Amstelveen

Six Months of CPS 230: What does the next phase of resilience look like?

As APRA sharpens its focus on operational risk and organisations continuously embed regulatory requirements, the evolving business continuity landscape has exposed key areas where organisations can evolve to build true operational resilience.

CPS 230 Embedment Retrospective

It has now been six months since the Australian Prudential Regulatory Authority (APRA) has enforced Prudential Standard (CPS) 230 for Operational Risk Management and is now visiting organisations to understand their compliance mechanisms. The regulatory change seeks to ensure APRA-regulated entities' resilience by harmonising operational risk, business continuity, and service provider management principles. The Standard has introduced key concepts, such as:

- Critical Operations (COs) - processes undertaken by an APRA-regulated entity which, if disrupted beyond tolerance levels, would have a material adverse impact on its customers, or its role in the financial system.
- Material Service Providers (MSPs) - entities relied on to undertake a CO or that expose it to material operational risk.

> **"The aim of this Prudential Standard is to ensure that an APRA-regulated entity is resilient to operational risks and disruptions. An APRA-regulated entity must effectively manage its operational risks, maintain its critical operations through disruptions, and manage the risks arising from service providers." - CPS 230**

In the lead-up to the effective date and during ongoing implementation, there are shared challenges across banks, insurance companies and superannuation funds in their compliance and embedment journeys for end-to-end resilience of processes in consideration of COs and beyond. Specific difficulties have been spotlighted as some APRA visitations have already been completed. It would appear APRA is particularly interested in the design and operating effectiveness of CPS 230 mechanisms and frameworks thus far, and how those embedded aspects support CPS 220 Risk Management under an operational risk management lens. By cross-examining the common areas of concern experienced by our clients and what may be topics of interest for the regulator, Amstelveen has compiled the following key considerations to guide prioritisation and long-term pathways to green.

Key Challenges

1 **Risk Profiles:** There is a lack of clarity and consistency in how risk profiles are consolidated, rated, and managed across divisions, particularly in relation to governance triggers, third-party performance, and incident response. The absence of a unified methodology for control ownership and integration hinders the development of enterprise-wide risk profiles.

Key activities to ensure risk profiles are Board ready as they are *"ultimately accountable for oversight of an entity's operational risk management" (para. 20, CPS 230)*:

Develop a standardised risk aggregation framework with clear definitions, thresholds (relative to tolerance levels for COs) and enterprise-level risk taxonomy to ensure consistency in how risks are rolled up at the enterprise-wide level. Reporting and risk assessments should always reflect if business units are operating within appetite.

Identify sources of key risk data from all business units and where possible, third-party systems, to develop a centralised view. This likely means working on the limitations of current Governance, Risk and Compliance (GRC) systems to reflect resilience, third-party risk, obligations and data governance performance.

Assign clear accountability for Business Impact Analysis (BIAs) and IT General Controls (ITGCs) as they tend to have undefined ownership at the divisional and enterprise levels.

Develop a shared control library for instances where enterprise-wide controls can be mapped to business units for their respective dependencies and a control ownership model where a single BU can own a control but dependent teams can validate effectiveness and applicability.

Asset Registers: It is difficult to accurately tier assets due to the absence of a complete asset register, unclear ownership, and lack of clarity around asset criticality, substitutability, and reliance within COs and business processes. 2

Strategic priorities to ensure the maintenance of *"capabilities required to execute the Business Continuity Plan (BCP)" (para. 41, CPS 230)*:

Establishment of an asset register

Asset registers for dependencies should be informed by the BIA and include details, such as:

- Asset name, description and type - ensure clear identification and purpose
- Business and technical owner - agree on who is accountable for the asset and who responsible for its maintenance
- Dependencies - map the other systems or process the asset either relies on or supports
- Criticality tier - consider role in CO or important business services
- Recovery objectives and contractual SLAs, especially for third-party hosted/managed services

Adoption of an end-to-end value chain

Shifting to an end-to-end value chain perspective means moving beyond siloed, traditional risk profiles to assess how risks impact COs across interconnected processes. This approach requires identifying how each asset or control contributes to value delivery and where vulnerabilities may disrupt the value chain. It also has implications for how critical processes are prioritised, monitored and recovered in the event of disruption. More mature organisations have a fourth party view to account where key dependencies are externalised outside of their direct relationships (e.g. AWS may itself be critical to the organisation directly but may also be a key dependency for their MSPs).

Criticality is not binary, it requires thorough and integrated understanding of how an asset's failure ripples across systems, processes and teams and its ultimate impact on your customers and role in the financial system.

Assessment of critical vs non-critical assets

Evaluating the criticality of assets has been an area that has required nuance and has been contentious to differentiate what is most important to the organisation and what the lower tiers of commensurate risk management look like. The below are considerations that can be incorporated in criticality assessments:

- Delineate between being "used" and "relied on" - can the process be executed without the asset?
- Identify if there are workarounds available and if they exist, the limitations of the alternative methods, such as sustainability of the workaround relative to tolerance levels.
- Explore tiering Maximum Allowable Outages, such as 0-24 hours = Business Critical, 24-72 hours = Business Important, 72+ hours = Non-critical.
- Ensure that dependencies that are relied upon should have recovery objectives less or equal to their Maximum Tolerable Period of Disruption and Maximum Allowable Data Loss.
- Consider where there are genuine limitations to recovery objectives of a critical asset, such as inability to remediate contracted SLAs; in which case, the business should evaluate means to avoid or agree on a Risk Acceptance.
- Evaluate the impact if the asset experiences a sustained failure in line with the organisation's existing risk assessments e.g. financial, regulatory, internal impacts.

