CPS 230 Operational Risk Management

Final Rule
July 2023

On 17 July 2023, APRA formally released its much-anticipated final Prudential Standard CPS 230 – Operational Risk Management, alongside the draft supporting Guidance CPG 230.

In the finalised prudential standard APRA have confirmed requirements that bolster operational risk management practices across the Financial Services sector. While the final standard contains few changes to APRA's earlier draft, **the new accompanying draft Prudential Practice Guide (CPG) provides materially more detail around expectations across Operational Risk Management, Business Continuity Planning and the Management of Service Providers.** In particular, the guidance around Operational Risk Management is broad and reflects many aspects of better practice across leading entities in the industry.

APRA's invitation for consultation on the draft guidance by 13 October 2023 is an opportunity for industry stakeholders to provide input to these enhanced or recommended practices. In this paper we have noted the key changes to the Standard, but more importantly our view of the newer considerations within the Guidance.

Summary of key standard changes

- Although the Standard is materially in line with the initial draft released in July 2022, a few notable amendments are outlined below:
- Extension of the effective date for the Standard to 1 July 2025, and 1 July 2026 for the amendment of pre-existing contractual arrangements with Material Service Providers (MSP).
- Flexibility on prescribed critical operations and service providers with an 'unless otherwise justified' provision.
- Information Technology Infrastructure has been replaced with IT capability, which we would interpret as increasing the scope from systems to broader elements such as people.
- The notification requirement to APRA has changed from the point of Business Continuity Plan (BCP) activation to the time the entity has *'suffered a disruption to a critical operation outside of tolerance'*.
- Modifications so that only material arrangements with MSPs are captured in relation to certain requirements, rather than all arrangements.
- Removal of requirement to determine if the MSP is systemically important in Australia.

APRA's guidance and expectations

Supporting the new Standard, APRA has outlined its expectations in applying it through the supporting Guidance CPG 230. Some of the key takeaways from CPG 230 are as follows:

Roles and Responsibilities

- While the Board remains accountable for oversight of Operational risk, the Business line management are responsible for embedding operational risk management practices and are the owners of operational risk across *end-to-end processes*.
- While the Board approves the entity's overall tolerance levels, *senior management are able to set more granular tolerance levels and indicators*, consistent with Board approved levels.
- Information provided to the Board on operational risk is targeted, relevant and sufficient.

Operational Risk Considerations

- Business processes are clearly defined end-to-end to enable the identification of risks, *obligations, key data,* controls and *resources*.
- Ensuring that control design and operating effectiveness as well as the operational risk profile is *reassessed* when issues, incidents and breaches occur. This effectively evolves from a periodic risk and control self-assessment to one that is more trigger based and dynamic in nature.
- Root cause analysis is expected to be based on a *clearly defined, documented and tested methodology* that considers the role and interaction of the key elements of people, processes and systems in the entity's business operations.

- Data quality is an important input to ensure accurate risk profile reporting. *Key data should be identified* and ensure data risk is managed appropriately.
- Information systems enable real time and aggregated reporting and *integrate risk data across different components of the framework*, e.g. risks, obligations and key data (including controls, issues, incidents and breaches).

"Disruptions to financial services can cause a major detrimental impact to the people who rely on them."

– John Lonsdale, APRA Chair

Business Continuity/Resilience

- *Proportionality* should also be applied to the level of granularity including when documenting processes, resources and scenario analysis for Critical Operations.
- Entities that are currently working with APRA to develop resolution plans under CPS 900 will need to classify *critical functions for resolution planning as critical operations*. There are benefits in developing frameworks for both regulatory requirements in conjunction to ensure they are aligned to meet this.
- Tolerance levels are *clearly justified* and subject to review, challenge and reassessment.

Management of Service Provider Arrangements

- The policy should include expectations of how *all* service provider arrangements are to be managed and clear criteria for identifying material arrangements.
- For material arrangements, entities should be able to demonstrate their understanding and management of all relevant risks. *This may include process mapping of services, control monitoring and onsite visits.*
- Consideration and management of risks associated with fourth parties *(and downstream service providers)* for critical operations.
- Entities should manage the risks associated with *cohorts of service providers* where the aggregate impact is material, but each individual provider is not.
- Inclusion of considerations for determining MSPs, for example, those supporting a critical business operation, totality of services, exposure to material operational risk, difficulty in exiting or transitioning the arrangement and those involved with sensitive or critical information classified under CPS 234.

