



CPS 230 Operational Risk Update

**A change of date, and change of approach.
May 2023**

Across the full spectrum of domestic and international banks, insurers and super funds, KPMG has met with over 60 organisations in the past month to discuss and debate the road ahead to comply with CPS 230.

In its update released recently, APRA has clarified:

1. The release date for the final standard has moved to mid-2023, with draft supporting guidance to be provided.
2. The effective date for the new standard has been extended from 1 January 2024 to 1 July 2025.
3. For third parties that fall under the definition of 'material service providers', the requirements in the standard will apply from the earlier of the next contract renewal date or 1 July 2026 at the latest.

While this provides additional and much needed time to comply, it is our view that the 18-month extension does not give cause to pause or slow down efforts to comply, but rather generates heightened expectations on the maturity expected across the three primary areas covered by the standard:

1. New operational resilience measures to cover critical operations.
2. Enhanced requirements for operational risk relative to CPS 220.
3. New requirements for material service providers.

Many of our global and local clients consider operational resilience as a key differentiator and that CPS 230 (or the equivalent global rules) makes good business sense. Particularly in an environment where business and personal environments are increasingly digital and 'always on'. So apart from achieving compliance it is useful to pose the question: What does your organisation want most out of this regulation?

"So apart from achieving compliance it is useful to pose the question: What does your organisation want most out of this regulation?"

The breathing room created by the extension provides a short window to take stock and re-evaluate your priorities, allowing boards and executive teams to recalibrate their programs in the near term.

Start planning implementation now

In our view, APRA's update challenges all organisations to carefully sequence and prioritise activities in line with criticality but also those that require the most effort and resourcing. Our international experience suggests that the burden of implementation is likely to include resource mapping, higher volumes of service provider profiling and working through your 'golden sources' of data to ensure they are complete and accurate enough to facilitate that resource mapping. Technology support can also have a long lead time.

As part of this, scaling your ambition to provide longer-term benefits could be a key part of the decision-making process. Opportunities that our clients considered but were constrained by the original compliance date included policy rationalisation and consistency of regulatory terms.

Our experience implementing similar PRA operational resilience regulations in the UK has taught us that even two years into implementation there remains a significant workload for equivalent organisations. So now is not the time to reduce momentum.

Go strategic and sustainable, not tactical

Tactical solutions that achieve the minimum regulatory letter of the rule are probably less palatable considering the new deadline, and in our view are not a good use of investment funding.

Organisational resilience is recognised under all major global jurisdictions as a key area of focus and many multinationals are already on the journey.

The extended deadline enables organisations to focus on sustainable longer-term solutions that not only meet operational resilience requirements but go further to integrate operational resilience and operational risk in a comprehensive way (something that the UK regulation did not require). In effect, operational resilience is an outcome of operational risk management and not an independent activity.

“In effect, operational resilience is an outcome of operational risk management and not an independent activity.”

This more strategic approach includes, but is not limited to, the following:

1. Completing full and comprehensive resourcing mapping for a really sharp number of genuinely critical operations, providing much deeper insight on dependencies than you would have capacity for in a broad-based approach.
2. Piloting the resilience operating model end-to-end with a number of varied use cases that ensures confidence in the model, and which can demonstrate value to the businesses that own these critical operations. This would include testing the operating model.
3. Building out a resilience technology solution that ingests and links key resource data to critical operations and links to GRCs and the risk architecture.
4. Tackling data implications that impact critical operations (e.g. technology and data inventories).
5. Further strengthening genuine end-to-end risk culture in the organisation, including accountability.

Australian-made: integrating operational risk with operational resilience

Unlike some resilience regulation in other global jurisdictions, the APRA standard challenges the market to integrate operational risk and operational resilience. While much discussion in the market has and is focused on resilience, we believe there is a great deal of opportunity and value from bringing your operational risk and resilience frameworks, controls and processes seamlessly together. Whilst resilience testing scenarios and investing to mitigate any tolerance gaps is expected, prevention of such outages is inextricably linked.

Considering these in a holistic way enables your organisation to proactively monitor the risk of disruption through visibility and ongoing assessment of the ‘input’ resources in your operating model that support the operations. This optimised future creates an ecosystem of preventative operational risk management of causes, and responsive resilience when circumstances unfortunately prevail.

“This optimised future creates an ecosystem of preventative operational risk management of causes, and responsive resilience when circumstances unfortunately prevail.”

Conclusion

In conclusion, we recommend boards and executive teams should prioritise focus on what your organisation can and should have in place by 1 July 2025 for CPS 230, leading to a business case for funding a multi-year program of work that will have a longer duration but will achieve a deeper impact for the benefit of your customers and your stakeholders.

Contact us



Gavin Rosettenstein
**Operational & Service
Provider Risk Management**
T: +61 2 9335 8088
E: gavin1@kpmg.com.au



Matt Tottenham
Partner
**Operational Risk, Strategy
and Frameworks**
T: +61 2 9335 8516
E: mtottenham@kpmg.com.au



Campbell Logie-Smith
Director
Cyber Resilience
T: +61 3 9288 5920
E: clogiesmith@kpmg.com.au



Kat Conner
Partner
Risk & Regulation
T: +61 3 9346 5636
E: katconner@kpmg.com.au



Dr Lisa Butler Beatty
**Partner and Practice Lead,
Superannuation Advisory**
T: +61 2 9346 5541
E: lisabbeatty@kpmg.com.au



Karlie Lytas
**Partner, Wealth & Asset
Management, Risk Lead**
T: +61 2 9335 8750
E: klytas@kpmg.com.au



Sheila Mistry
Partner
People & Change
T: +61 2 9273 5015
E: smistry7@kpmg.com.au



Caroline Leong
Partner
Operations Advisory
T: +61 2 9295 3971
E: cleong1@kpmg.com.au



Louise Rose
Partner
Enterprise Advisory
T: +61 2 9335 8103
E: lrose2@kpmg.com.au



Simon Taylor-Allan
**Director, Operational Risk
Management**
T: +61 2 9335 7729
E: staylorallan@kpmg.com.au

KPMG.com.au

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

©2023 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Liability limited by a scheme approved under Professional Standards Legislation.

May, 2023. 1111378768FS.