Deadline for implementation of APRA's Prudential Standard CPS 234 on information security takes effect from 1 July 2020

Sources: www.apra.gov.au

Date: 6 July 2020

Abstract:

Unless an extension has been granted by the Australian Prudential Regulatory Authority (APRA), all APRA-regulated entities will need to ensure they have taken appropriate measures to withstand and guard against information security incidents, as the deadline for compliance with the APRA's Prudential Standard CPS 234 (CPS 234) has passed.

This is APRA's first prudential standard relating to information security. Essentially, there are two key categories of requirements under CPS 234:

1. Information security practices that must be established by APRA entities, including:
    - actively maintain information security capabilities which enable their continued and sound operation;
    - establish information security controls to protect information assets across their lifecycle;
    - implement systemic testing programs which test the effectiveness of its information security controls;
    - develop robust mechanism and plans to detect and respond to information security incidents that could plausibly occur; and
    - ensure internal activities incorporate a review of the design and operating effectiveness of information security controls.
2. Assessment and review by APRA entities to determine the adequacy of their service providers' security practices when it comes to protecting information assets they manage.

Although CPS 234 commenced on 1 July 2019, the deadline was extended if a third party manages the information assets, as is commonly the case in the banking sector. For regulated entities using external service providers, requirements take effect from the earlier of the next contract renewal date with the third party or 1 July 2020.

However, in April 2020, with the onset of the COVID-19 pandemic, APRA announced the availability of six-month extensions, to 1 January 2021, on a case-by-case basis only.

This means regulated entities engaging third party service providers should be reviewing service providers terms and conditions and ensuring CPS 234 requirements are "back to back". Hence the relevance of the contract renewal process. If the service provider agreement is not up for renewal during the relevant period, entities will need to agree on a schedule of amendments consistent with the CPS 234 by 1 July 2020 or alternatively, apply for an extension from APRA.

For service providers obliged to step up their security practices, it may be preferable to separate the assets they manage that belong to APRA entities from those of other clients, so these practices can apply selectively, thus decreasing the overall burden.

CPS 234 is available here. Useful resources on compliance with CPS 234 are available from the APRA's website. APRA's April 2020 announcement regarding extensions is available here.

.