CPS 234 INFORMATION SECURITY TRIPARTITE AUDIT

In his speech to the Financial Services Assurance Forum on 26 November 2020, Executive Board Member Geoff Summerhayes announced APRA's one-off tripartite independent cyber security reviews across all APRA regulated industries. To quote — "We are also going to take a much more targeted approach to ensuring CPS 234 is being fully complied with, and holding boards and management accountable where it is not.

As background, at the end of 2020, APRA supervisors reached out to their entities to directly ask if they were CPS 234 compliant. Around 100 entities confessed to shortcomings and requested more time, but most provided generally positive accounts of their compliance status. Yet when our IT Risk specialist team has conducted cyber reviews of some of these entities, we've discovered significant weaknesses in every instance, in areas such as testing programs, control environments and incident response capabilities.

In response APRA will shortly be requesting one-off tripartite independent cyber security reviews across all our regulated industries. Starting in 2021, APRA will be asking boards to engage an external audit firm to conduct a thorough review of their CPS 234 compliance and report back to both APRA and the board. We haven't made a final determination on which entities this will apply to, but all entities should prepare accordingly."

In line with Mr. Summerhayes' speech, the tripartite audits have commenced and RSM is one of those few organisations that are uniquely qualified to perform the audit and report in line with the ASAE 3150 standards required by APRA.

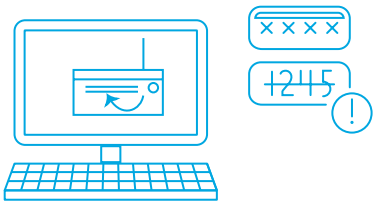
A complete assessment — CPS 234 Tripartite Audit

Our audit methodology will ensure a thorough analysis of your CPS 234 environment. The ASAE 3150 audit will cover the following areas:

- A fair presentation of the **system description**
- **Suitability of design and implementation of controls** to achieve the required control objectives
- **Operating effectiveness of controls** as designed throughout the 12 months prior to the start of the assessment.

RSM credentials

- We have conducted a number of CPS 234 audits for APRA regulated entities in Australia
- We have assisted APRA regulated entities through the design and implementation of controls to meet CPS 234 compliance
- We have worked with APRA regulated entities to improve information security controls, control effectiveness testing programs, third party control assessments and incident response capabilities
- We have extensive information security control framework experience and use specialist information security auditors to complete the audits
- We have completed ASAE 3150 reports for compliance with the Consumer Data Right information security requirements to become an accredited data recipient for Open Banking
- We are fiercely independent in our role to ensure the highest integrity in our work



RSM

What is the CPS 234 Tripartite Audit?

The CPS 234 Tripartite Audit is a one-off audit requested by APRA in response to an increasing number of cyber incidents and data breaches reported to the Australian Cyber Security Centre (ACSC). The audit must be completed by an independent assurance practitioner (a registered public audit firm) to assess the design and operating effectiveness of the controls in place against predefined control objectives that are based upon the requirements in the CPS 234 – Information Security Standard. The outcome of the Tripartite Audit is a detailed report developed in accordance with the ASAE 3150 Assurance Engagements on Controls issued by the Australian Auditing and Assurance Standards Board, with three key participants – APRA, the organisation in focus, and the independent assurance practitioner.

Who should comply with CPS 234?

It is not a matter of who should comply with CPS 234, but who must comply. All APRA regulated entities must comply with the CPS 234 – Information Security Standard. This includes Authorised deposit-taking institutions (ADIs or banks), including foreign ADIs, credit unions, building societies, friendly societies, general insurance and reinsurance companies, life insurers, private health insurers, and a large part of the superannuation industry.organisation in focus, and the independent assurance practitioner.

