (SG)

with your questions on APRA CPS 234 today

Sources:
https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services

Privasec

GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS

RED RED TEAMING & ADVANCED ETHICAL HACKING

DRONE SEC UAS HACKING, HARDENING & DEFENCE

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+603 2788 3709 (MY)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 2, 64 Clarence Street
Sydney 2000
NSW, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Singapore Office
138 Robinson Road
Oxley Tower #10-01
Singapore 068906

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia