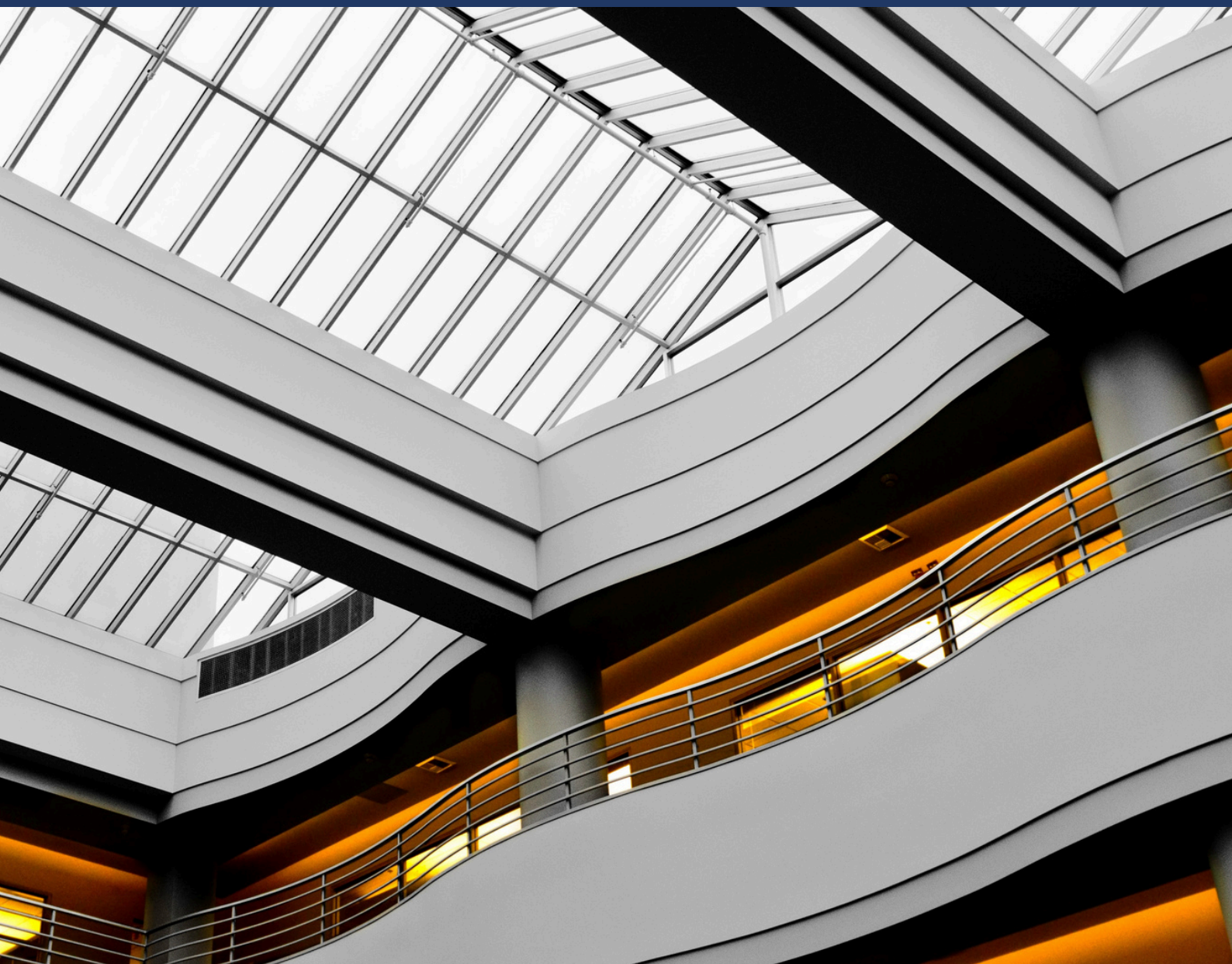
Amstelveen

CPS 230: Moving from Implementation to Operating Discipline



A new phase of regulatory expectations

Since 1 July 2025, APRA-regulated entities have been implementing CPS 230 Operational Risk Management (the Standard). This has involved identifying critical operations, establishing tolerance levels, uplifting business continuity arrangements, and strengthening service provider governance. The 1 July 2026 milestone marks a shift in expectations. With transition arrangements now complete, regulated entities must demonstrate that resilience frameworks are not only established but embedded and operating effectively in practice. The recent amendments do not fundamentally redesign the standard. This next phase of CPS 230 is about how operational risk, business continuity, and service provider management are managed consistently on an ongoing basis so organisations can manage disruption in practice.

Key changes effective 1 July 2026

Completion of contract remediation: A key milestone is the end of the transition period for pre-existing contractual arrangements with material service providers (MSPs). For existing contracts with MSPs, CPS 230 requirements apply from the next renewal date, or by 1 July 2026 at the latest. This includes provisions relating to audit rights, business continuity obligations, subcontracting controls and termination rights. The focus is no longer only on negotiating contractual provisions but on how they operate in practice, requiring organisations to actively monitor service provider performance, enforce contractual rights and demonstrate effective governance over these arrangements.

