

Unlocking Cyber Resilience: Is Your Organisation APRA-Ready for Enhanced Operational Risk Management Compliance? - blueAPACHE

Canonical: <https://www.blueapache.com/blog/unlocking-cyber-resilience-is-your-organisation-apra-ready-for-enhanced-operational-risk-management-compliance>

Details:

November 9, 2023

Understanding CPS 234 and CPS 230

This November 2023 article discussed CPS 234, in effect since July 2019, and preparations for CPS 230. CPS 230 commenced on 1 July 2025, so the original article's description of it as upcoming is historical. It addresses operational risk, continuity of critical operations and service-provider risk. Refer to APRA's CPS 230 standard for the current requirements.

How our Strategic Partnerships Meet CPS 230 Needs

The original article identified CyberArk and Rapid7 as partners intended to support CPS 230 readiness. It described three contributions: identifying and mitigating operational risks, protecting essential customer services, and providing expertise and technology to support alignment with the standard.

These are the article's stated partnership benefits. Using a partner's technology does not by itself establish regulatory compliance; the regulated entity must assess its controls, continuity arrangements and service-provider obligations. Contact us to confirm the current partnership scope and the services suitable for your requirements.

References

APRA warns finance sector on cybersecurity non-compliance — Security — CRN Australia
Draft Prudential Standard CPS 230 Operational Risk Management

What is CPS 234 and when did it take effect?

CPS 234 is APRA's information security standard that has been in effect since July 2019. It addresses foundational cybersecurity issues and focuses on ensuring financial institutions can defend against evolving threats.

What is CPS 230 and when does it take effect?

CPS 230 is APRA's Operational Risk Management standard. It commenced on 1 July 2025 and addresses operational risks, continuity of critical operations and service-provider risks. The article's

2023 description of it as upcoming is historical; consult APRA's current standard for applicable requirements.

What prompted blueAPACHE to publish this blog post?

The post references a CRN Australia article in which the Australian Prudential Regulation Authority (APRA) issued a stern warning about cybersecurity non-compliance in the finance sector.

Which industry partners do you work with to help meet CPS 230 needs?

The November 2023 article identified CyberArk and Rapid7 as partners intended to support CPS 230 readiness. Confirm the current partnership and engagement scope with blueAPACHE.

How do your partnerships contribute to CPS 230 compliance?

The original article described support for identifying and mitigating operational risks, securing essential services and preparing for compliance. These are stated contributions, not a guarantee that using the technologies establishes compliance.

Who is the target audience for CPS 230 compliance?

The target audience is APRA-regulated entities, particularly those in the financial sector, which must proactively prepare for compliance with CPS 230's operational risk management requirements.

How can an organisation get help with APRA CPS 234 and CPS 230 compliance from you?

Contact blueAPACHE to discuss the relevant security services and engagement scope. The regulated entity remains responsible for assessing and meeting its applicable APRA requirements.

What sources does the blog post cite regarding APRA regulations?

The post cites a CRN Australia article titled 'APRA warns finance sector on cybersecurity non-compliance' and APRA's own draft document, 'Draft Prudential Standard CPS 230 Operational Risk Management,' available on APRA's website.