3 **Materials Service Providers:** Organisations face difficulty in effectively governing and testing their MSPs including assessing their impact on COs, integrating them into business continuity planning, and balancing oversight without straining relationships.

Enablers that support effective risk management of MSPs:

Classification of MSPs should reflect and be integrated with information asset policies and mirror similar considerations on CO relevance, recovery objectives and sustained failure impacts.

Articulate to Relationship Owners the risk appetite when governing MSPs. As organisations attempt to apply governance commensurate to these 'highest risk' service providers, they must balance the risk of imposing requirements that the service providers may not be able to meet or degrades quality of relationship.

Focus on service provider governance should extend beyond checklist requirements and into relationship building, especially in gaining access to MSP's BCP testing or even their inclusion in internal BCP testing. This is exemplified in conversations on contractual remediation due 1 July 2026.

Contract remediation should have a RACI Matrix [Responsible, Accountable, Consulted, Informed] for stakeholders across Legal, Business Owner of Service, Technical Owner of Service (particularly for software-based MSPs), and Three Lines of Defence representatives.

Recent major disruptions have shown that true organisational resilience demands embedding continuity enterprise-wide and with key service providers.

3LoD: The regulator is likely scrutinising how the Three Lines of Defence Model is being executed and are seeking evidence that roles are clearly defined, guidance is documented and oversight is effective. 4

Key areas of focus where CPS 230 project teams raised that guidance and oversight can be improved:

Line 2 oversight of Line 1 risk and control assessment processes for CPS 230 needs clearer communication, with traceability mapped through policies, standards and frameworks to evidence how corresponding compliance mechanisms are embedded.

As responsibilities are changed or introduced - particularly for senior management and the Board, a clear approach from Line 2 eases embedment to effectively cascade change management and training initiatives. Otherwise messaging is fragmented for the large volume of change and results in a lack of standardisation.

A consistent approach to continuously identify COs across Business Groups must be employed and should be based on shared criteria and comprehensive of all applicable processes. Current approaches often fails to reflect different business units varying levels of risk / resilience maturity.

Line 3 must be ready to demonstrate they can or have effectively enhanced the entity's BCP and testing procedures and can delineate between who is responsible and accountable for improvements between Lines 1 and 2. Appropriate forums must also be established to report on MSP arrangements.

5 **Tolerance Level:** The operationalisation of CO tolerance levels has revealed the difficulty in practically defining and monitoring them, particularly Minimum Service Levels, due to unclear timing, accountability and integration with broader crisis management processes which has created gaps in preparedness and response effectiveness.

Critical factors for effectively addressing the resilience of tolerance levels and COs:

Minimum service levels should reflect the actual capabilities of the responsible business and technology teams, using a level of granularity that allows them to confidently understand, manage and demonstrate their processes are functioning as intended on a BAU basis.

The required *"triggers to identify a disruption"* must be coherent with tolerance level management in BCP scenario testing. Identifying explicit triggers enables timely decision-making when a CO approaches or breaches its tolerance level and helps stakeholders understand what truly threatens operational continuity.

Processes on tolerance level management must clearly depict responsibilities and accountabilities in establishing what is the timer (including who starts it, where it can be found, when should it start and end) and escalation of CO-relevant incident management.

The CO Incident and Crisis Management policies and processes must fit in to the organisation's broader crisis management infrastructure, with Communication Plans that provide coverage on who is notified and appropriate channels and forums.

Technology & Systems: Organisations use multiple poorly connected (and often, disconnected) systems to manage operational risk, resilience and third-party risk, making it difficult to integrate critical data. This fragmentation hinders timely incident awareness and complicates the identification of COs' dependencies and their failures. 6

Focus areas to strengthen observed weaknesses created by fragmented systems and data include:

Understand where there are gaps in the end-to-end visibility of risks, incidents and controls to enable strategic planning on where data across systems can be consolidated, so organisations can demonstrably show they are within (or working towards being within) risk appetite.

Establish clearer protocols for incident notification, especially between technology and business teams to avoid delays in recognising impacts (material or otherwise) to COs, including who needs to be informed and when, based on risk appetite and operational roles.

Strengthen forums and governance structures to support cross-functional risk awareness and decision-making. In substitution of a single-source system, people tend to bear the responsibility of creating and sharing key insights into CO resilience without a complete view of the CO's health.

Map across systems where interdependencies across *"people, technology, information, facilities and service providers...and the associated risks, obligations, key data and controls"* are documented to support resilience planning.

CPS 230 implementation has shown that operational resilience demands large-scale coordination, rigorous governance and proactive preparedness.

Conclusion

The implementation of APRA's Prudential Standard CPS 230 has revealed significant areas of improvement across regulated entities in operationalising resilience, particularly around ensuring people, systems and processes are equipped to execute best practices in operational risk, service provider and business continuity management. It has been an incredible milestone by CPS 230 project teams to have uplifted operational risk practices, as well defined and began embedment of governing Critical Operations and Material Service Providers to the regulator's expectations. This next phase of resilience requires reflection on how the processes and third parties below those tiers should be managed to prevent or mitigate the impact of a disruption. Senior management and the Board have strategic imperatives to address where there is fragmentation in systems, accountabilities and methodologies to ensure they can execute their responsibilities and strengthen their organisations' resilience. All Three Lines of Defence must be cognisant of where there are critical areas of improvement and be prepared to demonstrate key priorities amongst the above.

To meet CPS 230 compliance and strengthen resilience, organisations must move forward from fragmented risk practices to integrated, accountable frameworks that supports timely disruption response and continuity.

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.

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.