> "The amendments introduce limited exemptions from specific contractual requirements in CPS 230 for material arrangements with certain categories of non-traditional service providers (NTSPs), like central banks and clearing and settlement facilities, where contractual compliance is not practicable." - APRA

Service provider exemptions: APRA has introduced targeted amendments to better accommodate arrangements with NTSPs, including situations where full contractual compliance is not practical. Limited exemptions apply to certain service providers listed in the Attachment to the Standard ('Categories of exempt service providers'), including government agencies, regulators, central banks, financial market exchanges, clearing and settlement facility operators, payment system and scheme operators, and financial messaging infrastructure providers, where arrangements use standardised terms or are not documented in a formal agreement. These exemptions apply only to specific CPS 230 contractual and service-level requirements (including paragraphs 53, 54, 55(d) and 59(c)) relating to formal agreements, audit and access rights, business continuity, subcontracting, termination and service-level obligations. While exemptions provide practical relief where full contractual compliance is not feasible, organisations are still required to actively manage the operational risks associated with these arrangements and demonstrate appropriate oversight.

Exempt service provider classification: The amendments clearly set out which service providers can be treated as exempt under paragraph 27 of the Standard and the Attachment. The clarification requires organisations to implement a consistent approach to identifying these providers, assessing associated risks and applying appropriate governance across the business. APRA has also introduced a provision allowing it to exempt an arrangement that does not meet the defined criteria; however, the onus lies with the organisation to apply to APRA.

Guidance and reporting updates: Updates to supporting guidance, including CPG 230 and the Material Service Provider Register template, reinforce the need for organisations to maintain a clear and current view of service provider dependencies, and to demonstrate how risks are actively managed across the ecosystem. APRA expects entities to apply exemptions on a targeted basis, limited to specific paragraphs that cannot reasonably be satisfied, and to take all reasonable steps to manage the operational risks of NTSP arrangements within practical constraints.

What does CPS 230 look like going forward

The July 2026 milestone and updated Standard reflect a progression in core obligations. As APRA has noted, the limited exemption is intended to "provide relief that is narrowly targeted, administratively efficient and responsive to industry concerns, while preserving the core objectives of CPS 230." Organisations are expected to demonstrate that resilience capabilities are credible, controls operate as intended and disruptions can be managed within established tolerance levels.

While the amendment addresses one of the practical difficulties experienced by APRA-regulated entities in applying service provider governance requirements, broader implementation challenges remain across the Standard. Based on our experience supporting CPS 230 implementations and conducting embedment reviews, a number of consistent themes continue to emerge.

Key opportunities to strengthen resilience include:

Deepening of service provider oversight

Organisations should strengthen service provider oversight by monitoring performance against SLAs, assessing the impact of partial outages on tolerance levels, and improving visibility of upstream and downstream dependencies, including fourth-party risk. Where gaps exist, formal risk acceptance and mitigation strategies should be clearly defined.

Validation of tolerance levels

Organisations should leverage scenario-based testing and real incident analysis to validate tolerance levels, ensuring they are practical, measurable and aligned to system capabilities. This includes reassessing tolerance levels post-disruption to confirm they remain appropriate and achievable.

Establishment of reporting capability

Organisations should strengthen resilience reporting by addressing data fragmentation and integrating insights across risk domains, enabling end-to-end visibility of dependencies, risks and control effectiveness aligned to critical operations. Reporting should clearly link to accountability across the Three Lines of Defence.

These were explored in more detail in our earlier analysis, 'Six Months of CPS 230: What does the next phase of resilience look like?', which remains relevant as organisations transition to operating effectiveness.

Conclusion

CPS 230 is now operating as an embedded discipline rather than an implementation program. Organisations must demonstrate that resilience is integrated into day-to-day decision making, service provider oversight is ongoing and risk-based, and disruption response arrangements are tested and effective. This requires clear accountability, operating controls and resilience capabilities that can be relied upon in practice.

Our Authors

Poppy Fassos
Partner

With almost 30 years' experience, Poppy is a C-level executive with success in delivering and supporting some of the largest enterprise transformations in corporate Australia, building fit-for-purpose risk and compliance capabilities at an enterprise level, for Financial Services and Critical Infrastructure. Poppy offers experience in taking organisations on the full lifecycle of building and delivering risk and compliance capability and transformation through process and cultural change to enable business objectives and the right risk outcomes.

Lauren Daluz
Senior Consultant

Lauren is a Risk Transformation practitioner with controls assurance experience aligned to CPS 230, CPS 234 and PCI-DSS across private and public sector clients. She has recently supported a global financial services group to manage CPS230 compliance, leading resilience and service provider governance project streams. Lauren has delivered a change management program, including developing material to uplift stakeholder readiness on regulatory and internal requirements across middle management to the C-suite level.

Meet Vyas
Consultant

Meet is a risk consultant with experience supporting internal audit, technology risk and process improvement activities across financial services. He applies analytical and technical skills to strengthen controls, improve system-enabled processes and uplift risk frameworks. His work includes controls testing, data integrity reviews and technology risk assessments across cybersecurity, general IT controls and data management.

Amstelveen equips organisations to identify, assess and mitigate their most significant risks. Our risk, compliance and technology professionals support clients to improve the governance of their organisations. We provide specialist support to the largest public and private organisations in Australia and New Zealand.