How is the CPS 234 Tripartite Audit conducted

Our audit methodology has been customised to the CPS 234 standard based on years of experience working with APRA regulated entities and assisting them with CPS 234 compliance. The methodology is depicted below:

Engagement process

Engagement planning

- Confirm key personnel
- Clarify roles and responsibilities
- Distribute documentation request list
- Commence engagement

System and controls identification

- Prepare system description and identify controls to meet control objectives
- Perform a preliminary review of the control environment
- Evaluate the reasonableness of the control objectives
- Evaluate the completeness, accuracy and fair presentation of the System Description

Controls testing

- Provide evidence and documentation as requested. This may include other audit reports to place reliance on
- Evaluate the design of specific controls and ensure they will achieve the control objectives
- Perform tests of controls to ascertain whether there is reasonable assurance that control have been implemented as designed and achieve their objectives, and are operating effectively as designed

Reporting

- Prepare "long-form" ASAE 3150 report (Type 2)
- Distribute draft findings to key stakeholders and obtain agreement
- Document management comments and finalise report
- Share final report with APRA

Regular progress updates to key stakeholders and management – operate on a 'no surprises' basis throughout engagement

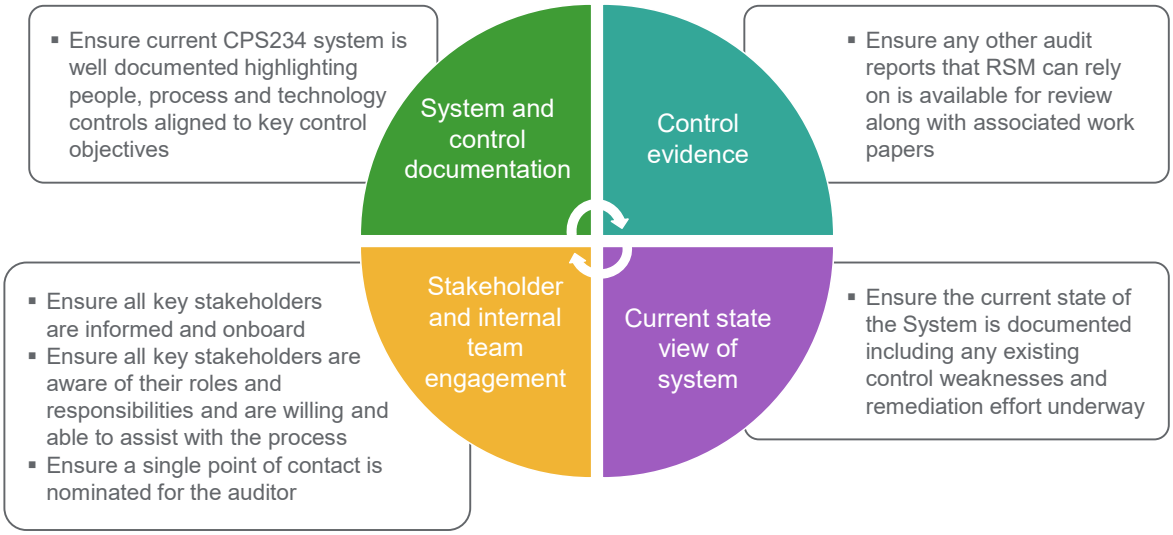
- Entity Responsibility
- RSM Responsibility
- Joint Responsibility

RSM

Items for Audit Entity to Consider

Depicted below are key items for the audit entity to consider particularly if this is their first audit related to CPS 234. This will help guide and prepare the Entity prior to the audit:

Key Items for Entity to Note for Audit



What we deliver

RSM will provide an independent assurance report in the "long-form" as described in ASAE 3150 and include all the elements required by ASAE 3150.

For more info please contact:

Ashwin Pal *Partner, Sydney*
T 02 8226 4500
E ashwin.pal@rsm.com.au

Darren Booth *Partner, Melbourne*
T 03 9286 8158
E darren.booth@rsm.com.au

Riaan Bronkhorst *Principal, Perth*
T 08 9261 9272
E Riaan.Bronkhorst@rsm.com.au