The time to act is now

Eleven months since the release of the draft standard, many organisations are in the early stages of implementing requirements identified as likely gaps. This sentiment was echoed by APRA Chair John Lonsdale:

"We expect regulated entities to be proactive in preparing for implementation, rather than waiting until the last minute to get ready to meet the new requirements."

To meet APRA's expectations, it is recommended that the key focal areas below are prioritised in the near-term:

1. Impact assessment and preliminary Target Operating Model (TOM)

- Have you performed an impact assessment and identified gaps in relation to CPS 230?
- Have you considered your future state operating model to guide your implementation journey and ensure the new requirements are embedded and sustainable?

2. Critical Operation identification and end-to-end process and resource mapping.

- Have you developed a framework for classifying and prioritising Critical Operations?
- Have you documented end-to-end processes, including resources, risks, controls and obligations?

3. Development of disruption tolerance methodology

- Have you considered the inputs and data sources required to adequately determine disruption tolerances appropriate for your organisation?
- Have you identified any gaps between tolerance levels and recovery capability?

4. Development of service provider arrangement management methodology and program

- Have you developed a methodology and operating program to effectively identify, assess, classify and manage service providers?

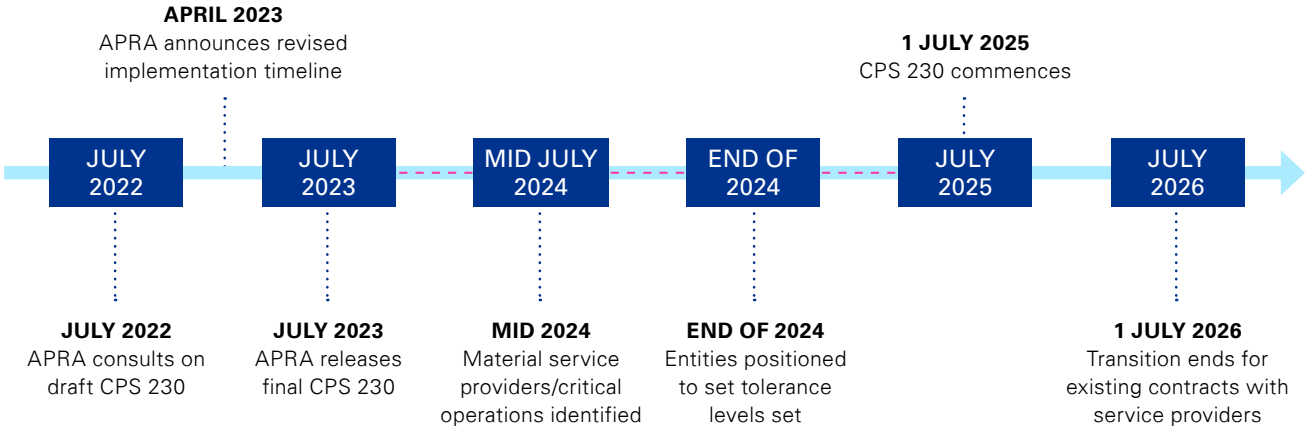
Conclusion

With APRA's release of the final rule, all organisations are now able to fully mobilise their CPS 230 implementation programs. Given our experience with the effort required for similar regulation outside Australia, we continue to recommend that Boards and Executive teams prioritise focus on the key requirements ahead of the effective date 1 July 2025.

APRA – Operational Risk Manage >

APRA's suggested CPS 230 implementation timeline

Source: Response Paper – Operational Risk Management, APRA



- - - - - - = proactive transition period, regulated entities prepare for the new requirements

Contact us

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

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

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

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

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

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

Kat Conner
Partner, Regulatory & Compliance
T: +61 3 9346 5636
E: katconner@kpmg.com.au

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

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

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

KPMG.com.au

July, 2023. 1162883778FS.